PENINSULA
PUBLISHING LLC

SHIFRA
Vol. **(2025)**, 2025, **pp**. 141–202
ISSN: 3078-3186

Research Article

Blockchain and Quantum Machine Learning Approach for Securing Smart Water Management Systems: A Scoping Review

Guma Ali[1,2,*], Maad M. Mijwil[3,4], Ioannis Adamopoulos[5], Klodian Dhoska[6]

[1] *Department of Computer and Information Science, Faculty of Technoscience, Muni University, Arua, Uganda*

[2] *Department of Computer Science and Engineering, Saveetha School of Engineering, Saveetha Institute of Medical and Technical Sciences, Chennai, Tamil Nadu, India*

[3] *College of Administration and Economics, Al-Iraqia University, Baghdad, Iraq*

[4] *Computer Techniques Engineering Department, College of Engineering Technologies, Al-Iraqia Science University, Baghdad, Iraq*

[5]*Department of Public Health Policy, Sector of Occupational & Environmental Health, School of Public Health, University of West Attica, 11521, Athens, Greece.*

[6] *Department of Mechanics. Polytechnic University of Tirana, Albania*

ARTICLEINFO

Article History
Received 20 May 2025
Revised: 11 Jul 2025
Accepted 12 Aug 2025
Published 1 Sep 2025

Keywords
Smart water management,
Blockchain,
quantum machine learning,
cybersecurity,
IoT,
scoping review

ABSTRACT

Smart water management systems (SWMS) increasingly rely on Internet of Things (IoT) devices to enhance water distribution, detect leaks, and support sustainable resource use, but this reliance also heightens exposure to cyberattacks, data manipulation, and privacy risks. Conventional security approaches often fall short due to the decentralized design and real-time demands of these systems. This scoping review analyzes 266 studies published between January 2022 and December 2025 to assess how integrating Blockchain and quantum machine learning (QML) can strengthen the security, privacy, and reliability of SWMS. The review examines Blockchain-enabled water management, quantum computing applications, and QML-based security frameworks, using thematic analysis to categorize emerging architectures and challenges. Findings of the focused studies show growing adoption of Blockchain for secure data logging, access control, and tamper-proof auditing. At the same time, QML demonstrates strong potential in anomaly detection, predictive maintenance, and optimizing distribution networks. Although these technologies offer a promising foundation for resilient water infrastructure, most research remains conceptual, with limited real-world deployment or scalability assessments. Integrating Blockchain with QML could create robust, privacy-preserving SWMS frameworks. However, significant barriers persist, including the computational intensity of quantum models, interoperability issues with existing IoT infrastructures, and the absence of standardized protocols. Addressing these gaps is essential for practical implementation. This review underscores the need for scalable hybrid designs, applied validation, and cross-disciplinary standards to advance secure, efficient, and sustainable smart water management solutions.

1. INTRODUCTION

Water is a finite and essential resource that underpins sustainable development and national economic competitiveness [1][2]. It supports critical sectors such as drinking water supply, sanitation, agriculture, and industry [3]. However, population growth, rapid urbanization, industrialization, climate change, and rising demand are intensifying pressure on water systems, resulting in shortages, uneven distribution, and frequent leakage [4]. The United Nations estimates that by 2050, 4.8–5.7 billion people will experience water scarcity for at least one month each year, and 3.2–5.4 billion will face severe shortages [5]. More than 4 billion people already endure severe scarcity annually, a trend expected to worsen in the coming decades [6-8]. Contributing factors include outdated distribution systems, excessive consumption, and poor maintenance of supply infrastructure [9]. Globally, water waste caused by leaks, inefficient use, and overflow from poorly maintained reservoirs or tanks remains a critical challenge [1]. Overall, freshwater demand is projected to increase by 20–30% by 2050 [10].

*Corresponding author email: a.guma@muni.ac.ug
DOI: https://doi.org/10.70470/SHIFRA/2025/011

In many regions, water management is hindered by inefficient distribution, leakage, and inadequate quality control, leading to financial losses and public health risks [11]. Traditional management practices, marked by aging infrastructure, manual processes, and reactive strategies, lack the capacity to support sustainable supply, equitable distribution, and environmental protection. These systems often do not provide real-time monitoring [8][11][12], leading to excessive waste, rising operational costs, and mounting environmental concerns [13]. Conventional monitoring methods are labor-intensive, slow, and unable to deliver timely data for rapid interventions. These limitations underscore the need for intelligent systems capable of monitoring, predicting, and optimizing water use in real time to reduce waste and promptly detect issues such as leaks or unauthorized consumption [14-16].

Technological advancements have created new opportunities to modernize water management [2][10]. SWMS integrates the IoT, Artificial Intelligence (AI), Digital Twins, and cloud computing to enable real-time monitoring, predictive analytics, and automated control of water infrastructure [13][17]. Using smart meters and Automatic Meter Reading/Infrastructure (AMR/AMI), these systems collect high-frequency data on flow, pressure, acoustics, and water quality, with flow sensors playing a central role in leak detection. This data supports optimized distribution, improved demand forecasting, and better infrastructure planning while reducing water loss and strengthening system resilience [4][18][19]. Machine learning models such as Random Forests enhance decision-making by predicting demand, identifying leaks, and detecting anomalies [20][21]. Real-time monitoring of flow rates, pressure, quality, and reservoir levels enables utilities to respond quickly to leaks, contamination, and overuse, reducing non-revenue water and improving resource allocation. Smart irrigation, dashboards, and mobile applications further empower users, farmers, and authorities by enabling interactive control and promoting efficient water use [19][22]. As cities adopt these systems, improvements in efficiency, reliability, and service quality highlight their growing value [2][7]. Real-world implementations reinforce this potential: Singapore uses sensors and AI to minimize non-revenue water; Amsterdam employs digital twins to manage canals and predict floods; Barcelona’s IoT-enabled irrigation system has reduced park water use by 25%; the Murray-Darling Basin relies on remote sensing and Geographic Information System (GIS) for efficient allocation; and Bengaluru’s AI-powered leak detection has reduced losses by 30%. These examples demonstrate how smart technologies enhance sustainability by reducing waste, anticipating failures, and optimizing resource use [6].

Despite these benefits, SWMS face extensive cybersecurity risks, including data breaches, malware, ransomware, insider threats, rogue device injection, false data injection, denial-of-service (DoS) and distributed DoS (DDoS) attacks, supply chain and side-channel attacks, supervisory control and data acquisition (SCADA) manipulation, programmable logic controller (PLC) hijacking, 51% and eclipse attacks, watering hole attacks, network eavesdropping, jamming, wormhole and Sybil attacks, man-in-the-middle (MitM) attacks, advanced persistent threats (APTs), weak authentication, and zero-day exploits, among many others [23-35]. These threats compromise the integrity, safety, and reliability of water services and can lead to serious incidents, such as contamination or operational disruptions. Cyberattacks against water infrastructure have intensified in recent years, exposing critical operational systems to significant risk. In 2021, an attacker attempted to contaminate the water supply in Oldsmar, Florida, by modifying chemical levels, and in April 2024, hackers disrupted several water utilities in Texas, overflowing a water tank and compromising SCADA-based hydraulic controls. In November 2023, intruders also breached the Municipal Water Authority of Aliquippa in Pennsylvania by infiltrating the pumping system regulator [23][27]. Many incidents go unreported due to concerns about reputation and customer confidence. Attackers often enter the operational technology (OT) environment through the information technology (IT) network—typically via phishing, ransomware, or similar vulnerabilities and once inside, manipulate SCADA systems, PLCs, and sensors to alter essential operating parameters [27].

The rising frequency of these incidents highlights the need for more robust security solutions. Integrating Blockchain and QML offers a promising pathway to strengthen SWMS against evolving threats [36]. Blockchain enhances security and transparency by enabling tamper-resistant, decentralized data storage and enabling secure verification of water usage, billing, maintenance records, and quality monitoring. It supports operational efficiency through smart contracts and strengthens accountability through immutable logging, transparent governance, and provenance-aware data sharing [37-39]. Meanwhile, QML leverages quantum principles such as superposition, interference, and entanglement to accelerate data processing, modeling, and learning, enabling faster and more accurate threat detection than classical methods. It enhances threat detection, anomaly identification, encryption, and optimization, outperforming many classical methods [40]. Studies demonstrate QML’s potential to improve classification, regression, and clustering of complex data, making it a valuable tool for detecting and preventing cyber intrusions in SWMS [36][41]. Blockchain, combined with QML, enhances predictive analytics and anomaly detection in SWMSs by delivering strong security and intelligent decision-making capabilities. This integration supports stronger encryption, improved cyber-threat prediction, and optimized security protocols [40][42].

Although research on Blockchain in critical infrastructure and QML in predictive analytics is growing, their combined application in SWMS remains limited. Existing studies often address security or predictive modeling separately, leaving a significant gap in integrated approaches. This scoping review addresses that gap by mapping current research and identifying research needs. It analyzes water-sector challenges, Blockchain design considerations, QML capabilities and limitations, and pathways toward quantum-safe transitions [39][43][44]. This scoping review, therefore, aims to systematically analyze current literature on the application of Blockchain and QML in securing SWMS, with a focus on (i) identifying prevailing security threats, attacks, challenges and solutions, (ii) evaluating the role of QML in predictive analytics and anomaly detection, and (iii) highlighting existing research gaps and future opportunities for developing secure and intelligent SWMS.

To summarize, this scoping review makes the following contributions:

- Provide an overview of SWMS, i.e., typical SWMS layered architecture, key enabling technologies, and common SWMS applications.
- Explain the cybersecurity threats, attacks, and challenges in SWMS.
- Describe the Blockchain and QML application for securing SWMS.
- State the synergistic benefits of integrating Blockchain and QML for securing SWMS.
- Analyze the cost-benefit of implementing Blockchain and QML for securing SWMS.
- Outline the case studies and practical implementations of Blockchain and QML in securing SWMS.
- List the challenges and limitations encountered while implementing Blockchain and QML in securing SWMS.
- Examine future research directions for implementing Blockchain and QML to secure SWMS.

The rest of this review is organized as follows: Section 2 discusses materials and methods. Section 3 explains the fundamentals and background of SWMS, while Section 4 explores cybersecurity in SWMS. Section 5 discusses the application of Blockchain technology in SWMS, and Section 6 analyzes how QML can be applied in securing SWMS. Section 7 proposes a taxonomy for integrating the Blockchain and QML framework tailored to secure SWMS. Section 8 presents real-world implementations and case studies of such frameworks, while Section 9 outlines the key challenges and limitations associated with their deployment. Section 10 recommends future research directions, and Section 11 concludes the study.

2. MATERIALS AND METHODS

This study employed a scoping review approach, guided by the Preferred Reporting Items for Systematic Reviews and Meta-Analyses extension for Scoping Reviews (PRISMA-ScR), to ensure methodological rigor, transparency, and reproducibility. Given the exploratory nature of the topic, at the intersection of Blockchain technology, QML, and SWMS, this methodology was considered suitable for systematically mapping the existing literature, identifying research gaps, and synthesizing insights on how these technologies can be integrated to enhance the security and efficiency of water management. This scoping review was structured around the following overarching research questions (RQs) that guided its scope, focus, and analysis.

- RQ1. What cybersecurity threats, attacks, and vulnerabilities in SWMS have been documented between 2022 and 2025?
- RQ2. How has Blockchain been applied to enhance security, transparency, or governance in water management and critical infrastructure contexts?
- RQ3. What roles does QML play in anomaly detection, intrusion detection, and resilience against cyber threats in cyber-physical systems?
- RQ4. How can Blockchain and QML be combined to provide quantum-resilient cybersecurity architectures for SWMS?
- RQ5. What gaps remain in research and practice that justify further investigation of Blockchain and QML approaches in securing SWMS?

These questions are designed to identify existing knowledge gaps, assess potential synergies, and outline a comprehensive research agenda.

To maintain the study’s relevance and methodological rigor, explicit inclusion and exclusion criteria were established in advance. Studies were included if they focused on Blockchain, quantum computing, machine learning, or their integration in enhancing the security of SWMS. Eligible publications addressed at least one of the following: SWMS cybersecurity; Blockchain applications in water systems, IoT, or critical infrastructure; QML for anomaly detection or cybersecurity; or post-quantum cryptography (PQC) in Blockchain. Only peer-reviewed journal articles, conference proceedings, systematic or scoping reviews, technical reports from recognized organizations, and high-quality white papers from established research institutions were considered. The review encompassed studies published in English between January 2022 and December 2025, capturing recent advances in Blockchain, QML, and SWMS security. This included research employing empirical analyses, simulations, conceptual frameworks, or case studies.

Studies were excluded if they met any of the following criteria: opinion pieces, editorials, commentaries, blog posts, or other non-peer-reviewed works lacking verifiable methodology; preprints without evidence of peer review unless highly cited and originating from reputable research groups; publications released before 2022, as they may not reflect recent advancements in Blockchain, QML, and PQC relevant to SWMS; research unrelated to water management or security; studies on water management that did not address cybersecurity aspects, such as purely hydrological models or policy analyses without ICT components; research papers that did not involve Blockchain or quantum computing/machine learning applications; review articles without primary empirical or simulation data; and publications not available in English or whose full texts could not be accessed through database or institutional searches.

A comprehensive literature search was conducted across major academic databases, including IEEE Xplore, MDPI, ScienceDirect, IGI Global, Nature, Springer, Frontiers, PLoS ONE, the ACM Digital Library, and Google Scholar. To incorporate relevant sectoral insights and standards, grey literature was also reviewed from authoritative sources such as the U.S. Environmental Protection Agency (EPA), the Cybersecurity and Infrastructure Security Agency (CISA), the National Institute of Standards and Technology (NIST), the Global Risk Institute, and the European Union Agency for Cybersecurity (ENISA). Furthermore, reference lists of selected studies were examined to ensure the search was exhaustive and comprehensive.

A structured search strategy, incorporating Boolean operators and controlled vocabulary, was employed to identify relevant studies. The search combined the terms (“Smart Water Management” OR “Water and Wastewater Systems” OR “Cyber-Physical Water Systems”) AND (“Blockchain” OR “Distributed Ledger” OR “Smart Contract”) AND (“Quantum Machine Learning” OR “QML” OR “Quantum AI”) AND (“Post-Quantum Cryptography” OR “Quantum-Safe Blockchain”) AND (“Cybersecurity” OR “Intrusion Detection” OR “Data Integrity”). Boolean operators were used to refine results across subdomains related to the integration of Blockchain and QML for securing SWMS. The search strings were iteratively refined and adapted to the functionalities and indexing systems of each database to ensure comprehensive coverage and inclusion of only the most relevant literature.

The study selection involved a systematic, multi-stage process to ensure rigor and minimize bias. Initially, two independent reviewers screened publications by title and abstract to exclude clearly irrelevant studies and identify those relevant to Blockchain, QML, or smart water systems. Publications that passed this stage underwent a full-text review to confirm eligibility, with any disagreements resolved through discussion or consultation with a third reviewer. All records were managed using Zotero and screened via Rayyan; duplicates were removed before evaluation. At each stage, exclusion reasons were documented, and the remaining studies were organized into a consistent format for accurate data extraction. To further ensure reliability, the reviewers employed a test-retest approach, repeatedly reassessing randomly selected papers to maintain consistency and minimize bias throughout the selection process. A PRISMA-ScR flow diagram was created to outline the stages of identification, screening, eligibility, and inclusion. From an initial retrieval of 2,200 publications, 1,180 were excluded based on title screening. Of the remaining 1,020, 754 were further excluded after abstract review, leaving 266 full-text publications for in-depth analysis, specifically examining the integration of Blockchain and QML for securing SWMS. Figure 1 presents the PRISMA-ScR diagram, summarizing the review process across all stages.

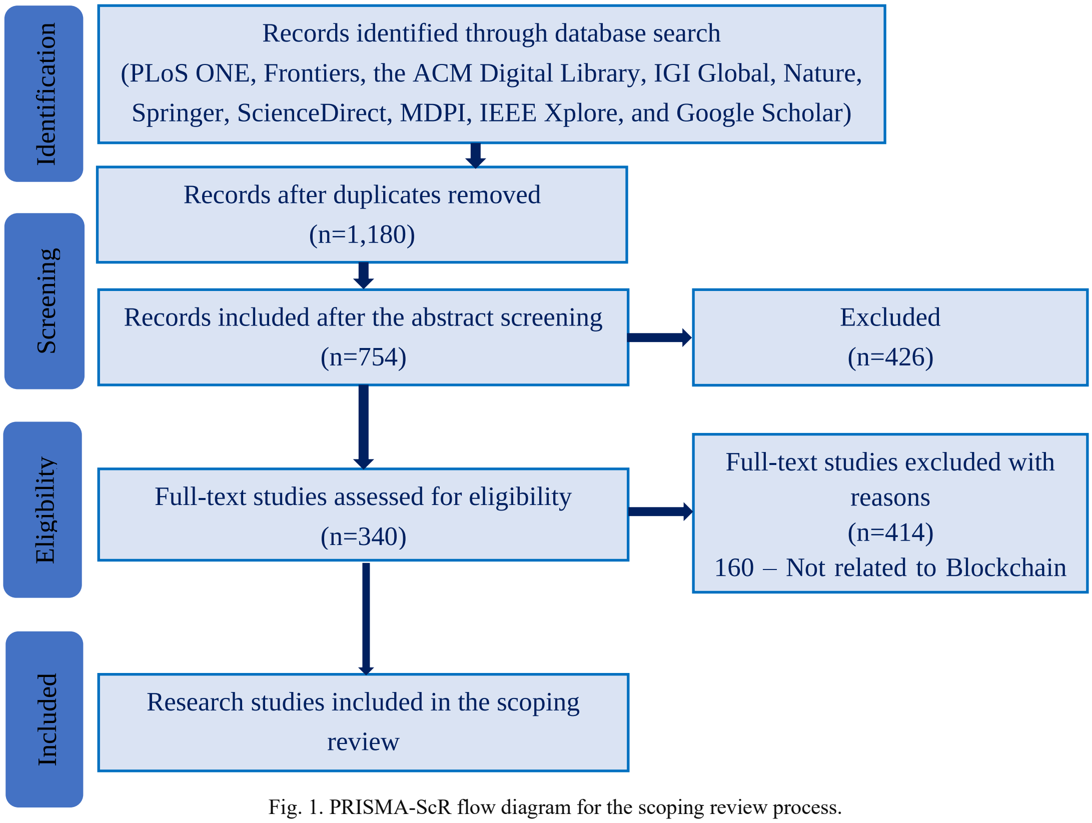
Identification
Records identified through database search (PLoS ONE, Frontiers, the ACM Digital Library, IGI Global, Nature, Springer, ScienceDirect, MDPI, IEEE Xplore, and Google Scholar)
Screening
Records after duplicates removed (n=1,180)
Records included after the abstract screening (n=754)
Excluded (n=426)
Eligibility
Full-text studies assessed for eligibility (n=340)
Full-text studies excluded with reasons (n=414)
160 – Not related to Blockchain
Included
Research studies included in the scoping review

Fig. 1. PRISMA-ScR flow diagram for the scoping review process.

A standardized data-charting form was developed and piloted to extract relevant information from each included study. The variables collected encompassed bibliographic details (authors, year, venue), study type (empirical, simulation, conceptual, review, policy/standards), domain focus (Blockchain, QML, SWMS), Blockchain architecture (e.g., private, public, consortium), QML models employed (e.g., quantum neural networks, quantum SVMs), SWMS applications (e.g., leak detection, demand forecasting, water quality monitoring), application areas (data integrity, anomaly detection, governance, secure telemetry, compliance), key findings and contributions, reported limitations and future directions, and relevance to SWMS cybersecurity. Data extraction was conducted independently by two reviewers and subsequently cross-verified for accuracy.

Given the exploratory nature of the study, a qualitative thematic synthesis was employed, in which the researchers conducted an in-depth qualitative analysis of the collected data. Findings were validated through consultation with subject-matter experts, comparison with prior studies, and critical evaluation of their robustness. Only high-quality studies were included, selected via a grading system assessing methodological rigor, reliability, and relevance to integrating Blockchain and QML for securing SWMS. As the study used exclusively published research, ethical approval was not required, though all sources were cited correctly. Data were coded inductively and organized into four thematic categories corresponding to the research questions. Narrative synthesis integrated sector-specific insights with emerging technical frameworks.

The study has several limitations. It may have overlooked relevant research outside the selected databases and relied on studies originally published in languages other than English that were later translated into English. The review does not comprehensively address the integration of Blockchain and QML for securing SWMS. By emphasizing theoretical applications, it neglects practical challenges such as cost, scalability, user acceptance, and real-world implementation barriers. Additionally, the rapid evolution of these technologies may have outpaced the literature included, potentially limiting the review's current relevance.

3. FUNDAMENTALS AND BACKGROUND

3.1 Overview of Smart Water Management System

A SWMS is an integrated cyber-physical framework that leverages distributed sensors and actuators, communication networks, and edge or cloud-based data processing to enable real-time monitoring, modeling, and control of water infrastructure. By incorporating automated sensing, event detection, predictive analytics, and closed-loop control, SWMSs replace or augment traditional manual inspections and static maintenance schedules. This intelligent automation enhances water conservation, reduces energy consumption, accelerates leak detection and response, and strengthens water-quality management [10][45]. In essence, smart water management leverages IoT technologies to ensure water quality and availability, prevent losses, facilitate proactive infrastructure maintenance, and promote consumer engagement in sustainable water use [46].

By integrating distributed sensing, low-power communication, edge and cloud computing, data analytics, and automated control, SWMSs enable utilities to gain real-time operational visibility and predictive insights. These capabilities facilitate proactive maintenance, leak detection, demand forecasting, and compliance. The approach transitions water utilities from reactive, manual operations to data-driven, adaptive management practices, enabling more resilient, efficient water services [7][45]. Figure 2 depicts the overall architecture and functionality of a SWMS.

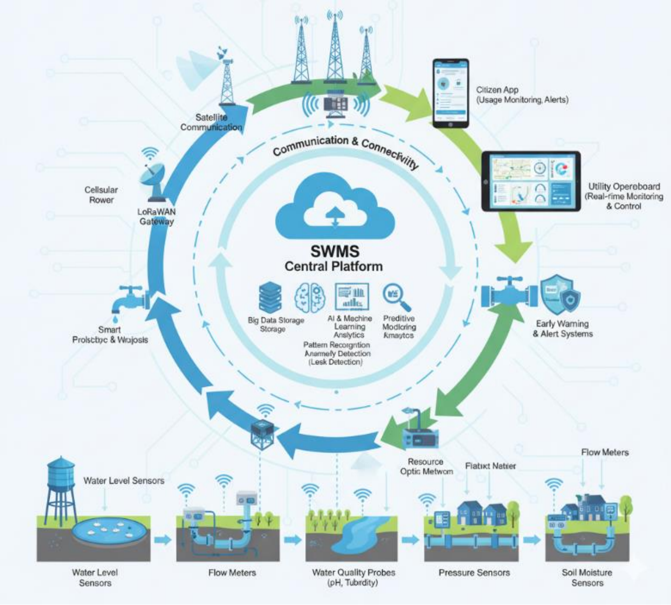

Fig. 2. Illustrates the overall architecture and functionality of a SWMS.

3.2 Typical layered architecture for SWMS

Modern SWMS are typically designed as modular, layered architectures that distinctly separate functions such as perception (sensing and actuation), communication, edge and cloud processing, data and trust management (often integrating cloud, federated, and Blockchain components), analytics, and application services or presentation layer. This structured separation enhances scalability, fault isolation, interoperability among heterogeneous devices, and supports incremental security improvements [45][47]. This layered perspective is consistently reflected in recent reviews and system implementations as described below.

3.2.1. Perception (sensing and actuation) layer

Flow meters, pressure transducers, level sensors, and water-quality probes (pH, turbidity, chlorine, and conductivity) capture hydraulic and quality data at critical points, while motorized valves, pumps, and controlled reclosures regulate system operation. These edge devices use low-power microcontrollers such as Arduino or ESP32, or LoRaWAN-enabled nodes with onboard analog-to-digital converters, and firmware that handles sampling, filtering, event detection (e.g., leak thresholds), and device health monitoring. Many operate on energy-efficient power sources, including solar options for remote sites [45]. Sampling rates depend on the application—higher for transient pressure events and lower for metering—while on-device preprocessing, such as aggregation, compression, and anomaly filtering, reduces bandwidth use and conserves battery life [1][48-50].

3.2.2. Communication layer

Field devices connect to local gateways using protocols such as LoRaWAN, NB-IoT, Sigfox, cellular links, or mesh networks, depending on deployment constraints. Gateways preprocess data and forward it to cloud or private data stores, with LPWAN technologies favored for long-range, low-power scenarios [38]. The common short-range options include Bluetooth Low Energy (BLE) and IEEE 802.15.4 (Zigbee). At the same time, NB-IoT supports broader metropolitan coverage, and LoRa/LoRaWAN, Sigfox, and cellular NB-IoT address remote deployments. Backhaul connections typically rely on cellular (3G/4G/5G), wired broadband, or metro fiber to link gateways with cloud platforms or operational support systems (OSS). Gateways also translate protocols (e.g., MQTT, CoAP, HTTP/HTTPS) and enforce security through TLS or DTLS. Overall, network-layer design must balance latency for real-time alerts, throughput for telemetry, energy efficiency, cost, gateway reliability, quality of service for alarms, and secure over-the-air firmware updates (FOTA) [47-51].

3.2.3. Edge/cloud processing and storage layer

In modern SWMS, data are filtered, aggregated, and stored across distributed layers, with edge nodes performing lightweight analytics, such as anomaly filtering and data compression. At the same time, cloud platforms manage databases, digital twins, and large-scale analytics. Digital twin models, which serve as real-time virtual replicas of hydraulic networks, enable simulation, forecasting, and scenario testing [10]. The key functionalities include real-time event detection (e.g., pressure transients, burst detection), data filtering and anonymization, local actuator control logic, and lightweight machine learning or neural network inference for anomaly detection and predictive maintenance. Edge nodes also provide local caching and resilient buffering to address connectivity disruptions, enforce access control policies, and handle PKI/TLS termination. This distributed design reduces network load, enhances responsiveness for critical control operations such as automated valve shutoff, and establishes a secure boundary for sensitive data before large-scale aggregation. Consequently, recent SWMS architectures increasingly adopt an edge-tier approach as a best practice [1][47][51].

3.2.4. Data & trust management layer

This layer ensures secure long-term data storage, immutable logging, provenance tracking, and decentralized trust among stakeholders, including utilities, regulators, consumers, and third-party analytics providers. It integrates time-series databases or data lakes (e.g., InfluxDB, Timescale, AWS Timestream) for telemetry, alongside metadata and provenance stores to monitor sensor calibration, firmware versions, and data lineage. A permissioned Blockchain (e.g., Hyperledger Fabric, Quorum) supports immutable audit trails, smart contracts for enforcing service-level agreements, billing automation, and multi-stakeholder data sharing, offering controlled membership and higher throughput than public Blockchains. Gateways or Blockchain nodes record transaction summaries or batches of hashed data on-chain, while raw telemetry remains off-chain in time-series databases—balancing integrity with scalability. Smart contracts enable automated billing, alerts, and conditional payments such as water trading or irrigation credits. Recent reviews highlight the value of Blockchain in ensuring integrity, transparency, and trust in water systems, while underscoring the importance of hybrid on-chain/off-chain architectures to address throughput, storage, and privacy constraints [38][39].

3.2.5. Analytics & application services layer

This layer utilizes statistical methods, classical machine learning, and increasingly deep learning or transformer-based models to support functions such as demand forecasting, leak detection, pump scheduling, and water quality prediction.

The resulting outputs integrate with GIS dashboards, operator alerts, and automated control systems, enabling both decision support and closed-loop automation [10][45]. Its core capabilities include batch analytics for trend discovery and model training using cloud or distributed frameworks; real-time analytics and streaming machine learning for rapid fault detection and alarm generation; and the integration of digital twins and hydraulic models with live telemetry for scenario analysis and predictive testing [1][47-50].

3.2.6. Application/service/presentation layer

This layer provides dashboards, APIs, mobile applications, billing systems, and operator SCADA/ICS interfaces. Its key modules include operator dashboards with real-time KPIs, GIS overlays, and alarm management; customer portals for monitoring consumption, bills, and alerts; and APIs that enable third-party analytics and integration with municipalities. It also supports automated control actions, such as work order generation and actuator commands, implemented with human-in-the-loop safeguards. The user interface/user experience must clearly present confidence measures for automated decisions, particularly those driven by machine learning or QML models. Role-based access control and Blockchain-derived audit trails should be visible to both users and auditors. Interfaces are designed for operators, regulators, and consumers and encompass billing portals, mobile apps, and regulatory reporting tools. Additionally, smart contracts and auditable logs are sometimes integrated to ensure transparent transactions and the provenance of critical measurements [1][38][48][50].

Figure 3 depicts the layered architecture of the SWMS.

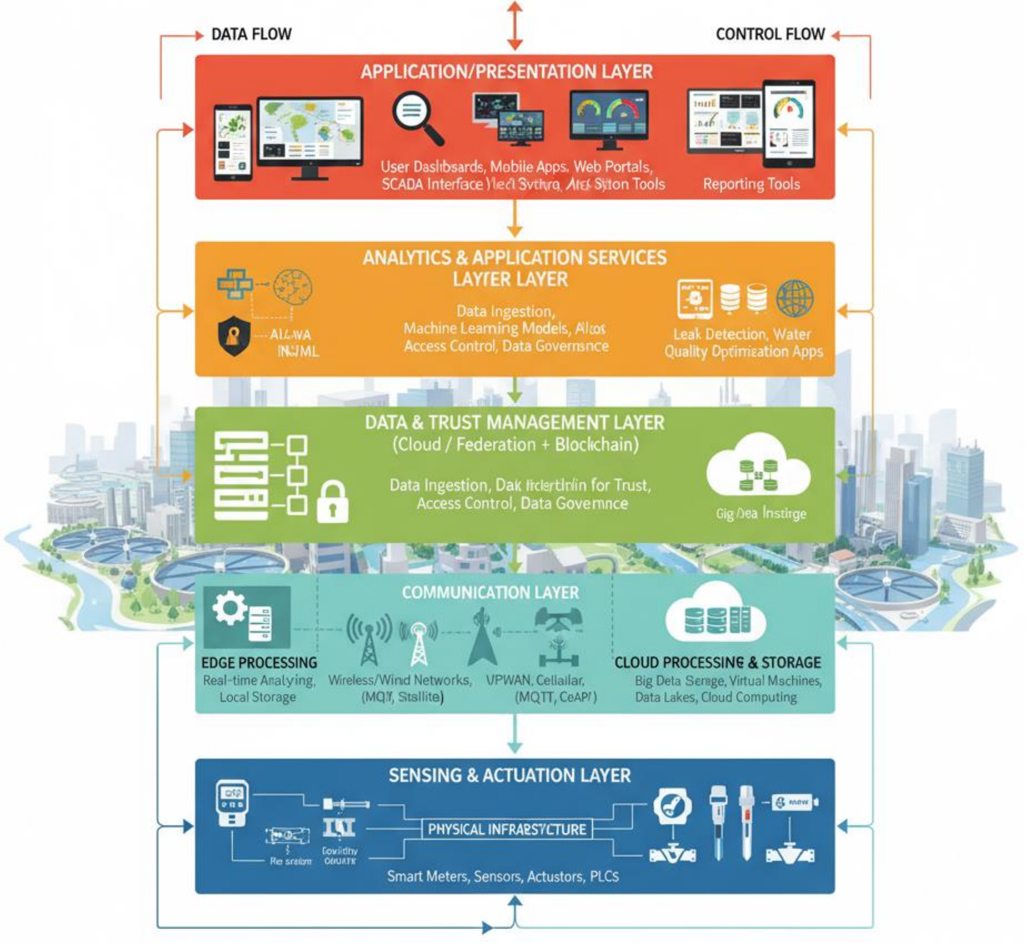
DATA FLOW
CONTROL FLOW
APPLICATION/PRESENTATION LAYER
User Daslibsards, Mobiie Apps. Web Portals,
SCADA Interface Yled Svthra, Ats Siton Tools
Reporting Tools
ANALYTICS & APPLICATION SERVICES
LAYIER LAYER
ALLAVA
IN-JML
Data Ingestion,
Machine Learning Models, Alcot
Access Control, Data Governsnce
Leak Detection, Water
Quality Dptimization Apps
DATA & TRUST MANAGEMENT LAYER
(Cloud / Federation + Blockchain)
Data Ingestion, Dak lrclertlnin for Trust,
Access Control, Data Govemnce
Gig Dea Instirge
COMMUNICATION LAYER
EDGE PROCESSING
Real-time Analying,
Local Storage
Wireless/Wind Networks,
(MQT, Stsllite)
VPWAN, Cellailar,
(MQTT, CeAP)
CLOUD PROCESSINE & STORAGE
Big Deta Serege, Virtual Mschines,
Data Lakes, Cloud Computing
SENSING & ACTUATION LAYER
PHYSICAL INFRARSTCTURE
Re sralom
Coviidhy
OBUAEK
Smart Meters, Sensors, Actustors, PLCS

Fig. 3. Illustrates the layered architecture for the SWMS.

3.3 Key Enabling Technologies for SWMS

SWMS effectiveness relies on a set of enabling technologies that support real-time monitoring, predictive analytics, automated decision-making, and transparent governance of water resources. Together, these technologies integrate diverse data sources, ensure secure communication, and optimize water distribution and quality management. Below are the detailed descriptions of the core technologies for SWMS.

3.3.1. Internet of Things and smart sensors

IoT and smart sensors form the technological backbone of SWMS, enabling real-time monitoring, data-driven decision-making, and automated control across the water supply chain [52]. By connecting reservoirs, treatment plants, pipelines, pumping stations, and consumer endpoints through wired and wireless protocols such as LoRaWAN, NB-IoT, ZigBee, and 5G, IoT collects data continuously from sensors that measure flow, pressure, pH, turbidity, and leakage, transmitting it to centralized platforms for analysis [5][53-56]. This system rapidly detects leaks and anomalies, automates valve and pump operations, and supports remote management through cloud platforms. By integrating AI and Blockchain analytics, IoT shifts SWMS from reactive to predictive management, improving water quality, optimizing energy and resource use, ensuring transparent operations, and promoting demand-side conservation through smart metering [45].

3.3.2. Wireless sensor networks

Wireless Sensor Networks (WSNs) are a core element of SWMS, enabling real-time monitoring, data collection, and control across water distribution, treatment, and consumption. These networks consist of spatially distributed sensor nodes equipped with sensing, processing, and communication functions that autonomously measure parameters such as flow, pressure, turbidity, pH, temperature, leakage, and contamination, and transmit the data to centralized or cloud platforms for analysis and AI-driven control. Their wireless, scalable, and energy-efficient architecture, supported by low-power devices and energy-harvesting techniques, reduces deployment costs, enables flexible expansion, and supports reliable operation in remote areas. By providing continuous, non-intrusive monitoring, WSNs enhance operational visibility, enable leak detection, optimize pressure management, facilitate predictive maintenance, and strengthen water-quality protection, helping address challenges such as water scarcity, aging infrastructure, and contamination risks. A typical WSN-enabled SWMS includes a sensing layer for water measurements, a communication layer using protocols such as Zigbee, LoRaWAN, or Bluetooth, and a head-end system for data aggregation, visualization, and intelligent control [56-58].

3.3.3. Wireless communication networks

Wireless communication networks support scalable and efficient SWMS operations by enabling real-time data exchange among distributed sensors, actuators, smart meters, and control centers across urban, industrial, and agricultural systems. They continuously collect and transmit data on water quality, consumption, leakage, pressure, and distribution efficiency, allowing timely analysis, monitoring, and automated control. Core technologies include cellular networks (4G/5G/6G) for high-speed, wide-area connectivity; Low Power Wide Area Networks (LPWAN) such as LoRaWAN and NB-IoT for long-range, energy-efficient communication; WSNs for localized monitoring; Wi-Fi and Bluetooth for short-range environments; and satellite links for remote areas. These networks provide scalability, reliability, low latency, energy efficiency, and interoperability with cloud, edge, and AI-driven platforms. However, they face challenges from interference, signal attenuation, cybersecurity threats, and high deployment costs. Researchers address these issues using hybrid communication models, energy harvesting, quantum-secured channels, and Blockchain-based authentication, guided by standards like IEEE 802.15.4g, ZigBee, LoRa, NB-IoT, and Wi-Fi [38][56][59].

3.3.4. Cloud computing

Cloud computing underpins SWMS by delivering scalable, flexible, and cost-efficient infrastructure for storing, processing, and analyzing heterogeneous water data from sensors, IoT devices, smart meters, and edge gateways. It integrates real-time analytics to detect leaks, forecast demand, optimize distribution, automate responses, and dynamically allocate resources during peak or emergency loads. Centralized platforms enable remote monitoring and control through web or mobile interfaces, giving operators access to system status, historical trends, and management tools. By leveraging advanced analytics, AI, and QML, cloud systems support predictive maintenance, anomaly detection, energy optimization, and resilient network operations. Standardized APIs and middleware improve interoperability across municipalities, industries, and smart city ecosystems, while strong security mechanisms, including encryption, identity management, access control, and emerging Blockchain and PQC technologies, safeguard operational and consumer data. Cloud environments also enable real-time consumption tracking, automated billing, and personalized conservation insights, strengthening transparency, customer engagement, and sustainable water management across urban, industrial, and agricultural sectors [51][60-62].

3.3.5. Edge computing

Edge computing decentralizes data processing by analyzing information close to its source, such as sensors, actuators, and IoT devices, rather than relying solely on cloud servers. In SWMS, it enhances efficiency, responsiveness, and reliability by enabling real-time monitoring of water quality, flow, pressure, leakage, and infrastructure health. Edge nodes instantly detect anomalies, reduce latency for time-critical actions, optimize bandwidth through selective data transmission, and sustain operations during network disruptions. Local AI and machine learning models provide predictive analytics for forecasting water demand, anticipating equipment failures, and planning maintenance, while strengthening data security and privacy. This layered architecture of sensing devices, edge units, and cloud integration supports adaptive water distribution, energy efficiency, and overall system resilience [63][64].

3.3.6. Blockchain technology

Blockchain is transforming SWMS by offering a decentralized, secure, and transparent infrastructure for monitoring, distributing, and managing water resources. As a distributed ledger, it records transactions, sensor outputs, and management actions in a tamper-proof and auditable format, ensuring data integrity, traceability, and accountability for stakeholders such as government agencies, utilities, and consumers [33][39][65][66]. Its decentralized architecture eliminates single points of failure, and smart contracts automate key functions, including leak detection, billing, and demand-responsive distribution, thereby improving efficiency and reducing manual involvement. Integrated with IoT sensors, AI, and cloud platforms, Blockchain enables real-time, data-driven decision-making that supports equitable and sustainable urban water management [33][38][39][66].

3.3.7. AI and machine learning

AI and machine learning are reshaping SWMS by enabling automated, data-driven, and predictive monitoring, treatment, and distribution. By integrating diverse datasets from sensors, IoT devices, and remote sensing technologies, these tools forecast water demand, detect anomalies, and assess water quality in real time. Predictive models anticipate seasonal consumption, identify potential contamination, and guide proactive infrastructure maintenance, while AI-driven optimization of pumping schedules, reservoir management, and distribution routing improves energy efficiency and operational sustainability. These technologies also strengthen irrigation planning, flood forecasting, and wastewater treatment, supporting smart agriculture through optimized water use and continuous crop-stress monitoring. Overall, AI and ML deliver real-time analytics, predictive intelligence, and autonomous control, enhancing the efficiency, resilience, and sustainability of SWMS [10][67].

3.3.8. Big data analytics

Big data analytics now plays a central role in modern SWMS by enabling utilities to collect, process, and analyze large, heterogeneous datasets spanning the entire water supply chain—from source and treatment to distribution, consumption, and wastewater. By integrating data from IoT sensors, smart meters, remote sensing, and even social platforms, and leveraging cloud computing and machine learning, utilities shift from reactive to predictive operations. These capabilities support real-time monitoring of flow, pressure, and water quality, improve demand forecasting and leak detection, strengthen infrastructure planning, and inform conservation and emergency response. Leveraging environmental, hydrological, and historical usage data, utilities transform raw information into actionable insights that enhance efficiency, maintain water quality, and strengthen resilience against climate and urbanization pressures. Ultimately, big data analytics drives intelligent, sustainable, and reliable SWMS operations [60][68][69].

3.3.9. Cybersecurity solutions

Cybersecurity plays a critical role in protecting SWMS by maintaining the integrity, availability, and confidentiality of essential water infrastructure data. As urban water networks increasingly adopt IoT devices, cloud computing, AI, and automation, they become more vulnerable to threats such as unauthorized access, ransomware, false data injection, and data manipulation [70-72], which can disrupt distribution, compromise water quality, and inflict environmental and economic harm. To mitigate these risks, operators deploy AI-driven intrusion and anomaly detection, automated log management, real-time monitoring, and end-to-end encryption—especially for remote systems using LoRaWAN or Wize. Integrating Blockchain with digital twins further strengthens data authenticity, predictive maintenance, and operational transparency. Resource-constrained entities can leverage automated and open-source cybersecurity frameworks for cost-effective protection. Coupled with risk assessments, tailored security architectures, workforce training, and adherence to sector-specific governance standards, these measures collectively enhance the resilience and sustainability of SWMS [73][74].

3.3.10. Digital twins

Digital twin technology is revolutionizing SWMS by creating dynamic, real-time digital replicas of physical water infrastructure. By integrating IoT sensors, machine learning, and AI, digital twins continuously monitor pipelines, pumps, tanks, and treatment facilities, enabling utilities to visualize system performance, detect anomalies, forecast demand, and optimize maintenance schedules. They support operational scenario simulations, predictive analytics, leak detection, water quality monitoring, energy optimization, and resilience assessments by aggregating data from SCADA systems, advanced metering infrastructure (AMI), and IoT devices. The incorporation of deep learning, reinforcement learning, and Blockchain further enhances predictive accuracy, automation, and data security, establishing digital twins as a cornerstone of smart, sustainable, and resilient water management [75-77].

3.3.11. Geographic information systems and remote sensing

Geographic information systems (GIS) and satellite-based remote sensing (RS) are vital for modern water resource management, enabling the collection, integration, and analysis of spatial and temporal data. They enable comprehensive monitoring of watersheds, groundwater, land-use patterns, and environmental parameters, including precipitation, evapotranspiration, soil moisture, and water quality. In SWMS, GIS facilitates resource mapping, infrastructure management, and risk assessment by linking hydrological, environmental, and socio-economic datasets. At the same time, RS provides large-scale, real-time observations to inform disaster response and track the impacts of climate and land-use changes. Integrating GIS with data from satellites, UAVs, and ground-based sensors supports multi-scale, multi-temporal mapping and monitoring for applications including sustainable irrigation, flood and drought mitigation, and river and reservoir management. GIS-based visualization and participatory tools further engage stakeholders, enabling adaptive, data-driven policies that enhance the resilience and sustainability of water systems [78-80].

3.3.12. Quantum computing and QML

Quantum computing leverages the principles of superposition, entanglement, and interference to perform calculations beyond the reach of classical computers. Unlike classical bits, quantum bits (qubits) can exist in multiple states simultaneously, enabling concurrent processing of complex combinatorial problems. In SWMS, quantum computing optimizes resource allocation in water distribution networks, supports real-time simulation and forecasting of hydrological and environmental processes, and strengthens cybersecurity through quantum-resistant encryption. When combined with machine learning in QML, it enhances system intelligence by analyzing large, complex datasets to detect patterns, manage uncertainties, and optimize predictions in dynamic, nonlinear water systems [81][82]. Applications include predictive maintenance of pumps, valves, and pipelines; anomaly detection for water quality; precise demand forecasting based on climate and consumption trends; and energy-efficient operations through optimized treatment and pumping schedules. By integrating quantum computing with QML, SWMS can achieve advanced optimization, accelerate hydrological simulations, and maintain robust data security, enabling more efficient, resilient, and sustainable water resource management even as scalable quantum hardware continues to develop [83].

3.3.13. Robotics and autonomous systems

Robotics and autonomous systems are transforming modern SWMS by enabling precise, reliable, and minimally supervised operations across complex water infrastructures. Autonomous drones, underwater vehicles, and robotic crawlers continuously monitor pipelines, reservoirs, dams, and treatment facilities, detecting leaks, corrosion, blockages, or contamination using advanced sensors such as LiDAR, ultrasonic devices, and thermal cameras. These systems reduce human exposure to hazards, lower operational costs, and provide real-time data for predictive maintenance. Integrated AI and machine learning enhance fault detection, optimize water distribution, forecast failures, and support dynamic demand management, while IoT-enabled sensors enable in-situ assessment of water quality parameters, including pH, turbidity, dissolved oxygen, and microbial presence. Key applications include smart irrigation, early contamination detection, pipeline inspection, and water treatment or remediation via micro- and nanorobots. Emerging technologies such as swarm robotics, AI-driven repair robots, and fully integrated cyber-physical systems promise coordinated monitoring, self-optimizing operations, and improved resilience, positioning robotics and autonomous systems as central to intelligent, adaptive, and sustainable water management [84-86].

3.3.14. Smart metering and advanced metering infrastructure

Smart metering employs digital water meters that record, process, and transmit real-time usage data, offering a clear improvement over traditional manual meters [46][87][88]. These meters deliver high-resolution, time-stamped data that enable utilities and consumers to monitor consumption patterns, detect leaks or unauthorized use, and identify potential system failures, thereby reducing water loss and improving network reliability. When integrated into SWMS with AMI, they create a comprehensive ecosystem of hardware, software, and communication networks that enable two-way communication, automated meter reading, remote configuration, and real-time alerts. This integration optimizes water distribution, supports anomaly detection and predictive maintenance, and enhances emergency response, while engaging customers through actionable consumption insights. AMI's interoperability with IoT sensors and predictive analytics further improves operational efficiency, billing accuracy, and water conservation, enabling advanced applications such as machine learning–based demand forecasting and Blockchain-secured data, which strengthen the sustainability and resilience of urban water networks [46][88].

3.3.15. Renewable energy integration

Integrating renewable energy into SWMS enhances sustainability, efficiency, and resilience by powering energy-intensive processes such as water pumping, treatment, and desalination with solar, wind, or micro-hydro sources. This approach reduces reliance on fossil fuels, lowers operational costs, and minimizes environmental impact. Coupled with energy storage, renewable-driven systems maintain critical operations during grid failures or low-generation periods, supporting both off-grid and urban water infrastructures. Advanced IoT monitoring and AI-based energy management enable predictive control, dynamically adjusting pumping, treatment, and irrigation schedules to match renewable availability, optimizing performance, and cutting carbon emissions [60][89][90]. Practical applications include solar- and wind-powered pumps, renewable-driven desalination in arid regions, smart IoT-integrated irrigation, and energy recovery technologies such as Pumped-As-Turbines (PAT). Integrated renewable microgrids further improve cost efficiency, resilience, and grid stability, collectively transforming SWMS into sustainable, reliable, and environmentally responsible water infrastructures [60][89][90].

3.3.16. Human–machine interfaces and decision support systems

Human–machine interfaces (HMIs) in SWMS provide operators with intuitive, real-time access to data from sensors, actuators, and IoT devices, enabling monitoring of flow rates, pressure, reservoir levels, pump status, and water quality, while supporting both manual control and automated operations via SCADA integration. Modern HMIs feature interactive dashboards, geospatial mapping, and predictive visualizations that allow rapid anomaly detection, event prioritization, and informed decision-making. Complementing these interfaces, decision support systems (DSS) apply machine learning, statistical modeling, and optimization algorithms to forecast demand, detect potential failures, and recommend actions for efficient water distribution, treatment, and energy management [91-93]. DSS also performs risk assessment, scenario modeling, and integration with IoT, GIS, SCADA, and Blockchain frameworks, enhancing system resilience, transparency, and stakeholder engagement. By combining HMIs and DSS, operators can leverage real-time monitoring, predictive planning, and agile responses, fostering sustainable, resilient smart water management [91-93].

3.4 Common Applications of SWMS

SWMS use digital technologies to enhance water monitoring, distribution, and conservation across various sectors, with their primary applications summarized in Table I.

TABLE I. BRIEF DESCRIPTIONS OF THE TYPICAL APPLICATIONS OF SWMS.

S/No	Applications	Brief Description	References
1	Real-time water quality monitoring	Real-time water quality monitoring provides continuous assessment of conditions across distribution networks, reservoirs, treatment plants, and natural sources. These systems use interconnected sensors, IoT devices, and analytics to measure key parameters, including pH, turbidity, dissolved oxygen, temperature, conductivity, salinity, and contaminants such as heavy metals, nitrates, and pathogens. Sensor data travels through wireless networks to centralized platforms, where edge and cloud infrastructures enable rapid analysis, anomaly detection, and predictive modeling. AI and machine learning strengthen trend analysis, risk forecasting, and operational decision-making, while Blockchain enhances data security, transparency, and integrity. This integrated approach allows operators to quickly detect contamination events, leaks, and infrastructure issues, ensuring regulatory compliance, protecting public health, and supporting sustainable water use in domestic, agricultural, and industrial settings.	[4][16]
2	Leak detection and pipeline monitoring	Leak detection and pipeline monitoring form essential functions within SWMS, reducing the 20–40% of global water loss caused by leaks, bursts, and unauthorized consumption. SWMS employs acoustic, pressure, flow, and fiber-optic sensors to gather real-time data on pressure shifts, flow patterns, and vibrations, which IoT networks transmit for analysis. Machine learning models identify anomalies associated with leaks or pipeline deterioration, enabling proactive maintenance, while GIS and digital twins enhance system visualization and prediction. Blockchain preserves data integrity, and QML enhances detection accuracy in dynamic environments. In residential systems, smart monitors alert users to tap leaks through mobile applications, supporting responsible water use and lowering costs. Collectively, these technologies shift water management from reactive practices to predictive, data-driven operations that reduce costs, limit service disruptions, mitigate contamination risks, and improve the efficiency, resilience, and sustainability of water distribution networks.	[94-96]
3	Smart metering and consumption monitoring	Smart metering and consumption monitoring provide utilities, municipalities, and consumers with real-time visibility into water use by integrating sensors, communication modules, and data processing for automated, remote measurement. Using IoT devices and wireless technologies such as NB-IoT, LoRaWAN, and 5G, these systems transmit data to centralized platforms, enabling rapid detection of leaks, bursts, or unauthorized use and reducing water loss and operational costs. Households and industries access dashboards and mobile apps that reveal consumption patterns and highlight inefficiencies, supporting informed conservation decisions. Advanced analytics and AI further strengthen these systems by forecasting demand, optimizing distribution, improving billing accuracy, and	[50][97]

		enabling dynamic pricing that promotes sustainable use. As water scarcity and climate pressures intensify, smart metering plays a critical role in advancing efficient, transparent, and equitable water management.	
4	Irrigation and agriculture management	SWMS support irrigation and agricultural operations—an area that consumes nearly 70% of global freshwater—by integrating IoT, AI, remote sensing, and Blockchain to optimize water use and strengthen sustainability. IoT sensors and wireless networks provide real-time data on soil moisture, weather, groundwater, and crop water needs. At the same time, AI-driven models generate adaptive irrigation schedules and forecast water demand under shifting climatic conditions. GIS and satellite-based remote sensing enable spatially targeted irrigation, and Blockchain adds transparency and traceability to water allocation. Climate-smart components, such as renewable-energy pumps and intelligent scheduling, reduce carbon emissions, and emerging approaches, such as QML, improve resilience by predicting system failures and optimizing large-scale networks. Through this data-driven, proactive approach, SWMS boost water efficiency, increase crop yields, and promote sustainable agricultural practices.	[50]
5	Flood and stormwater management	Flood and stormwater management has become a key application of SWMS as climate change, urbanization, and extreme weather intensify flooding risks. SWMS uses IoT sensors, predictive models, and early warning systems to monitor rainfall, runoff, and river and reservoir water levels, enabling proactive, adaptive responses that reduce damage. When integrated with GIS and digital twins, these systems improve situational awareness, support scenario analysis, and guide real-time decision-making. At the same time, automated pumps, gates, and valves allow remote regulation of water flow. This combination strengthens climate resilience, optimizes infrastructure use, and supports sustainability goals such as water reuse and ecosystem protection, as demonstrated in cities like Singapore, Rotterdam, and Copenhagen.	[98][99]
6	Reservoir and dam monitoring	Reservoirs and dams serve essential roles in water supply, irrigation, flood control, hydropower generation, and ecosystem regulation, and their safe, efficient operation depends on continuous monitoring supported by modern SWMS. These systems use advanced sensing technologies, IoT connectivity, real-time analytics, and AI-driven decision-support tools to track structural integrity, hydrological conditions, and environmental parameters. Structural health sensors such as piezometers, strain gauges, inclinometers, and vibration monitors measure stress, displacement, and seepage, while hydrological and hydraulic sensors, including water-level sensors, radar-based flow meters, and weather-driven forecasting tools, optimize water allocation and system performance. Environmental sensors monitor dissolved oxygen, turbidity, and nutrient levels to maintain ecological compliance. The system transmits sensor data to the cloud or centralized platforms for remote monitoring, automated alerts, and real-time decision-making, while microcontroller-based automation (NodeMCU, Arduino, and PLCs) operates actuators such as sluice gates and valves for precise flow control. Integration with SCADA and HMI systems enhances visibility, predictive maintenance, and risk management, supported by AI and Blockchain for secure data exchange, early warnings, and coordinated emergency response.	[100][101]
7	Pressure management and control	Pressure management and control play a critical role in SWMS by improving distribution efficiency, extending infrastructure lifespan, and ensuring reliable service. Excessive or poorly regulated pressure often causes pipe bursts, leaks, non-revenue water losses, and unnecessary energy consumption. However, modern systems address these challenges through real-time monitoring, predictive analytics, and automated control. Networks of pressure, flow, and leakage sensors connected to IoT platforms supply continuous data to centralized or cloud-based systems, where machine learning and predictive algorithms optimize pressure settings and anticipate maintenance needs. Key components such as Pressure-Reducing Valves, throttle control valves, and variable-frequency drives dynamically adjust pressure in response to demand, while advanced approaches like time-based scheduling and hybrid PRV/TCV configurations further reduce variability and operational stress. Integrating AI, digital twins, and Blockchain strengthens these capabilities by simulating hydraulic behavior, forecasting demand, enabling adaptive control, and ensuring secure, transparent data sharing, ultimately reducing leakage by up to 30%, improving energy recovery, and supporting sustainable, equitable water service.	[54]
8	Wastewater and sewage management	Wastewater and sewage management are central to SWMS, supporting sustainable sanitation, environmental protection, and public health. As urbanization, climate change, and industrial discharges intensify system pressures, SWMS integrate IoT sensors, AI, Blockchain, and advanced analytics to enable real-time monitoring, predictive management, and	[52][102]

		efficient resource use. Distributed sensors continuously track parameters such as flow rate, pH, pollutant concentrations, and hazardous gases, transmitting data to cloud platforms for anomaly detection, maintenance forecasting, and process optimization. Automated, remotely controlled systems improve operational efficiency by enabling rapid responses to blockages or abnormal conditions and reducing the need for manual interventions. Machine learning models forecast inflow patterns, equipment failures, and pollutant loads, supporting proactive maintenance and energy-efficient treatment adjustments through smart aeration systems and membrane bioreactors. These technologies also advance circular economy goals by recovering water, nutrients, and energy for reuse, while Blockchain enhances transparency and regulatory compliance. Incorporating wastewater epidemiology and digital twins further strengthens early warning capabilities, supports climate-resilient urban planning, and improves the management of sewage and stormwater.	
9	Water demand forecasting	Water demand forecasting plays a vital role in SWMS by enabling utilities, policymakers, and urban planners to anticipate consumption patterns and allocate resources efficiently amid urbanization, population growth, and climate variability. Accurate forecasts guide infrastructure development, including pipelines, reservoirs, and treatment facilities, while supporting demand-side strategies such as tiered pricing, conservation measures, and leakage reduction. Modern systems improve prediction accuracy by combining classical statistical methods, machine learning, and deep learning. Time-series models like ARIMA and SARIMA analyze historical trends. In contrast, machine learning techniques such as Random Forest and Support Vector Machines (SVM) capture nonlinear patterns driven by socio-economic and environmental factors. Deep learning architectures, including Long Short-Term Memory (LSTM) and Convolutional Neural Networks (CNNs), model complex temporal and spatial dependencies, and hybrid approaches incorporating feature selection, attention mechanisms, or ensemble learning enhance reliability under non-stationary, noisy conditions. By integrating high-frequency data from smart meters, IoT sensors, and SCADA systems with weather, demographic, and land-use information, these systems produce granular forecasts at household, district, and city scales, improving operational efficiency, reducing non-revenue water, and enabling evidence-based, sustainable planning.	[103]
10	Energy efficiency in water treatment	Energy efficiency has become a critical priority in water treatment, particularly in SWMS, due to the high energy demands of conventional processes, during which Water treatment plants can consume 30–50% of municipal energy through pumping, aeration, filtration, desalination, and chemical dosing. SWMS enhances efficiency by leveraging IoT sensors, AI, digital twins, and Blockchain-enabled monitoring to optimize energy use, reduce operational costs, and lower carbon emissions. Real-time monitoring and AI-driven predictive models dynamically adjust aeration, pumping, and chemical dosing, improving process control, detecting faults, and supporting maintenance scheduling. By integrating renewable energy sources, such as solar PV, biogas from sludge, and micro-hydropower, and simulating energy-saving scenarios via digital twins, plants can align energy-intensive operations with off-peak electricity periods. Additional strategies, including high-efficiency pumps, membrane filtration, biogas recovery, and emerging methods such as electrocoagulation, forward osmosis, and membrane distillation, can reduce energy demand by 20–50% while maintaining or improving water quality standards.	[104-106]
11	Asset management and predictive maintenance	In SWMS, utilities vigorously monitor, track, and optimize water infrastructure, including pipelines, pumps, valves, reservoirs, and treatment plants, using IoT sensors, GIS, and advanced analytics. These tools provide real-time insights into asset condition, location, and utilization, enabling up-to-date inventories, spatial mapping, and performance evaluation to identify aging or underperforming components. Data-driven decision support allows utilities to prioritize maintenance, plan upgrades, and allocate resources efficiently, reducing operational costs, minimizing water losses, and enhancing reliability. By leveraging predictive maintenance, historical trends, and machine learning, SWMS anticipate failures, detect anomalies such as pump degradation or pipe corrosion, and schedule interventions before breakdowns occur. Integrating digital twins, IoT networks, and AI-driven analytics further refines condition assessment and forecasts remaining useful life, transforming operations from reactive to proactive, extending infrastructure lifespan, and generating significant economic benefits.	[97][107][108]
12	Smart water distribution	Smart water distribution is the core of SWMS, delivering water efficiently, reliably, and sustainably from treatment plants to end users. Traditional networks often suffer from leakage, uneven pressure, unplanned downtime, and high energy consumption. By integrating IoT sensors, smart meters, and	[50][69]

		advanced communication and control technologies, SWMS transforms these networks into intelligent, data-driven systems. It monitors flow, pressure, and water quality in real time; detects leaks and manages losses using machine learning and acoustic sensors; dynamically controls pressure to prevent pipe bursts and optimize energy use; and forecasts demand with load balancing based on historical and real-time data. Digital twins enable system optimization through virtual modeling, scenario analysis, and maintenance planning, while automated valves, pumps, and dashboards allow adaptive distribution under changing demand or emergency conditions. These technologies collectively enhance reliability, minimize water loss, reduce energy consumption, and support sustainable urban water management.	
13	Water theft detection	Water theft—caused by illegal connections, meter tampering, or unauthorized extraction—challenges urban and rural water utilities, resulting in financial losses and disrupting equitable distribution, especially in water-scarce regions. SWMS combat these issues using IoT-enabled meters and sensors, machine learning, geospatial monitoring, and cloud-based analytics to detect and prevent theft in real time. Smart meters and flow sensors monitor consumption, pressure, and flow anomalies, while GIS-based mapping pinpoints potential illicit activity. Automated alerts, remote-controlled valves, and GSM modules enable rapid intervention, minimizing losses and ensuring reliable service. Machine learning algorithms analyze usage patterns to identify anomalies, predict high-risk areas, and support immediate response and long-term planning. Cloud platforms and dashboards facilitate remote monitoring, transparent billing, and visualization of consumption trends, improving operational efficiency, consumer accountability, and sustainable water management. Blockchain integration further secures data logging and creates immutable audit trails, enhancing transparency and accountability across the distribution network.	[38][109]
14	Consumer engagement and feedback	Consumer engagement and feedback drive SWMS by connecting utilities and end users through real-time analytics, advanced communication technologies, and user-centered platforms. These systems allow consumers to monitor water usage via smart meters, mobile apps, or web dashboards, providing detailed insights that promote efficient use and enable early detection of leaks or inefficiencies. Interactive tools such as chatbots, online portals, and mobile applications let users report issues directly to utilities, which respond promptly. At the same time, personalized notifications inform users about billing, maintenance, peak demand, and water-saving strategies. Incentives and gamification further encourage sustainable behaviors, and aggregated analytics help utilities optimize operations, conduct proactive maintenance, and manage demand. Empirical evidence, including a study in Valencia, Spain, shows that households receiving frequent feedback reduced water use by an average of 8% over two years. By fostering two-way communication, accountability, and trust, SWMS transform water management into a participatory, data-driven ecosystem that enhances transparency, conservation, and service quality.	[110]
15	Real-time anomaly detection	Real-time anomaly detection enhances the reliability and resilience of water distribution networks by continuously monitoring sensor and smart meter data to detect irregularities in flow, pressure, or consumption that indicate leaks, pipe bursts, unauthorized use, or equipment failures. Advanced analytics, machine learning, and predictive modeling enable these systems to detect issues promptly, allowing utilities to perform proactive maintenance, reduce water loss, and prevent service disruptions. By integrating real-time dashboards and automated alerts, utilities can respond quickly, safeguard water quality, and keep both managers and consumers informed. At the same time, accumulated data continually refine predictive models, optimize maintenance schedules, and support long-term planning for a more sustainable water management ecosystem.	[107]
16	Enhancement in operational efficiency	Smart water management technologies enhance operational efficiency by using IoT and AI to monitor and control water treatment processes in real time. By optimizing operations, they reduce energy consumption and allow utilities to allocate resources more precisely, improving both economic performance and environmental outcomes. These technologies also lower carbon emissions, advancing global sustainability goals.	[107]
17	Conserve precious water resources	Smart water management preserves valuable water resources by combining IoT-enabled monitoring with AI-driven process optimization. Smart meters enable consumers to track and manage their water usage, fostering accountability and conservation, while AI optimizes treatment processes to reduce waste and improve efficiency. This integrated approach advances sustainability by addressing water scarcity and promoting responsible consumption.	[107]
18	Improves the robustness of water systems	Integrating IoT with AI strengthens water system resilience by quickly detecting anomalies and enabling prompt corrective actions. AI algorithms	[107]

		automatically adjust treatment processes or alert operators to emerging issues, ensuring timely interventions that prevent contamination and maintain continuous access to safe water for communities.	

3.5 Cybersecurity Threats, Attacks, and Challenges in SWMS

Despite advancements in SWMS, their increasing reliance on interconnected digital technologies exposes critical water infrastructure to diverse cyber threats, jeopardizing its safety, security, and reliability.

3.5.1. Data breaches

Data breaches in SWMS occur when attackers gain unauthorized access to personal, financial, or operational data flowing through billing systems, asset management platforms, and control networks. These incidents expose utilities to privacy violations, financial fraud, industrial espionage, and legal penalties, undermining public trust and regulatory compliance. Cybercriminals target the high-value data produced by extensive sensor networks, smart meters, and IoT devices, exploiting weak authentication, unpatched software, insecure communication channels, and insider threats to steal information, manipulate operations, or disrupt services. They also frequently compromise SCADA systems, communication networks, and sensors through phishing and malware, while the systems' complexity and heterogeneity impede timely detection and contribute to widespread underreporting [23][71].

3.5.2. Insider threats

Insider threats pose a serious cybersecurity risk to SWMS, as employees, contractors, or third-party vendors with legitimate access can intentionally or unintentionally compromise system integrity [111]. Malicious insiders exploit their knowledge of system architecture and security protocols to manipulate sensor data, alter water flow, or disrupt treatment processes. In contrast, negligent insiders weaken defenses through poor password practices, misconfigurations, or susceptibility to phishing [74]. Weak identity and access management, excessive privileges, insecure IoT endpoints, and limited real-time monitoring further increase these risks [111], potentially causing service disruptions, water contamination, financial losses, and public safety hazards, as demonstrated by the 2023 Pennsylvania water treatment breach and the 2021 Kansas utility shutdown, both resulting from delayed credential revocation and inadequate access controls [23]. Detecting insider threats remains difficult because malicious actions often mimic legitimate system use, a challenge compounded by low cybersecurity awareness and the complexity of interconnected infrastructures.

3.5.3. Malware

Malware continues to threaten SWMS, including viruses, worms, trojans, ransomware, spyware, and rootkits that compromise system confidentiality, integrity, and availability. It targets SCADA systems, IoT sensors, PLCs, and cloud-based management platforms, disrupting operations by manipulating control signals, altering chemical treatment processes, shutting down pumps or valves, or exfiltrating sensitive data [111]. Real-world incidents, such as the 2021 Oldsmar Water Plant breach and Mirai-style IoT attacks, illustrate how false sensor data and unauthorized control actions can endanger water safety. These risks increase when systems run outdated or unpatched software, use weak authentication, or employ insecure communication channels, particularly in IoT devices such as smart meters [24]. Operational disruptions, data corruption, and financial and reputational losses—often amplified by ransomware—highlight the urgent need for robust, adaptable cybersecurity strategies [112].

Ransomware poses a particularly severe threat by encrypting critical data and demanding payment for decryption. SWMS' dependence on interconnected sensors, IoT devices, PLCs, and SCADA networks creates exploitable vulnerabilities, enabling attackers to disable pumps and valves, disrupt treatment operations, and trigger shortages, contamination, or flooding. These attacks endanger public health by impeding the removal of pathogens and chemicals and inflict financial and reputational damage through ransom demands, recovery costs, regulatory penalties, and data breaches [25]. Incidents such as the 2022 South Staffordshire Water intrusion, the Clop exploitation of MOVEit software, and the Atlanta ransomware attack demonstrate how legacy systems, insecure remote access, and third-party dependencies expand the attack surface across water infrastructure.

3.5.4. Social engineering

Social engineering poses a significant threat to SWMS by exploiting human behavior rather than technical vulnerabilities. Attackers manipulate employees, contractors, and stakeholders to disclose confidential information or grant unauthorized access, bypassing protections on SCADA systems, IoT devices, sensors, and cloud platforms. Common tactics include phishing, spear phishing, pretexting, impersonation, baiting, and quid pro quo schemes, often delivered under the guise of water authorities or vendors [74][111]. By leveraging trust, curiosity, and deference to authority, adversaries can gain SCADA access, manipulate water operations, compromise data, and jeopardize water quality. High-profile incidents such as the 2021 Oldsmar water treatment attack and CISA's 2024 alerts on impersonation scams illustrate how social engineering remains difficult to detect, especially when insider risks and inadequate training blur the line between legitimate and malicious activity [74][111].

Phishing remains a primary vector for social engineering in SWMS, exploiting human vulnerabilities to steal credentials, deploy malware, or gain remote access [74]. Attackers exploit deceptive emails, messages, and spoofed websites that mimic trusted regulators or vendors, sometimes presenting as firmware updates or official communications from municipal authorities. These attacks can grant adversaries backdoor access to SCADA systems, cloud platforms, or Blockchain mechanisms, disrupting operations, compromising data integrity, causing financial and reputational harm, and even endangering public health by interfering with pumps, valves, or chemical dosing systems. Phishing also serves as a gateway for ransomware, APTs, and DDoS attacks, as demonstrated by the 2020 malicious email campaign targeting an Israeli water facility, highlighting the persistent vulnerabilities of critical infrastructure in the face of evolving cyberthreats [74].

3.5.5. Supply chain attacks

Supply chain risks in SWMS stem from the complex interdependencies among vendors, suppliers, integrators, operators, and maintainers who assemble and update hardware, software, firmware, and services. Vulnerabilities such as defects, backdoors, or susceptibility to tampering and counterfeiting can compromise system integrity, mainly as SWMS increasingly rely on sensors, actuators, control systems, and interconnected IoT devices. The use of cloud platforms and advanced data processing enlarges the attack surface, enabling attackers to exploit insecure APIs, software updates, or IoT devices to implant malicious code or gain persistent access. Such breaches can disrupt operations, compromise data integrity, and erode stakeholder trust [74]. High-profile incidents, including the SolarWinds attack (2020–2021), the Oldsmar water utility breach (2021), XIoT exploits (2022–2023), the MOVEit file transfer attack (2023), and the 2025 American Water cyberattack, demonstrate how compromised supply chains can trigger cascading failures across critical infrastructure and underscore persistent challenges such as limited visibility into supplier security practices and the emerging vulnerabilities introduced by IoT, AI, and Blockchain integration [113].

3.5.6. Side-channel attacks

Side-channel attacks pose a significant threat to SWMS by exploiting indirect information leaks from distributed sensors, controllers, and embedded devices [114][115]. Adversaries extract sensitive data or disrupt operations by analyzing power consumption, electromagnetic emissions, timing variations, and even acoustic or thermal patterns. Techniques such as differential power analysis, timing attacks, and electromagnetic monitoring have successfully revealed encryption keys, authentication secrets, and operational states in smart meters, treatment systems, and environmental sensors [116]. These attacks are difficult to detect on resource-constrained IoT devices. They are becoming increasingly sophisticated through machine-learning methods, highlighting the urgent need to integrate side-channel defenses into SWMS cybersecurity frameworks.

3.5.7. Rogue device injection

Rogue device injection poses a critical cyber threat to SWMS by allowing attackers to covertly introduce unauthorized hardware that mimics legitimate sensors, actuators, gateways, or controllers. These devices can bypass weak authentication to exfiltrate data, manipulate commands, inject false measurements, or launch attacks such as DDoS, data poisoning, and lateral infiltration. Given SWMS's reliance on IoT devices, SCADA systems, and wireless networks for water distribution and treatment, such intrusions directly compromise system integrity and public safety. For example, a malicious flow sensor could trigger excessive pumping, causing energy waste, leaks, or reservoir depletion, while compromised actuators could disrupt supply, contaminate water, or damage infrastructure. Attackers may exploit insecure wireless protocols, tamper with hardware during procurement or maintenance, or physically insert devices at remote sites, making robust detection and mitigation strategies essential to prevent operational disruptions, false data, and physical hazards [71][117].

3.5.8. Replay attacks

Replay attacks target SWMS by exploiting the trust among their sensors, actuators, communication networks, and control systems. Adversaries capture legitimate transmissions and resend them to provoke unauthorized or redundant actions. Since these messages remain valid and unaltered, detecting such attacks requires strong cryptographic safeguards or precise timing mechanisms. Their impact can be substantial: replayed SCADA commands may cause pumps to operate at improper times, leading to pressure fluctuations, service interruptions, or equipment damage, while retransmitted sensor readings can trigger unnecessary treatments, delay leak detection, distort billing, or mask maintenance needs. Empirical studies demonstrate that replay attacks can stealthily manipulate SWMS by mimicking authentic data streams. Such attacks can lower smart meter charges, trigger erratic pump cycling that stresses equipment, and block timely repairs by falsifying "no-leak" signals, thereby compromising the system's operational integrity [26].

3.5.9. False data injection attacks

False data injection attacks (FDIAs) threaten SWMS by deliberately inserting misleading information into sensors, actuators, or communication channels, undermining system reliability [27]. Attackers stealthily manipulate SCADA systems by falsifying sensor measurements, exploiting tolerance for minor discrepancies to disguise false readings as normal noise. This manipulation can bias operational decisions, such as regulating pond outflows, resulting in flooding, equipment inefficiencies, or physical damage. By targeting critical infrastructure and exploiting uncertainties in water demand, attackers can bypass anomaly detection, disrupt water distribution, increase energy consumption, trigger pressure surges, or compromise hydraulic integrity. Real-world incidents include falsifying water-quality readings to conceal contaminants, misrepresenting flow measurements, or altering pump sensors to reduce efficiency, demonstrating the significant operational, economic, and public-safety risks posed by FDIAs [27][71].

3.5.10. Privilege escalation

Privilege escalation in SWMS represents a critical cybersecurity risk, as attackers exploit system vulnerabilities to gain higher-level access from low-level entry points. SWMS rely on SCADA, IoT sensors, and cloud computing to optimize water distribution, treatment, and monitoring, but these technologies increase the attack surface. Attackers can escalate vertically, moving from standard users to administrators, or horizontally, accessing data from other users at the same privilege level. Legacy SCADA systems, weak authentication, unpatched software, and misconfigured access controls often exacerbate these vulnerabilities. With elevated privileges, attackers can manipulate treatment processes, disrupt distribution, compromise data confidentiality, or install malware, threatening operational safety and integrity. Incidents such as the 2021 attempted chemical manipulation at a Florida water treatment facility and the 2024 breach of Tipton Municipal Utilities' wastewater plant demonstrate how exploiting weak security or trusted software can produce dangerous operational disruptions [74][112].

3.5.11. 51% attack

In a decentralized Blockchain, a single entity controlling over 50% of the network's computing power—a 51% attack—can manipulate transaction records, block new transactions, or execute double-spending, directly threatening decentralization. In SWMS that combine Blockchain and IoT for automated decision-making and decentralized data handling, such attacks can alter water-use records, disrupt processes such as distribution and quality monitoring, and create financial vulnerabilities. These risks compromise operational integrity, regulatory compliance, and stakeholder trust. Although 51% attacks in SWMS are rare, past incidents, such as the 2011 Springfield, Illinois case, in which hackers remotely accessed and damaged the city's water utility, highlight the critical need for robust cybersecurity in Blockchain-enabled water infrastructure [118].

3.5.12. Eclipse attack

Eclipse attacks, a network-layer DoS threat, isolate Blockchain or peer-to-peer nodes by monopolizing their connections and feeding false or delayed information [119]. In SWMS that integrate IoT devices, SCADA systems, and real-time analytics, such attacks can compromise data integrity, disrupt operations, and cause nodes to act on outdated or falsified information. As SWMS increasingly adopt Blockchain for secure data management, their susceptibility to Eclipse attacks grows, highlighting the need for robust network security and anomaly detection [119]. While documented cases specifically targeting SWMS are limited, incidents against water infrastructure illustrate the threat: in 2020, hackers allegedly attempted to alter chlorine levels in Israel's water supply, and in 2024, cyber intrusions disrupted SCADA operations at several Texas water plants, emphasizing the urgency of developing mitigation strategies for Blockchain-enabled water systems.

3.5.13. Watering hole attacks

Attackers execute watering hole attacks by compromising websites frequently visited by targeted groups, such as utility company employees or regulators, to deliver malware and infiltrate systems. In SWMS, which integrate IoT devices, SCADA systems, and advanced analytics to monitor water distribution and quality, such attacks pose severe risks due to the interconnectivity of these networks. By infecting sites commonly accessed by SWMS engineers or administrators, such as vendor portals, regulatory platforms, or industry forums, attackers gain access to internal networks, IoT devices, and SCADA environments. They then escalate privileges, move laterally, and disrupt operations or manipulate data. Real-world incidents illustrate these threats: in 2011, hackers exploited vendor credentials at a Springfield, Illinois, water utility, destroying a pump, and in 2025, Russian-backed actors reportedly manipulated floodgates at a dam in Bremanger, Norway, demonstrating how watering hole attacks can exploit supply chain vulnerabilities and compromise smart water infrastructure [120][121].

3.5.14. Network eavesdropping

Network eavesdropping, or packet sniffing, poses a severe cybersecurity threat to SWMS, which rely on IoT devices, SCADA systems, and digital communication networks to manage water treatment and distribution. Attackers can intercept unencrypted data transmitted over Wi-Fi, cellular, or satellite networks to access operational information, control commands, and user credentials. By analyzing communication protocols such as Modbus, DNP3, or OPC, they can identify vulnerabilities and map network topologies for further exploitation, compromising system confidentiality and disrupting real-time monitoring. Real-world incidents illustrate these risks: in 2021, an attacker remotely accessed a water treatment facility in Oldsmar, Florida, via TeamViewer to attempt chemical manipulation; in 2011, hackers used compromised vendor credentials to sabotage a SCADA-controlled pump in Springfield, Illinois; and the 2018 Piping Botnet research demonstrated how smart irrigation systems could disrupt urban water services. These examples highlight that unsecured communication channels leave critical water infrastructure vulnerable to data interception and operational manipulation [28].

3.5.15. Jamming and interference

Deliberate jamming floods a wireless communication channel with noise or false signals, preventing sensors and control systems in SWMS from exchanging critical data and leading to inaccurate readings or failures in water-quality, flow-rate, and pressure monitoring. It can also disrupt ICS by delaying or blocking commands to pumps and valves while concealing concurrent cyber threats. In contrast, interference arises unintentionally from environmental factors, equipment faults, or electromagnetic noise, degrading communication, reducing packet delivery rates, increasing latency, and raising sensor energy consumption. Both jamming and interference undermine wireless protocols like IEEE 802.15.4, compromise operational efficiency, and threaten public safety and the integrity of water infrastructure, as demonstrated by experiments such as WaterJam and GPS disruption incidents [122].

3.5.16. Wormhole attack

A wormhole attack is a sophisticated network-layer threat in which an attacker creates a low-latency link between two distant malicious nodes, capturing packets at one end and relaying them to the other, leading the network to believe a shorter route exists. This attack distorts routing protocols, allowing attackers to intercept, alter, or block critical data, enabling traffic manipulation, data injection, and DoS activities that compromise network integrity. In SWMS that depend on WSNs and IoT devices for real-time monitoring and control, wormhole attacks can cause false data reporting, resource misallocation, system downtime, and security breaches. Although documented cases in SWMS are limited, similar vulnerabilities in environmental and IoT monitoring networks show that such attacks can severely disrupt communication, compromise data integrity, and threaten operational efficiency and public safety [123].

3.5.17. Sybil attack

A Sybil attack occurs when a single adversary creates multiple fake identities, or Sybil nodes, to gain undue influence over a network. In SWMS, which rely on interconnected IoT devices for real-time monitoring and control, such attacks threaten security by exploiting weak authentication or spoofed device identifiers. Attackers can inject false data, distort routing paths, and overwhelm system resources, resulting in inaccurate water quality readings, delayed transmissions, and DoS conditions. The distributed, resource-constrained nature of WSNs in SWMS makes conventional security measures too computationally intensive to implement effectively, thereby increasing vulnerability [124]. Sybil attacks also undermine data integrity, network communication, and energy efficiency, while enabling adversaries to bypass authentication and launch further intrusions, ultimately compromising the reliability and safety of water infrastructure [124]. Similar threats occur in IoT-based patient monitoring systems, where falsified data can lead to incorrect diagnoses, and in Vehicular Ad Hoc Networks (VANETs), where fake nodes disrupt routing, underscoring the potential for analogous disruptions in SWMS.

3.5.18. Packet sniffing

Malicious actors intercept and analyze network traffic to capture sensitive information such as control commands, sensor data, credentials, and encryption keys. While tools like Wireshark and tcpdump serve legitimate diagnostic purposes, attackers exploit them to eavesdrop on communications, identify vulnerabilities, and execute spoofing, replay, or MitM attacks. Breaches can compromise the confidentiality, integrity, and availability of water operations, enabling unauthorized access, data manipulation, or service disruption [125]. Real-world incidents illustrate these dangers: in 2011, hackers infiltrated Springfield, Illinois's SCADA system by stealing vendor credentials, destroying a water pump, and the "Piping Botnet" attack showed how compromised smart irrigation devices could disrupt urban water services. These examples highlight the urgent need for robust encryption, network segmentation, and intrusion detection to protect SWMS from packet sniffing and related threats.

3.5.19. Routing attacks

Attackers exploit vulnerabilities in network-layer routing protocols to disrupt data flow, manipulate or misroute information, and inject malicious packets, compromising both operational efficiency and data integrity. Common attacks include DoS, MitM, routing table poisoning, replay attacks, and variants such as blackhole, sinkhole, wormhole, Sybil, selective forwarding, spoofing, and hello flood attacks, all of which can degrade network performance and mislead traffic. These attacks can distort critical sensor data, undermine water quality monitoring and automated controls, trigger service outages, delay responses to leaks or contamination, and even enable physical sabotage. Real-world incidents illustrate these risks: in 2011, hackers in Springfield, Illinois, used stolen credentials to damage a water pump through the city's SCADA system, and in 2024, cyberattacks on rural Texas water systems, including Muleshoe, caused overflows, underscoring the growing geopolitical dimension of threats to critical water infrastructure [126].

3.5.20. Weak authentication mechanisms

Weak authentication mechanisms pose a significant threat to SWMS by exposing IoT devices, SCADA systems, and PLCs to cyberattacks that can manipulate water distribution and treatment systems. Using default passwords, lacking multi-factor authentication, or implementing poor access controls allows attackers to gain unauthorized access, escalate privileges, and execute malicious commands, such as altering chemical dosing, disabling alarms, or locking out operators, thereby compromising system integrity and water safety. IoT components, including smart meters, pumps, and sensors, are particularly vulnerable when deployed with weak authentication or outdated firmware, which enables remote exploitation, data manipulation, or service disruption. Additionally, insecure authentication increases the risk of insider misuse. It allows attackers to impersonate legitimate users or devices, creating entry points for advanced attacks such as replay, masquerade, and MitM exploits, while also risking privacy breaches and regulatory non-compliance [74].

3.5.21. SCADA Manipulation

Attackers who gain unauthorized access to SCADA systems pose a significant cyber threat to SWMS by manipulating operations that ensure water safety and quality. They can alter chemical dosages, adjust flow and pressure settings, inject false data, or exploit remote access vulnerabilities [29][127][128]. Notable incidents include the 2021 breach of a U.S. water treatment facility in Oldsmar, Florida, where a hacker attempted to raise sodium hydroxide levels from 100 to 11,100 parts per million, the 2024 cyberattack on Texas water utilities that caused a tank overflow by targeting SCADA-controlled valves, and the 2016 Kemuri Water Company attack, which exploited compromised remote access protocols to manipulate chemical dosing. These attacks demonstrate SCADA systems’ vulnerability to data tampering, command manipulation, and operator deception, threatening public health, utility reputations, and economic stability. By exploiting weaknesses in communication protocols, authentication mechanisms, or network architectures, attackers can induce unsafe water conditions and prolong recovery, underscoring the urgent need for robust cybersecurity in modern water management systems.

3.5.22. Programmable logic controller (PLC) hijacking

Malicious actors can compromise PLCs the core control units of SWMS to manipulate physical processes and disrupt essential services. They exploit network vulnerabilities, weak authentication, default credentials, or unpatched firmware to modify control logic, falsify sensor data, or send malicious commands that open or close valves, alter pressure settings, deactivate pumps, and ultimately cause water shortages, tank overflows, pipe bursts, flooding, or equipment damage. Attackers also deploy Ladder Logic Bombs (LLBs), execute pin control attacks, or exploit firmware vulnerabilities, as demonstrated by the Stuxnet worm. At the same time, advanced threats may involve malware injections, memory manipulation, time-delayed payloads, or rootkits to evade detection. These intrusions jeopardize critical infrastructure components, compromise water quality, generate financial losses, and undermine public trust. Real-world incidents, including the 2023 Unitronics PLC breach at a U.S. water facility, the Aliquippa water pressure attack in Pennsylvania, coordinated attacks on Texas utilities in April 2024, and Iranian state-backed intrusions into a U.S. water authority, highlight the escalating operational and geopolitical risks of PLC-targeted cyberattacks [129].

3.5.23. Firmware tampering

Attackers tamper with firmware by modifying or replacing the low-level software that governs hardware functions, enabling them to inject malicious code into PLCs, sensors, and actuators to gain persistent control and evade traditional defenses. They exploit weak update mechanisms, absent integrity checks, physical access, vulnerabilities in PLC firmware, or supply chain compromises that introduce backdoors during manufacturing or distribution. This manipulation allows adversaries to alter device behavior, disable alarms, manipulate sensor data, or exfiltrate sensitive information often without immediate detection leading to unauthorized access, operational disruption, physical damage, water quality issues, financial losses, and reputational harm to utilities. Real-world incidents, including the 2011 Springfield, Illinois case, the 2021 Oldsmar, Florida breach, and the 2024 Muleshoe, Texas attack attributed to Russian actors, underscore the critical need to ensure firmware integrity throughout the SWMS lifecycle [130].

3.5.24. Advanced persistent threats

APTs pose a growing cybersecurity risk to SWMS that rely on interconnected technologies such as IoT, AI, and digital twins to manage water distribution and quality. Well-resourced adversaries, including nation-states, hacktivists, and cybercriminals, exploit vulnerabilities in networks, operational technologies, and industrial control systems (ICS), such as PLCs and HMIs, using methods such as spear-phishing, weak authentication, and unpatched IoT devices [74]. Once inside, they escalate privileges and maintain persistent access to manipulate data, disrupt services, or compromise system integrity, often pursuing espionage, sabotage, or operational disruption. The proliferation of IoT devices complicates detection and mitigation, increasing the risk of service outages, data breaches, financial losses, and reputational damage [74]. Real-world incidents illustrate these threats, including the 2021 Oldsmar, Florida, attack on a SCADA system, ransomware-induced manual operations in Maine and California, intrusions exploiting unpatched systems in Texas and Pennsylvania, the 2025

Russian-led breach of a Norwegian dam, and the 2013 Iranian attempt on a New York dam, thwarted only by manual intervention. These events underscore the sophistication and persistence of APTs and highlight the urgent need for adaptive, resilient cybersecurity strategies in SWMS.

3.5.25. Denial-of-service (DoS) and Distributed DoS (DDoS) attacks

DoS and DDoS attacks threaten water management systems by overwhelming them with traffic or exploiting vulnerabilities, disrupting access, control, and communication, and causing operational delays and costly recovery. Interconnected infrastructures, such as power and internet networks, can amplify these disruptions by disabling pumps or severing communication links. Modern ICS in water networks, particularly those relying on SCADA and IoT-based sensors, have become prime targets for sophisticated cyber operations and APTs [74]. In SWMS, DDoS attacks can halt or delay treatment and distribution, compromise data integrity, produce false readings, and obscure attempts to inject misleading data, endangering water quality and resource management. Mitigating these attacks requires additional computing and network resources, increasing operational costs. Real-world incidents, such as the 2023 cyberattacks on water systems in Muleshoe, Hale Center, and Lockney, Texas, where a Russian hacktivist group caused service disruptions and physical overflows, highlight the growing geopolitical stakes of these threats.

3.5.26. Man-in-the-Middle (MitM) attacks

Adversaries execute MitM attacks by intercepting and manipulating communications between SWMS components, such as sensors, controllers, and supervisory units, exploiting vulnerabilities such as unencrypted transmissions, weak authentication, or insecure network configurations. These attacks enable eavesdropping, data falsification, and manipulation of control commands, compromising data integrity, disrupting operations, and threatening public health by altering water quality or treatment processes [131]. MitM attacks often employ advanced tactics such as false data injection, replay, or session hijacking, making them difficult to detect in real-time automated systems [132]. Real-world incidents, including the 2021 Oldsmar, Florida, attack, where an intruder attempted to modify chemical levels in the water supply, and the remote manipulation of an Israeli irrigation system, along with simulations on LoRaWAN-connected IoT devices, illustrate the severe operational, financial, and safety risks posed by communication vulnerabilities in SWMS [131][132].

3.5.27. Insecure IoT devices

Insecure IoT devices within SWMS provide entry points for cyberattacks due to weak security controls. Resource-constrained and heterogeneous components, such as sensors, actuators, and controllers, often lack strong encryption, authentication, and intrusion detection mechanisms. Vulnerabilities like default or weak credentials, outdated firmware, and unencrypted communications expose SWMS to unauthorized access, data manipulation, malware infections, and botnet recruitment [30][133]. Cloud-based architectures further expand the attack surface, increasing privacy and security risks. Real-world incidents, including the 2016 Mirai Botnet Attack and the Devil's Ivy vulnerability in the gSOAP library, illustrate how attackers can exploit insecure IoT devices to disrupt water system operations, compromise water quality monitoring, and undermine treatment and distribution processes [30][133].

3.5.28. DNS cache poisoning

Attackers carry out DNS cache poisoning, or DNS spoofing, by injecting forged DNS records into a resolver's cache or by intercepting DNS queries and redirecting users and devices to malicious IP addresses. By exploiting weaknesses in DNS protocols, randomization, or network configurations, they manipulate responses that DNS resolvers subsequently cache. In SWMS that rely on cloud platforms, IoT devices, SCADA systems, and real-time dashboards, such attacks can disrupt operations by tricking operators into interacting with attacker-controlled interfaces that display falsified data, potentially leading to improper valve control or water misallocation [134]. Intercepting communication between IoT sensors, control units, and cloud servers also enables attackers to steal or manipulate data, facilitating malware distribution, phishing, or DoS attacks. Real-world incidents, such as DNS poisoning targeting the Aliquippa municipal water authority, demonstrate the vulnerability of water utilities. At the same time, research highlights that IoT-based water sensors using LoRaWAN and NB-IoT remain susceptible to spoofing, threatening service reliability, data integrity, and privacy, and creating entry points for advanced cyberattacks [31][134][135].

3.5.29. Credential stuffing

Credential stuffing is a sophisticated cyberattack in which attackers use stolen username–password pairs to gain unauthorized access to systems, posing a critical threat to SWMS that integrate IoT devices, cloud platforms, and data analytics. Attackers deploy automated tools to test large volumes of compromised credentials on SWMS dashboards and cloud interfaces, exploiting users' password reuse across services. Successful breaches can allow attackers to manipulate control panels, disrupt water supply, alter quality parameters, and expose sensitive operational and customer data, violating privacy regulations [32][136]. Compromised accounts can also serve as gateways for ransomware or system sabotage. Real-world incidents highlight this risk: Norton LifeLock's 2023 breach affected 6,500 password vaults, PayPal's 2022 attack exposed approximately 35,000 accounts, and General Motors experienced unauthorized redemptions of rewards, demonstrating that credential stuffing threatens not only financial services but also critical infrastructure.

3.5.30. Drone-based attacks

Unmanned aerial vehicles (UAVs), or drones, increasingly threaten SWMS by enabling cyber and physical attacks on critical water infrastructure. Agencies such as the EPA and WaterISAC have warned that drones pose significant risks to water utilities. Equipped with high-resolution sensors, drones can conduct unauthorized surveillance to identify vulnerabilities, interfere with SCADA networks to disrupt pumps and valves, deliver hazardous payloads to chemical storage and treatment facilities, or deploy malware through insecure wireless channels. The growing integration of IoT devices, wireless networks, and industrial control systems has expanded attack surfaces. At the same time, many utilities remain vulnerable due to outdated systems, open portals, and limited detection capabilities. Exploiting weaknesses in authentication, communication protocols, or the broader smart city ecosystem, drones can enable wireless intrusions, data manipulation, physical tampering, and reconnaissance, potentially halting water distribution, compromising data integrity, and amplifying cyber threats such as DoS attacks and false data injection [137]. Real-world incidents highlight this danger: Russian drone strikes in Ukraine disrupted water supplies by targeting power infrastructure, the U.S. group "CyberAv3ngers" deployed malware against ICS, and Russian-affiliated actors in Poland and France manipulated water utilities, underscoring the global operational impact of drone-enabled attacks on water infrastructure.

3.5.31. Cloud service vulnerabilities

Relying on cloud services without robust security exposes SWMS to severe cyber risks, including data breaches, operational disruptions, and compromised system integrity. Cloud-based SWMS that use cloud computing for data analytics, remote monitoring, and control are vulnerable to attacks such as DoS and DDoS, insecure communication channels, weak or misconfigured authentication, and cross-tenant threats in multi-tenant environments [30]. Legacy systems incompatible with modern cloud security exacerbate these risks, as seen in the 2024 botnet attack on smart irrigation systems, the 2025 cyberattack on a Norwegian dam, and the 2024 American Water incident. These vulnerabilities can disrupt operations, compromise data integrity and privacy, affect water supply and quality, and erode regulatory compliance and public trust, underscoring the need for consistent security standards and proactive risk mitigation in cloud-integrated SWMS [30].

3.5.32. Zero-day vulnerabilities

Zero-day vulnerabilities previously unknown flaws in software or hardware allow attackers to exploit systems before patches are available. SWMS that integrate IoT devices, SCADA systems, and ICS to manage water distribution, treatment, and quality are particularly at risk due to their complexity and heterogeneity. These vulnerabilities can enable unauthorized access, manipulation of treatment processes, disruption of distribution, alteration of sensor data, or physical damage. At the same time, traditional signature-based security measures often fail to detect them [71][74]. Real-world incidents illustrate these dangers: in Oldsmar, Florida (2021), attackers attempted to raise sodium hydroxide levels via remote SCADA access; in Arkansas City, Kansas (2022), weaknesses in remote access protocols triggered a federal investigation; and in Muleshoe, Texas (2023), a cyberattack caused temporary overflow and service disruption linked to a Russian hacktivist group. These events highlight the urgent need for proactive strategies to detect and mitigate zero-day threats in SWMS, preventing operational disruptions and broader safety risks such as flooding, ransomware attacks, or data breaches.

3.5.33. Remote access exploits

Remote access protocols, including VPNs and remote desktop services, significantly increase cybersecurity risks to SWMS as remote work, IT–ICS integration, and IoT deployments expand. Attackers exploit weak authentication, outdated software, misconfigured access controls, and insecure communication protocols to gain unauthorized access [112][33]. High-profile incidents highlight these vulnerabilities: in 2021, hackers accessed the Oldsmar, Florida water treatment plant's SCADA system via TeamViewer; a U.S. drinking water facility suffered a breach due to weak passwords and obsolete systems; Limestone, Maine, experienced a ransomware attack that disrupted wastewater operations; and in 2011, attackers manipulated a water utility's SCADA system through a compromised software vendor. Such breaches can disrupt operations, compromise data integrity and confidentiality, damage critical infrastructure, and endanger public health, while also providing a foothold for advanced cyber-physical attacks [112]. Although remote connectivity is essential for managing distributed assets and enabling real-time monitoring, poorly secured access dramatically enlarges the attack surface, threatening service continuity, operational integrity, and sensitive data security.

3.5.34. Botnet attacks

Botnet attacks pose a critical cybersecurity threat to SWMS, which rely on interconnected IoT devices, Advanced Metering Infrastructure (AMI), and SCADA systems for water distribution and treatment. By compromising sensors, routers, or smart irrigation controllers, attackers can launch large-scale DDoS attacks, manipulate operational parameters, or steal sensitive data, potentially disrupting service, depleting water resources, and endangering public health [138]. Even a botnet of approximately 1,300 IoT devices can drain reservoirs or water towers within hours. Real-world incidents illustrate these risks: in 2021, hackers attempted to raise sodium hydroxide levels in Oldsmar, Florida, exploiting weak remote access controls; researchers have shown that vulnerabilities in smart irrigation systems could enable "piping botnets" to drain urban water infrastructure; and in January 2024, coordinated attacks on rural Texas water systems, attributed to the hacktivist group CyberArmyofRussia_Reborn, caused overflows and operational disruptions. These events underscore the urgent need for robust cybersecurity measures to protect SWMS from botnet-driven threats.

3.5.35. Brute force attacks

Brute force attacks pose a significant cybersecurity threat to SWMS by targeting weak authentication, default credentials, and unsecured interfaces in IoT-enabled sensors, PLCs, and SCADA systems. Attackers automate login attempts via SSH, Telnet, FTP, or web portals to compromise devices such as smart meters, pressure sensors, and valve controllers, enabling them to manipulate operational data, disrupt distribution schedules, or disable leak detection. The growing interconnectivity and reliance on remote monitoring exacerbate these vulnerabilities, especially when strong password policies and multi-factor authentication are absent. Analyses of ICS incidents in Europe and the United States show that attackers exploit weak VPN and remote access configurations to gain administrative control over critical operations, including pumps and dosing systems, risking unsafe water quality, service disruptions, data breaches, and ransomware deployment [34].

3.5.36. Malicious code injection

Malicious code injection attacks, such as SQL Injection (SQLi), Cross-Site Scripting (XSS), Command Injection, Buffer Overflow, and Cross-Site Request Forgery (CSRF), exploit weak input validation, insecure coding, or misplaced trust between web applications and authenticated users, enabling attackers to manipulate operations, exfiltrate data, or disrupt services. SQLi can compromise operational and customer data, misleading water distribution or contamination detection systems, while XSS can hijack operator sessions, steal credentials, or alter dashboards [139]. CSRF attacks in remote-access environments can trigger unauthorized pump activations, valve operations, or chemical dosing changes [140]. The integration of legacy systems, IoT, and 5G devices amplifies these risks in SWMS, potentially causing service disruptions, infrastructure damage, public health hazards, financial losses, and erosion of public trust.

3.5.37. Buffer overflow attacks

A buffer overflow attack occurs when an adversary exploits a software vulnerability by supplying data that exceeds the allocated memory buffer, overwriting adjacent memory, and potentially causing system crashes, DoS attacks, or remote code execution. In SWMS, such attacks threaten operational reliability and public safety, particularly on IoT devices and controllers such as smart meters, flow sensors, and PLCs, which often lack robust memory protection. Attackers can compromise device functionality, gain unauthorized access to SCADA or HMI applications, and manipulate pumps, valves, or chemical dosing mechanisms by sending oversized or malformed data. Exploitation may enable persistent access, privilege escalation, or disabling of alarm systems, resulting in operational disruptions, degraded water quality, or compromised data integrity [46]. Real-world incidents demonstrate this threat: legacy SCADA systems remain vulnerable due to outdated libraries and weak input validation, and a U.S. water facility experienced a breach caused by memory corruption, similar to a buffer overflow [141]. These examples underscore the urgent need for rigorous input validation, secure coding practices, and system hardening across SWMS infrastructures.

3.5.38. Geopolitical cyber warfare

SWMS have become prime targets in geopolitical cyber warfare as water infrastructure shifts from isolated, manually operated systems to IoT-enabled, networked systems, expanding the attack surface and exposing vulnerabilities such as insecure SCADA systems, weak authentication, outdated software, and poor network segmentation [120]. State and state-sponsored actors exploit these weaknesses to disrupt water supply, manipulate water quality, conduct espionage, or gain strategic leverage, seeking to destabilize societies, erode public trust, and achieve political or military objectives rather than financial gain [74][120]. Documented incidents, including the Iranian attack on the Bowman Avenue Dam in the U.S., Kremlin-linked malware targeting Ukrainian water utilities, attempts to manipulate Israel's water supply, the 2021 Oldsmar, Florida incident, and the alleged temporary takeover of a Norwegian dam by Russian hackers in 2025, highlight the high stakes of these attacks, which can provoke humanitarian crises, economic disruption, public panic, and potentially escalate broader conflicts.

3.5.39. Legacy operational technology (OT) systems

Many SWMS still operate on legacy OT, including outdated SCADA systems, PLCs, and sensors, which were designed for reliability rather than cybersecurity and often lack essential protections such as encryption, authentication, intrusion detection, and secure remote access. As SWMS adopt IoT devices, cloud-based analytics, and real-time monitoring, the integration of insecure legacy OT with modern digital technologies expands the attack surface [142]. Mission-critical systems cannot always be patched or upgraded without service disruptions, leaving them vulnerable to exploitation via unsecured remote access, privilege escalation, and control-command manipulation, as demonstrated by the 2021 Oldsmar, Florida water treatment plant attack and reports of compromised PLCs across Europe and North America [142]. Cybercriminal groups, including CyberAv3ngers, have exploited these weaknesses in ransomware campaigns and targeted attacks, threatening operational continuity, data integrity, and physical infrastructure. Ensuring secure integration of legacy systems with modern IoT and cloud environments remains a critical challenge, thereby increasing the risk of cyber-physical incidents in smart water infrastructure.

3.5.40. Privilege escalation

Privilege escalation poses a critical cybersecurity threat to SWMS, as attackers exploit software vulnerabilities, misconfigured permissions, or weak access controls to gain unauthorized high-level privileges. In systems integrating IoT devices, SCADA systems, cloud infrastructure, and Blockchain-based management layers, such attacks can bypass security controls, manipulate critical processes, and disrupt water distribution and treatment. Attackers can escalate vertically from standard users to administrators or root accounts, or move horizontally across accounts with equivalent privileges, compromising data confidentiality, altering valve operations, disabling alarms, or falsifying sensor readings. The combination of legacy components and modern IoT networks amplifies these risks [143]. Incidents like the 2021 Oldsmar, Florida water utility attack, in which adversaries attempted to modify chemical treatment levels, highlight the potential consequences. Recent vulnerabilities in IoT gateways (e.g., CVE-2023-46604 in Apache ActiveMQ and CVE-2023-23397 in Microsoft Outlook) and misconfigured cloud platforms demonstrate how privilege escalation allows attackers to modify commands, delete critical logs, and trigger service disruptions, financial losses, or environmental and public health hazards.

3.5.41. Cyber-physical attacks

Cyber-physical attacks pose severe threats to SWMS by targeting both digital infrastructure and the physical processes that manage water distribution, treatment, and monitoring. In these systems, IoT sensors, SCADA systems, PLCs, and cloud platforms directly control pumps, valves, and treatment units, creating vulnerabilities in communication protocols, device firmware, and control logic [74]. Attackers can exploit these weaknesses to falsify sensor data, manipulate control commands, or launch DDoS attacks, disrupting water flow, altering chemical dosing, causing mechanical failures, or halting critical operations, thereby compromising water quality, service continuity, and environmental safety. Weak authentication, insecure communication links, and inadequate separation between OT and IT networks often enable such intrusions, as demonstrated by the 2021 Oldsmar, Florida incident.

3.5.42. Physical security breaches

Physical security breaches in SWMS occur when unauthorized individuals access or tamper with components such as sensors, actuators, pumps, valves, or control rooms, enabling sabotage, theft, or operational manipulation. Breaches of water and wastewater management systems can endanger infrastructure and water quality. At the same time, opening avenues for cyber-physical attacks that enable attackers to install malware, disrupt communications, or disable safety mechanisms [120]. Real incidents demonstrate these threats: an ex-contractor in Maroochy Shire, Australia, released sewage by exploiting pumping station access; a remote attacker in Oldsmar, Florida (2021) altered sodium hydroxide levels at a treatment facility; hackers at Bremanger Dam, Norway (2025) manipulated dam valves; and intruders in Springfield, Illinois (2011) destroyed a pump via SCADA access. These cases reveal how physical and cyber vulnerabilities converge, creating public health risks, environmental harm, operational disruptions, and economic and reputational losses, challenges that are amplified by the distributed and often remote nature of SWMS infrastructure.

4. CYBER SECURITY IN SWMS

Conventional approaches to securing SWMS focus on protecting infrastructure, data, and communication channels from cyber threats. They employ network segmentation and isolation to limit exposure, firewalls and intrusion detection systems to monitor traffic and detect anomalies, and encryption to maintain data confidentiality and integrity. Strong authentication mechanisms, including digital certificates and multi-factor authentication, verify user and device identities, while access controls and physical safeguards protect critical components from tampering or theft. Routine monitoring, logging, security audits, and timely software updates help identify vulnerabilities and reduce risks [74][121].

Despite these measures, traditional cybersecurity techniques struggle to keep pace with the growing complexity, interconnectivity, and heterogeneity of SWMS. The widespread adoption of IoT sensors, edge computing, and automated control systems significantly expands the attack surface. Legacy components often lack built-in security or timely updates, leaving them vulnerable. Standard defenses, such as firewalls, password-based authentication, and signature-based intrusion detection, cannot reliably detect advanced threats, including APTs, zero-day exploits, data injection, ransomware, and DoS attacks. High volumes of diverse sensor data, combined with human error, limited security awareness, and the challenge of managing heterogeneous devices and protocols, further weaken system resilience. Conventional approaches also fail to enforce uniform security policies across distributed networks and struggle to protect sensitive operational and consumer data, particularly on resource-constrained IoT devices. Moreover, the interdependence of water systems with other urban infrastructures introduces cascading vulnerabilities that traditional frameworks cannot effectively manage [74][120][121].

Integrating Blockchain technology into SWMS offers a secure, decentralized framework that preserves data integrity, ensures traceability, and enhances transparency among stakeholders. Smart contracts can automate authentication, access control, and anomaly detection, reducing reliance on centralized authorities and minimizing single points of failure. When combined with QML, which analyzes large volumes of sensor and network data in real time, this integration enables proactive threat detection, optimized responses, and predictive maintenance. Together, Blockchain and QML strengthen operational resilience, safeguard continuity, and enhance the security and reliability of water supply networks in increasingly interconnected environments.

5. BLOCKCHAIN TECHNOLOGY IN SWMS

Blockchain technology, first introduced by Satoshi Nakamoto in 2008, is a decentralized, chronological chain of data blocks that functions as a distributed ledger and database [144]. Each block, as seen in systems like Bitcoin, contains a header with the current and previous block hashes, a timestamp, and Merkle tree information, along with a body that records transaction details and includes digital signatures [144][145]. Blockchain ensures security and transparency through its distributed network architecture, in which consensus algorithms validate new blocks and digital signatures authenticate transactions [145]. Bitcoin implements a proof-of-work (PoW) algorithm, requiring miners to solve computational puzzles to create blocks, while alternative approaches, such as proof-of-stake (PoS), delegated proof-of-stake (DPoS), and DPoS with node behavior and Bordacount (DPoSB), reduce energy consumption by avoiding intensive computations [145][146]. Byzantine fault-tolerant algorithms further allow networks to achieve consensus even in the presence of malicious nodes, enabling Blockchain applications beyond cryptocurrencies, including water management [147][148].

By combining a tamper-evident ledger with programmable automation via smart contracts, Blockchain addresses persistent challenges in water systems, such as unreliable sensor data, opaque billing, water rights trading, and vulnerabilities in centralized governance. Decentralization transfers control from a central authority to a distributed network, increasing transparency and reducing the need for trust among participants [149]. Immutability prevents alterations to recorded data; any corrections are made by adding new transactions that preserve both the original and corrective entries. Consensus mechanisms ensure that transactions are approved only with majority agreement before they are recorded [150][151].

Blockchain networks vary in structure depending on their access and governance. Public Blockchains, such as Bitcoin and Ethereum, are permissionless, allowing anyone to read, verify, or modify the ledger. Private Blockchains restrict access under a single authority, offering limited decentralization. Hybrid Blockchains combine public and private features, enabling sensitive data to be controlled while maintaining transparency. Consortium Blockchains are managed by pre-selected organizations that jointly support the network, making them suitable for sectors with shared responsibilities [37–39][144]. Although these features enhance security and transparency, public Blockchains may process transactions more slowly, and immutability can limit the ability to modify historical data.

In SWMS, Blockchain provides a reliable infrastructure for immutable sensor-data logging, auditable billing, automated enforcement of allocation rules, and incentive mechanisms that encourage conservation and accurate quality reporting [39]. By transparently and securely recording water usage, transactions, and quality data, and automating processes such as billing, allocation, and incident management, Blockchain reduces reliance on intermediaries and improves operational efficiency [152]. When integrated with IoT devices, it enables real-time monitoring for accurate reporting, leakage detection, and flow control [37][152]. Figure 4 illustrates how Blockchain technology is used in SWMS.

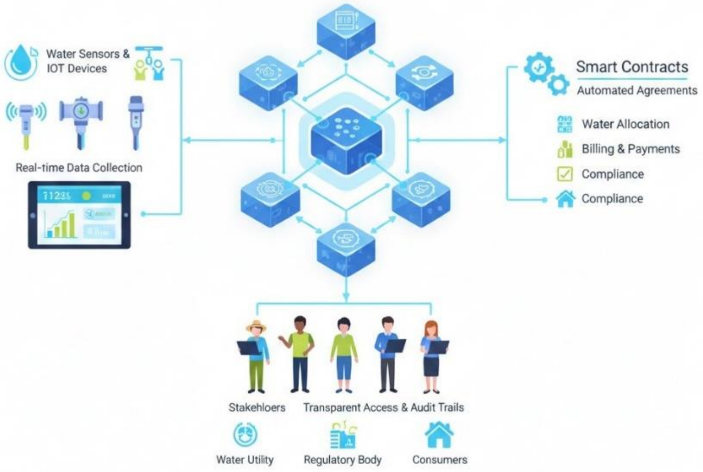

Fig. 4. An illustration of the application of Blockchain technology in SWMS.

Architectural patterns in SWMS commonly include permissioned ledgers, hybrid on-chain/off-chain deployments, and smart-contracted market and governance layers. Permissioned Blockchains, such as Hyperledger Fabric and Quorum, place validators under the control of utilities, regulators, and trusted partners. This arrangement enables efficient governance, fine-grained access control, and high throughput. At the same time, Byzantine- or crash-fault-tolerant consensus mechanisms reduce latency and energy consumption and maintain an immutable audit trail [39][153]. Hybrid deployments store high-volume sensor data, such as flow, pressure, and quality measurements, off-chain for efficiency, anchoring only cryptographic hashes and key metadata on-chain. Smart contracts link these on-chain records to the raw data, ensuring integrity and traceability [38][154]. Additionally, smart contracts facilitate water trading, dynamic pricing, and penalty/reward mechanisms, while tokenization, including semi-fungible tokens representing volumetric water rights, supports market-based resource allocation [154].

Blockchain technology enhances SWMS security by leveraging its decentralized architecture, in which each participant maintains a synchronized ledger, making attacks computationally and economically unfeasible. It enforces access control, ensuring only authorized users interact with the system, while validation mechanisms create transparent, auditable trails [33]. Data immutability and integrity are preserved through cryptographic links that secure records of water flow rates, quality parameters, and meter readings, making tampering detectable across all nodes. The technology protects IoT sensors and smart meters via device authentication and encryption, guarding against interception or manipulation [155]. Beyond security, Blockchain enables automation and efficient resource management: smart contracts handle billing, leak detection, and access control, reducing human error and fraud, while real-time sharing of validated water usage data supports demand–supply balancing, early leak detection, and optimized distribution. Integrating Blockchain with decentralized storage solutions like IPFS allows scalable, secure management of large datasets, while smart contracts promote fair billing, water conservation, and compliance with environmental and sustainability standards [37][153].

5.1. Key roles of Blockchain in enhancing the security of SWMS

Some of the key roles of Blockchain in improving the security of SWMS include the following:

5.1.1. Data integrity and tamper resistance

Blockchain enhances the security of SWMS by protecting data integrity and resisting tampering. It records each sensor reading and operational record with cryptographic hashes and timestamps, linking them to previous entries to create an immutable ledger that immediately reveals unauthorized changes. By leveraging consensus mechanisms such as Proof of Authority (PoA) or Byzantine Fault Tolerance (BFT), Blockchain validates data from authenticated devices and authorized personnel, eliminating single points of failure. Digital signatures, encrypted communication, and access control policies ensure confidentiality, authenticity, and accountability. At the same time, a transparent audit trail facilitates regulatory compliance and forensic analysis, ensuring that water-quality measurements, usage data, and maintenance logs are accurate and verifiable [37][39].

5.1.2. Secure data provenance and traceability

Blockchain strengthens SWMS security by ensuring data provenance and traceability for information from distributed sensors, IoT devices, and control systems. As this data moves through multiple intermediaries, it risks tampering, loss, or unauthorized access. By recording sensor readings with timestamps, digital signatures, and device identities, Blockchain preserves data integrity and authenticity while enabling continuous tracking of aggregation, analysis, sharing, and modifications [39][153]. Smart contracts automate validation, allowing only authenticated nodes to contribute data, and the decentralized architecture distributes trust among stakeholders, eliminating single points of failure. This comprehensive visibility enhances accountability, facilitates rapid forensic analysis during incidents such as contamination or leakage, and enables regulators, utilities, and consumers to verify accurate water-quality and operational records independently. Real-world deployments have demonstrated improved efficiency, reduced costs, and enhanced security across applications such as water-quality traceability, permit management, and infrastructure data archiving.

5.1.3. Decentralized trust management

Blockchain enhances the security and reliability of SWMS by replacing centralized trust with a decentralized, tamper-evident ledger maintained collaboratively by utilities, regulators, laboratories, and consumers. Distributed data validation prevents any single party from manipulating records. At the same time, consensus mechanisms like PBFT or PoA ensure collective agreement before new data is added, protecting against fraud, unauthorized access, and sensor tampering. Permissioned Blockchain architectures enable secure, transparent, and privacy-preserving data sharing, reducing information silos and improving coordination among stakeholders. Smart contracts automate compliance checks, resource allocation, and permit issuance, ensuring consistent, auditable, and trustless operations. Together, these features eliminate bottlenecks, enhance accountability through immutable audit trails, and support rapid, coordinated responses to contamination events or system faults [39][156].

5.1.4. Authentication and access control

Blockchain strengthens SWMS security by providing a decentralized, tamper-resistant framework for authentication and access control, replacing vulnerable centralized identity systems. Sensors, utility operators, regulators, and service providers authenticate using Blockchain-anchored cryptographic keys, ensuring that only authorized actors can publish, modify, or access data [33]. Devices digitally sign measurements to prevent spoofing, unauthorized onboarding, and data manipulation. Smart contracts enforce dynamic, fine-grained access policies, allowing regulators to access raw water-quality data, consumers to view aggregated records, and utilities to update permissions transparently in real time. The Blockchain ledger maintains immutable audit trails of authentication attempts and permission changes, supporting accountability and forensic analysis [33][157]. By integrating decentralized identity and verifiable-credential standards, the system preserves privacy, while lightweight consensus mechanisms and edge-compatible designs enable efficient operation in constrained environments. Overall, Blockchain delivers secure cryptographic authentication and decentralized access control through automated Role-Based Access Control (RBAC) and Attribute-Based Access Control (ABAC) policy enforcement, protecting the system against attacks such as MitM and replay attacks [33][157][158].

5.1.5. Secure IoT device communication

Blockchain enhances communication within SWMS by securing continuous data exchanges among IoT devices that monitor flow, pressure, quality, and system control. It applies cryptographic signing and timestamping to create tamper-evident records on a distributed ledger, ensuring data authenticity and integrity. By replacing centralized servers with a permissioned, decentralized trust model, Blockchain eliminates single points of failure and strengthens key management for reliable encryption, mutual authentication, and transparent credential updates [159]. Smart contracts enforce dynamic access control, permitting only authorized devices or users to access data streams or trigger actuators [160]. Additionally, Blockchain preserves an immutable audit trail that supports forensic analysis and regulatory compliance, enabling decentralized, tamper-resistant data exchange and scalable protection for high-volume IoT communications in SWMS [155][159][161].

5.1.6. Confidentiality through encryption and permissioned ledgers

Blockchain strengthens SWMS security by combining encryption with permissioned ledger architectures to protect sensitive data, including consumer usage patterns, billing information, and IoT sensor readings. It employs symmetric and asymmetric cryptography, along with advanced methods such as homomorphic encryption and zero-knowledge proofs, to enable secure computation over encrypted data [162]. Permissioned Blockchains limit access to authenticated participants, enforcing role-based permissions through smart contracts and access control lists, so only authorized stakeholders can view or modify information [163][164]. Platforms such as Hyperledger Fabric support private transactions and channel-based access, while immutable logs maintain auditability without exposing sensitive details. Together, these mechanisms safeguard data privacy, ensure regulatory compliance, and reinforce trust across the water management ecosystem.

5.1.7. Smart contract-based security automation

Smart contracts strengthen SWMS security by automatically enforcing policies, managing access control, and auditing activities. They validate access attempts, implement granular authorization rules, and record security events in immutable, timestamped logs [165]. Integrated with IoT telemetry, decentralized identity, and AI-driven anomaly detection, they autonomously detect unusual activity, isolate compromised nodes, trigger alerts, and initiate mitigation workflows or enforce service-level agreements [34]. By coordinating actions such as device isolation, configuration rollback, and stakeholder notification, smart contracts minimize human error and ensure rapid, consistent, and verifiable execution of security protocols across distributed water infrastructure [39][166].

5.1.8. Auditability and regulatory compliance

Blockchain enhances auditability and regulatory compliance in SWMS by maintaining an immutable, timestamped ledger that securely records sensor readings, meter data, maintenance activities, and water-quality metrics. By storing data or their cryptographic hashes on-chain, it immediately detects tampering and enables accurate reconstruction of incidents such as leaks or contamination events [39]. Permissioned Blockchain networks allow regulators to verify water usage, quality, and environmental metrics in real time while protecting consumer privacy, and smart contracts automate compliance checks, reporting, and enforcement, reducing administrative burdens and human error [167][168]. This integration of tamper-evident records, automated enforcement, and secure transparency strengthens accountability, builds stakeholder trust, and ensures consistent adherence to modern water governance standards [39][167].

5.1.9. Fraud prevention in billing and metering

Blockchain strengthens fraud prevention in SWMS billing and metering by maintaining an immutable, decentralized, and transparent ledger that secures meter readings, consumption data, and financial transactions [152]. It records data on-chain or stores hashed readings to create tamper-evident, verifiable usage records, while smart contracts automatically execute billing based on predefined tariffs, minimizing errors and manipulation. By enabling accurate reconciliation among utilities, regulators, and service providers, Blockchain fosters trust through transparent verification of meter readings, payments, and adjustments. Leveraging consensus algorithms and cryptography, it safeguards data integrity, prevents unauthorized access, meter tampering, and double-spending [169]. Pilot implementations demonstrate that Blockchain reduces billing discrepancies, streamlines auditing, supports flexible payment models, and enhances financial security in SWMS [38][39].

5.1.10. Secure data sharing and interoperability

Blockchain enhances secure data sharing and interoperability in SWMS by addressing weaknesses in traditional centralized systems, including unauthorized access, data tampering, and issues of stakeholder trust. In modern water networks, utilities, regulators, laboratories, service providers, and consumers exchange sensitive operational and environmental data. A permissioned Blockchain enforces role-based access control, ensuring that participants can access only the data relevant to them. It immutably records all transactions for auditing and compliance, while smart contracts automate data-sharing policies, specifying access rights, conditions, and durations to ensure transparency, trust, and privacy [39][155]. By standardizing on-chain data structures, Blockchain enables seamless interoperability among heterogeneous devices and platforms, such as IoT sensors, SCADA systems, edge devices, and analytical tools, supporting real-time monitoring, predictive analytics, and automated control. Combined with encryption, digital signatures, and decentralized consensus, it preserves data confidentiality, authenticity, and consistency across organizations. Integrating Blockchain with digital twins or IPFS further enhances cross-platform exchange, standardized data representation, and scalable storage for high-volume IoT data [155].

5.1.11. Resistance to DoS and data deletion attacks

SWMS face growing risks from DoS attacks and data tampering, given their reliance on IoT sensors, edge devices, and centralized platforms. Deploying Blockchain strengthens resilience by distributing data storage and transaction validation across multiple nodes, eliminating single points of failure and protecting sensor readings, meter logs, and operational records from unauthorized modification. Permissioned Blockchain frameworks further defend against DoS attacks by controlling transaction spikes, prioritizing legitimate operations, and restricting unauthorized access. Incorporating AI and machine learning enables real-time attack detection and automated mitigation, ensuring uninterrupted operation of critical functions such as leak detection, automated alerts, and billing, while maintaining data integrity, auditability, and overall system reliability [170].

5.1.12. Secure event logging and forensic analysis

Blockchain strengthens secure event logging and forensic analysis in SWMS by preserving the integrity, traceability, and non-repudiation of continuously generated data, including sensor readings, meter data, maintenance actions, and access logs. By recording events on a decentralized, append-only ledger, SWMS create immutable, timestamped logs that resist tampering and establish a verifiable chain of provenance for all system activities [39][171][172]. This enhances accountability and trust among utilities, regulators, and customers while enabling accurate incident reconstruction, anomaly detection, and regulatory compliance. Smart contracts can automatically trigger alerts and generate on-chain reports for anomalies, such as sudden drops in water pressure, while cryptographically signed log entries provide indisputable proof of event occurrence. The decentralized structure also removes dependence on trusted third parties and supports automated access control and chain-of-custody management, keeping sensitive forensic data secure and auditable [171][172].

5.1.13. Tokenization and incentive mechanisms for security compliance

Blockchain enhances security, compliance, and resource management in SWMS by leveraging tokenization, smart contracts, and incentive mechanisms. It transforms assets, rights, and actions, such as water usage quotas, access privileges, or compliance certifications, into unique, traceable digital tokens, enabling precise control and transparency for regulators and stakeholders. Smart contracts automatically enforce policies, from access control to water allocation rules, reducing fraud, disputes, and unauthorized activity. Incentive structures reward operators, maintenance teams, and sensors for compliant behaviors, such as timely leak reporting or proper data handling, while penalizing noncompliance. These mechanisms foster accountability, cooperation, and proactive reporting across multi-party water networks, ensuring that all transactions remain immutable, auditable, and trustless. Pilot studies show that token-based systems improve security adherence, optimize resource allocation, and encourage sustainable practices, with gamified and auction-based approaches further enhancing community engagement [39][154].

5.1.14. Privacy-preserving analytics via zero-knowledge proofs

Zero-knowledge proofs (ZKPs) enable privacy-preserving analytics in SWMS by allowing devices, such as water meters or IoT sensors, to generate cryptographic proofs that specific conditions or computations are satisfied without revealing sensitive data, such as consumption, billing, or operational records. Verifiers can validate these proofs on-chain, supporting secure billing, regulatory compliance, anomaly detection, and water trading while maintaining decentralization, tamper-resistant records, and operational transparency. Advances such as zk-SNARKs and optimized set membership proofs have made ZKP generation and verification efficient and scalable, allowing SWMS to ensure both strong privacy and accountability across large IoT networks [173][174].

5.1.15. Post-quantum security and future-proof cryptography

As quantum computing advances, traditional cryptographic schemes such as Rivest–Shamir–Adleman (RSA) and Elliptic Curve Cryptography (ECC) are increasingly vulnerable, posing a threat to SWMS security [175][176]. Incorporating PQC into Blockchain mitigates these risks by using quantum-resistant algorithms, such as lattice- or hash-based methods, to protect transactions, sensor data, and control commands [175-178]. Blockchain's decentralized structure ensures tamper-proof records and preserves data integrity even when individual nodes are compromised [39]. Smart contracts enforce quantum-secure authentication, access control, and compliance policies, while PQC on low-power IoT devices enables efficient, scalable operation. This integrated approach establishes a robust security model that safeguards critical water infrastructure and enhances resilience against both current and emerging cyber threats [176].

5.2. Limitations of Blockchain in securing SWMS

Although Blockchain technology can significantly enhance the security, transparency, and reliability of SWMS, its adoption presents challenges that can impede real-time data processing and overall system efficiency. Below are the brief descriptions of the limitations of Blockchain in securing SWMS.

5.2.1. Scalability and throughput constraints

Many SWMS deployments produce high-frequency telemetry from flow, pressure, and water-quality sensors, as well as smart meters, generating millions of readings per day in large networks. Most public Blockchains and many permissioned systems with heavy consensus protocols cannot process this volume, resulting in latency, storage pressure, and network congestion [39][147][155]. Recording all sensor data on-chain becomes impractical without aggregation, off-chain storage, or specialized architectures, and delayed transaction finalization can hinder timely alarm logging, weakening the Blockchain's forensic audit value [39][147]. Consensus mechanisms such as PoW and PoS further constrain throughput, making it difficult for resource-limited IoT devices to participate efficiently and reducing scalability [147]. Hybrid approaches, including Blockchain–IPFS integration, can ease storage and throughput limitations but add architectural complexity that must be carefully managed to support near-real-time SWMS monitoring and control.

5.2.2. Energy, cost, and consensus trade-offs

Energy-intensive consensus mechanisms like PoW are unsuitable for energy-constrained IoT devices in water networks because they raise operational costs and environmental impact. More efficient alternatives, such as PoS, PoA, and PBFT variants, reduce energy use but often introduce drawbacks, including reduced decentralization, reliance on trusted validators, or governance overhead [148]. Public Blockchains add further challenges by imposing fluctuating transaction fees that make routine sensor data logging costly, whereas private or consortium chains lower fees but require trust agreements among utilities and vendors [148][179]. Although IoT devices have limited energy budgets, careful system design can reduce the overhead of Blockchain operations. Emerging lightweight or application-specific consensus schemes and novel approaches, such as reputation-based or power-line-monitoring methods, aim to reduce energy consumption and block creation time further but may require additional infrastructure or weaken certain security guarantees [179][180].

5.2.3. Endpoint (IoT) security and the "garbage-in"/oracle problem

Blockchains secure data after it is recorded, but they cannot verify the authenticity of off-chain inputs from sensors, gateways, or oracles. Compromised IoT devices in SWMS can inject false readings that the Blockchain then stores immutably, creating an illusion of trustworthy provenance [39][147]. An attacker controlling a pressure sensor or telemetry gateway, for example, could submit artificially low values to conceal a leak, while the Blockchain records them as valid. Oracles that bridge off-chain data to smart contracts also introduce single points of failure, since manipulation at this layer can trigger incorrect automated actions [164]. Ensuring security, therefore, requires a layered strategy with hardened sensors, attested gateways, off-chain validation, intrusion detection, and robust oracle design, because Blockchain alone cannot stop malicious or erroneous data from entering the system.

5.2.4. Data immutability vs. privacy and regulatory compliance

Blockchains' append-only and immutable structure conflicts with data protection laws that grant individuals the right to correct or erase personal data, such as the GDPR's "right to be forgotten" [181][182]. When utilities place personally identifiable information, such as detailed water-usage records, location data, or operator logs, on-chain, they cannot comply with erasure or correction requests because fine-grained consumption data can reveal occupancy patterns. Mitigation strategies that store only hashes on-chain, keep personal data off-chain, or rely on encryption with key revocation reduce these risks but add complexity and still fail to resolve regulatory concerns fully. As a result, jurisdictions with strict data protection rules often favor hybrid or off-chain architectures that sacrifice some decentralization and immutability while maintaining auditability and trust in SWMS [181-183].

5.2.5. Storage bloat and long-term data management

Storing raw time-series data from IoT sensors and meters directly on the Blockchain rapidly inflates the ledger, overwhelming node storage capacity and degrading network performance [155][184][185]. As the chain grows, each node must retain the whole ledger, increasing hardware demands, slowing block validation, and reducing throughput—challenges that can hinder real-time water management. This expansion also raises sustainability concerns for SWMS by driving up storage costs, energy consumption, and the effort required to retrieve historical data [184]. To address these limitations, systems often offload data to archival storage or use Merkle-proof anchoring, but this shift places greater importance on the security and availability of off-chain repositories to preserve verifiable audit trails [39]. High redundancy from full ledger replication across nodes further compounds storage inefficiency [186].

5.2.6. Interoperability, standards, and vendor lock-in

Water utilities rely on diverse SCADA systems, vendor meters, telemetry standards, and reporting formats, making it challenging to integrate Blockchain solutions into existing operations. The fragmented Blockchain ecosystem—spanning platforms such as Ethereum, Hyperledger, and various private chains with differing protocols, data structures, and consensus models—further complicates interoperability with legacy infrastructure, municipal billing systems, third-party analytics, and IoT platforms. These integrations often demand middleware or substantial redesign, increasing configuration complexity, cost, and security exposure. The absence of standardized protocols, data models, APIs, and smart contract languages limits cross-chain data exchange. Relying on proprietary solutions increases the risk of vendor lock-in, limiting flexibility and slowing innovation in water management systems [39].

5.2.7. Smart contract vulnerabilities and automation risk

Smart contracts can automate key SWMS functions, including billing and valve control. Still, their code may contain bugs, logic flaws, or vulnerabilities such as reentrancy attacks, integer overflows, and weak access controls [39]. Exploiting these weaknesses can manipulate water usage, trigger incorrect actuator behavior, tamper with data, or disrupt services, causing physical damage or financial loss, as seen in the DAO and BEC token hacks. Detecting vulnerabilities is challenging: static analysis tools often produce false positives or negatives, and deep learning methods, while more precise, cover a limited range of flaws. Because deployed contracts execute automatically and immutably, errors or exploits can spread without simple remedies, increasing systemic risk. Effective mitigation requires formal verification, phased deployment, thorough testing, and strong governance, while also addressing Blockchain's transparency-related privacy concerns and risks from compromised IoT devices [39][155].

5.2.8. Governance, trust, and legal responsibility

Transparent governance is crucial for defining who operates validators, updates smart contracts, assumes liability for errors, and manages emergencies in decentralized Blockchain systems for water management [39]. In private consortium chains connecting multiple utilities, stakeholders must establish contractual mechanisms to resolve disputes over validator behavior, patching schedules, and emergency overrides, preventing operational bottlenecks. While Blockchain strengthens data integrity and transparency, trust relies on effective governance, regulatory oversight, and coordinated action among utilities, regulators, and communities. Its decentralized and often pseudonymous structure complicates legal accountability for smart contract failures, data inaccuracies, and water rights conflicts, and the lack of established legal frameworks creates uncertainty for operators, regulators, and users, constraining adoption and investment [39]. Therefore, robust governance, external validation, and alignment with existing legal and institutional frameworks are indispensable.

5.2.9. Attack vectors specific to distributed ledgers

Classic Blockchain threats, such as 51% attacks, validator collusion in permissioned networks, replay attacks, and network-level exploits like eclipse attacks, have direct analogues in SWMS, where their intersection with cyber-physical vulnerabilities can significantly amplify damage [39][147]. For instance, compromised vendors controlling colluding validators can manipulate audit logs or delay block confirmations, undermining the integrity of tamper-evident records in networks with few validators. Although Distributed ledger technologies (DLTs) strengthen SWMS security, they also expose the system to DDoS attacks that can overwhelm IoT sensors, increase latency, and disrupt data collection; consensus attacks such as selfish mining and 51% attacks that threaten ledger immutability; Sybil attacks that introduce large numbers of fake identities; double-spending and chain forking that undermine transaction integrity; network-layer exploits that leverage propagation delays; and smart contract vulnerabilities that enable unauthorized access or service disruption [187][188]. These risks intensify in large, heterogeneous, and resource-constrained SWMS environments, where detection and mitigation remain limited [188].

QML enhances Blockchain in SWMS by harnessing quantum parallelism and high-dimensional feature spaces, boosting security, increasing efficiency, and enabling more effective threat detection.

6. QUANTUM MACHINE LEARNING

Recent advances in quantum information science have enabled the integration of quantum computing with machine learning, giving rise to quantum machine learning (QML), a rapidly evolving interdisciplinary field [189]. QML applies quantum principles to machine learning tasks, addressing computational challenges that classical systems struggle to solve and enabling more powerful data processing, modeling, and learning [190-192]. By encoding data in qubits—units that can exist in superpositions of 0 and 1—QML captures complex information from physical processes such as quantum sensing or control. Unlike classical bits, qubits allow algorithms to evaluate multiple possibilities simultaneously through quantum interference and parallelism, improving performance in tasks such as classification, regression, clustering, and feature selection [144][145][190].

QML leverages fundamental quantum properties superposition, entanglement, interference, and inherent parallelism to accelerate machine learning and explore high-dimensional solution spaces. Classical data can be encoded into quantum states via basis, amplitude, or angle encoding, enabling richer representations and more expressive models. Quantum interference amplifies correct outcomes, while entanglement enables modeling complex dependencies, offering potential exponential speedups in optimization, pattern discovery, and high-dimensional data analysis [193][194]. Near-term quantum devices are increasingly accessible, attracting research interest for their potential to improve computational efficiency, reduce energy consumption, and overcome scalability challenges in classical machine learning.

Techniques such as variational quantum circuits (VQCs) extract nonlinear features from high-dimensional datasets, accelerate training, optimize hyperparameters, and manage complex network topologies. Quantum-enhanced methods also perform high-speed matrix and tensor operations and exploit quantum tunneling to achieve objectives more effectively than classical algorithms [195]. Foundational algorithms developed by Peter Shor and Lov Grover in the mid-1990s demonstrated quantum advantages in factorization and database searching, establishing a framework for applying quantum mechanics to machine learning. Advances in quantum hardware, including Noisy Intermediate-Scale Quantum (NISQ) devices, have enabled experimental validation of QML algorithms and observation of quantum speedups in specific tasks. As hardware continues to improve, QML applications are expanding across academia and industry, with platforms from IBM, Google, and D-Wave supporting active exploration [196].

QML algorithms process classical data by encoding it into quantum states, manipulating it with quantum circuits composed of quantum gates, and converting outputs back into classical form. This approach enhances data representation, storage, and computation speed. Researchers integrate QML with machine learning through four strategies: Classical-Classical (CC), which applies quantum-inspired algorithms on classical computers; Classical-Quantum (CQ), which executes quantum algorithms on classical datasets; Quantum-Classical (QC), which uses classical methods to analyze quantum data; and Quantum-Quantum (QQ), which employs both quantum data and algorithms to explore complex structures [197].

QML algorithms can be categorized as pure quantum, quantum-inspired, or hybrid classical–quantum. Pure quantum algorithms run entirely on quantum hardware, leveraging superposition and entanglement to accelerate operations like matrix inversion and classification, as seen in Quantum Support Vector Machines (QSVMs) and Quantum Neural Networks (QNNs). Quantum-inspired algorithms apply quantum principles on classical hardware, improving efficiency and accuracy without full quantum speedup. Hybrid approaches combine quantum and classical resources, using quantum devices for specific computations while relying on classical systems for other tasks, as exemplified by Variational Quantum Classifiers (VQCs) and Quantum Circuit Learning (QCL).

QML models span supervised, unsupervised, semi-supervised, and reinforcement learning. These models have achieved success in diverse domains, including classification, time-series analysis, natural language processing, generative modeling, and reinforcement learning [198]. By leveraging quantum properties, QML can explore multiple solutions simultaneously, capture complex correlations, and provide faster and more accurate analysis than classical machine learning methods.

- Quantum supervised learning is the most mature area of QML, in which quantum-enhanced models leverage labeled data for classification and regression. These models leverage parameterized quantum circuits, such as Variational Quantum Circuits (VQCs), or operate through quantum kernel evaluations. VQCs excel on small, noisy datasets by harnessing the expressive power of quantum circuits. Recent advancements have further enhanced their capabilities with quantum neurons and hybrid optics-based systems [189][199]. Quantum Support Vector Machines (QSVMs) extend classical SVMs by embedding data into high-dimensional quantum feature spaces using quantum kernels. This approach enables efficient separation of nonlinear data and offers potential speedups for complex datasets through fidelity-based similarity measures and quantum-accelerated optimization [196][200][201]. Quantum Neural Networks (QNNs) utilize parameterized quantum circuits to exploit superposition and entanglement, improving parallelism, pattern recognition, and optimization. However, their scalability is constrained by barren plateaus and current hardware limitations. Similarly, Quantum k-Nearest Neighbors (QKNN) accelerate distance calculations via quantum parallelism, while Quantum

Random Forests (QRFs) build ensembles of quantum decision trees through quantum bagging. Sequential and rule-based models have also been adapted into quantum frameworks. Quantum Long Short-Term Memory (QLSTM) networks and quantum decision trees capture complex patterns more efficiently than their classical counterparts. However, their performance is still affected by noise, decoherence, and limited qubit availability [202][203].

- Quantum unsupervised learning focuses on uncovering structure in unlabeled data by exploiting quantum mechanisms such as amplitude encoding, quantum state evolution, and efficient inner-product estimation. These quantum methods offer significant advantages over classical approaches that rely on iterative numerical procedures. Algorithms such as q-means accelerate clustering by leveraging quantum-state comparisons, while single-preparation strategies minimize the overhead of circuit initialization. Quantum Principal Component Analysis (QPCA) enables dimensionality reduction in intractable high-dimensional spaces by extracting principal components via quantum phase estimation. It offers potential exponential speedups, though current implementations remain limited by decoherence and hardware constraints [196][199][200]. Quantum Self-Organizing Maps (QSOMs) enhance classical SOMs by using Grover's search and amplitude amplification to identify winning neurons and update neighborhoods efficiently. Quantum fuzzy regression models uncertainty with adiabatic Hamiltonians rather than relying on rule-based logic, capturing complex probabilistic patterns more effectively. Other quantum approaches, including Quantum Approximate Optimization Algorithms (QAOA) and Quantum Generative Adversarial Networks (QGANs), exploit superposition and entanglement to explore combinatorial solution spaces and train generator–discriminator pairs via variational circuits. Quantum autoencoders, quantum k-means, and quantum Boltzmann machines further harness quantum parallelism to capture intricate correlations, compress high-dimensional data, and perform clustering. However, performance remains constrained by noise and limited qubit resources [199].
- Quantum semi-supervised learning extracts structure from partially labeled datasets by embedding labeled and unlabeled samples into shared quantum feature spaces, which enables models, including quantum GANs, kernel-based learners, and time-series classifiers, to share information through entanglement and expressive feature mappings. Semi-supervised quantum models benefit from parallelism and require fewer labeled examples, but they face challenges related to circuit depth, noise sensitivity, and complex data encoding, particularly for sequential inputs [189][199]. VQCs provide hybrid solutions for NISQ devices by encoding data via feature maps, processing it with parameterized circuits, and iteratively optimizing the parameters classically using noisy measurement outcomes. This approach exploits superposition and entanglement while tuning circuit parameters to minimize cost functions and define effective decision boundaries [199]; [204]. Quantum Least Squares SVMs (QLS-SVMs) similarly map data into high-dimensional spaces using kernel functions and minimize squared errors to identify support vectors for classification [199].
- Quantum reinforcement learning (QRL) integrates quantum computing with classical reinforcement learning to accelerate decision-making and control in dynamic environments. By leveraging superposition, entanglement, and amplitude amplification, quantum agents explore state–action spaces more efficiently than classical counterparts. Foundational work incorporated quantum operators into policy learning, allowing agents to evolve in Hilbert spaces through unitary transformations. Recent advances, including curriculum-based QRL for quantum control, demonstrate faster learning via progressively complex tasks. Quantum deep reinforcement learning (QDRL) extends these concepts through hybrid quantum–classical models that use parameterized quantum circuits as policy or value networks, as well as fully quantum approaches that implement native quantum feedback loops and measurement-driven updates. Other developments include Quantum Imitation Learning and quantum adaptations of standard RL components policies, reward functions, and environment models yielding algorithms such as quantum Q-learning, quantum deep Q-networks, policy gradient and actor–critic methods, quantum Monte Carlo tree search, multi-agent and bandit algorithms, and quantum reward estimation networks, all aimed at improving exploration efficiency, scalability, and convergence [196][201].
- Overall, QML leverages quantum-mechanical principles superposition, entanglement, and quantum parallelism to process information more efficiently than classical models, particularly in high-dimensional spaces and large datasets [205][206]. By exploiting these properties, QML accelerates optimization, clustering, and classification, enhances prediction accuracy, and improves the training of complex models through more effective exploration of solution spaces [207]. Quantum algorithms enable parallel evaluation of quantum states, reducing computational resources and enabling potential speedups for classically intensive tasks. This framework offers robust opportunities for advancing applications such as air-quality forecasting and other data-driven scientific and technological domains.

6.1. Quantum Machine Learning in SWMS

QML is transforming SWMS by integrating quantum computing with machine learning to tackle complex, data-intensive challenges. By exploiting quantum principles such as superposition and entanglement, QML accelerates data processing, improves predictive accuracy, and supports real-time decision-making for water distribution, quality monitoring, infrastructure maintenance, and resource optimization, making it especially effective for managing the large-scale, multifaceted data generated by urban water systems. Figure 5 illustrates the application of QML in SWMS.

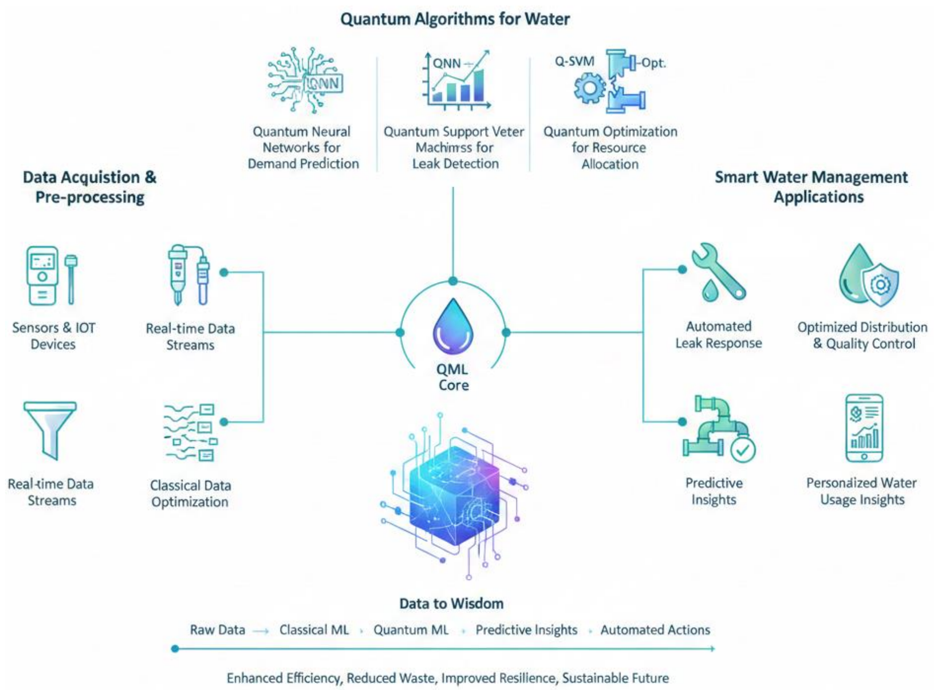
Quantum Algorithms for Water
QNN
QNN
Q-SVM
-Opt.
Quantum Neural Networks for Demand Prediction
Quantum Support Veter Machirss for Leak Detection
Quantum Optimization for Resource Allocation
Data Acquistion & Pre-processing
Sensors & IOT Devices
Real-time Data Streams
Real-time Data Streams
Classical Data Optimization
QML Core
Smart Water Management Applications
Automated Leak Response
Optimized Distribution & Quality Control
Predictive Insights
Personalized Water Usage Insights
Data to Wisdom
Raw Data → Classical ML › Quantum ML › Predictive Insights › Automated Actions
Enhanced Efficiency, Reduced Waste, Improved Resilience, Sustainable Future

Fig. 5. An illustration of the application of QML in SWMS.

The applications of QML in smart water management include

- Water quality prediction: QML enhances water quality monitoring by analyzing sensor data to predict contamination risks and enable timely interventions [208]. Techniques such as QSVMs and QNNs demonstrate superior accuracy compared to classical models. In South Africa's Umgeni Catchment, QSVMs with polynomial and radial basis function kernels outperformed traditional approaches in classifying water suitability for recreational use [141]. These models analyze chemical composition, microbial presence, and flow rates to generate accurate predictions for water management. By integrating QML with IoT sensors and classical algorithms such as Random Forest, efficiency is improved. In aquaculture, the QAOA reduced model training time by half, enabling real-time monitoring of temperature, dissolved oxygen, pH, and turbidity to maintain fish survival rates above 90% [209]. QML accelerates processing of high-dimensional data, leverages quantum phenomena such as superposition and entanglement to improve prediction accuracy, and adapts effectively to diverse environments using low-cost sensors that can operate locally or via the cloud.
- Leak detection and infrastructure optimization: QML enhances water distribution management by analyzing pressure, flow, and acoustic data to detect leaks and optimize infrastructure. Using quantum annealing algorithms, it identifies optimal pipe diameters to improve delivery efficiency, while quantum models uncover subtle patterns that indicate leaks even in noisy or incomplete datasets. By integrating real-time data from multiple sources, QML accelerates leak detection, guides proactive maintenance, predicts potential failure points, and prioritizes repair schedules, thereby reducing water loss, extending infrastructure lifespan, and lowering operational costs [208].
- Flood forecasting: QML enhances flood prediction by integrating quantum algorithms with neural networks, such as LSTM models. QNNs capture extreme flood events more accurately than classical models, achieving lower mean squared errors and higher R^2 values [210]. Hybrid quantum-classical approaches, such as the Quantum-Train LSTM (QT-LSTM), reduce the number of trainable parameters, improving computational efficiency while maintaining performance [71]. These systems deliver timely decision support for disaster management, efficiently handle large datasets, and bolster flood resilience.
- Groundwater monitoring: QML advances sustainable groundwater management by analyzing large datasets to detect patterns and anomalies. By integrating deep learning, ensemble methods, and hybrid models, it predicts groundwater levels, assesses quality, and optimizes monitoring networks, even in regions with limited data [211]. Quantum-enhanced models further boost pattern recognition and anomaly detection while supporting real-time processing. When combined with IoT-enabled monitoring systems, QML facilitates adaptive, self-learning management of aquifers and other groundwater resources, promoting sustainable water use.

- Infrastructure management: QML strengthens infrastructure management by assessing asset conditions and predicting failures, reducing service interruptions and long-term maintenance costs. Integrated with IoT and other smart technologies, QML enables real-time monitoring, predictive control, and efficient operation of water networks, enhancing security, reliability, and sustainability [208].

6.2. Potential Applications of the QML Approach in Securing SWMS

QML expands the potential to enhance SWMS security and resilience by introducing advanced analytical and defensive capabilities as described below.

6.2.1. Anomaly and cyber-attack detection on sensor/SCADA telemetry

QML models, including quantum kernel methods and quantum neural networks, analyze high-dimensional time-series telemetry from distributed sensors and SCADA systems to detect subtle, nonlinear anomalies indicative of cyber intrusions, such as false data injection, command spoofing, or sensor compromise. By mapping classical data into high-dimensional quantum feature spaces, these models improve the separability of malicious and benign patterns, enabling early detection even in noisy environments [141][210]. In water networks, QML identifies coordinated, small-magnitude changes in multimodal signals, such as flow, pressure, and conductivity, and then classifies them using classical classifiers, reducing response time for containment [212]. Training on extensive historical datasets, QML establishes robust baselines of regular operation, quickly detecting deviations and distinguishing minor leaks from major bursts. Leveraging quantum parallelism, it efficiently processes complex IoT sensor patterns in real time, providing rapid alerts for leaks, malfunctions, or cyber-physical attacks while minimizing false positives [213]. Hybrid quantum-classical frameworks, such as quantum autoencoders combined with KNNs, random forests, or one-class SVMs, further enhance detection across large-scale water infrastructure. QML-based intrusion detection systems can handle up to 100,000 events per second with 0.3-second latency, outperforming classical systems that process 15,000 events per second at 2.3-second latency and achieving higher accuracy 98.3% for known attacks and 92.7% for zero-day threats thereby strengthening the resilience and operational security of SWMS [40][41].

6.2.2. Predictive maintenance and secure fault isolation

QML models, including QNNs and quantum kernel regressors, can forecast equipment degradation in pumps, valves, and sensors while distinguishing failures caused by physical wear from those induced by malicious tampering. By jointly analyzing physical telemetry and cyber-event logs, these models separate natural faults from targeted attacks, reducing unplanned downtime and preventing cascade failures [141][210]. Quantum-enhanced feature extraction enables accurate predictions even with limited labeled failure data by capturing complex relationships in sensor readings. In SWMS, QML models based on approaches such as the QAOA accelerate training and inference, allowing real-time analysis of sensor streams and earlier detection of degradation. Integrating QAOA with IoT and classical machine learning has reduced training time by up to 50%, supporting rapid responses to changing water conditions [209]. Moreover, QML improves secure fault isolation by quickly identifying and containing faults or cyber-physical attacks, enhancing fault localization speed and accuracy across large networks. These capabilities capture subtle correlations in high-dimensional data, enable real-time decision-making, and scale efficiently across thousands of sensors and actuators, ultimately improving the reliability, safety, and resilience of water systems.

6.2.3. Secure data transmission and encryption

Quantum computing underpins advanced encryption methods that secure data transmission in SWMS by enhancing resilience against cyber threats and ensuring data confidentiality, integrity, and authenticity. By integrating quantum cryptography with QML, SWMS can defend against both classical and quantum attacks, providing future-proof security solutions [214]. Quantum-resistant hybrid encryption, which combines symmetric and asymmetric cryptography with quantum-resistant algorithms, safeguards communications from potential quantum attacks; for example, the QRHE-IoT framework has demonstrated robust security in smart grid simulations, offering a model applicable to SWMS [215]. Quantum Key Distribution (QKD) protocols like BB84 and quantum random number generators (QRNGs) produce truly random keys with information-theoretic security, eliminating vulnerabilities introduced by predictable pseudo-random generators [200][216]. Combining quantum computing with federated learning allows SWMS to process data locally, reducing exposure to centralized attacks and supporting secure real-time communication across large-scale networks [212]. Emerging techniques, including quantum steganography and customized quantum encryption, conceal sensitive data within quantum streams and enable reversible, privacy-enhanced encoding [217]. Recent implementations achieve secure key generation rates of 2.1 Mbps over 75-kilometer fiber links with quantum bit error rates as low as 1.8%, demonstrating the practical advantages of QML-enhanced quantum security for critical water infrastructure [40].

6.2.4. Real-time threat detection and response

QML significantly enhances security data analysis in SWMS by enabling real-time detection of cyber-physical threats. Leveraging quantum computing's parallelism, QML rapidly processes large, high-dimensional datasets to accurately identify both known and emerging attacks. Quantum-enhanced anomaly detection techniques, such as quantum autoencoders and QKNNs, uncover network anomalies and cyberattacks in data-intensive, interconnected industrial IoT environments with higher precision and lower delays than classical methods [213][218]. Hybrid quantum-classical models further strengthen threat detection, improving system resilience and safeguarding critical water infrastructure. QML also accelerates incident response and optimizes mitigation strategies, deploying countermeasures in constant time regardless of attack scale. Additionally, quantum-based registration, authentication, and federated learning frameworks secure sensitive data across thousands of distributed devices [219]. By analyzing over 10 million network traffic points per second with 96.8% accuracy, QML reduces the average time to threat prediction from six hours to 18 minutes, demonstrating a clear quantum advantage in predictive cybersecurity [40].

6.2.5. Quantum-enhanced anomaly detection

Quantum-enhanced anomaly detection uses QML to identify irregular patterns and cyber threats in SWMS with unprecedented speed and precision. Exploiting superposition and entanglement, QML simultaneously analyzes massive, high-dimensional datasets to uncover subtle anomalies that classical algorithms often overlook. Quantum autoencoders compress sensor readings and network traffic into lower-dimensional representations while retaining critical features, and QKNN algorithms classify real-time sensor data against extensive repositories of normal patterns to quickly flag deviations. By tackling computationally intensive tasks, such as analyzing complex correlations across sensors and network nodes, while classical systems handle control and response, this hybrid approach enables real-time detection and proactive intervention in large-scale, distributed deployments. Studies report that quantum-enhanced systems achieve a 99.1% true positive rate with only 0.8% false positives, outperforming classical systems' 85.3% and 12.4%, and reduce detection time for complex attack patterns by 94% [40].

6.2.6. Optimizing security protocols and defense strategies

QML enhances SWMS security by analyzing large volumes of streaming sensor and network data in real time to identify vulnerabilities and attack vectors that classical systems may overlook. It uses quantum algorithms to evaluate multiple mitigation strategies simultaneously, optimizing defense allocation during coordinated attacks on water treatment or distribution nodes and minimizing downtime and cascading failures. QML dynamically adjusts access controls, authentication measures, and network segmentation in response to detected anomalies, while integrating quantum-enhanced reinforcement learning with federated architectures to continuously improve threat detection and response without compromising privacy. Implementation data demonstrate that QML reduces average incident response times from 145 to 23 minutes, achieves a 97.2% success rate in containing threats before data exfiltration, and decreases the attack surface by 76% compared to traditional security methods, significantly strengthening the resilience of critical water infrastructure [40].

6.2.7. Faster and more accurate predictions

QML leverages superposition and entanglement to analyze multiple data states simultaneously, enabling rapid detection of subtle patterns in water quality. By processing real-time sensor data from rivers and reservoirs, QML models can accurately forecast events such as algae blooms or chemical spikes, supporting proactive interventions to prevent contamination [220]. Integrating algorithms such as the QAOA with IoT sensor networks accelerates model training. It enables near-instantaneous responses to changing water conditions, as demonstrated in aquaculture, where QAOA-driven models generated thousands of corrective actions while maintaining fish survival rates above 90% [209]. QSVMs and QNNs further enhance prediction accuracy, achieving up to 99.8% accuracy in water quality and flood prediction and outperforming classical models in both speed and precision [209][221]. QML also scales efficiently across large, data-intensive SWMS, handling complex, nonlinear relationships within extensive sensor networks and adapting to infrastructure growth and emerging threats.

6.2.8. Optimized water quality monitoring

Quantum-assisted models, such as Quantum-Assisted Variational Autoencoders (QAVAE), detect anomalies in high-dimensional time-series data from water-quality sensors by leveraging quantum circuits to identify subtle deviations that classical methods often miss, enabling timely interventions to ensure water safety. Integrated with IoT sensor networks, these models continuously monitor key parameters—temperature, dissolved oxygen, pH, and turbidity while combining QAOA with machine learning models, such as Random Forests, thereby reducing training time by up to 50% and enabling rapid detection of water quality changes and immediate corrective actions. In aquaculture, this approach supported over 6,000 real-time interventions, maintained fish survival rates above 90%, and demonstrated adaptability across urban and rural environments [209]. By efficiently processing large, complex datasets from distributed sensors, QML enhances predictive capabilities, accurately forecasting water quality trends, identifying contamination or system faults early, and scaling across both resource-constrained and cloud-based infrastructures to support reliable, sustainable, and flexible water management systems [209].

6.2.9. Secure and optimized resource management

Smart water systems optimize both physical infrastructure and operational efficiency, including energy use at pumping stations and water distribution. QML algorithms analyze large, complex datasets from distributed sensors and IoT devices in real time, enabling accurate predictions of water demand, supply, and distribution. By leveraging quantum-enhanced optimization and machine learning, these systems dynamically allocate resources, minimize losses, and adapt to changing environmental and consumption patterns. Quantum-inspired edge computing frameworks accelerate task offloading, improve resource scheduling, enhance stability, and increase overall resource utilization in IoT-driven environments [222]. Integrating QML with quantum encryption and federated learning secures data transmission and processing by leveraging techniques such as QKD and quantum cryptography, reducing the risk of data breaches while keeping sensitive data decentralized. Practical implementations have achieved up to an 85% reduction in breaches, a 20% improvement in resource utilization, and lower latency and power consumption [222]. Additionally, quantum optimization algorithms, such as quantum annealing, enable real-time load balancing and resource allocation, maintaining system stability even under cyberattacks. At the same time, QML models analyze logistical data to detect anomalies and flag potential threats. Together, these approaches enhance the efficiency, resilience, and security of SWMS.

6.2.10. Contamination detection and water-quality forensics

QML methods, including quantum kernels and QNNs, can enhance the analysis of chemical, biological, and spectral water-quality measurements to detect contaminants early. By capturing complex nonlinear relationships among indicators such as pH, conductivity, turbidity, and constituent spectra, QML identifies subtle changes that signal contamination events, even in small datasets with scarce labeled examples [141]. SWMS increasingly use IoT-enabled sensors to continuously monitor parameters such as dissolved oxygen, nitrates, and turbidity, while advanced machine learning models including attention-based neural networks and GANs achieve high accuracy in real-time detection. For example, attention-based models such as AODEGRU have reached 99.89% accuracy, and GAN-based frameworks enhance robustness by analyzing spatial and temporal data across multiple sensor sites, reducing false alarms [223]. Beyond detection, integrating classification models such as Random Forests with optimization algorithms enables SWMS to localize contamination sources, estimate event timing, and quantify concentrations in noisy networks. Emerging QML applications further accelerate training and inference, improve pattern recognition in high-dimensional sensor data, and support advanced forensic analytics, enabling earlier and more reliable detection of subtle or novel contamination events.

6.2.11. Privacy-preserving and secure federated QML for distributed sensors

Federated learning adapted to QML enables edge nodes, such as pump stations and local controllers, to collaboratively train detection models without sharing raw telemetry, enhancing model expressivity while preserving local data privacy [212]. This approach allows participants across different jurisdictions and vendors to leverage shared anomaly-detection and security models while complying with strict data-sharing constraints. By transmitting only model updates, federated QML addresses data heterogeneity, communication efficiency, and privacy concerns, which are critical for sensitive environmental and infrastructure information [224]. Utilities can further protect privacy by integrating cryptographic techniques, including lightweight digital signatures, two-factor authentication, and Blockchain-based frameworks. Privacy-preserving, Blockchain-enhanced architectures like PPFchain provide secure, low-latency support for distributed sensor networks while safeguarding both data and user privacy. QML accelerates federated learning by enabling faster convergence and improved pattern recognition in high-dimensional sensor data. Although direct QML applications in SWMS are emerging, combining quantum computing with federated learning promises to future-proof privacy, security, and scalability, delivering high predictive accuracy, robust system monitoring, and efficient management of thousands of distributed sensors [224][225].

6.2.12. Quantum-assisted optimization for resilient network reconfiguration

QML and quantum-inspired optimization techniques rapidly and securely reconfigure water distribution networks during attacks or contamination events by optimizing valve settings, isolation sequences, and water routing under multi-objective constraints, including safety, service continuity, and minimal disruption. These methods accelerate the development of effective intervention policies, enabling controllers to propose robust responses under uncertainty and reduce propagated harm. Quantum-assisted optimization, including quantum annealing and the QAOA, efficiently solves large-scale combinatorial problems that classical approaches struggle with, restoring critical services by dynamically reconfiguring network topologies, partitioning segments, and identifying optimal restoration paths and resource allocations [226][227]. Hybrid quantum-classical approaches and quantum-inspired algorithms, such as advanced quantum particle swarm optimization, enhance connectivity, reduce energy consumption, and minimize reconfiguration delays in heterogeneous sensor and control networks. Together, these solutions support scalable, efficient, and resilient operations, enabling faster restoration after disruptions, optimized resource use, and reliable service continuity across complex water systems.

6.2.13. Quantum-enhanced feature engineering for sensor fusion

QML encodes multimodal sensor data, such as acoustic vibrations, pressure transients, and chemical measurements, into quantum feature maps, uncovering latent correlations that classical feature engineering often misses [141][228]. By leveraging entanglement and interference, QML maps these signals into high-dimensional quantum spaces, enabling advanced feature extraction, robust data fusion, and the discovery of complex patterns across sensors. This allows QML models to classify operational states, cluster behaviors, and detect coordinated anomalies, including attacks that manifest only across multiple modalities. Its compact parameterization enhances performance with limited labeled data, making it particularly suitable for SWMS. Additionally, recent quantum protocols enable secure, distributed sensor measurements, optimizing information gain while preserving data integrity. Quantum cryptographic techniques, including QKD and quantum-walk-based authentication, protect data transmission and fusion, ensuring confidentiality and tamper resistance [229]. By integrating quantum-enhanced feature extraction with secure data fusion, QML improves the accuracy, efficiency, and resilience of SWMS, supporting real-time water quality monitoring and safeguarding critical infrastructure.

6.2.14. Post-quantum and quantum-safe integration (defense-in-depth)

QML enhances analytics in SWMS, but securing communications and control channels against quantum threats requires adopting PQC and quantum-safe networking. PQC protects telemetry and stored data from retrospective quantum decryption, while combining QML detection with PQC-enabled device authentication and secure aggregation creates a layered defense. Operators must safeguard detection models and underlying telemetry to prevent adversaries from exploiting encrypted data. A defense-in-depth approach integrates lattice-based PQC schemes like Dilithium-5, which resist quantum attacks while remaining efficient for distributed IoT sensors and controllers, with QKD to enable secure key exchange and information-theoretic channel protection [176][230]. Embedding PQC in Blockchain frameworks preserves data immutability, supports secure logging, access control, and audit trails, and can operate efficiently on resource-constrained devices used for water monitoring and control [176][175]. By combining QML analytics with PQC, QKD, and Blockchain, SWMS can maintain operational efficiency while resisting classical and quantum cyber threats. Implementing multiple quantum-safe layers ensures resilience and future-proof security, though standardization, interoperability, and integration challenges require careful design for robust long-term protection [175][230].

6.3. Advantages of the QML approach over classical machine learning in securing SWMS

QML offers distinct advantages over classical machine learning in enhancing the security and efficiency of SWMS as described below.

6.3.1. Enhanced data processing capabilities

QML harnesses superposition, entanglement, and quantum parallelism to process high-dimensional datasets more efficiently than classical machine learning. In smart water systems generating vast volumes of sensor and IoT data, QML enhances classification, pattern recognition, and anomaly detection by encoding data into quantum feature spaces and applying quantum-enhanced preprocessing. Quantum algorithms evaluate multiple solutions simultaneously, enabling real-time anomaly detection in large-scale sensor networks where classical methods often lag. Techniques such as QSVMs, quantum gradient boosting, and quantum neural networks accelerate training, optimize performance, and adapt quickly to emerging threats or system changes. By facilitating robust sensor fusion and proactive monitoring, QML improves water quality assessment and flood risk management while delivering higher accuracy, faster training, and greater resilience, security, and efficiency compared with classical approaches [141][221].

6.3.2. Superior pattern recognition in complex systems

QML effectively captures complex, nonlinear interactions in water quality data, such as correlations among ammonia, nitrate, and sedimentation, enabling precise analysis for informed water management decisions. Algorithms such as QSVMs and QNNs detect subtle, high-dimensional patterns in pipeline sensor and water-use data, enhancing anomaly detection and identifying potential security threats, including unauthorized access or tampering [231]. By leveraging quantum-enhanced feature spaces through entanglement and interference, QML maps data into exponentially larger dimensions, uncovering patterns those classical methods often overlook and improving classification in noisy, overlapping, or intricate datasets [231]. These richer quantum representations also support ensemble and deep learning models, facilitating early threat detection, integrating heterogeneous sensor data for comprehensive monitoring, and scaling efficiently to large, distributed datasets. Experimental results show that quantum resources, such as entangled probe states, can reduce classification errors beyond classical limits, demonstrating QML’s practical advantages for secure, high-stakes water system management.

6.3.3. Improved predictive accuracy and efficiency

QML models outperform classical approaches in predictive tasks such as flood forecasting by exploiting quantum superposition and entanglement to process large datasets in parallel, thereby enabling faster, more accurate predictions. Hybrid models that integrate classical and QML techniques have enhanced prediction accuracy and efficiency for daily flood events along Germany's Wupper River, demonstrating QML's potential for climate change adaptation and disaster risk management [221]. Quantum algorithms, including QSVM, Quantum Gradient Boosting, and optimization methods like QAOA, accelerate model training and inference, reducing training time by up to 50% in practical SWMS applications [209][221]. By employing quantum data embedding and feature mapping—particularly within ensemble frameworks—QML achieves higher R^2 and lower mean squared error than classical models on identical datasets. These capabilities allow QML-powered SWMS to simulate multiple threat scenarios simultaneously, identify vulnerabilities, and deliver real-time monitoring across distributed sensor networks, supporting proactive, scalable, and data-driven interventions for sustainable water management.

6.3.4. Robust security and anomaly detection

Integrating QML into smart water systems strengthens security by detecting anomalies and cyber threats more effectively. Quantum algorithms rapidly analyze large, complex datasets, uncovering subtle irregularities in water flow, pressure, or chemical composition that classical models may overlook. Techniques such as quantum autoencoders, QSVMs, and QNNs efficiently process high-dimensional sensor and network data, leveraging quantum parallelism and entanglement to handle the noisy, imbalanced datasets typical of SWMS. Studies show that QML-based anomaly detection maintains high performance under real-world conditions and is robust to various types of quantum noise [213][232]. Hybrid quantum-classical architectures improve scalability and resilience, enabling distributed, adaptive security across complex water networks. By integrating QML with quantum-resilient cryptography, such as lattice-based encryption, and AI-driven anomaly detection, smart water systems achieve a multi-layered defense that both detects cyber-physical attacks and safeguards data integrity and communications against quantum-augmented threats [232][233].

6.3.5. Scalability and adaptability for future challenges

QML provides a scalable, adaptable solution for the growing complexity of water management systems. By leveraging quantum algorithms that exploit parallelism and entanglement, QML efficiently processes high-dimensional data from SWMS sensors and IoT devices, enabling real-time modeling of intricate water networks and adaptive responses to changing conditions [191][212][234]. Quantum-enhanced models quickly retrain to adapt to new data patterns, operational shifts, and emerging threats while upholding security and regulatory compliance. By combining federated learning with edge computing, QML allows distributed SWMS nodes to collaborate without centralizing data, strengthening privacy and system resilience. Its efficient computations support real-time anomaly detection, threat mitigation, and system optimization, enabling SWMS to operate autonomously and adaptively in dynamic environments while maintaining high performance as networks grow [234].

6.3.6. Better handling of high-dimensional data

SWMS generate massive, high-dimensional datasets from sensors, valves, and usage logs, which challenge classical analysis methods. QML addresses these challenges by leveraging quantum properties, such as superposition and entanglement, to represent and process exponentially larger feature spaces, enabling real-time monitoring, anomaly detection, and cyber-physical security. Quantum algorithms like QSVM and quantum-enhanced boosting (QBoost) map data into high-dimensional Hilbert spaces, revealing subtle patterns and correlations that classical models often miss or require excessive resources to identify. This approach accelerates training and prediction on large, heterogeneous datasets, improves accuracy in applications such as flood prediction and anomaly detection, enhances resilience against sophisticated cyberattacks, and optimizes resource allocation for timely operational responses [221].

6.3.7. Stronger encryption and data privacy integration

QML strengthens the security of operational and consumption data in SWMS by applying quantum cryptography techniques. It trains models directly on encrypted data, preserving privacy while maintaining prediction accuracy. By exploiting superposition, entanglement, and the no-cloning theorem, QML secures data processing and communication, preventing adversaries from intercepting or reconstructing sensitive information [235]. Studies show that QML models can use differentially private optimization algorithms to protect individual data points while maintaining high accuracy, and quantum implementations achieve stronger privacy guarantees with less artificial noise [236]. Quantum federated learning protocols allow decentralized training with only encrypted updates, and advanced quantum communication techniques, including gradient hiding and secure multiparty computation, prevent eavesdropping and gradient inversion attacks. Hybrid quantum–classical neural networks further protect sensitive data by encrypting inputs for quantum cloud processing without compromising performance [235]. Together, these approaches create a robust framework for secure, high-utility SWMS operations.

6.3.8. Robustness against adversarial attacks

QML models resist adversarial attacks more effectively than classical machine learning models, enhancing the security of SWMS against inputs designed to compromise anomaly detection or predictive maintenance. Unlike neural networks, which remain vulnerable to carefully crafted perturbations, quantum classifiers exploit superposition and entanglement to access features beyond the reach of classical models, making attacks more difficult [237]. While some adversarial strategies can transfer between quantum and classical systems, quantum models typically require more sophisticated approaches, especially when combined with regularization, hybrid quantum-classical architectures, or quantum kernel methods, which can reduce attack success rates by 40–60% compared to conventional deep learning [237][238]. Techniques such as quantum adversarial training and controlled quantum noise further strengthen resilience against both gradient-based and gradient-free attacks. By improving anomaly detection, leak detection, water quality monitoring, and automated control, QML-based systems enhance reliability and mitigate threats, offering a significant security advantage for critical water management operations [238].

6.3.9. Efficient optimization for resource management

QML enhances the secure and efficient management of water distribution networks by exploiting quantum phenomena such as superposition and entanglement to process vast solution spaces in parallel. This capability allows quantum algorithms to optimize valve schedules, pump operations, and other control tasks while addressing security constraints and real-time threats. Compared to classical methods, which often struggle with the combinatorial complexity of SWMS, QML solves complex optimization problems, including leak detection and demand forecasting, more rapidly. QNNs and parameterized quantum circuits model nonlinear relationships in water systems with high expressivity, improving prediction accuracy and supporting efficient resource allocation as networks scale. By requiring fewer parameters, QML reduces computational overhead and accelerates convergence, enabling real-time water management. Hybrid quantum-classical frameworks further boost efficiency by combining quantum computing’s strength in high-dimensional search with classical computing’s data-handling capabilities, achieving better generalization and practical applicability on current hardware [239]. Together, these advances enable real-time adaptive control, predictive maintenance, and optimal scheduling under uncertainty, significantly improving sustainable water distribution practices [239].

6.3.10. Adaptive learning in dynamic environments

SWMS experience fluctuating usage patterns and evolving cyber threats that demand rapid adaptation. QML exploits quantum parallelism and entanglement to process large, complex, and time-varying datasets more efficiently than classical models, enabling faster anomaly detection and the identification of emerging patterns for real-time monitoring and continuous security updates. Parameterized quantum circuits and QNNs capture complex nonlinear relationships and adapt to changing data distributions more effectively [239]. At the same time, QRL accelerates learning, allowing agents to identify optimal policies and respond to new scenarios quickly with fewer data samples [239]. Hybrid quantum-classical frameworks combine rapid quantum model updates with robust classical data handling, reducing complexity, improving generalization, and enhancing SWMS resilience against shifting water quality, demand fluctuations, infrastructure changes, and evolving cyber-physical threats [239].

6.3.11. Enhanced fault tolerance and error mitigation

Quantum models inherently manage probabilistic states, enabling them to process noisy, incomplete, or corrupted sensor data more effectively than classical systems. By exploiting superposition and entanglement, QML encodes and processes information in ways that enhance resilience to errors and noise, which is critical for maintaining data integrity and operational continuity in secure SWMS [221]. Studies show that QML models, including QSVMs and QNNs, achieve higher prediction accuracy and competitive training times under noisy conditions, such as in flood prediction, where they demonstrate improved robustness to data variability and potential system faults. Leveraging quantum error correction and high-dimensional Hilbert spaces, QML isolates and corrects errors efficiently, mitigating risks from data corruption, adversarial attacks, and hardware faults. Although large-scale, fault-tolerant quantum computers are not yet widely available and direct studies on QML for SWMS are limited, advances in quantum hardware and algorithms suggest that QML could substantially enhance SWMS resilience against both random faults and targeted cyber-physical threats [221].

7. INTEGRATING BLOCKCHAIN AND QML FOR SECURE SWMS

The proposed framework integrates Blockchain and QML to create a secure, resilient, and intelligent infrastructure for SWMS. Blockchain provides a decentralized, tamper-resistant platform for storing sensor data, managing access, and enabling transparent decision-making, protecting against data manipulation, unauthorized access, and single points of failure. QML enhances the system by analyzing high-dimensional IoT data in real time, enabling anomaly detection, predictive analytics, and adaptive optimization to detect leaks, contamination, and cyber threats early. By combining these technologies, the framework ensures verifiable, trustworthy data while strengthening operational intelligence and resilience, improving cyber-physical security, reinforcing consumer trust, and supporting sustainable water resource management. Figure 6 illustrates the technical architecture for integrating Blockchain and QML to secure SWMS.

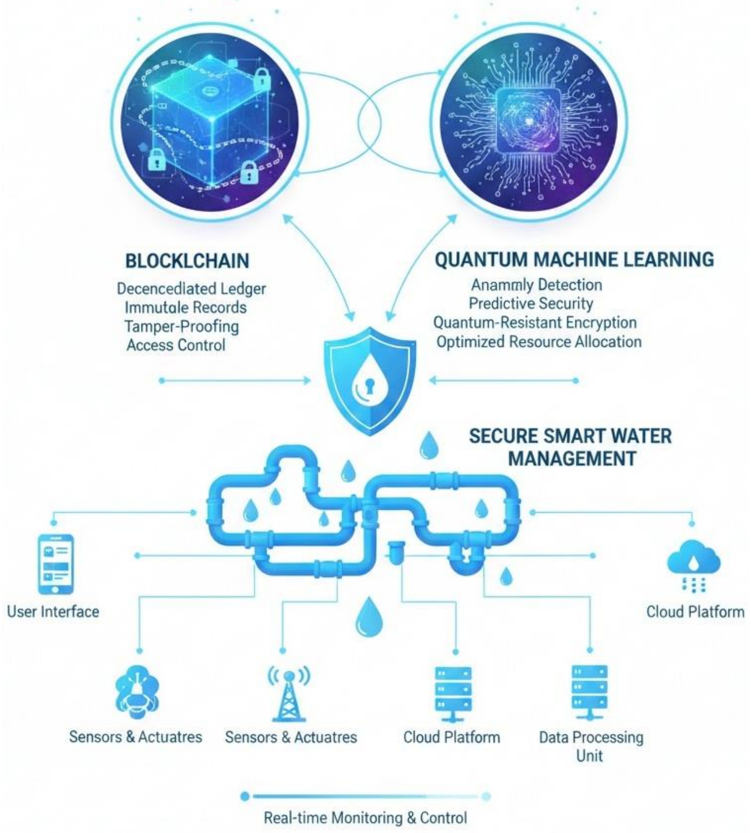

Fig. 6. Illustrates the proposed framework that leverages Blockchain and QML for securing SWMS.

The proposed framework employs a multi-layered architecture that integrates Blockchain and QML to enhance the security and efficiency of SWMS. Below are the brief descriptions of the layers.

- The perception layer actively gathers real-time data from IoT-enabled sensors and actuators installed in pipelines, reservoirs, and treatment facilities, monitoring flow rates, pressure, water quality, and consumption patterns. Devices secure their transmissions with lightweight encryption to maintain data confidentiality and integrity. Key inputs include sensor readings of flow, pressure, chemical composition, turbidity, and leakage, metrics from SCADA systems, and external factors such as weather conditions, reservoir levels, and consumption forecasts, enabling seamless interaction with the physical infrastructure.
- The network layer establishes secure, reliable, low-latency communication among sensors, actuators, Blockchain nodes, and QML modules. It combines wired technologies, such as fiber-optic links and Ethernet, with wireless technologies, including LoRaWAN, NB-IoT, and 5G, to maintain continuous data flow throughout the water management system. End-to-end encryption using TLS/SSL and quantum-resistant protocols protects transmitted information and preserves the integrity of logged data.
- The edge processing layer cleans, normalizes, and extracts features from raw sensor streams to prepare them for integration with the Blockchain. It employs quantum-inspired preprocessing, such as quantum kernel techniques and annealing, to reduce dimensionality, identify immediate anomalies, and limit the volume of data sent upstream. These operations reduce latency and ensure that only the most relevant information reaches the Blockchain layer.
- The Blockchain layer serves as a decentralized, tamper-resistant foundation for managing sensor data and operational commands. It stores water flow measurements, quality metrics, consumption data, and control signals as hashed, timestamped transactions validated via lightweight consensus mechanisms such as PBFT or PoA. Smart contracts automate leak detection, demand response, predictive maintenance, and water allocation, while advanced cryptographic tools, including asymmetric encryption and zero-knowledge proofs, maintain data confidentiality and controlled visibility. Scalability features such as sharding, sidechains, and off-chain storage sustain high throughput and supply trustworthy inputs to the QML layer.

- The QML layer performs advanced analytics on high-dimensional data originating from IoT sensors, smart meters, and distribution networks. After Blockchain verification, classical data is encoded into quantum states and processed on hybrid quantum-classical platforms. Quantum-enhanced algorithms detect anomalies, forecast demand and potential failures, and optimize resource allocation using techniques such as QAOA. Methods like QPCA and quantum autoencoders further reduce dimensionality and computational load, improving processing efficiency and minimizing Blockchain storage requirements. The system records predictions and alerts on the Blockchain, enabling automated, auditable responses through smart contracts.
- The application layer delivers real-time dashboards, visualizations, and controls for operators, regulators, and stakeholders. It provides predictive insights, system alerts, and automated actuation of pumps, valves, and reservoirs based on QML outputs. Immutable Blockchain records strengthen compliance, auditing, and long-term trend analysis. The layer enforces strong identity and access management with smart contracts and quantum-resistant cryptography, translating user actions and sensor updates into consistent, traceable Blockchain transactions and QML inputs. It also connects with external services and smart city platforms through APIs to support predictive maintenance, leakage mitigation, and adaptive water distribution.

Figure 7 illustrates the layers in the proposed framework, which integrates Blockchain and QML to enhance the security of SWMS.

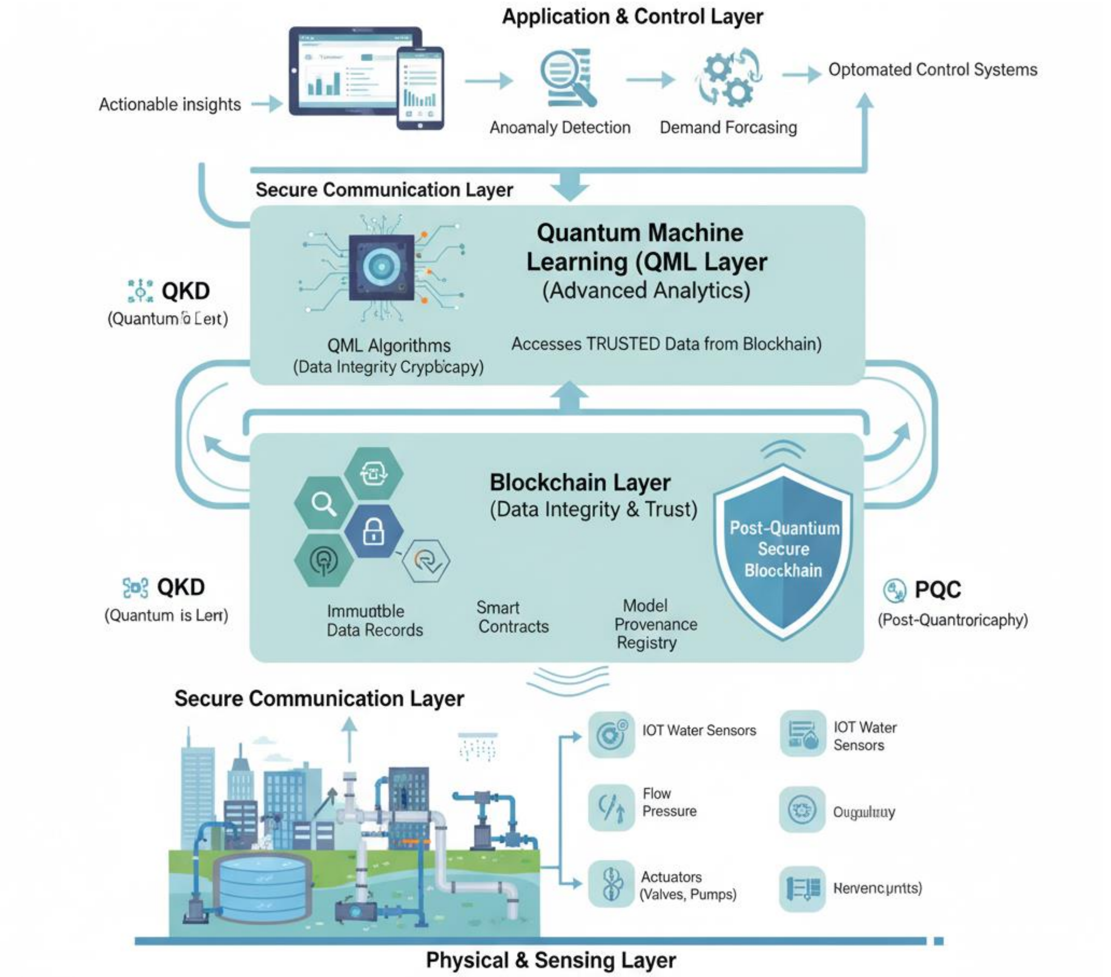

Fig. 7. Illustrates the layers in the proposed framework, which integrates Blockchain and QML to enhance the security of SWMS.

7.1. Synergistic benefits of integrating Blockchain and QML for secure SWMS

Integrating Blockchain with QML in a SWMS enhances security, optimizes efficiency, and improves resource management. This approach establishes an intelligent, resilient, and trustworthy water infrastructure that surpasses the capabilities of traditional systems. The synergistic benefits of integrating Blockchain and QML for secure SWMS include:

7.1.1. Enhanced security and data integrity

Blockchain establishes a decentralized, tamper-resistant ledger in SWMS, recording all transactions, sensor data, and control commands while eliminating reliance on a single authority, thereby preventing unauthorized access, data manipulation, and replay attacks. This transparency builds trust among utilities, regulators, and consumers by ensuring that system updates and sensor readings are verifiable. QML enhances security by using quantum algorithms to detect, predict, and mitigate advanced cyber threats in real time, identifying subtle deviations in water flow, pressure, and consumption patterns that may indicate breaches, sensor faults, or fraud. Registering QML model parameters on the Blockchain protects against model poisoning, while integrating PQC and QKD safeguards the system from both current and emerging quantum-enabled attacks. This combined approach ensures immutable records, tamper-proof models, and resilient, future-proof water infrastructure, enabling utilities to operate securely, regulators to access accurate compliance data, and consumers to trust water quality and distribution information.

7.1.2. Superior intelligence and analytics

Integrating Blockchain and QML into SWMSs enhances intelligence, analytics, and operational resilience. QML exploits quantum algorithms to uncover complex, nonlinear correlations in high-dimensional datasets, such as sensor readings, consumption patterns, and weather data, enabling rapid anomaly detection, predictive modeling, and adaptive decision-making. Blockchain ensures that all data feeding QML models is authentic, tamper-proof, and transparently recorded, eliminating biases from compromised or falsified datasets. Together, these technologies allow utilities to detect leaks, contamination, or cyber intrusions, optimize energy-efficient pump scheduling and water distribution, forecast demand with precision, and allocate resources effectively. By integrating QML's computational capabilities with Blockchain's data-integrity mechanisms, the system enables stakeholders to improve sustainability, lower operational costs, reduce risks, and enhance the overall resilience of water infrastructure.

7.1.3. Increased efficiency and operational resilience

Integrating Blockchain with QML improves the efficiency, resilience, and transparency of SWMSs by creating a decentralized, tamper-proof infrastructure that accelerates data exchange and enables near real-time validation of water quality, consumption, and distribution data. QML rapidly analyzes large, heterogeneous datasets, including sensor readings, weather forecasts, and consumption patterns, to generate predictive insights on demand fluctuations, leakage risks, and potential contamination. These insights allow utilities to adjust operations proactively and allocate resources more effectively, while Blockchain's distributed consensus preserves system continuity during cyberattacks or node failures. Smart contracts automate functions such as emergency valve shut-offs, water redistribution, and maintenance alerts triggered by QML-detected anomalies. By permanently recording each transaction, the Blockchain layer ensures data integrity, supports regulatory compliance, and maintains an auditable operational history, thereby strengthening risk mitigation and service reliability.

7.1.4. Quantum-resilient threat detection

The proposed Blockchain–QML framework enhances SWMS security by enabling quantum-resilient threat detection. By integrating QML with Blockchain, it analyzes large, heterogeneous data streams from IoT sensors, smart meters, and control systems in real time, rapidly identifying anomalies and sophisticated attack patterns such as coordinated intrusions or stealthy data manipulation. QML leverages quantum parallelism and entanglement to improve detection speed and accuracy beyond classical methods. At the same time, the Blockchain layer ensures tamper-proof logging and decentralized threat verification, preventing attackers from altering records or suppressing alerts. Incorporating post-quantum cryptographic primitives further protects communication, transaction validation, and model updates against quantum attacks. By combining immutable ledger technology with advanced quantum-based pattern recognition, the framework establishes a resilient, adaptive defense that can withstand both classical and quantum cyber threats.

7.1.5. Privacy preservation in data sharing

Effective water management depends on collaboration among municipalities, regulators, and private service providers, and the proposed framework leverages a permissioned Blockchain to secure sensitive data while enabling controlled sharing. The framework employs privacy-preserving techniques secure multi-party computation, encrypted transactions, and quantum-resistant cryptography to protect customer usage data, billing records, industrial discharge information, and operational metrics while maintaining verifiability and auditability. Access is restricted to verified entities such as utility operators or authorized analytics services, reducing privacy risks and preventing unauthorized profiling. Within SWMS, the Blockchain's immutable, decentralized ledger records all transactions cryptographically, ensuring accountability and secure, transparent data exchanges. By integrating QML methods, the framework enables encrypted or obfuscated data analytics for anomaly detection, predictive maintenance, and consumption forecasting. Together, these technologies protect data throughout its lifecycle, support regulatory compliance, and strengthen trust among users and stakeholders.

7.1.6. Improved transparency and accountability

Blockchain immutably logs every operation in the SWMS, such as valve control, water distribution, and anomaly detection, creating a traceable, auditable record that strengthens accountability. Regulators and utility operators can verify compliance with sustainability standards, water safety requirements, and environmental policies. QML analyzes complex network data in real time to identify anomalies, inefficiencies, or unauthorized access, and automatically records these events on the Blockchain. Combined with cryptographic safeguards that restrict data access to authorized stakeholders, the integrated Blockchain–QML framework delivers precise operational tracking, enhances transparency, reduces fraud risk, and promotes responsible governance across the water supply chain.

7.1.7. Robustness against quantum-enabled attacks

The proposed framework secures SWMS against quantum-computing threats by integrating post-quantum cryptographic schemes into Blockchain-based transaction authentication and consensus mechanisms. It leverages QML to analyze high-dimensional sensor and IoT data, detecting subtle patterns indicative of intrusions or malicious activity and enabling proactive defenses against evolving attack vectors. By combining a decentralized Blockchain architecture with quantum-resistant protocols, the system ensures data immutability, tamper-evident records, and resilience against both classical and quantum-driven cyberattacks. Together, these components create a robust, future-proof security framework that preserves the integrity, trustworthiness, and operational continuity of critical water infrastructure.

7.1.8. Real-time decision support

QML enhances predictive analytics in water management by modeling demand, leakage risks, and contamination events with high accuracy. By integrating QML with Blockchain, the framework ensures that data from IoT sensors, smart meters, and water treatment facilities is verified and tamper-proof, enabling decision-makers to act on reliable information without delays. QML algorithms analyze this data in near real-time, detecting anomalies, forecasting failures, and providing prescriptive recommendations for proactive interventions, such as adjusting pump operations or issuing alerts. The system supports automated decision-making and stakeholder collaboration through real-time dashboards, allowing municipal authorities, utility operators, and emergency responders to coordinate responses efficiently. Continuous QML adapts predictions to evolving conditions, while Blockchain preserves historical integrity, creating a self-improving, proactive framework that safeguards water quality, optimizes resource allocation, and minimizes operational risks.

7.1.9. Scalability and interoperability

The modular integration of Blockchain and QML enables the system to scale efficiently across diverse regions and infrastructures by directly interoperating with smart meters, IoT-based water-quality sensors, and existing SCADA systems, forming a unified, secure water management ecosystem. Blockchain allows new sensors, devices, and monitoring stations to join seamlessly while preventing single points of failure and distributing data processing across multiple nodes, supporting horizontal scaling as the network grows. QML processes large-scale, high-dimensional data on water usage, flow, and quality, enabling real-time analytics, predictive modeling, and adaptive insights such as anomaly detection and predictive maintenance. By standardizing data formats and access protocols, the framework ensures consistent data integrity and seamless communication across heterogeneous components, reduces integration costs, supports vendor-neutral expansion, and facilitates regulatory compliance. Together, Blockchain and QML create a future-proof solution that can handle rapid growth in connected devices and data volume while maintaining operational efficiency.

7.1.10. Resilience to insider and supply chain attacks

The system enhances resilience against insider threats and compromised devices by decentralizing authority through Blockchain consensus and employing QML for anomaly detection. Even if some nodes or devices are compromised, the distributed trust model sustains continuous operations without risking catastrophic failure. By recording every transaction—from sensor readings to operational commands—on an immutable, cryptographically secured Blockchain ledger, the framework prevents insiders from altering historical data and ensures a tamper-evident, auditable trail. It also mitigates supply chain attacks by verifying all updates, firmware, and third-party inputs, while QML continuously monitors operational data for subtle anomalies indicating compromise. By combining immutable verification with adaptive anomaly detection, the system preserves data integrity, strengthens threat detection, and ensures uninterrupted water distribution, safeguarding public health and trust in critical urban infrastructure.

7.1.11. Cost efficiency in the long run

Integrating Blockchain and QML into SWMSs enhances long-term cost efficiency by enabling predictive, data-driven operations. QML algorithms process vast sensor data streams in real time to detect inefficiencies, forecast maintenance needs, and optimize water distribution, minimizing energy and water consumption while extending infrastructure lifespan. Blockchain secures data management, preventing fraud, unauthorized access, and reporting errors, ensuring reliable operational decisions. Predictive maintenance allows proactive interventions before equipment failures or pipe bursts, reducing downtime and emergency repair costs. Together, Blockchain and QML support scalable, transparent, and efficient water networks by dynamically optimizing pumping, treatment, and distribution schedules, reducing operational expenses, conserving resources, and advancing sustainability.

7.1.12. Sustainability and public trust

A secure and transparent SWMS enhances sustainability by optimizing water use, minimizing waste, and ensuring equitable distribution. It leverages QML to analyze complex datasets from sensors, IoT devices, and consumption records, predicting demand patterns, detecting anomalies, and optimizing distribution networks in real time. Simultaneously, Blockchain preserves the integrity and traceability of operational and transactional data, reducing losses from leaks or mismanagement and providing verifiable records of water quality, consumption, and distribution. By integrating these technologies, water utilities and municipalities can implement dynamic allocation, predictive maintenance, and adaptive conservation strategies, anticipate system failures or contamination events, and maintain transparent, auditable records without compromising sensitive data, thereby fostering public trust, encouraging citizen participation, and promoting responsible, sustainable water management.

7.2. Comparative analysis of Blockchain and QML for an Efficient SWMS with recent state-of-the-art approaches

Recent studies highlight the complementary potential of Blockchain and QML to advance smart water management. Blockchain enhances data security, transparency, and traceability by protecting IoT sensor data, preventing tampering, and enabling automated actions through smart contracts. In smart aquaculture, for example, Blockchain secures water quality records and supports traceable alerts. Machine learning models such as ARIMA, random forest, and KNN predict pollution indices to guide rapid interventions, with random forest achieving the highest prediction accuracy for water quality [240]. Reviews also emphasize Blockchain's role in digitalizing asset management, automating monitoring, and fostering stakeholder trust, although real-world adoption remains limited by scalability and interoperability issues [39].

QML, often integrated with advanced nanodevices, provides powerful analytical and optimization capabilities for water and agricultural systems. Quantum nanodevices rapidly process large sensor datasets, enabling real-time optimization of irrigation, crop scheduling, and resource distribution. When combined with Blockchain, QML enhances both operational efficiency and data security by delivering accurate predictions while safeguarding system data. In smart farming, QML supports AI-driven optimization and genetic algorithms to improve resource utilization and overall performance [241].

Comparative analyses reveal complementary strengths. Blockchain ensures data integrity and builds trust among stakeholders, while QML offers superior computational speed and predictive accuracy for complex, large-scale datasets. Integrating these technologies promises secure and efficient smart water management, though applications remain experimental or limited to pilot studies. Key challenges persist: Blockchain must address scalability and interoperability, and QML's practical deployment in water management is still emerging. Table II summarizes the comparative features of Blockchain and QML in smart water management.

TABLE II. COMPARATIVE FEATURES OF BLOCKCHAIN AND QML IN SMART WATER MANAGEMENT.

Technology	Key Strengths	Main Applications	Limitations/Challenges	References
Blockchain	Data security, transparency, traceability	Water quality monitoring, asset management, automated alerts	Scalability, interoperability, and limited real-world deployment	[39][240]
QML	Fast, complex data analysis, optimization	Resource allocation, predictive analytics, and smart farming	Early-stage deployment, integration complexity	[241]
Combined	Secure, efficient, real-time optimization	Smart aquaculture, precision agriculture, and water distribution	Integration, standardization, empirical validation	[240][241]

7.3. Cost-benefit analysis of implementing SWMS

Cost-benefit analysis quantifies whether an investment's anticipated benefits exceed its costs, typically by evaluating multiple scenarios to identify conditions for profitability. Organizations often measure these using indicators such as Net Present Value (NPV), Internal Rate of Return (IRR), Return on Investment (ROI), and Payback Period [153]. In the context of SWMS, which leverage digital technologies like IoT sensors, AI, and data analytics to optimize water use and enhance operational efficiency, recent studies demonstrate significant economic, environmental, and operational benefits.

7.3.1. Economic benefits and costs

Implementing SWMS demands significant upfront investment in infrastructure, sensors, and digital platforms, but it delivers substantial long-term benefits. Smart metering and AI-driven leak detection can reduce non-revenue water losses by up to 23% and cut operational costs by 18% in urban settings [110][242][243]. In comparison, smart irrigation and grid systems improve efficiency by decreasing water use by 38–50% and lowering energy consumption [242-244]. As water prices rise, these savings make the payback period for smart irrigation and metering systems financially viable [242-244].

7.3.2. Environmental and social impacts

SWMS reduce water loss, energy consumption, and carbon emissions while improving monitoring, predictive maintenance, and service quality [110][243][244]. They enhance reliability, water quality, and customer satisfaction, promoting equitable access [13][110][242]. With low-cost, scalable designs, SWMS adapt easily to diverse environments from agriculture to urban campuses making them broadly applicable and accessible [13][244][245].

7.3.3. Challenges and limitations

High upfront costs significantly hinder adoption, particularly in resource-constrained regions [110][242]. Successful implementation requires integrating systems effectively, ensuring strong cybersecurity, and employing personnel with specialized technical skills [110][242]. Moreover, outdated regulations and the lack of standardized frameworks further restrict deployment and scalability [110][246].

7.3.4. Decision-making criteria

Recent studies apply multi-criteria decision frameworks to assess effectiveness, risk management, resource efficiency, integration feasibility, environmental impact, ROI, and long-term sustainability. Strategies such as smart metering, demand management, and smart irrigation consistently achieve the highest cost-effectiveness and overall impact [242][244][246]. Table III presents the cost-benefit outcomes for SWMS.

TABLE III. SUMMARY OF COST-BENEFIT OUTCOMES FOR SWMS.

S/No	Benefit/Cost Category	Typical Findings	References
1	Water loss reduction	23–80% reduction in non-revenue water	[110][242-244]
2	Operational cost savings	18–40% reduction in operational expenditure	[110][242-244]
3	Payback period	Short to medium term (context-dependent)	[242-244]
4	Environmental impact	Significant Carbon dioxide and energy savings	[110][243][244]
5	Main barriers	High initial cost, cyber risks, and regulation	[110][242]

8. REAL-WORLD SCENARIOS AND PRACTICAL IMPLEMENTATIONS

Below are some case studies and practical implementations of Blockchain and QML in securing SWMS.

8.1. Barcelona’s smart water network

Mondal [4] highlights Barcelona as a leading city in applying AI and IoT to smart water management. The city uses an extensive network of IoT sensors throughout its water distribution system to monitor consumption, detect leaks, and maintain water quality. AI models analyze real-time sensor data to optimize water flow, detect and address leaks early, and uphold quality standards. Through these integrated technologies, Barcelona has cut water losses by 25% and improved distribution efficiency by 30%.

8.2. Singapore’s intelligent water grid

Mondal [4] reported that Singapore’s Public Utilities Board (PUB) operates an intelligent water grid that uses AI and IoT to manage the nation’s water resources. The system uses IoT sensors, cloud-based analytics, and AI models to track consumption, predict demand, and optimize distribution, enabling the city to maintain a reliable and sustainable water supply while minimizing waste. It also monitors water quality in real time to detect contaminants and ensure safety. With AI-driven predictive analytics, the PUB anticipates peak-period demand and allocates resources efficiently.

8.3. SWMS in a state university in the Philippines

Austria and Lacbay [13] developed a SWMS for a Philippine university that integrates IoT sensors, machine learning, and real-time monitoring to optimize water use and reduce waste. The system employs predictive maintenance, demand forecasting, and leak detection to address inefficiencies, prevent service disruptions, and adapt to evolving campus needs. Despite financial constraints, technical complexity, and coordination challenges, it delivers notable advantages, including cost savings, better resource allocation, and stronger sustainability performance. By providing data-driven predictions and anomaly detection, the machine learning components improve planning accuracy, helping the university advance its goals for technological innovation and environmental stewardship while offering a scalable model for sustainable water management in educational settings.

8.4. AI-IoT-based SWMS for smart city and rural development

Chittesh and Sathiyapriya [19] developed an AI-IoT–based SWMS that supports both urban and rural applications. IoT sensors monitor flow, pressure, quality, and water levels across sources, reservoirs, pipelines, and irrigation systems, transmitting data through LoRaWAN and 5G to a cloud platform for analysis. AI models predict consumption patterns, detect leaks and contaminants, and optimize distribution by combining real-time sensor inputs with climate data. In rural areas, soil-moisture sensing and AI-driven analytics improve irrigation efficiency and reduce water use. The system also strengthens community participation by providing tools that enable stakeholders to report issues, receive alerts, and access system information. Although it enhances water efficiency, reduces waste, and improves irrigation outcomes, successful deployment depends on managing implementation costs, ensuring data security, and maintaining reliable connectivity in remote areas.

8.5. A virtual cybersecurity department (VCD) for securing digital twins in water distribution systems

Homaei et al. [34] introduce a VCD to secure Digital Twins in water distribution systems, offering an affordable, automated solution tailored for small and medium-sized enterprises (SMEs). The VCD employs open-source tools, using Zabbix proxies deployed on Raspberry Pi units to collect real-time data from SCADA, PLCs, and IoT sensors, along with Suricata for intrusion detection, Fail2Ban for blocking repeated login attempts, and simple firewall configurations. Building on this framework, it integrate a machine-learning-based IDS trained on the OD-IDS2022 dataset using an enhanced ensemble model to strengthen threat detection. It evaluated the system with simulated attacks, including port scanning, SSH brute-force attempts, and DoS attacks, and consistently generated accurate alerts, logs, and IP-blocking actions. The model detects threats such as brute-force attacks, remote code execution, and network flooding with 92% accuracy and reduced false alarms, providing SMEs with a practical, low-cost, and easy-to-manage cybersecurity solution for water systems.

8.6. Blockchain-enabled IoT-based water management system for smart cities

Chowdhary et al. [38] developed a Blockchain-enabled IoT model that delivers a consistent and transparent water management system for smart city residents. IoT devices monitor real-time water consumption patterns, including flow rates, water level, pH, turbidity, and total dissolved solids, while Blockchain secures these measurements in an immutable ledger. By combining IoT with Blockchain, the system enhances water conservation, operational efficiency, and consumer satisfaction. It offers reliable and secure data storage, efficient information transmission, and strong traceability of water quality issues. However, integrating Blockchain with IoT in water management still faces challenges, including limited interdepartmental data sharing, unresolved legal considerations, and the absence of standardized frameworks.

8.7. Predicting water quality using QML: The case of the Umgeni catchment (U20A) study region

Khan et al. [141] applied QML techniques to predict water quality in the U20A region of the Umgeni Catchment in Durban, South Africa. They implemented both QSVC and QNN models, finding that QSVC was easier to implement and achieved higher accuracy. For QSVC, they tested linear, polynomial, and radial basis function (RBF) kernels and observed identical performance between the polynomial and RBF kernels. For QNN, they explored various optimizers, learning rates, circuit noise, and weight initializations, but the model consistently encountered the dead neuron problem. Consequently, they compared QNN performance only in terms of accuracy and loss, showing that the Adam optimizer yielded the best results, though it still underperformed QSVC.

8.8. A hybrid Blockchain-IPFS solution for secure and scalable data collection and storage for smart water meters

Nododile and Nyirenda [155] designed a hybrid Blockchain-IPFS model to improve storage efficiency, boost throughput, and shorten block times by offloading large amounts of data to IPFS while maintaining on-chain integrity. They developed a substrate-based private Blockchain to store smart water meter data and conducted controlled experiments comparing Blockchain performance with and without IPFS. They analyzed key metrics, including block size, block time, and transaction throughput, across different data volumes and node counts. The results demonstrate that integrating IPFS significantly reduces on-chain storage requirements, producing smaller block sizes, higher throughput, and faster block times. These findings underscore the effectiveness of hybrid Blockchain-IPFS systems for securely managing large-scale IoT data.

8.9. Blockchain application in sustainable smart water and wastewater management

Afzal and Hassan [247] examine how integrating Blockchain, IoT, and machine learning can strengthen urban water systems by improving transparency, data integrity, and operational efficiency. Blockchain ensures secure, tamper-resistant records, while IoT devices deliver real-time information on water quality and flow, and machine learning models optimize distribution and enable predictive maintenance. Together, these technologies help cities address water scarcity, pollution, and inefficient allocation, as illustrated by cases such as Cape Town’s drought and the Flint water crisis. Their study underscores the economic, environmental, and social value of adopting these innovations to build resilient, sustainable water and wastewater infrastructure capable of withstanding pressures from population growth and climate change.

8.10.Blockchain-enabled water quality monitoring

Thuy et al. [248] demonstrate that integrating Blockchain with IoT-enabled sensing networks can overcome major weaknesses in traditional water quality monitoring (WQM). Blockchain’s decentralized, tamper-resistant ledger strengthens data integrity, transparency, traceability, and automated compliance. Case studies in Tunisia, Taiwan, and Colombia illustrate how hybrid on-chain/off-chain architectures with oracle-based validation mitigate “garbage-in, garbage-out" risks, prevent Sybil attacks, and handle high-frequency sensor data without congestion. By securing validated, real-time measurements, Blockchain enables faster contamination detection, more accountable water governance, and smart-contract-driven alerts and regulatory enforcement. Current evidence indicates that Blockchain-enabled WQM supports adaptive governance, enhances public trust, and empowers stakeholders through transparent access to information, thereby providing a robust digital foundation for sustainable water management in both urban and rural settings.

8.11. Smart water governance with Blockchain technology: Blockchain water management

Banerjee [249] explores how Blockchain can transform water management by enabling secure, transparent, and efficient processes. The technology records water-related data, such as usage, quality, and distribution, in a tamper-proof ledger, reducing inefficiencies and strengthening trust among stakeholders.

8.12. Blockchain technology for sustainable management of electricity and water consumption

Alrammal et al. [250] present a Blockchain-based system for managing electricity and water services that connects multiple entities through smart contracts to automate processes and ensure transparent, secure transactions. The system incorporates three dashboards that streamline service management and provide a shared digital ledger to enhance trust among stakeholders. A mobile application enables users to view and pay bills, monitor consumption, and conduct secure online transactions while maintaining privacy. The solution also supports environmental sustainability by reducing paper usage, promoting energy-efficient equipment, and improving resource management. The study concludes with a meta-analysis of related work to underscore the significance of their approach.

8.13. A Blockchain-based framework for efficient water management and leakage detection in urban areas

Naqash et al. [251] present a Blockchain-based water management architecture that leverages IoT sensors to authenticate and share real-time data with a water distribution dashboard, thereby improving reporting accuracy and enabling effective leakage detection in urban systems. By ensuring the reliability and integrity of sensor data, the framework supports informed decision-making, efficient resource allocation, and more sustainable water distribution. Its modular API further enables leakage detection and flow control, reducing waste. While the approach offers significant potential to enhance the sustainability and resilience of urban water systems, its implementation remains complex and requires continued research and stakeholder collaboration.

8.14. An AI-driven cyber-physical testbed for intelligent water systems

Batarseh et al. [252] introduce AI & cyberbiosecurity for water & agriculture (ACWA), a cyber-physical testbed designed to test, simulate, and evaluate advanced technologies, including AI and cybersecurity solutions, for intelligent water systems. Motivated by the need to modernize water-resource management, ACWA targets challenges such as cyberbiosecurity, resource optimization, water accessibility, sustainability, and data-driven decision-making. The testbed integrates diverse components, including multiple topologies, sensors, computational nodes, pumps, tanks, smart water devices, databases, and AI models. The ACWA simulator complements it, a software-based digital twin that uses fluid and constituent-transport principles to generate theoretical time series for comparison with real measurements from the physical system.

9. CHALLENGES AND LIMITATIONS

Integrating Blockchain and QML into SWMS enhances security, efficiency, and scalability, but this convergence poses significant challenges that require careful resolution for successful implementation. Below is a detailed description of those challenges and limitations.

9.1. Scalability of Blockchain in high-volume IoT environments

Blockchain's limited transaction throughput and latency create significant constraints for SWMS that rely on large-scale IoT deployments [147][155][253]. Conventional consensus mechanisms, such as PoW, process only a small number of transactions per second, causing bottlenecks when millions of sensor readings, such as flow rate, water quality, pressure, and leak data, need continuous recording. These delays impede real-time monitoring, anomaly detection, and automated leak response, while the expanding ledger places an additional burden on resource-constrained devices. Although lightweight approaches like PoS, DPoS, and PoA reduce energy consumption, they can compromise decentralization and trust [147][253]. As networks grow, devices struggle to maintain full nodes, satisfy storage and synchronization requirements, and supply high-quality data for QML models. Integrating Blockchain with QML, therefore, requires optimizing throughput, lowering consensus overhead, reducing latency, and addressing device limitations to support secure and efficient processing across heterogeneous IoT environments.

9.2. Data privacy concerns

Integrating Blockchain and QML into SWMS introduces substantial data privacy risks, as these systems continuously collect sensitive information, including household consumption patterns, industrial usage, and infrastructure parameters. While Blockchain enhances transparency, immutability, and decentralized storage, it can also expose private data to all network participants, complicating compliance with regulations like the General Data Protection Regulation (GDPR) [34]. QML enables advanced analysis of complex datasets but also introduces additional vulnerabilities, as adversaries may use inversion or membership inference attacks to reconstruct private information. Although methods such as differential privacy, homomorphic encryption, and federated learning can reduce these risks, they often come with trade-offs, including reduced model accuracy, higher computational overhead, and limited compatibility with quantum algorithms.

9.3. Integration complexity with legacy systems

Integrating Blockchain and QML into SWMS poses significant technical, operational, and organizational challenges, particularly when interfacing with legacy SCADA systems, PLCs, and proprietary protocols that lack the computational power, storage, and networking capacity required for cryptographic operations and advanced analytics [254]. Incompatible data formats, limited bandwidth, and heterogeneous devices can introduce latency, create data silos, and expose security vulnerabilities [39][255]. Successful implementation demands hardware upgrades, middleware development, staff training, and strict compliance with regulatory requirements. The scarcity of interdisciplinary expertise in quantum computing, Blockchain, and water management further hinders adoption. Without carefully planned hybrid or phased deployment strategies, these integrations risk disrupting operations, compromising reliability, and undermining the resilience they are intended to strengthen [255].

9.4. High computational and energy costs

Integrating Blockchain and QML into SWMS significantly increases computational and energy demands, challenging both scalability and sustainability. Blockchain consensus mechanisms, including PoW and alternatives such as state machine replication and consortium Blockchains, consume substantial processing power to validate transactions, maintain distributed ledgers, and secure the network, thereby straining resource-limited IoT devices [256]. Meanwhile, QML algorithms for anomaly detection and demand forecasting require specialized quantum hardware, error correction, and hybrid quantum–classical setups, further raising computational and energy costs [256]. Storing and processing QML-derived insights on the Blockchain generates high transaction volumes, and real-time monitoring adds additional pressure on system resources, increasing operational expenses, shortening device lifespan, and raising environmental concerns, which could hinder large-scale deployment of Blockchain–QML-enabled SWMS.

9.5. Limited availability of quantum hardware

Quantum hardware’s limited availability and early developmental stage constrain the practical deployment of Blockchain and QML for securing SWMS. Most quantum computers operate under the NISQ paradigm, offering few qubits, short coherence times, high error rates, and limited connectivity, which restrict the complexity, reliability, and scalability of QML algorithms and quantum-secure Blockchain protocols. Integrating QML with Blockchain further increases computational demands, while cloud-based access to proprietary devices introduces latency, cost, and data privacy concerns. Current hybrid approaches that rely on simulators before executing tasks on quantum backends fail to exploit QML and pose significant synchronization challenges. Moreover, deploying quantum solutions requires significant investment in hardware, research, and training, limiting widespread adoption. Until fault-tolerant processors, broader hardware access, and standardized integration protocols become available, Blockchain-QML frameworks in SWMS will remain largely experimental and confined to small-scale or pilot implementations [255].

9.6. Lack of standardization

The effective deployment of Blockchain and QML to secure SWMS is constrained by the lack of standardized frameworks, protocols, and interoperability guidelines [254]. SWMS produce heterogeneous data from diverse sensors and devices, but the absence of standard data models and communication protocols complicates data fusion, real-time monitoring, and advanced analytics. Integrating Blockchain and QML with existing infrastructure is further hindered by disparate protocols, legacy systems, and varying hardware architectures, which create data silos, limit scalability, and increase complexity [39][257]. Inconsistent security practices and access controls also compromise the Blockchain's immutability and the reliability of QML-based anomaly detection [39][257]. The scarcity of standardized benchmarks, regulatory guidance, and real-world deployments slows adoption and generates uncertainty for stakeholders [39].

9.7. Regulatory and compliance challenges

Implementing Blockchain and QML in SWMS presents significant regulatory and compliance challenges, as both technologies and the legal frameworks governing water management, data privacy, and digital infrastructure are rapidly evolving. Existing regulations focus on water quality, safety, and accessibility, but rarely address advanced digital technologies, creating uncertainty for utilities and technology providers [39][55][107]. The decentralized nature of Blockchain and the data-intensive operations of QML complicate issues of data ownership, user consent, privacy, and cross-jurisdictional compliance, particularly under laws such as GDPR [55][107]. Rapid technological advances outpace regulatory development, creating gaps in policies for automated decision-making, decentralized architectures, and smart contracts, and raising ambiguities in liability and accountability [55][107]. Ethical and governance concerns demand mechanisms to ensure transparency, explainability, and responsible AI use in critical infrastructure.

9.8. Cybersecurity risks

Implementing Blockchain and QML in SWMS introduces significant cybersecurity risks despite their inherent security features. Attackers can exploit smart contract vulnerabilities or weaknesses across Blockchain layers, while QML models remain susceptible to data poisoning, adversarial inputs, and inference attacks [258]. Limited IoT device resources, legacy infrastructure integration, and complex system interactions expand the attack surface, making the system only as secure as its weakest component. Key threats include quantum attacks on cryptographic systems, compromised keys, misconfigured consensus or smart contract mechanisms, and supply-chain or side-channel attacks on hardware [175]. Immutable Blockchain logs can preserve malicious data, amplifying the effects of poisoning and complicating remediation, and real-time operational demands force trade-offs between security and availability. Interoperability challenges, insider threats, immature defenses, and cascading failures further exacerbate vulnerabilities, as compromises in data, models, or on-chain actions can propagate through the system and trigger incorrect control actions or physical damage.

9.9. Quantum algorithm development

Developing quantum algorithms for SWMS faces significant technical challenges due to the field's complexity, immaturity, and interdisciplinary demands [255][259]. QML can accelerate data processing and improve predictive modeling, but practical implementation requires expertise in quantum mechanics, machine learning, cryptography, and water management. Researchers must design scalable algorithms that handle large, heterogeneous SWMS datasets, integrate with Blockchain protocols and IoT devices, and mitigate errors [175][176]. Noise and decoherence in current quantum hardware necessitate hybrid quantum-classical models and error-correction techniques, yet standardized solutions remain limited. Moreover, immature development frameworks and the opacity of QML models complicate testing, reproducibility, and stakeholder trust. Overcoming these obstacles is crucial to applying QML effectively for secure, real-time SWMS monitoring and decision-making.

9.10. Data quality and integrity

High data quality and integrity are essential for implementing Blockchain and QML in SWMS because the reliability of IoT sensor data directly affects predictive performance and operational decisions [34]. SWMS gather heterogeneous data from sensors, actuators, and SCADA systems, such as flow rates, pressures, chemical concentrations, and consumption patterns, that often contain noise, missing values, or inconsistencies. Without real-time validation and anomaly detection, erroneous or malicious data can enter the system. While Blockchain provides immutability and traceability, it cannot correct poor-quality data once recorded, and QML models amplify the impact of even small perturbations. Integrating diverse datasets further complicates alignment of formats, units, and temporal resolutions, and scaling validation across city-level networks increases computational demands [260]. Therefore, SWMS must implement robust mechanisms, including sensor fusion, real-time cleansing, intelligent consensus protocols, and automated validation, to ensure that only trustworthy, high-fidelity data feeds the Blockchain-QML framework, balancing timeliness with integrity to support accurate and reliable decision-making [260].

9.11. Stakeholder engagement and trust

Building trust among stakeholders is essential for adopting Blockchain and QML in SWMS, but several challenges hinder this process [247]. Non-technical stakeholders may hesitate or resist due to the complexity of integrating these technologies. At the same time, privacy concerns and data-sharing constraints can limit access to the high-quality data needed for accurate predictions [261]. Although Blockchain ensures data integrity and tamper-proof records, and QML enhances predictive analytics and anomaly detection, stakeholders may still question their reliability, interpretability, and ethical use [39]. Coordinating municipal authorities, utility providers, regulators, technology vendors, and end-users adds further complexity, as differing priorities can impede consensus and system alignment. Limited real-world deployments and external factors such as security incidents or market volatility can further erode confidence. Overcoming these barriers requires clear communication, participatory design, capacity building, and robust governance to ensure stakeholders understand, trust, and actively engage with Blockchain-QML frameworks in SWMS.

9.12. Resource constraints in developing regions

Implementing Blockchain and QML in SWMS in developing regions faces significant challenges due to resource constraints that limit feasibility, scalability, and sustainability [247]. High upfront and operational costs for hardware, sensors, connectivity, and computational resources often exceed the budgets of local water utilities and communities

[55][107]. Unreliable power supplies, low-bandwidth networks, and underdeveloped data centers hinder real-time data collection, processing, and secure storage, which are necessary for Blockchain and QML operations [55][209]. A shortage of skilled personnel in digital technologies, water management, and cybersecurity complicates system deployment and maintenance, increasing the risk of performance and security issues [55][107]. Interoperability challenges from diverse IoT devices and the lack of standardized protocols further impede seamless data exchange and raise costs [55][107]. To address these barriers, SWMS in developing regions require low-cost, energy-efficient, and context-appropriate technologies, such as edge computing and long-range, low-power networks, to ensure effective and sustainable deployment [209][268].

9.13.Ethical and social implications

Integrating Blockchain and QML into SWMS enhances data security, transparency, and operational efficiency, but it also introduces significant ethical and social challenges [55]. SWMS handle large volumes of sensitive water usage and quality data, making privacy, informed consent, and data ownership critical concerns [55][69][107]. The high computational demands and technical complexity of these technologies may disadvantage resource-constrained communities and exacerbate digital inequities. The opacity of QML models and the decentralized structure of Blockchain can reduce transparency and accountability, while biases in training data may perpetuate social or environmental inequities [107][153]. Energy-intensive operations raise environmental sustainability concerns, and the lack of adaptive legal and regulatory frameworks complicates responsible deployment. To foster public trust and ensure fair, effective adoption, stakeholders must implement technical safeguards, inclusive governance, proactive community engagement, regulatory oversight, and mechanisms that guarantee transparency, equity, and sustainability [55][107][153].

9.14.Latency and real-time processing

Integrating Blockchain and QML into SWMS enhances data integrity, security, and predictive capabilities but introduces significant latency that can impede real-time operations [34]. Blockchain consensus mechanisms—whether PoW, PoS, or lightweight IoT-focused protocols—delay transaction validation and propagation, slowing anomaly detection and response to events such as leaks or contamination [34][39]. QML algorithms, including hybrid quantum-classical models, require extensive preprocessing, data encoding, and iterative optimization, further delaying decision-making [69][209][234]. Coordinating QML with Blockchain compounds these delays, as models must access, decode, and process data from the distributed ledger. These combined latencies strain IoT devices, limit throughput, and challenge system scalability, complicating timely responses to pressure anomalies or abnormal consumption patterns. To balance security, predictive accuracy, and real-time responsiveness, SWMS must optimize Blockchain protocols for IoT, leverage edge computing, and adopt asynchronous or lightweight quantum-classical models.

10. FUTURE RESEARCH DIRECTIONS

The integration of Blockchain and QML into SWMS offers a transformative path toward more secure, efficient, and sustainable water management. Future research should outline a clear roadmap for advancing work at the intersection of these technologies and their application in SWMS. Below are the brief descriptions of the future research directions for the study:

10.1.Quantum-enhanced Blockchain consensus mechanisms

Quantum-resistant consensus algorithms are critical for securing Blockchain-based SWMS against emerging quantum threats. As quantum computers advance, they threaten to break classical cryptographic schemes, highlighting the need for quantum-safe alternatives [259]. Quantum-enhanced consensus mechanisms exploit superposition, entanglement, and quantum key distribution to strengthen security, improve efficiency, and support scalability in large IoT-driven SWMS. Techniques such as quantum PoW, quantum-assisted Byzantine fault tolerance, and Quantum DPoS accelerate block validation, enhance fault tolerance, mitigate attacks, including 51% attacks, and reduce energy and computational overhead. Quantum zero-knowledge proofs and quantum-generated randomness further bolster fairness, privacy, and resistance to coordinated malicious behavior. Although current quantum consensus algorithms remain vulnerable to noise, decoherence, and hardware limitations, they are well-suited for small-scale or hybrid classical-quantum deployments. Progress in this field requires developing lightweight, trustless, privacy-preserving quantum protocols for SWMS and validating them on quantum simulators and early quantum hardware to assess their practicality and performance.

10.2.QML for predictive water quality monitoring

QML offers a fast, accurate, and scalable approach to predictive water-quality monitoring in SWMS by exploiting quantum principles, such as superposition and entanglement, to accelerate computations over complex, high-dimensional datasets [262]. Techniques including QSVM, QNN, variational quantum algorithms, and QAOA-based methods enable real-time detection of contaminants, forecasting of water-quality parameters, and rapid responses to dynamic conditions, surpassing conventional machine learning models in handling large, high-velocity sensor streams. Integrating QML with Blockchain further strengthens SWMS by securing data, enabling decentralized validation of predictions, and supporting privacy-preserving federated analytics across utilities. Future research should advance quantum algorithms, develop hybrid QML-Blockchain architectures, and design resource-efficient deployment strategies to provide reliable, cost-effective monitoring in both urban and rural settings [209].

10.3. Blockchain-enabled real-time data integrity in SWMS

Integrating Blockchain into SWMS creates a decentralized, tamper-resistant framework that ensures real-time data integrity across distributed water networks [248]. Recording sensor readings, operational metrics, and water quality data as immutable, cryptographically linked transactions prevents unauthorized modifications, mitigates single points of failure, and strengthens device-level authentication. Smart contracts validate data, while hybrid on-chain/off-chain architectures enhance scalability in high-volume, low-latency environments. These secure, verifiable data streams improve predictive analytics and QML models for leak detection, demand forecasting, and contamination monitoring, enabling real-time monitoring, automated alerts, and responsive maintenance [34][39][155]. Despite these advantages, interoperability, performance optimization, and large-scale deployment challenges underscore the need for standardized protocols, hybrid consensus mechanisms, and empirical validation through real-world implementations.

10.4. Quantum-driven optimization of water distribution networks

QML and quantum-driven optimization provide a robust framework for enhancing SWMS by efficiently tackling the combinatorial complexity, real-time performance demands, and security requirements of large-scale water networks [259]. By formulating tasks such as pump scheduling, leak detection, demand forecasting, pressure regulation, and network reconfiguration as optimization problems, quantum annealing, QAOA, and quantum-inspired algorithms can rapidly explore large solution spaces to allocate resources optimally, detect anomalies faster, and improve demand predictions. When combined with AI and digital twins, these techniques enable predictive analytics, scenario simulation, and adaptive control, enhancing energy efficiency, reliability, and water quality [77][186]. Integrating Blockchain further secures optimization decisions through tamper-resistant smart contracts, strengthening resilience against cyber-physical threats. Nonetheless, limitations in current quantum hardware, the need for scalable hybrid frameworks, and challenges in achieving low-latency Blockchain integration remain key research priorities for deploying quantum-enhanced SWMS in dynamic urban environments.

10.5. Hybrid Blockchain-quantum systems for secure SWMS

Hybrid Blockchain–quantum systems strengthen the security, scalability, and efficiency of SWMS by combining Blockchain's decentralized, tamper-resistant data management with quantum-enhanced computation and cryptography [263]. They use post-quantum cryptographic algorithms to protect sensor and operational data from quantum attacks, apply QML to improve predictive analytics for leakage detection and infrastructure failures, and implement quantum-assisted consensus mechanisms to accelerate block validation and reduce energy consumption. By supporting secure data exchange across distributed IoT devices and hybrid on-chain/off-chain storage for high-volume sensor data, these systems enhance real-time monitoring and decision-making while maintaining data integrity [37][155][176]. Key research challenges involve developing standardized interoperability frameworks, validating system performance through real-world deployments, and creating quantum-aware consensus protocols and smart contracts that leverage quantum capabilities to enhance the resilience and efficiency of SWMS operations [39][155].

10.6. Quantum algorithms for anomaly detection in water systems

Quantum algorithms offer a powerful approach for efficient, high-precision anomaly detection in SWMS by rapidly analyzing large volumes of high-dimensional sensor data to identify leaks, contamination, unauthorized use, or cyberattacks [34]. Methods such as QSVM, QPCA, VQCs, quantum clustering, quantum normalizing flows, and quantum density estimation enhance pattern recognition, multivariate modeling, and change-point detection, enabling the sensitive detection of subtle or emerging anomalies. When integrated with Blockchain frameworks, these algorithms strengthen system security by ensuring data integrity, supporting decentralized alert dissemination, and enabling privacy-preserving collaboration through quantum-enhanced federated learning. Future research should develop hybrid quantum–classical pipelines, optimize data-encoding strategies, improve robustness in noisy sensor environments, and incorporate post-quantum-secure Blockchain mechanisms to deliver resilient, tamper-proof anomaly detection in real-world SWMS deployments.

10.7. Blockchain-based smart contracts for automated water management

Blockchain-based smart contracts offer a powerful tool for automating and securing water management in emerging Blockchain–QML–enabled SWMS. By embedding allocation rules, billing procedures, and compliance requirements directly on the Blockchain, these contracts execute actions transparently and immutably without intermediaries. When combined with IoT sensors, they can monitor consumption, regulate distribution, and incentivize conservation through tokenized mechanisms. Integrating QML enhances predictive and adaptive capabilities, supporting optimized resource allocation, anomaly detection, and proactive fault mitigation. Applications across urban water supply, wastewater treatment, and precision agriculture illustrate how smart contracts boost efficiency, accountability, and stakeholder trust [39][165]. Future research should address scalability, interoperability with existing infrastructure, quantum-secure contract design, regulatory compliance, and the development of user-friendly tools for non-expert deployment and customization.

10.8. QML for climate impact modeling

QML can significantly improve climate impact modeling in SWMS by efficiently processing large, heterogeneous environmental datasets with greater accuracy than classical methods [81]. By leveraging quantum principles such as superposition and entanglement, QML algorithms, including QNNs, QSVMs, and VQCs, capture complex nonlinear interactions among climate variables, hydrological processes, and human activities, enabling precise forecasts of rainfall, droughts, floods, water demand, emissions, and pollution. Quantum parallelism accelerates simulations of multiple climate scenarios, allowing SWMS to anticipate extreme events and optimize operations in real time. Integrating QML with Blockchain enhances data integrity and transparency while enabling secure, automated resource allocation through smart contracts. This combined approach offers scalable solutions for managing urban, agricultural, and industrial water networks. However, further advances in quantum hardware, hybrid quantum–classical models, generalization, explainability, and seamless integration with IoT are essential [264].

10.9. Decentralized water management systems using Blockchain

Blockchain-enabled decentralized water management systems distribute control and data among stakeholders, enhancing transparency, reducing corruption, and fostering community participation. As urban water networks grow more complex due to population pressures and climate variability, these systems optimize distribution, monitoring, and treatment while maintaining resilience. They record water usage, quality metrics, sensor data, and maintenance activities on an immutable ledger spanning treatment units, reservoirs, pumping stations, and smart meters. Smart contracts automate allocation, billing, leakage detection, water trading, and conservation incentives. Integrating quantum machine learning further improves predictive capabilities for anomaly detection, demand forecasting, contamination prediction, and maintenance, all based on verified Blockchain data. However, challenges remain in scalability, interoperability with legacy systems, quantum-resilient security, privacy-preserving data sharing, user interface design, and regulatory compliance, highlighting the need for real-world pilots to validate performance and feasibility [39][153].

10.10. Quantum-enhanced data compression for IoT in SWMS

Quantum computing can significantly improve data compression for IoT devices in SWMS, reducing bandwidth and storage demands while enabling secure, real-time analytics [259]. By applying QML techniques such as quantum autoencoders and QPCA, SWMS can encode high-dimensional sensor data, including water quality, flow, pressure, and consumption, into compact representations that retain essential information. This quantum-enhanced compression reduces storage load on distributed ledgers, optimizes network bandwidth, and lowers energy consumption, while quantum-safe encryption preserves data integrity and security. Integrating compressed data with Blockchain enables secure, immutable transmission while supporting scalable, AI-driven analytics for predictive maintenance, anomaly detection, and adaptive water management. Future research should develop hybrid quantum-classical compression frameworks, tailor quantum autoencoder architectures for SWMS datasets, and integrate them seamlessly with Blockchain and QML analytics to address hardware limitations and enable real-world deployment.

10.11. Blockchain for water rights and usage verification

Blockchain technology can revolutionize SWMS by offering a decentralized, transparent, and tamper-proof platform for managing water rights and monitoring usage. Recording rights, transactions, and consumption data on an immutable ledger ensures accountability, reduces disputes, and enables real-time enforcement through smart contracts. Tokenizing water rights allows transparent trading and adaptive allocation, while integration with IoT devices provides accurate, real-time information on flow, quality, and usage [39][167]. Incorporating QML enhances predictive analytics, optimizes distribution, and detects unusual patterns to prevent misuse. Practical applications include automated permit issuance, usage monitoring via unique digital IDs, and stakeholder engagement through decentralized governance [37][39][167]. Future research should prioritize developing interoperable frameworks that combine Blockchain with existing infrastructure and QML, addressing scalability and regulatory challenges, and establishing standardized protocols for secure, privacy-conscious, and large-scale SWMS deployment [37][39].

10.12. QML for water demand forecasting

QML enhances water demand forecasting in SWMS by efficiently processing high-dimensional data from smart meters, sensors, and environmental monitoring systems [262]. Exploiting quantum phenomena such as superposition, entanglement, and parallelism, QML algorithms, including QNN, QSVM, and variational quantum algorithms, identify complex temporal and spatial consumption patterns, accelerate model training, and surpass classical methods like LSTM and hybrid neural networks in predictive accuracy [69][186]. Integrating QML with Blockchain secures data exchange, ensures transparency, and enables decentralized model training, protecting sensitive information while maintaining auditability. Future research should focus on developing quantum-enhanced models for time-series water demand prediction, scaling QML for real-time city-wide analytics, and incorporating explainable outputs with uncertainty quantification to support operational planning, anomaly detection, and adaptive resource allocation, thereby improving efficiency, resilience, and sustainability in urban water networks [69][186].

10.13. Integration of Blockchain and QML in flood risk management

Integrating Blockchain with QML transforms flood risk management in SWMS by securing data, improving predictive accuracy, and enabling real-time decision-making [221]. Blockchain establishes a decentralized, tamper-resistant ledger that ensures transparency and traceability of flood-related data from IoT sensors, drones, and meteorological stations. At the same time, smart contracts automate alerts, resource allocation, and insurance processes [39]. QML rapidly analyzes high-dimensional environmental data, uncovering complex patterns to enhance flood prediction, anomaly detection, and risk assessment [266]. Together, these technologies allow SWMS to share and verify data across distributed nodes, conduct real-time risk assessments, and trigger automated responses based on predictive models, fostering trust and collaboration among government agencies, utilities, insurers, and communities. Future research should focus on developing scalable, interoperable frameworks, adapting QML models to hydrological data, establishing standards for data sharing and smart contract execution, and conducting pilot studies to validate operational benefits [39].

10.14. Blockchain for water quality data sharing across jurisdictions

Blockchain can transform SWMS by enabling secure, transparent, and interoperable sharing of water quality data across jurisdictions [248]. Decentralized, tamper-proof ledgers provide municipalities, regulatory agencies, research institutions, and the public with consistent, verifiable information from IoT sensors, treatment plants, and monitoring stations [39]. Smart contracts automate access control, data validation, and compliance checks, while cryptographic techniques safeguard sensitive information. By standardizing data formats and protocols, Blockchain supports seamless integration across diverse monitoring systems, facilitates real-time anomaly detection and early warnings, and strengthens accountability by identifying responsible parties in cases of pollution or data manipulation. Future research should focus on scaling high-frequency, real-time data, optimizing costs, establishing universal interoperability standards, integrating advanced analytics, such as QML, to enable predictive and privacy-preserving insights, and validating these frameworks through cross-jurisdictional pilot deployments to ensure practical effectiveness and resilience [39].

10.15. QML for water treatment process optimization

QML is revolutionizing the optimization of complex water treatment processes by leveraging quantum properties, such as superposition and entanglement, to analyze high-dimensional datasets [262] efficiently. In SWMS, QML models nonlinear relationships among operational parameters, water quality indicators, and process outcomes, enabling accurate predictions and adaptive control of pH, chemical dosing, filtration rates, and energy consumption [228]. Quantum-classical hybrid algorithms, including QCL and QAOA, accelerate model training, support real-time anomaly detection, and enhance predictive maintenance of pumps, valves, and treatment units, even on NISQ devices [209][228]. When integrated with Blockchain, QML-driven analytics strengthen data integrity, traceability, and secure automated decision-making, promoting resilient and sustainable water networks [209]. Future research should prioritize developing low-depth, noise-resilient hybrid models, scalable real-time optimization, secure Blockchain-QML integration, and standardized benchmarks to enable practical deployment of intelligent, safe, and energy-efficient SWMS [209][228][267].

11. CONCLUSION

This scoping review examines how integrating Blockchain and QML can enhance the security, reliability, and efficiency of SWMS. Traditional water infrastructure faces critical challenges, including data breaches, unauthorized access, and operational inefficiencies, that can compromise water quality, distribution, and resource allocation. The study analyzed recent advancements to explore how Blockchain and QML address these vulnerabilities. Blockchain provides decentralized, tamper-resistant data management, ensuring transparency, traceability, and integrity. QML delivers advanced predictive analytics for real-time anomaly detection, enabling intelligent decision-making in complex, high-dimensional water networks.

Combining Blockchain and QML creates a synergistic effect. Blockchain secures and audits data, while QML drives precise, data-driven operations. Together, they reduce cyber-attack risks and prevent unauthorized data manipulation, improving both cybersecurity and operational efficiency. However, practical implementations remain limited by computational demands, scalability constraints, energy consumption, and the need for specialized infrastructure. Other challenges include interoperability with legacy systems and compliance with regulatory requirements, both of which must be addressed for widespread adoption.

Future research should focus on optimizing QML models for low-latency water networks and developing lightweight Blockchain protocols suitable for IoT environments. Pilot studies deploying hybrid Blockchain-QML architectures in municipal water systems can validate their feasibility and performance. Cross-disciplinary collaboration among quantum computing experts, cybersecurity researchers, and water system engineers will be crucial to translating theoretical concepts into practical solutions. Establishing standardized evaluation frameworks can help quantify security, efficiency, and environmental impact.

In conclusion, integrating Blockchain and QML offers a transformative approach to smart water management. This convergence strengthens resilience against cyber threats, enhances data-driven operations, and improves the trustworthiness of water infrastructure. As these technologies mature, their strategic deployment could redefine sustainable and secure urban water management, supporting global water security and efficient resource utilization.

Funding:

No external financial assistance or institutional funding was utilized for conducting this research. The authors assert that all research-related activities were self-financed.

Conflicts of Interest:

The authors declare that there are no competing interests associated with this work.

Acknowledgment:

The authors would like to thank their institutions for their steadfast encouragement and logistical support throughout this research journey.

References

[1] J. Rajanbabu, G. Venkatakrishnan, R. Rengaraj, M. Rajalakshmi, and N. Jayaprakash, "An integrated smart water management system for efficient water conservation," *Int. J. Electr. Comput. Eng. (IJECE)*, vol. 15, no. 1, pp. 635–644, 2025, doi: 10.11591/ijece.v15i1.pp635–644.

[2] V. Slany *et al.*, "Smart Water-IoT: Harnessing IoT and AI for efficient water management," *ACM Comput. Surv.*, vol. 57, no. 12, pp. 1–36, 2025, doi: 10.1145/3744338.

[3] I. Ahamed, M. L. Ali, and N. Salehin, "IoT-based Smart Water Consumption Monitoring System for Residential Complex," in *Proc. 2nd Int. Conf. Inf. Commun. Technol. (ICICT)*, Dhaka, Bangladesh, Oct. 2024, pp. 46–50, doi: 10.1109/ICICT64387.2024.10839689.

[4] P. Mondal, "AI and IoT in smart water management for urban sustainability," *Uncertainty Discourse and Applications*, vol. 1, no. 2, pp. 151–157, 2024, doi: 10.48313/uda.v1i2.36.

[5] A. Abebe, "Internet of Things (IoT) Enabled Water Distribution System for Smart Water Management," *Int. J. Wireless Commun. Mobile Comput.*, vol. 11, no. 1, pp. 1–10, 2024, doi: 10.11648/j.wcmc.20241101.11.

[6] D. D. Olodu, F. Inegbedon, and O. I. Ihenyen, "Smart Water Management Systems: Engineering Innovations for Water Conservation and Distribution," *J. Stud. Adv. Technol.*, vol. 3, no. 1, pp. 13–31, Jun. 2025, doi: 10.63063/jsat.1613583.

[7] Y. Dai, Z. Huang, N. Khan, and M. S. Labbo, "Smart Water Management: Governance Innovation, Technological Integration, and Policy Pathways Toward Economic and Ecological Sustainability," *Water*, vol. 17, no. 13, pp. 1–22, 2025, doi: 10.3390/w17131932.

[8] G. Jeyalakshmi *et al.*, "IoT-Enabled Smart Water Management System using ESP32 and RFID for Urban Applications," in *Proc. Int. Conf. Modern Sustainable Syst. (CMSS)*, Shah Alam, Malaysia, Aug. 2025, pp. 364–369, doi: 10.1109/CMSS66566.2025.11182353.

[9] V. Muthukumar, V. Selvakumar, M. Nalini, and B. Chitradevi, "Cloud-based Smart Water Management System," in *Proc. Int. Conf. Sustainable Comput. Smart Syst. (ICSCSS)*, Coimbatore, India, Jun. 2023, pp. 1633–1638, doi: 10.1109/ICSCSS57650.2023.10169753.

[10] T. A. Syed *et al.*, "Smart Water Management with Digital Twins and Multimodal Transformers: A Predictive Approach to Usage and Leakage Detection," *Water*, vol. 16, no. 23, pp. 1–26, 2024, doi: 10.3390/w16233410.

[11] B. Sridevi *et al.*, "HydroML: AI-Driven Smart Water Management using Hybrid Deep HydroNet (HDH-Net) for Real-Time Monitoring, Anomaly Detection, and Automated Distribution," in *Proc. ICPCSN*, Salem, India, May 2025, pp. 1149–1154, doi: 10.1109/ICPCSN65854.2025.11035397.

[12] M. Chandan, "AI-Powered Smart Water Management Systems: Ensuring Sustainability in Urban Areas," *Int. J. Sci. Res. Eng. Trends*, vol. 11, no. 2, pp. 2076–2080, 2025.

[13] L. Austria and M. Lacbay, "Smart Water Management System in a State University in the Philippines: Challenges and Opportunities," *Latin Am. Bus. Sustain. Rev.*, vol. 2, no. 1, pp. 48–58, 2025, doi: 10.70469/labsreview.v1i2.23.

[14] N. Bawankar, A. Kriti, S. S. Chouhan, and S. Chaudhari, "IoT-Enabled Water Monitoring in Smart Cities With Retrofit and Solar-Based Energy Harvesting," *IEEE Access*, vol. 12, pp. 58222–58238, 2024, doi: 10.1109/ACCESS.2024.3392852.

[15] A. A. Master *et al.*, "IoT-Based Smart Water Management System with Notification and Real-Time Data Analysis," in *Proc. ICRITO*, Noida, India, Mar. 2024, pp. 1–6, doi: 10.1109/ICRITO61523.2024.10522234.

[16] A. A. A. Bakar *et al.*, "IoT-Based Real-Time Water Quality Monitoring and Sensor Calibration for Enhanced Accuracy and Reliability," *Int. J. Interact. Mobile Technol.*, vol. 19, no. 1, pp. 155–170, 2025, doi: 10.3991/ijim.v19i01.51101.

[17] Y. Luo, X. Qian, and Y. Li, "Implementation of a small-scale intelligent water management supervision system," in *Proc. ICCEA*, Hangzhou, China, Apr. 2024, pp. 1588–1593, doi: 10.1109/ICCEA62105.2024.10604215.

[18] G. Rajan and S. Li, "A Systematic Literature Review on Flow Data-Based Techniques for Automated Leak Management in Water Distribution Systems," *Smart Cities*, vol. 8, no. 3, p. 78, 2025, doi: 10.3390/smartcities8030078.

[19] P. Chittesh and P. Sathiyapriya, "AI-IoT Based Smart Water Management System for Smart City and Rural Development," in *Proc. ICETEA*, Puducherry, India, Jun. 2025, pp. 1–5, doi: 10.1109/ICETEA64585.2025.11100005.

[20] K. B. Vignesh and Michael, “Enhanced automation, operation, and management of rural water supply systems using IoT technologies,” *Deleted Journal*, vol. 2, no. 8, pp. 2618–2621, 2024, doi: 10.47392/irjaem.2024.0380.

[21] A. Z. Al-Qaisi, R. A. Ogla, and Z. H. Ali, “Smart Water Systems: The Role of Technology and Engineering in Optimizing Urban Water Resources,” *J. Inf. Syst. Eng. Manage.*, vol. 10, no. 21s, pp. 833–846, 2025.

[22] A. Kumar, J. Saravanan, R. Gowthamraja, and A. S. Babu, “Design and Implementation of Smart Water Management System using IoT Technology,” in *Proc. ICAISS*, Trichy, India, May 2025, pp. 874–881, doi: 10.1109/ICAISS61471.2025.11042079.

[23] N. Raza and F. Moazeni, “Optimal cybersecurity framework for smart water system: Detection, localization and severity assessment,” *Water Res.*, vol. 281, p. 123517, 2025, doi: 10.1016/j.watres.2025.123517.

[24] J. M. Nambundo, O. de Souza Martins Gomes, A. D. de Souza, and R. C. S. Machado, “Cybersecurity and Major Cyber Threats of Smart Meters: A Systematic Mapping Review,” *Energies*, vol. 18, no. 6, p. 1445, 2025, doi: 10.3390/en18061445.

[25] T. Shah and D. Danang, “Optimizing Blockchain-Based Cybersecurity Systems to Strengthen Resilience Against Ransomware Attacks: A Systematic Literature Review,” *Systematic Literature Review Journal*, vol. 1, no. 1, pp. 21–34, 2025, doi: 10.70062/slrj.v1i1.52.

[26] X. Zhao, W. Xing, X. Wang, and N. Zhao, “Stochastic Event-Triggered Feedback Physical Watermarks Against Replay Attacks,” *IEEE Trans. Netw. Sci. Eng.*, vol. 12, pp. 814–822, 2025, doi: 10.1109/TNSE.2024.3519624.

[27] A. A. Albustami and A. F. Taha, “Breaking the flow and the bank: Stealthy cyberattacks on water network hydraulics,” *Water Res.*, vol. 283, pp. 1–16, 2025, doi: 10.1016/j.watres.2025.123719.

[28] F. Tao and D. Ye, “Active Eavesdropping Attack Scheduling for Cyber–Physical Systems With Operation Constraints,” *IEEE Internet Things J.*, vol. 12, pp. 3067–3075, 2025, doi: 10.1109/JIOT.2024.3478312.

[29] A. Mughaid *et al.*, “Simulation-based framework for authenticating SCADA systems and cyber threat security in edge-based autonomous environments,” *Simul. Model. Pract. Theory*, vol. 140, p. 103078, 2025, doi: 10.1016/j.simpat.2025.103078.

[30] N. Singh, R. Buyya, and H. Kim, “Securing Cloud-Based Internet of Things: Challenges and Mitigations,” *Sensors*, vol. 25, no. 1, p. 79, 2025, doi: 10.3390/s25010079.

[31] H. Gattu, J. Karimireddy, and K. G., “DNS Under Siege: Ethical DNS Spoofing and Countermeasures,” *Int. Res. J. Innov. Eng. Technol.*, vol. 9, no. INSPIRE’25, pp. 250–254, 2025, doi: 10.47001/irjiet/2025.inspire40.

[32] A. Sarwath, R. Gulmeher, and Z. Sultana, “Neural Network Model Using An Enhanced Whale Optimization Method For Cyber Threat Detection,” *IRJAEH*, vol. 3, no. 02, pp. 164–171, 2025, doi: 10.47392/irjaeh.2025.0022.

[33] S. Mondal and S. Chakraborty, “TruChain: A Blockchain-based Access Control to Improve the Security of Smart Water Grid Systems,” in *Proc. COMSNETS*, Bengaluru, India, Jan. 2025, pp. 881–885, doi: 10.1109/COMSNETS63942.2025.10885771.

[34] M. Homaei *et al.*, “A Virtual Cybersecurity Department for Securing Digital Twins in Water Distribution Systems,” *arXiv*, pp. 1–7, 2025, doi: 10.48550/arXiv.2504.20266.

[35] W. Rajeh, M. Aborokbah, T. Alashoor, and K. P., “TabNet-SFO: An Intrusion Detection Model for Smart Water Management in Smart Cities,” *Int. J. Intell. Syst.*, pp. 1–17, 2025, doi: 10.1155/int/6281847.

[36] D. Abreu, D. Moura, C. E. Rothenberg, and A. Abelém, “QuantumNetSEC: Quantum Machine Learning for Network Security,” *Int. J. Netw. Manage.*, vol. 35, no. 4, pp. 1–20, 2025, doi: 10.1002/nem.70018.

[37] A. Y. Al-Zoubi, M. Aldmour, A. Khoury, and D. Al-Thaher, “Blockchain of Things for Securing and Managing Water 4.0 Applications,” *Int. J. Online Biomed. Eng.*, vol. 20, no. 11, pp. 4–15, 2024, doi: 10.3991/ijoe.v20i11.50277.

[38] R. Chowdhary *et al.*, “Blockchain Enabled IoT-Based Water Management System for Smart Cities,” *IJERT*, vol. 13, no. 5, pp. 1–4, 2024.

[39] T. K. Satilmisoglu, Y. Sermet, M. Kurt, and I. Demir, “Blockchain Opportunities for Water Resources Management: A Comprehensive Review,” *Sustainability*, vol. 16, no. 6, pp. 1–36, 2024, doi: 10.3390/su16062403.

[40] A. Awasthi, “The Role of Quantum Machine Learning in Cybersecurity,” *IRJMETS*, vol. 07, no. 01, pp. 5223–5228, 2025, doi: 10.56726/IRJMETS66777.

[41] R. I. Minu, G. Nagarajan, J. J., and G. Yamini, “Quantum Machine Learning of Bigdata Set Using Randomized Measurements,” in *Proc. ICCPCT*, Kollam, India, Aug. 2024, pp. 32–35, doi: 10.1109/ICCPCT61902.2024.10673223.

[42] S. Kumar, T. Adeniyi, A. Alomari, and S. Ganguly, “Design of Quantum Machine Learning Course for a Computer Science Program,” in *Proc. QCE*, Bellevue, WA, USA, Sep. 2023, pp. 68–77, doi: 10.1109/QCE57702.2023.20326.

[43] A. Bellante *et al.*, “Evaluating the potential of quantum machine learning in cybersecurity: A case-study on PCA-based intrusion detection systems,” *Computers & Security*, p. 104341, 2025, doi: 10.1016/j.cose.2025.104341.

[44] A. Wicaksana, “A survey on quantum-safe blockchain security infrastructure,” *Comput. Sci. Rev.*, vol. 57, p. 100752, 2025, doi: 10.1016/j.cosrev.2025.100752.

[45] N. J. Okoli and B. Kabaso, “Building a Smart Water City: IoT Smart Water Technologies, Applications, and Future Directions,” *Water*, vol. 16, no. 4, pp. 1–25, 2024, doi: 10.3390/w16040557.

[46] É. Soares Ascenção *et al.*, “Applications of Smart Water Management Systems: A Literature Review,” *Water*, vol. 15, no. 19, p. 3492, 2023, doi: 10.3390/w15193492.

[47] G. Iancu, S. N. Ciolofan, and M. Drăgoicea, “Real-time IoT architecture for water management in smart cities,” *Deleted Journal*, vol. 6, no. 4, pp. 1–19, 2024, doi: 10.1007/s42452-024-05855-9.

[48] A. Marathe, A. Lodha, O. Lolage, P. Lodha, and L. Herald, “Smart Water Management System for Housing Societies,” in *Proc. 2nd Int. Conf. Emerging Trends Eng. Med. Sci. (ICETEMS)*, Nagpur, India, Nov. 22–23, 2024, pp. 457–461, doi: 10.1109/ICETEMS64039.2024.10965023.

[49] N. R. Gayathri, S. Manjula, W. T. Chembian, V. Dhivya, and K. R. A. Dhanunjay, “Smart Water Quality Monitoring and Management System,” in *Proc. Int. Conf. Power, Energy, Control and Transmission Systems (ICPECTS)*, Chennai, India, Oct. 8–9, 2024, pp. 1–4, doi: 10.1109/ICPECTS62210.2024.10780355.

[50] B. Baranitharan *et al.*, “IoT-Based Smart Irrigation Water Management System,” in *Proc. 4th Int. Conf. Sentiment Analysis and Deep Learning (ICSADL)*, Bhimdatta, Nepal, Feb. 18–20, 2025, pp. 496–500, doi: 10.1109/ICSADL65848.2025.10933011.

[51] A. Morchid *et al.*, “IoT-Based Smart Irrigation Management System to Enhance Agricultural Water Security using Embedded Systems, Telemetry Data, and Cloud Computing,” *Results in Engineering*, vol. 23, pp. 1–16, 2024, doi: 10.1016/j.rineng.2024.102829.

[52] S. Cairone *et al.*, “Revolutionizing wastewater treatment toward circular economy and carbon neutrality goals…,” *J. Water Process Eng.*, vol. 62, pp. 1–15, 2024, doi: 10.1016/j.jwpe.2024.105486.

[53] S. Tedjojuwono and J. Jahja, “Smart Water Management System Using IoT based Sensors,” *IOP Conf. Ser.: Earth Environ. Sci.*, vol. 1324, pp. 1–8, 2024, doi: 10.1088/1755-1315/1324/1/012106.

[54] S. Vani *et al.*, “Smart Water Management Grid,” *Int. J. Innov. Sci. Res. Technol.*, vol. 9, no. 5, pp. 854–859, 2024, doi: 10.38124/ijisrt/ijisrt24may931.

[55] N. M. A. Dada *et al.*, “Review of smart water management: IoT and AI in water and wastewater treatment,” *World J. Adv. Res. Rev.*, vol. 21, no. 1, pp. 1373–1382, 2024, doi: 10.30574/wjarr.2024.21.1.0171.

[56] Y. Singh and T. Walingo, “Smart Water Quality Monitoring with IoT Wireless Sensor Networks,” *Sensors*, vol. 24, no. 9, pp. 1–22, 2024, doi: 10.3390/s24092871.

[57] E. Hassan, A. Alharbi, A. Oshaba, and A. El-Emary, “Enhancing Smart Irrigation Efficiency: A New WSN-Based Localization Method for Water Conservation,” *Water*, vol. 16, no. 5, pp. 1–17, 2024, doi: 10.3390/w16050672.

[58] M. Meriç, “Implementation of a wireless sensor network for irrigation management in drip irrigation systems,” *Scientific Reports*, vol. 15, pp. 1–20, 2025, doi: 10.1038/s41598-025-97303-w.

[59] Y. K. Kushwaha, A. Joshi, R. K. Panigrahi, and A. Pandey, “Development of a smart irrigation monitoring system employing the wireless sensor network for agricultural water management,” *J. Hydroinformatics*, vol. 26, no. 12, pp. 1234–1245, 2024, doi: 10.2166/hydro.2024.123.

[60] B. Et-Taibi *et al.*, “Enhancing Water Management in Smart Agriculture: A Cloud and IoT-Based Smart Irrigation System,” *Results in Engineering*, vol. 22, pp. 1–15, 2024, doi: 10.1016/j.rineng.2024.102283.

[61] D. Sharma *et al.*, “Harnessing IoT and Machine Learning for Efficient Water Management in Urban Infrastructure,” in *Proc. Int. Conf. Pervasive Computational Technologies (ICPCT)*, Greater Noida, India, Feb. 8–9, 2025, pp. 70–74, doi: 10.1109/ICPCT64145.2025.10940600.

[62] R. Oppong, “Integration of IoT-based sprinklers, embedded systems, data, and cloud computing for smart irrigation management,” *World J. Adv. Res. Rev.*, vol. 25, no. 3, pp. 126–151, 2025, doi: 10.30574/wjarr.2025.25.3.0695.

[63] D. Santos *et al.*, “Environmental Health Assessment… Phorcus lineatus,” *Water*, vol. 16, no. 1, pp. 1–18, 2024, doi: 10.3390/w16010005.

[64] F. A. Silaban and A. Firdausi, “Neural Network Based Smart Irrigation System with Edge Computing Control…,” *Buletin Ilmiah Sarjana Teknik Elektro*, vol. 6, no. 4, pp. 234–333, 2024, doi: 10.12928/biste.v6i4.11965.

[65] P. Agarwal *et al.*, “Digital Innovation in Water Governance: Exploring the Synergy of Digital Twins and Blockchain,” in *Proc. SmartNets*, Harrisonburg, VA, USA, May 28–30, 2024, pp. 1–7, doi: 10.1109/SmartNets61466.2024.10577727.

[66] A. Alzahrani, S. Chauhdary, and A. Alshdadi, “Efficient wastewater management for smart cities using Internet of Things (IoT) and blockchain technology,” *Int. J. Adv. Appl. Sci.*, vol. 11, no. 10, pp. 147–156, 2024, doi: 10.21833/ijaas.2024.10.017.

[67] S. Cojbasic *et al.*, “Application of machine learning in river water quality management: a review,” *Water Sci. Technol.*, vol. 88, no. 9, pp. 2297–2308, 2023, doi: 10.2166/wst.2023.331.

[68] Z. Akhayeva, A. Zakirova, and V. Zhmud, “Optimization of Water Resources Management Using Big Data and Machine Learning in Smart Cities,” *Eurasian J. Math. Comput. Appl.*, vol. 12, no. 2, pp. 4–15, 2024, doi: 10.32523/2306-6172-2024-12-2-4-15.

[69] R. Taloma, F. Cuomo, D. Comminiello, and P. Pisani, “Machine learning for smart water distribution systems: exploring applications, challenges and future perspectives,” *Artif. Intell. Rev.*, vol. 58, no. 120, pp. 1–56, 2025, doi: 10.1007/s10462-024-11093-7.

[70] D. Balta *et al.*, “Cybersecurity-aware log management system for critical water infrastructures,” *Appl. Soft Comput.*, vol. 169, p. 112613, 2024, doi: 10.1016/j.asoc.2024.112613.

[71] C. Lin, Y. Yang, and F. Moazeni, “Flood Risks of Cyber-Physical Attacks in a Smart Storm Water System,” *Water Resources Research*, vol. 60, no. 1, pp. 1–17, 2024, doi: 10.1029/2023WR034827.

[72] B. Nsoh *et al.*, “Internet of Things-Based Automated Solutions Utilizing Machine Learning for Smart and Real-Time Irrigation Management: A Review,” *Sensors*, vol. 24, no. 23, pp. 1–36, 2024, doi: 10.3390/s24237480.

[73] C. Alexandra *et al.*, “Cyber-physical systems in water management and governance,” *Curr. Opin. Environ. Sustain.*, vol. 62, pp. 1–11, 2023, doi: 10.1016/j.cosust.2023.101290.

[74] T. Szádeczky, “Water 4.0 in Hungary: Prospects and Cybersecurity Concerns,” *Acta Polytech. Hung.*, vol. 20, no. 7, pp. 211–230, 2023, doi: 10.12700/aph.20.7.2023.7.12.

[75] T. C. Pereira, R. V. Arbos, and A. Andrade-Campos, “Multiservice System for Water Supply Systems: A Smart Predictive Digital Twin Proposal,” in *Proc. ETFA*, Padova, Italy, Sept. 10–13, 2024, pp. 1–4, doi: 10.1109/ETFA61755.2024.10710851.

[76] S. Plitsos, E. Kostaki, C. Bardaki, and P. Eirinakis, “Enabling digital twins for industrial water management,” *Intell. Decision Technol.*, 2025, doi: 10.1177/18724981251352389.

[77] G. Restuccia, F. Giuliano, and D. Garlisi, “LoRaWAN AI-Powered Digital Twins for Smart Water Distribution Networks,” in *Proc. IEEE WCNC*, Milan, Italy, Mar. 24–27, 2025, pp. 1–3, doi: 10.1109/WCNC61545.2025.10978232.

[78] M. A. Hamada, O. Tolkyn, and G. M. Hamada, “Leveraging Geographic Information Systems and Remote Sensing for Enhanced Water Resource Management in Kazakhstan,” in *Proc. ICTACS*, Tashkent, Uzbekistan, Nov. 13–15, 2024, pp. 1287–1292, doi: 10.1109/ICTACS62700.2024.10840765.

[79] S. B. Tarate *et al.*, “Geospatial Technology for Sustainable Agricultural Water Management in India—A Systematic Review,” *Geomatics*, vol. 4, no. 2, pp. 91–123, 2024, doi: 10.3390/geomatics4020006.

[80] U. Mukhtorov, B. Kakhorov, Z. Khafizova, D. Murodova, and R. Egamberdiev, “Study of monitoring of water bodies using remote sensing data and GIS technologies (Talimarjan water reservoir),” *IOP Conf. Ser.: Earth Environ. Sci.*, vol. 1420, pp. 1–9, 2024, doi: 10.1088/1755-1315/1420/1/012007.

[81] C. Maraveas, D. Konar, D. K. Michopoulos, K. G. Arvanitis, and K. P. Peppas, “Harnessing quantum computing for smart agriculture: Empowering sustainable crop management and yield optimization,” *Comput. Electron. Agric.*, vol. 218, p. 108680, 2024, doi: 10.1016/j.compag.2024.108680.

[82] S. Rahman *et al.*, “Climate change through quantum lens: Computing and machine learning,” *Earth Syst. Environ.*, vol. 8, pp. 705–722, 2024, doi: 10.1007/s41748-024-00411-2.

[83] A. Singh, R. Ranjan, A. Kapil, R. Govil, and P. Raghav, “Smart intelligent control application using quantum computation and machine learning,” in *Proc. ICICAT*, Gorakhpur, India, Nov. 23–24, 2024, pp. 1113–1119, doi: 10.1109/ICICAT62666.2024.10923437.

[84] A. P. Murdan and B. M. W. H. Lang, “An IoT-based robotic irrigation system for optimal water management,” in *Proc. ETIS 2025*, Trivandrum, India, 2025, pp. 1–6, doi: 10.1109/ETIS64005.2025.10961321.

[85] Y. Chen, Y. Yip, H. Tran, S. Shin, and W. Kim, “Artificial intelligence-driven robotic sensing system for noninvasive crop health monitoring and autonomous irrigation management,” *Adv. Intell. Syst.*, vol. 7, no. 7, pp. 1–11, 2025, doi: 10.1002/aisy.202500198.

[86] D. Guth and D. Herák, “Modern water treatment technology based on Industry 4.0,” *Sensors*, vol. 25, no. 6, p. 1925, 2025, doi: 10.3390/s25061925.

[87] N. Sushma *et al.*, “A unified metering system deployed for water and energy monitoring in smart city,” *IEEE Access*, vol. 11, pp. 80429–80447, 2023, doi: 10.1109/ACCESS.2023.3299825.

[88] D. Bačnar, I. Petrijevčanin, and J. Lerga, “Cloudization of smart metering and advanced metering infrastructure,” in *Proc. ELMAR*, Zadar, Croatia, Sept. 11–13, 2023, pp. 91–95, doi: 10.1109/ELMAR59410.2023.10253910.

[89] M. A. Al-Obaidi *et al.*, “Integration of renewable energy systems in desalination,” *Processes*, vol. 12, no. 4, p. 770, 2024, doi: 10.3390/pr12040770.

[90] M. Ahmed *et al.*, “Modern advancements of energy storage systems integrated with hybrid renewable energy sources for water pumping application,” *Eng. Sci. Technol. Int. J.*, vol. 62, pp. 1–23, 2025, doi: 10.1016/j.jestch.2025.101967.

[91] S. Vatikiotis, I. Avgerinos, S. Plitsos, and G. Zois, “A decision support system for optimised industrial water management,” *Expert Syst. Appl.*, vol. 271, p. 126673, 2025, doi: 10.1016/j.eswa.2025.126673.

[92] A. Loomba, G. Aaboen, P. Soni, and M. Stanko, “Transforming produced water management with a decision support system,” in *Proc. Offshore Technol. Conf.*, Houston, USA, May 5–8, 2025, doi: 10.4043/35993-ms.

[93] S. Moosavi, R. Radfar, and S. Setayeshi, “Development of a fuzzy case-based reasoning decision support system for water management in smart agriculture,” *Manag. Strateg. Eng. Sci.*, vol. 7, no. 1, pp. 91–99, 2025, doi: 10.61838/msesj.7.1.10.

[94] M. Mudholkar and P. Mudholkar, “Smart IoT-enabled tap water leakage monitoring system with mobile integration for sustainable water management,” in *Proc. IC3I*, Greater Noida, India, Sept. 18–20, 2024, pp. 330–337, doi: 10.1109/IC3I61595.2024.10829157.

[95] M. D. R. Palati *et al.*, “Smart water leakage alert system for residential buildings,” in *Proc. ICESC*, Coimbatore, India, Aug. 7–9, 2024, pp. 357–362, doi: 10.1109/ICESC60852.2024.10689969.

[96] M. Warimani *et al.*, “Sustainable smart temperature and water leakage detection system using IoT,” in *Proc. B-HTC*, Belagavi, India, Apr. 25–26, 2025, pp. 1–4, doi: 10.1109/B-HTC64616.2025.11116403.

[97] S. Mehta and A. Aneja, “Smart water management in agriculture: IoT solutions for reducing water consumption,” in *Proc. ICMACC*, Hyderabad, India, Dec. 19–21, 2024, pp. 19–23, doi: 10.1109/ICMACC62921.2024.10894488.

[98] B. Vivek *et al.*, “Smart rainwater management system for flood mitigation for house,” in *Proc. ICCCNT*, Kamand, India, June 24–28, 2024, pp. 1–5, doi: 10.1109/ICCCNT61001.2024.10725565.

[99] P. S. Thanigaivelu *et al.*, “Revolutionizing urban drainage: A smart IoT approach to stormwater management using AdaBoosting algorithm,” in *Proc. AMATHE*, Shivamogga, India, May 16–17, 2024, pp. 1–6, doi: 10.1109/AMATHE61652.2024.10582217.

[100] P. Ahire, “Smart dam monitoring system,” *Int. J. Sci. Res. Eng. Manag.*, vol. 9, no. 2, pp. 1–5, 2025, doi: 10.55041/ijsrem41290.

[101] L. Han, M. Han, H. Shi, and P. Li, “Design of reservoir environmental monitoring system based on IoT technology,” in *Proc. BDCIA 2024*, Huanggang, China, Nov. 15–17, 2024, pp. 1355010-1–1355010-8, doi: 10.1117/12.3059590.

[102] S. Madhavi *et al.*, “Smart sewage system with advanced remote monitoring for efficient urban infrastructure management,” in *Proc. AIMLA*, Namakkal, India, Mar. 15–16, 2024, pp. 1–4, doi: 10.1109/AIMLA59606.2024.10531479.

[103] M. Kavya, A. Mathew, P. Shekar, and P. Sarwesh, “Short term water demand forecast modelling using artificial intelligence for smart water management,” *Sustain. Cities Soc.*, vol. 95, p. 104610, 2023, doi: 10.1016/j.scs.2023.104610.

[104] I. Skoczko, “Energy efficiency analysis of water treatment plants: Current status and future trends,” *Energies*, vol. 18, no. 5, p. 1086, 2025, doi: 10.3390/en18051086.

[105] H. Eleweuwa *et al.*, “Analysis of energy efficiency in water treatment plants: Present conditions and future directions,” *World J. Adv. Res. Rev.*, vol. 25, no. 3, pp. 1717–1723, 2025, doi: 10.30574/wjarr.2025.25.3.0893.

[106] G. Colajanni, D. Sciacca, and L. Paone, “Optimal energy management of water networks under quality conditions,” *Int. Trans. Oper. Res.*, pp. 1–26, 2025, doi: 10.1111/itor.70039.

[107] S. Movva, “Analysis of intelligent water management: Integration of IoT and AI in water and wastewater treatment,” *Int. J. Sci. Res.*, vol. 13, no. 3, pp. 1444–1448, 2024, doi: 10.21275/sr24322073844.

[108] N. N. I. Prova *et al.*, “Advancing predictive maintenance and asset management through digital twin technology,” in *Proc. CE2CT*, Bhimtal, India, Feb. 21–22, 2025, pp. 1179–1185, doi: 10.1109/CE2CT64011.2025.10939840.

[109] D. Reddy *et al.*, “Aadhaar enabled water distribution system,” *Water Resour. Manag.*, vol. 38, pp. 2279–2291, 2024, doi: 10.1007/s11269-024-03759-2.

[110] T. Olatunde, F. Adelani, and Z. Sikhakhane, “A review of smart water management systems from Africa and the United States,” *Eng. Sci. Technol. J.*, vol. 5, no. 4, pp. 1231–1242, 2024, doi: 10.51594/estj.v5i4.1014.

[111] F. A. Adeshina, M. T. Olatunde, and J. Oliha, “Theoretical perspectives on cybersecurity challenges in critical water infrastructure,” *Int. J. Front. Eng. Technol. Res.*, vol. 6, no. 2, pp. 001–007, 2024, doi: 10.53294/ijfetr.2024.6.2.0029.

[112] F. A. Adelani, T. M. Olatunde, and J. S. Oliha, “Theoretical perspectives on cybersecurity challenges in critical water infrastructure,” *Int. J. Front. Eng. Technol. Res.*, vol. 6, no. 2, pp. 001–007, 2024, doi: 10.53294/ijfetr.2024.6.2.0029.

[113] A. Shoomal, M. Jahanbakht, P. Componation, and D. Ozay, “Enhancing supply chain resilience and efficiency through internet of things integration,” *Internet Things*, vol. 27, p. 101324, 2024, doi: 10.1016/j.iot.2024.101324.

[114] R. Tsoupidi, E. Troubitsyna, and P. Papadimitratos, “Thwarting code-reuse and side-channel attacks in embedded systems,” *arXiv*, pp. 1–17, 2023, doi: 10.48550/arXiv.2304.13458.

[115] Y. Meng and H. Zhu, “Wireless traffic analysis based side-channel attacks and countermeasure in smart home,” in *Proc. ACM Turing Award Celebration Conf. China*, Wuhan, China, July 28–30, 2023, pp. 150–151, doi: 10.1145/3603165.3607446.

[116] V. Rega *et al.*, “Profiling running applications in connected devices through side-channel and machine learning techniques,” *IEEE Access*, vol. 12, pp. 170923–170935, 2024, doi: 10.1109/ACCESS.2024.3491916.

[117] N. Raza and F. Moazeni, “Chance-constrained vulnerability assessment of smart water distribution systems against stealthy false data injection attacks,” *Int. J. Crit. Infrastruct. Prot.*, vol. 44, p. 100645, 2023, doi: 10.1016/j.ijcip.2023.100645.

[118] A. Murillo, R. Taormina, N. Tippenhauer, and S. Galelli, “High-fidelity cyber and physical simulation of water distribution systems II: Enabling cyber-physical attack localization,” *J. Water Resour. Plan. Manag.*, vol. 149, no. 5, p. 04023010, 2023, doi: 10.1061/jwrmd5.wreng-5854.

[119] Z. Rehman, M. Gregory, I. Gondal, H. Dong, and M. Ge, “Eclipse attacks in blockchain networks: Detection, prevention, and future directions,” *IEEE Access*, vol. 13, pp. 25918–25933, 2025, doi: 10.1109/ACCESS.2025.3538837.

[120] A. Bello, S. Jahan, F. Farid, and F. Ahamed, “A systemic review of the cybersecurity challenges in Australian water infrastructure management,” *Water*, vol. 15, no. 1, p. 168, 2023, doi: 10.3390/w15010168.

[121] M. M. Aslam, A. Tufail, K.-H. Kim, R. A. A. H. M. Apong, and M. T. Raza, “A comprehensive study on cyber attacks in communication networks in water purification and distribution plants: Challenges, vulnerabilities, and future prospects,” *Sensors*, vol. 23, no. 18, p. 7999, 2023, doi: 10.3390/s23187999.

[122] Y. Su, G. Pan, L. Li, and R. Fan, “An active jamming-based helper deployment scheme for underwater acoustic sensor networks,” *Ad Hoc Networks*, vol. 157, p. 103086, 2024, doi: 10.1016/j.adhoc.2024.103086.

[123] A. Abdullah, A. Albaihani, B. Osman, and Y. Omar, “Detecting wormhole attack in environmental monitoring system for agriculture using deep learning,” *J. Adv. Res. Appl. Sci. Eng. Technol.*, vol. 51, no. 2, pp. 153–176, 2024, doi: 10.37934/araset.51.2.153176.

[124] M. Hussain, Z. Hanapi, A. Abdullah, M. Hussin, and M. Ninggal, “An efficient secure and energy resilient trust-based system for detection and mitigation of sybil attack detection (SAN),” *PeerJ Comput. Sci.*, vol. 10, pp. 1–30, 2024, doi: 10.7717/peerj-cs.2231.

[125] B. Liu, X. Yao, K. Guo, and P. Zhu, “Consortium blockchain based lightweight message authentication and auditing in smart home,” *IEEE Access*, vol. 11, pp. 68473–68485, 2023, doi: 10.1109/ACCESS.2023.3293401.

[126] Z. Alansari, N. Anuar, A. Kamsin, and M. Belgaum, “A systematic review of routing attacks detection in wireless sensor networks,” *PeerJ Comput. Sci.*, vol. 8, pp. 1–44, 2022, doi: 10.7717/peerj-cs.1135.

[127] H. Skrodelis, R. Kelle, and A. Romanovs, “Cybersecurity in SCADA systems with advanced AI and ML techniques,” in *Proc. 2024 IEEE ITMS*, Riga, Latvia, Oct. 2024, pp. 1–5, doi: 10.1109/ITMS64072.2024.10741936.

[128] C. Kallesøe and R. Wisniewski, “Cyber-attack and fault detection using a digital twin of the controller software,” *IFAC-PapersOnLine*, vol. 58, no. 4, pp. 97–102, 2024, doi: 10.1016/j.ifacol.2024.07.200.

[129] P. Huang, J. Kim, P. Kumar, J. Rajendran, and P. Enjeti, “Enhancing cybersecurity for industrial control systems: Innovations in protecting PLC-dependent industrial infrastructures,” *IEEE Internet Things J.*, vol. 11, pp. 36486–36493, 2024, doi: 10.1109/JIOT.2024.3408098.

[130] T. Bakhshi, B. Ghita, and I. Kuzminykh, “A review of IoT firmware vulnerabilities and auditing techniques,” *Sensors*, vol. 24, no. 2, p. 708, 2024, doi: 10.3390/s24020708.

[131] L. Oatu, “Combating man-in-the-middle attacks within IoT systems,” *Int. J. Inf. Secur. Cybercrime*, vol. 13, no. 1, pp. 59–65, 2024, doi: 10.19107/ijisc.2024.01.05.

[132] D. Sun, I. Hwang, and J. Goppert, “A stealthy man-in-the-middle attack strategy for switched systems,” *Int. J. Syst. Sci.*, vol. 55, pp. 1206–1223, 2024, doi: 10.1080/00207721.2024.2304127.

[133] U. Tariq, I. Ahmed, A. K. Bashir, and K. Shaukat, “A critical cybersecurity analysis and future research directions for the Internet of Things: A comprehensive review,” *Sensors*, vol. 23, no. 8, p. 4117, 2023, doi: 10.3390/s23084117.

[134] O. Alsad and Q. Al-Haija, “DNS cache poisoning attack detection: A systematic review,” in *Proc. IET SCS 2023*, 2023, doi: 10.1049/icp.2024.0962.

[135] V. Vajrobol et al., “Identify spoofing attacks in Internet of Things (IoT) environments using machine learning algorithms,” *J. High Speed Netw.*, vol. 31, pp. 61–70, 2024, doi: 10.1177/09266801241295886.

[136] K. Jyothi et al., “A novel optimized neural network model for cyber attack detection using enhanced whale optimization algorithm,” *Sci. Rep.*, vol. 14, pp. 1–11, 2024, doi: 10.1038/s41598-024-55098-2.

[137] S. Ashraf et al., “IoT empowered smart cybersecurity framework for intrusion detection in internet of drones,” *Sci. Rep.*, vol. 13, pp. 1–20, 2023, doi: 10.1038/s41598-023-45065-8.

[138] M. Nasir, J. Arshad, and M. Khan, “Collaborative device-level botnet detection for Internet of Things,” *Comput. Secur.*, vol. 129, p. 103172, 2023, doi: 10.1016/j.cose.2023.103172.

[139] R. Alqura’n et al., “Advancing XSS detection in IoT over 5G: A cutting-edge artificial neural network approach,” *IoT*, vol. 5, no. 3, pp. 478–508, 2024, doi: 10.3390/iot5030022.

[140] Y. Singh, P. Goel, S. Aggarwal, R. Chaudhary, and I. Budhiraja, “Mitigating cross-site request forgery vulnerabilities: An examination of prevention systems,” in *Proc. IEEE ANTS 2024*, Dec. 2024, pp. 55–60, doi: 10.1109/ANTS63515.2024.10898830.

[141] M. Khan, J. Al-Karaki, and M. Omar, “Predicting water quality using quantum machine learning: The case of the Umgeni Catchment (U20A) study region,” *arXiv*, pp. 1–13, 2024, doi: 10.48550/arXiv.2411.18141.

[142] É. S. Ascenção et al., “Applications of smart water management systems: A literature review,” *Water*, vol. 15, no. 19, pp. 1–16, 2023, doi: 10.3390/w15193492.

[143] M. Alalfi, A. Zaid, and A. Miri, “A model-driven-reverse engineering approach for detecting privilege escalation in IoT systems,” *J. Object Technol.*, vol. 22, no. 1, pp. 1–21, 2023, doi: 10.5381/jot.2023.22.1.a1.

[144] G. Ali et al., “Post-quantum secure blockchain-based federated learning framework for enhancing smart grid security,” *Iraqi J. Comput. Inform.*, vol. 51, no. 2, pp. 157–224, 2025, doi: 10.25195/ijci.v51i2.637.

[145] G. Ali et al., “Integration of artificial intelligence, blockchain, and quantum cryptography for securing the Industrial Internet of Things (IIoT): Recent advancements and future trends,” *Appl. Data Sci. Anal.*, pp. 19–82, 2025, doi: 10.58496/ADSA/2025/004.

[146] G. Ali et al., “Fusion of blockchain, IoT, artificial intelligence, and robotics for efficient waste management in smart cities,” *Int. J. Innov. Technol. Interdiscip. Sci.*, vol. 8, no. 3, pp. 388–495, 2025.

[147] E. U. Haque et al., “A scalable blockchain based framework for efficient IoT data management using lightweight consensus,” *Sci. Rep.*, vol. 14, pp. 1–11, 2024, doi: 10.1038/s41598-024-58578-7.

[148] S. M. Habibullah et al., “Blockchain-based energy consumption approaches in IoT,” *Sci. Rep.*, vol. 14, pp. 1–10, 2024, doi: 10.1038/s41598-024-77792-x.

[149] A. Denis et al., “A survey on artificial intelligence and blockchain applications in cybersecurity for smart cities,” *SHIFRA*, pp. 1–45, 2025, doi: 10.70470/SHIFRA/2025/001.

[150] K. S. Kumar et al., “A secure and efficient blockchain and distributed ledger technology-based optimal resource management in digital twin beyond 5G networks,” *IEEE Access*, vol. 12, pp. 110331–110352, 2024, doi: 10.1109/ACCESS.2024.3435847.

[151] G. Ali et al., “Blockchain and federated learning in edge-fog-cloud computing environments for smart logistics,” *Mesopotamian J. CyberSecurity*, vol. 5, no. 2, pp. 735–769, 2025.

[152] S. Mohamed et al., “Blockchain-powered smart system platform development: Use case – water meter readings,” *J. Inf. Assur. Secur.*, vol. 19, pp. 214–232, 2024, doi: 10.2478/ias-2024-0015.

[153] A. R. Furones and J. I. T. Monzón, “Blockchain applicability in the management of urban water supply and sanitation systems in Spain,” *J. Environ. Manage.*, vol. 344, p. 118480, 2023, doi: 10.1016/j.jenvman.2023.118480.

[154] K. Donaghy, Z. Li, and F. Rezwan, “Water Ledger: A blockchain-based smart water resource management platform,” in *Proc. SDLT 2024*, Brisbane, 2024, pp. 119–124, doi: 10.1007/978-981-96-4442-1_8.

[155] T. Nododile and C. Nyirenda, “A hybrid blockchain-IPFS solution for secure and scalable data collection and storage for smart water meters,” *arXiv*, pp. 1–9, 2025, doi: 10.48550/arXiv.2502.03427.

[156] R. Islam et al., “Decentralized trust framework for smart cities: A blockchain-enabled cybersecurity and data integrity model,” *Sci. Rep.*, vol. 15, pp. 1–30, 2025, doi: 10.1038/s41598-025-06405-y.

[157] M. Merlec and H. In, “SC-CAAC: A smart-contract-based context-aware access control scheme for blockchain-enabled IoT systems,” *IEEE Internet Things J.*, vol. 11, pp. 19866–19881, 2024, doi: 10.1109/JIOT.2024.3371504.

[158] T. Bishtawi et al., “Integrating blockchain technology for secure access control in smart home environments: A comprehensive review,” *Int. J. Data Netw. Sci.*, vol. 9, pp. 373–384, 2025, doi: 10.5267/j.ijdns.2025.4.003.

[159] S. Erukala et al., “A secure end-to-end communication framework for cooperative IoT networks using hybrid blockchain system,” *Sci. Rep.*, vol. 15, pp. 1–33, 2025, doi: 10.1038/s41598-025-96002-w.

[160] I. Shahzad, M. Maqsood, S. Latif, and H. Ijaz, “Decentralized IoT-based architectures for tamper-proof agricultural sensor networks: Ensuring end-to-end data integrity and transparent governance,” *Kashf J. Multidiscip. Res.*, vol. 2, no. 05, pp. 39–55, 2025, doi: 10.71146/kjmr442.

[161] D. Kumar et al., “A blockchain-based intelligent IoT communication system for enhanced security, reliability, and efficiency,” in *Proc. ICoACT 2025*, Sivalasi, India, Mar. 2025, pp. 1–5, doi: 10.1109/ICoACT63339.2025.11005316.

[162] D. Rawal, J. Seedorf, and B. Patil, "An approach that utilizes blockchain to effectively and securely preserve data privacy for location data from IoT in smart cities," *Int. Arch. Photogrammetry Remote Sens. Spatial Inf. Sci.*, vol. XLVIII-4/W13-2025, pp. 201–208, 2025, doi: 10.5194/isprs-archives-xlviii-4-w13-2025-201-2025.

[163] O. Popoola et al., "A critical literature review of security and privacy in smart home healthcare schemes adopting IoT and blockchain: Problems, challenges and solutions," *Blockchain Res. Appl.*, vol. 5, no. 2, p. 100178, 2023, doi: 10.1016/j.bcra.2023.100178.

[164] H. D. Zubaydi, P. Varga, and S. Molnár, "Leveraging blockchain technology for ensuring security and privacy aspects in Internet of Things: A systematic literature review," *Sensors*, vol. 23, no. 2, p. 788, 2023, doi: 10.3390/s23020788.

[165] T. Sarantakos et al., "A tool to facilitate the design of smart contracts in smart water distribution networks," in *Proc. IFIP Networking 2024*, Thessaloniki, Greece, Jun. 2024, pp. 708–713, doi: 10.23919/IFIPNetworking62109.2024.10619818.

[166] V. Villa, L. Gioberti, M. Domaneschi, and N. Catbas, "Conceptual advancements in infrastructure maintenance and management using smart contracts: Reducing costs and improving resilience," *Buildings*, vol. 15, no. 5, p. 680, 2025, doi: 10.3390/buildings15050680.

[167] S. Patil et al., "The use of blockchain for water rights in irrigation management," *Int. Water Irrig.*, vol. 44, no. 1, pp. 1–6, 2024, doi: 10.52783/iwi.v44i1.82.

[168] A. Mithal and B. Thankachan, "A comprehensive review on blockchain-based systems for groundwater conservation and wastewater management," *Environ. Manage.*, vol. 75, pp. 2225–2243, 2025, doi: 10.1007/s00267-025-02247-6.

[169] A. Shamaseen, M. Qatawneh, and B. Elshqeirat, "Smart grid system based on blockchain technology for enhancing trust and preventing counterfeiting issues," *Energies*, vol. 18, no. 13, p. 3523, 2025, doi: 10.3390/en18133523.

[170] V. Prasad et al., "Blockchain enhanced distributed denial of service detection in IoT using deep learning and evolutionary computation," *Sci. Rep.*, vol. 15, pp. 1–24, 2025, doi: 10.1038/s41598-025-06568-8.

[171] N. Xiao, Z. Wang, X. Sun, and J. Miao, "A novel blockchain-based digital forensics framework for preserving evidence and enabling investigation in industrial Internet of Things," *Alexandria Engineering Journal*, vol. 86, pp. 631–643, 2024, doi: 10.1016/j.aej.2023.12.021.

[172] J. D. Morillo Reina and T. J. Mateo Sanguino, "Decentralized and secure blockchain solution for tamper-proof logging events," *Future Internet*, vol. 17, no. 3, p. 108, 2025, doi: 10.3390/fi17030108.

[173] Z. Ren, E. Yan, T. Chen, and Y. Yu, "Blockchain-based CP-ABE data sharing and privacy-preserving scheme using distributed KMS and zero-knowledge proof," *Journal of King Saud University – Computer and Information Sciences*, vol. 36, p. 101969, 2024, doi: 10.1016/j.jksuci.2024.101969.

[174] M. Aleisa, "Blockchain-enabled zero trust architecture for privacy-preserving cybersecurity in IoT environments," *IEEE Access*, vol. 13, pp. 18660–18676, 2025, doi: 10.1109/ACCESS.2025.3529309.

[175] H. Gharavi, J. Granjal, and E. Monteiro, "Post-quantum blockchain security for the Internet of Things: Survey and research directions," *IEEE Communications Surveys & Tutorials*, vol. 26, pp. 1748–1774, 2024, doi: 10.1109/COMST.2024.3355222.

[176] A. Castiglione *et al.*, "Integrating post-quantum cryptography and blockchain to secure low-cost IoT devices," *IEEE Transactions on Industrial Informatics*, vol. 21, pp. 1674–1683, 2025, doi: 10.1109/TII.2024.3485796.

[177] B. Sezer, S. Akleylek, and U. Nuriyev, "PP-PQB: Privacy-preserving in post-quantum blockchain-based systems: A systematization of knowledge," *IEEE Access*, vol. 13, pp. 41382–41405, 2025, doi: 10.1109/ACCESS.2025.3545943.

[178] D. Commey, B. Mai, S. Hounsinou, and G. Crosby, "Securing blockchain-based IoT systems: A review," *IEEE Access*, vol. 12, pp. 98856–98881, 2024, doi: 10.1109/ACCESS.2024.3428490.

[179] R. Sadooghi *et al.*, "Peer-to-peer energy management of distributed ledgers in renewable smart energy systems," *Electric Power Systems Research*, vol. 242, p. 111451, 2025, doi: 10.1016/j.epsr.2025.111451.

[180] C. Yapa *et al.*, "Power line monitoring-based consensus algorithm for performance enhancement of energy blockchain applications in smart grid 2.0," *IEEE Transactions on Smart Grid*, vol. 16, pp. 277–287, 2025, doi: 10.1109/TSG.2024.3445659.

[181] O. Akanfe, D. Lawong, and H. Rao, "Blockchain technology and privacy regulation: Reviewing frictions and synthesizing opportunities," *International Journal of Information Management*, vol. 76, p. 102753, 2024, doi: 10.1016/j.ijinfomgt.2024.102753.

[182] G. Liyanaarachchi, G. Viglia, and F. Kurtaliqi, "Addressing challenges of digital transformation with modified blockchain," *Technological Forecasting and Social Change*, vol. 201, p. 123254, 2024, doi: 10.1016/j.techfore.2024.123254.

[183] A. Zafar, "Reconciling blockchain technology and data protection laws: Regulatory challenges, technical solutions, and practical pathways," *Journal of Cybersecurity*, vol. 11, no. 1, pp. 1–20, 2025, doi: 10.1093/cybsec/tyaf002.

[184] J. Heo, G. Ramachandran, A. Dorri, and R. Jurdak, "Blockchain data storage optimisations: A comprehensive survey," *ACM Computing Surveys*, vol. 56, pp. 1–27, 2024, doi: 10.1145/3645104.

[185] Y. Alzoubi and A. Mishra, "Techniques to alleviate blockchain bloat: Potentials, challenges, and recommendations," *Computers and Electrical Engineering*, vol. 116, p. 109216, 2024, doi: 10.1016/j.compeleceng.2024.109216.

[186] Y. Wang, H. Wang, and Y. Cao, "Comprehensive review of storage optimization techniques in blockchain systems," *Applied Sciences*, vol. 15, no. 1, p. 243, 2025, doi: 10.3390/app15010243.

[187] H. Baniata and A. Kertész, "Partial pre-image attack on proof-of-work based blockchains," *Blockchain: Research and Applications*, vol. 5, no. 3, p. 100194, 2024, doi: 10.1016/j.bcra.2024.100194.

[188] K. G. Arachchige, P. Branch, and J. But, “An analysis of blockchain-based IoT sensor network distributed denial of service attacks,” *Sensors*, vol. 24, no. 10, p. 3083, 2024, doi: 10.3390/s24103083.

[189] Y. Y. Hong and D. J. D. Lopez, “A review on quantum machine learning in applied systems and engineering,” *IEEE Access*, vol. 13, pp. 144607–144631, 2025, doi: 10.1109/ACCESS.2025.3599147.

[190] L. Li *et al.*, “An overview of quantum machine learning research in China,” *Applied Sciences*, vol. 15, no. 5, p. 2555, 2025, doi: 10.3390/app15052555.

[191] R. M. Devadas and T. Sowmya, “Quantum machine learning: A comprehensive review of integrating AI with quantum computing for computational advancements,” *MethodsX*, vol. 14, pp. 1–17, 2025, doi: 10.1016/j.mex.2025.103318.

[192] R. U. Shaik *et al.*, “Quantum machine learning with limited data: A remote sensing perspective,” in *Proc. IEEE IGARSS*, Brisbane, Australia, Aug. 2025, pp. 2645–2650.

[193] R. Ho *et al.*, “EEG-based dementia classification using CS-EMD synchrony features and quantum machine learning,” *IEEE Transactions on Consumer Electronics*, vol. 71, no. 2, pp. 2849–2863, May 2025, doi: 10.1109/TCE.2025.3548303.

[194] M. Ziiatdinov *et al.*, “Comparing quantum machine learning approaches in astrophysical signal detection,” in *Proc. IEEE QSW*, Helsinki, Finland, July 2025, pp. 92–103, doi: 10.1109/QSW67625.2025.00020.

[195] H. Chen *et al.*, “Projection valued-based quantum machine learning adapting to differential privacy algorithm for word-level lipreading,” in *Proc. IEEE ICASSP*, Hyderabad, India, Apr. 2025, pp. 1–5, doi: 10.1109/ICASSP49660.2025.10890305.

[196] O. F. Olaitan *et al.*, “Quantum computing in artificial intelligence: A review of quantum machine learning algorithms,” *Path of Science*, vol. 11, no. 5, pp. 7001–7009, 2025, doi: 10.22178/pos.117-25.

[197] A. Rani *et al.*, “Quantum machine learning: Redefining computational boundaries,” in *Proc. CCICT*, Sonepat, India, Apr. 2025, pp. 48–54, doi: 10.1109/CCICT65753.2025.00018.

[198] X. Dai *et al.*, “Quantum machine learning architecture search via deep reinforcement learning,” in *Proc. IEEE QCE*, Montreal, Canada, Sept. 2024, pp. 1525–1534, doi: 10.1109/QCE60285.2024.00179.

[199] U. Ullah and B. Garcia-Zapirain, “Quantum machine learning revolution in healthcare: A systematic review of emerging perspectives and applications,” *IEEE Access*, vol. 12, pp. 11423–11450, 2024, doi: 10.1109/ACCESS.2024.3353461.

[200] S. Rani, R. Kaur, C. Desai, and R. P. Ambilwade, “Quantum machine learning: Leveraging quantum computing for enhanced learning algorithms,” *IJFMR*, vol. 6, no. 5, pp. 1–15, 2024.

[201] S. Bhowmik and H. Thapliyal, “Quantum machine learning for anomaly detection in consumer electronics,” in *Proc. ISVLSI*, Knoxville, USA, July 2024, pp. 544–550, doi: 10.1109/ISVLSI61997.2024.00104.

[202] M. F. Shahriyar and G. Tanbhir, “Advancements and challenges in quantum machine learning for medical image classification,” in *Proc. ISACC*, India, Feb. 2025, pp. 1126–1133, doi: 10.1109/ISACC65211.2025.10969166.

[203] C. Aishwarya, M. Venkatesan, and P. Prabhavathy, “A scoping survey of quantum machine learning and deep learning for real-world applications,” *Procedia Computer Science*, vol. 258, pp. 633–646, 2025, doi: 10.1016/j.procs.2025.04.297.

[204] D. Abreu, C. E. Rothenberg, and A. Abelém, “QML-IDS: Quantum machine learning intrusion detection system,” in *Proc. IEEE ISCC*, Paris, France, June 2024, pp. 1–6, doi: 10.1109/ISCC61673.2024.10733655.

[205] G. Nagarajan *et al.*, “Quantum machine learning on big data: A randomized measurement approach,” in *Proc. ICoICC*, India, May 2025, pp. 1–6, doi: 10.1109/ICoICC64033.2025.11052091.

[206] P. Lamichhane and D. B. Rawat, “Quantum machine learning: Recent advances, challenges, and perspectives,” *IEEE Access*, vol. 13, pp. 94057–94105, 2025, doi: 10.1109/ACCESS.2025.3573244.

[207] D. Santhiyagu, G. Nagarajan, and J. Refonaa, “Enhanced air quality forecasting with quantum machine learning,” in *Proc. ICISS*, India, Mar. 2025, pp. 1048–1052, doi: 10.1109/ICISS63372.2025.11076208.

[208] L. Abdulameer *et al.*, “The role of artificial intelligence in managing sustainable water resources: A review of smart solution implementations,” *Water Conservation & Management*, vol. 9, no. 2, pp. 281–291, 2025, doi: 10.26480/wcm.02.2025.281.291.

[209] R. Baena-Navarro *et al.*, “Intelligent prediction and continuous monitoring of water quality in aquaculture,” *Water*, vol. 17, no. 1, p. 82, 2025, doi: 10.3390/w17010082.

[210] L. Zhen and A. Bărbulescu, “Quantum neural networks approach for water discharge forecast,” *Applied Sciences*, vol. 15, no. 8, pp. 1–17, 2025, doi: 10.3390/app15084119.

[211] T. Weng *et al.*, “Groundwater level prediction by wavelet deep learning with smart pumping data,” *Water Resources Management*, vol. 39, pp. 2717–2742, 2025, doi: 10.1007/s11269-024-04088-0.

[212] [D. Javeed *et al.*, “Quantum-empowered federated learning and 6G wireless networks for IoT security,” *Future Generation Computer Systems*, vol. 160, pp. 577–597, 2024, doi: 10.1016/j.future.2024.06.023.

[213] M. Hdaib, S. Rajasegarar, and L. Pan, “Quantum deep learning-based anomaly detection for enhanced network security,” *Quantum Machine Intelligence*, vol. 6, no. 26, pp. 1–18, 2024, doi: 10.1007/s42484-024-00163-2.

[214] L. Thirupathi *et al.*, “Cyber-physical systems security and quantum computing applications in disaster recovery for Industry 6.0,” in *Advances in Science, Technology & Innovation*, pp. 221–235, 2024, doi: 10.1007/978-3-031-73350-5_14.

[215] J. Xiong *et al.*, “Enhancing IoT security in smart grids with quantum-resistant hybrid encryption,” *Scientific Reports*, vol. 15, no. 1, pp. 1–11, 2025, doi: 10.1038/s41598-024-56789-0.

[216] M. Bakyt *et al.*, “Application of quantum key distribution to enhance data security in agrotechnical monitoring systems using UAVs,” *Applied Sciences*, vol. 15, no. 4, p. 1987, 2025, doi: 10.3390/app15041987.

[217] S. Biswas, R. Goswami, and K. H. K. Reddy, “Advancing quantum steganography: A secure IoT communication with reversible decoding and customized encryption technique,” *Cluster Computing*, vol. 27, pp. 1–15, 2024, doi: 10.1007/s10586-024-04321-2.

[218] T. Kim and S. Madhavi, “Quantum intrusion detection system using outlier analysis,” *Scientific Reports*, vol. 14, pp. 1–12, 2024, doi: 10.1038/s41598-024-78389-0.

[219] D. Namakshenas *et al.*, “Federated quantum-based privacy-preserving threat detection model for consumer Internet of Things,” *IEEE Transactions on Consumer Electronics*, vol. 70, pp. 5829–5838, 2024, doi: 10.1109/TCE.2024.3377550.

[220] S. S. Ajibosin and D. Cetinkaya, “Implementation and performance evaluation of quantum machine learning algorithms for binary classification,” *Software*, vol. 3, no. 4, pp. 498–513, 2024, doi: 10.3390/software3040024.

[221] M. Grzesiak and P. Thakkar, “Flood prediction using classical and quantum machine learning models,” *arXiv*, pp. 1–24, 2024, doi: 10.48550/arXiv.2407.01001.

[222] J. Cao, Z. Yu, X. Xu, B. Zhu, and J. Yang, “Quantum-enhanced edge offloading and resource scheduling with privacy-preserving machine learning,” *Computers, Materials & Continua*, vol. 83, no. 3, pp. 5235–5257, 2025, doi: 10.32604/cmc.2025.062371.

[223] P. Arepalli and K. Naik, “Water contamination analysis in IoT enabled aquaculture using deep learning based AODEGRU,” *Ecological Informatics*, vol. 79, p. 102405, 2024, doi: 10.1016/j.ecoinf.2023.102405.

[224] M. Ramadan, M. Ali, S. Khoo, and M. Alkhedher, “SecureIoT-FL: A federated learning framework for privacy-preserving real-time environmental monitoring in industrial IoT applications,” *Alexandria Engineering Journal*, vol. 114, pp. 681–701, 2025, doi: 10.1016/j.aej.2024.11.069.

[225] T. M. Mengistu, T. Kim, and J.-W. Lin, “A survey on heterogeneity taxonomy, security and privacy preservation in the integration of IoT, wireless sensor networks and federated learning,” *Sensors*, vol. 24, no. 3, p. 968, 2024, doi: 10.3390/s24030968.

[226] N. Nikmehr *et al.*, “Quantum annealing-infused microgrids formation: Distribution system restoration and resilience enhancement,” *IEEE Transactions on Power Systems*, vol. 40, pp. 463–475, 2025, doi: 10.1109/TPWRS.2024.3399122.

[227] M. Liu *et al.*, “Quantum computing as a catalyst for microgrid management: Enhancing decentralized energy systems through innovative computational techniques,” *Sustainability*, vol. 17, no. 8, p. 3662, 2025, doi: 10.3390/su17083662.

[228] Y. Mohamed *et al.*, “Quantum machine learning regression optimisation for full-scale sewage sludge anaerobic digestion,” *npj Clean Water*, vol. 8, no. 1, pp. 1–13, 2025, doi: 10.1038/s41545-025-00440-y.

[229] S. Moore and J. Dunningham, “Secure quantum-enhanced measurements on a network of sensors,” *Physical Review A*, pp. 012616-1–012616-12, 2024, doi: 10.1103/PhysRevA.111.012616.

[230] H. Shekhawat and D. Gupta, “A survey on lattice-based security and authentication schemes for smart-grid networks in the post-quantum era,” *Concurrency and Computation: Practice and Experience*, vol. 36, no. 14, 2024, doi: 10.1002/cpe.8080.

[231] M. Rath and H. Date, “Quantum data encoding: A comparative analysis of classical-to-quantum mapping techniques and their impact on machine learning accuracy,” *arXiv*, pp. 1–18, 2023, doi: 10.48550/arXiv.2311.10375.

[232] A. Khatoon and R. Riaz, “Quantum computing impacts on smart city cybersecurity through resilient defense framework,” *Ubiquitous Technology Journal*, vol. 1, no. 1, pp. 23–31, 2025, doi: 10.71346/utj.v1i1.8.

[233] V. Barletta, D. Caivano, M. De Vincentiis, A. Pal, and M. Scalera, “Hybrid quantum architecture for smart city security,” *Journal of Systems and Software*, vol. 217, p. 112161, 2024, doi: 10.1016/j.jss.2024.112161.

[234] A. Mektepayeva, A. Sakipov, V. Rystygulova, D. Kaibasova, and L. Belgibayeva, “Optimizing machine learning with quantum enhancements for real-time dynamic systems,” *Vestnik KazATK*, vol. 135, no. 6, pp. 243–254, 2024, doi: 10.52167/1609-1817-2024-135-6-243-254.

[235] S. Huang, Y. Chang, Y. Lin, and S. Zhang, “Hybrid quantum–classical convolutional neural networks with privacy quantum computing,” *Quantum Science and Technology*, vol. 8, 2023, doi: 10.1088/2058-9565/acb966.

[236] H. X. Yang, Z. Li, Z. Liu, and W. Pedrycz, “Improved differential privacy noise mechanism in quantum machine learning,” *IEEE Access*, vol. 11, pp. 50157–50164, 2023, doi: 10.1109/ACCESS.2023.3274471.

[237] M. Wendlinger, K. Tscharke, and P. Debus, “A comparative analysis of adversarial robustness for quantum and classical machine learning models,” in *Proc. IEEE QCE*, Montreal, Canada, pp. 1447–1457, 2024, doi: 10.1109/QCE60285.2024.00171.

[238] D. Kejriwal, A. Goel, and A. Sharma, “Advancing adversarial robustness in cybersecurity: Gradient-free attacks and quantum-inspired defenses for machine learning models,” *Int. J. Innovative Science and Research Technology*, vol. 10, no. 4, pp. 54–65, 2025, doi: 10.38124/ijisrt/25apr469.

[239] C. Liu *et al.*, “Quantum-Train: Rethinking hybrid quantum-classical machine learning in the model compression perspective,” *arXiv*, pp. 1–12, 2024.

[240] M. Hachicha, R. Halima, and T. Frikha, “PreSA: An intelligent blockchain-based platform for monitoring and predicting water quality for smart aquaculture,” *Neural Computing and Applications*, vol. 37, pp. 22129–22140, 2024, doi: 10.1007/s00521-024-10877-w.

[241] M. Lavanya *et al.*, “Quantum nanodevice innovation for smart farming: Integrating machine learning and blockchain technology,” *SSRN Electronic Journal*, pp. 1–9, 2025, doi: 10.2139/ssrn.5083248.

[242] A. Zaki *et al.*, “Smart water systems: The role of technology and engineering in optimizing urban water resources,” *Journal of Information Systems Engineering and Management*, vol. 10, no. 21s, pp. 833–846, 2025, doi: 10.52783/jisem.v10i21s.3445.

[243] H. M. Ramos *et al.*, “Smart water grids and digital twin for management of system efficiency in water distribution networks,” *Water*, vol. 15, no. 6, p. 1129, 2023, doi: 10.3390/w15061129.

[244] S. Di Gennaro, D. Cini, A. Berton, and A. Matese, “Development of a low-cost smart irrigation system for sustainable water management in the Mediterranean region,” *Smart Agricultural Technology*, vol. 9, p. 100629, 2024, doi: 10.1016/j.atech.2024.100629.

[245] P. Hamel *et al.*, “Low-cost monitoring systems for urban water management: Lessons from the field,” *Water Research X*, vol. 22, p. 100212, 2024, doi: 10.1016/j.wroa.2024.100212.

[246] A.-A. Bouramdane, “Optimal water management strategies: Paving the way for sustainability in smart cities,” *Smart Cities*, vol. 6, no. 5, pp. 2849–2882, 2023, doi: 10.3390/smartcities6050128.

[247] S. Afzal and S. I. Hassan, “Blockchain application in sustainable smart water and wastewater management,” in *Transactions on Computer Systems and Networks*, pp. 273–297, 2025, doi: 10.1007/978-981-96-4074-4_10.

[248] T. L. Thuy *et al.*, “Blockchain-enabled water quality monitoring: A comprehensive review of digital innovations and challenges,” *Water*, vol. 17, no. 17, pp. 1–18, 2025, doi: 10.3390/w17172522.

[249] B. Banerjee, “Smart water governance with blockchain technology,” in *Advances in Water Resources Management*, pp. 123–145, 2025, doi: 10.4018/978-1-7998-8126-4.ch007.

[250] M. Alrammal *et al.*, “Blockchain technology for sustainable management of electricity and water consumption,” *Engineering Proceedings*, vol. 59, no. 1, pp. 1–12, 2023, doi: 10.3390/engproc2023059223.

[251] M. T. Naqash *et al.*, “A blockchain based framework for efficient water management and leakage detection in urban areas,” *Urban Science*, vol. 7, no. 4, p. 99, 2023, doi: 10.3390/urbansci7040099.

[252] F. A. Batarseh *et al.*, “ACWA: An AI-driven cyber-physical testbed for intelligent water systems,” *arXiv*, 2023, doi: 10.48550/arXiv.2310.17654.

[253] A. A. Maftei, A. I. Petrariu, V. Popa, and A. Lavric, “A blockchain framework for scalable, high-density IoT networks of the future,” *Sensors*, vol. 25, no. 9, p. 2886, 2025, doi: 10.3390/s25092886.

[254] D. Quintana, L. C. Felix-Herran, J. C. Tudon-Martinez, and J. d. J. Lozoya-Santos, “On smart water system developments: A systematic review,” *Water*, vol. 17, no. 17, pp. 1–28, 2025, doi: 10.3390/w17172571.

[255] A. Marengo and V. Santamato, “Quantum algorithms and complexity in healthcare applications: A systematic review with machine learning-optimized analysis,” *Frontiers in Computer Science*, vol. 7, pp. 1–30, 2025, doi: 10.3389/fcomp.2025.1584114.

[256] M. Yan *et al.*, “Blockchain for secure decentralized energy management of multi-energy system using state machine replication,” *Applied Energy*, vol. 337, p. 120863, 2023, doi: 10.1016/j.apenergy.2023.120863.

[257] M. Mohammed *et al.*, “Industrial Internet of Water Things architecture for data standardization based on blockchain and digital twin technology,” *Journal of Advanced Research*, vol. 66, pp. 1–14, 2023, doi: 10.1016/j.jare.2023.10.005.

[258] S. Mollajafari and K. Bechkoum, “Blockchain technology and related security risks: Towards a seven-layer perspective and taxonomy,” *Sustainability*, vol. 15, no. 18, p. 13401, 2023, doi: 10.3390/su151813401.

[259] A. R. Jami and A. Haleem, “Quantum computing as an enabler for sustainable circular economy implementation in Industry 4.0: A study,” *Human Settlements and Sustainability*, vol. 1, no. 2, pp. 1–18, 2025, doi: 10.1016/j.hssust.2025.05.005.

[260] V. K. Mololoth, S. Saguna, and C. Åhlund, “Blockchain and machine learning for future smart grids: A review,” *Energies*, vol. 16, no. 1, p. 528, 2023, doi: 10.3390/en16010528.

[261] B. Banerjee, U. Sen, S. Pramanik, and A. Banerjee, “Smart water governance with blockchain technology,” in *IGI Global eBooks*, pp. 311–344, 2025, doi: 10.4018/979-8-3373-1424-2.ch011.

[262] R. S. Gupta *et al.*, “A systematic review of quantum machine learning for digital health,” *npj Digital Medicine*, vol. 8, no. 1, pp. 1–15, 2025, doi: 10.1038/s41746-025-01597-z.

[263] Y. Y. Ghadi *et al.*, “A hybrid AI-blockchain security framework for smart grids,” *Scientific Reports*, vol. 15, no. 1, pp. 1–33, 2025, doi: 10.1038/s41598-025-05257-w.

[264] L. Pastori, A. Grundner, V. Eyring, and M. Schwabe, “Quantum neural networks for cloud cover parameterizations in climate models,” *arXiv*, pp. 1–39, 2025.

[265] A. H. Elias, F. A. Khairi, and A. H. Elias, “Hybrid machine-learning framework for predicting student placement,” *Journal of Transactions in Systems Engineering*, vol. 3, no. 2, pp. 403–419, 2025, doi: 10.15157/JTSE.2025.3.2.403-419.

[266] A. Expósito and E. D. Cebollero, “How the digital revolution is reshaping water management and policy: A focus on Spain,” *Utilities Policy*, vol. 96, pp. 1–9, 2025, doi: 10.1016/j.jup.2025.102020.

[267] B. Divya and J. Samraj, “Comparative analysis of deep learning algorithms integrated with blockchain for flood risk management,” in *Proc. ICNWC*, Chennai, India, pp. 1–11, 2024, doi: 10.1109/ICNWC60771.2024.10537567.

[268] A. T. Alhasani, “Unsupervised clustering of multivariate sports activity data using K-means: A study on the Sport Data Multivariate Time Series dataset,” *Journal of Transactions in Systems Engineering*, vol. 3, no. 2, pp. 367–381, 2025.