PENINSULA PUBLISHING LLC

SHIFRA
Vol. **(2025)**, 2025, **pp.** 1–45
ISSN: 3078-3186

Research Article

A Survey on Artificial Intelligence and Blockchain Applications in Cybersecurity for Smart Cities

Asiku Denis [1], Adebo Thomas [1], Wamusi Robert [1], Aziku Samuel [1], Simon Peter Kabiito [1], Zaward Morish [1], Malik Sallam[2,3,*], Guma Ali [1,*], Maad M. Mijwil [4],

[1] *Department of Computer and Information Science, Faculty of Technoscience, Muni University, Arua, Uganda*
[2] *Department of Pathology, Microbiology and Forensic Medicine, School of Medicine, The University of Jordan, Amman 11942, Jorda n*
[3] *Department of Clinical Laboratories and Forensic Medicine, Jordan University Hospital, Amman 11942, Jordan*
[4] *College of Administration and Economics, Al-Iraqia University, Baghdad, Iraq*

ARTICLEINFO

Article History
Received 3 Oct 2024
Revised: 20 Nov 2024
Accepted 20 Dec 2024
Published 10 Jan 2025

Keywords
Artificial Intelligence,
Blockchain Technology,
Cybersecurity,
Smart Cities,
Cyber-attacks and Vulnerabilities.

ABSTRACT

Smart cities rapidly evolve into transformative ecosystems where advanced technologies work together to improve urban living. These interconnected environments use emerging technologies to offer efficient services and sustainable solutions for urban challenges. As these systems become more complex, their vulnerability to cybersecurity threats also increases. Integrating artificial intelligence (AI) and Blockchain technologies to address these challenges presents promising solutions that ensure secure and resilient infrastructures. This study provides a comprehensive survey of integrating AI, Blockchain, cybersecurity, and smart city technologies based on an analysis of peer-reviewed journals, conference proceedings, book chapters, and websites. Seven independent researchers reviewed relevant literature published between January 2021 and December 2024 using ACM Digital Library, Wiley Online Library, Taylor & Francis, Springer, ScienceDirect, MDPI, IEEE Xplore Digital Library, IGI Global, and Google Scholar. The study explores how AI can enhance threat detection, anomaly detection, and predictive analytics, enabling real-time responses to cyber threats. It examines various AI methodologies, including machine learning and deep learning, to identify vulnerabilities and prevent attacks. It discusses the role of Blockchain in securing data integrity, improving transparency, and providing decentralized control over sensitive information. Blockchain's tamper-proof ledger and smart contract capabilities offer innovative solutions for identity management, secure transactions, and data sharing among smart city stakeholders. The study also highlights how combining AI and Blockchain can create robust cybersecurity frameworks, enhancing resilience against emerging threats. The survey concludes by outlining future research directions and offering recommendations for policymakers, urban planners, and cybersecurity professionals. This study identifies emerging trends and applications for enhancing the security and resilience of smart cities through innovative technological solutions. The survey provides valuable insights for researchers and practitioners who aim to utilize AI and Blockchain to improve smart city cybersecurity.

1. INTRODUCTION

This According to a recent United Nations (UN) report, 55% of the world's population resides in cities. However, the forecasts made by the UN shed light on the possibility that by 2050, urban areas will house 6.5 billion people, representing 68% of the global population [1-3]. This shift results from urbanization, and as urbanization accelerates, cities will encounter significant challenges, including congestion, pollution, greenhouse gas emissions, resource depletion, environmental degradation, insufficient infrastructure, energy shortages, inadequate healthcare and education systems, urban poverty, and soaring land prices, which will increasingly strain urban resources and infrastructure [4]. To address these challenges, urban planners, decision-makers, and researchers actively seek ways to enhance urban livability and sustainability [5]. In response, smart cities have gained prominence in recent decades by leveraging emerging technologies [2][3][6].

*Corresponding author email: a.guma@muni.ac.ug
DOI: https://doi.org/10.70470/SHIFRA/2025/001

A smart city, also known as a digital, intelligent, or knowledge city, leverages advanced technologies to enhance quality of life, reduce pollution, and improve efficiency in urban areas. By utilizing smart devices, sensors, 5G technologies, IoT, edge computing, robotics, digital twins, Web 3.0, smart grids, big data analytics, and AI tools, smart cities create an interconnected urban ecosystem. This ecosystem seamlessly facilitates interactions between people and objects, enabling efficient urban planning, citizen engagement, and better infrastructure management. Core areas such as traffic, transportation systems, utilities, water networks, waste disposal, and public services benefit significantly from these technologies [7-13]. Smart cities integrate essential sectors into a unified system, including transportation, healthcare, energy, safety, environment, economy, and governance. This integration allows for informed decision-making, optimized resource usage, and enhanced service delivery [14][15]. By collecting, transmitting, and analyzing data from sensors, devices, and applications, these cities improve urban planning, drive sustainability, accelerate economic growth, and boost citizen satisfaction [16]. The ability to make intelligent decisions, optimize energy use, enhance building performance, and effectively manage mobility and waste strengthens their functionality and appeal. Ultimately, smart cities aim to develop more resilient, adaptable, and livable environments that dynamically respond to their inhabitants' evolving needs. These advancements create sustainable and innovative metropolitan areas prioritizing current and future generations [17-21].

In 2023, connected smart cities worldwide reached 1.73 billion, growing to 2.20 billion by 2024, with projections indicating a rise to 2.76 billion in 2025, 3.45 billion in 2026, 4.26 billion in 2027, and 5.29 billion by 2028. The global smart cities market, valued at US$392.9 billion in 2019, is expected to surge to US$1,380.21 billion by 2030 [22]. China is set to lead the market in 2024 with revenue of US$43.22 billion, followed by the United States at US$18.71 billion, expected to reach US$27.42 billion by 2028. Germany, Japan, and India will also contribute significantly, with revenues of US$3.61 billion, US$3.11 billion, and US$2.60 billion, respectively. Between 2024 and 2028, India is predicted to achieve the fastest CAGR of 15.71%, followed by China at 13.01%, Germany at 11.15%, Japan at 10.58%, and the United States at 10.03%. This rapid growth underscores the increasing revenue of companies delivering technologies that enhance urban environments through data and information alongside providers of essential infrastructure, such as cloud computing and connectivity technologies, which drive the adoption and implementation of these advancements [23].

Smart cities evolve through investments in technological infrastructure, human capital, and social programs [24]. These cities integrate cutting-edge technologies, utilize data-driven decision-making, and prioritize resilience and sustainability, setting them apart from traditional urban environments [25][26]. They enhance urban mobility, build advanced digital infrastructure, and foster connectivity while actively engaging citizens and promoting collaborative governance through simulation tools [27]. The smart city framework operates within two main paradigms: (1) hard domains, which focus on infrastructure, logistics, resource management, and mobility, and (2) soft domains, which address cultural dimensions, computational technologies, education, governance, and political systems.

Integrating emerging technologies in smart cities exposes them to numerous cyber-attacks, threats, and vulnerabilities. These include data privacy concerns, data breaches, unauthorized access, ransomware, malware, insider threats, replay attacks, phishing, denial-of-service (DoS) and distributed DoS attacks, man-in-the-middle (MitM) attacks, SQL injection, zero-day exploits, supply chain vulnerabilities, side-channel attacks, and advanced persistent threats (APTs). Smart cities also face cryptojacking, black hole, gray hole, sinkhole, wormhole, Sybil, illusion, sleep denial, and fake node injection attacks, as well as buffer overflows and vulnerabilities in IoT devices, critical infrastructure, and connected systems. Additional threats include artificial intelligence-driven attacks, smart grid and building security vulnerabilities, Blockchain weaknesses, Wi-Fi attacks, physical security breaches, radio-frequency interference, cloud malware injection, signature wrapping, web browser attacks, traffic analysis, RFID spoofing, routing information assaults, selective forwarding, voice-based and GPS spoofing attacks, API vulnerabilities, cyber espionage, and risks stemming from insecure communication protocols and a lack of standardization [9][21][28-35]. Experts highlight incidents like chemical manipulation in water supplies and hacked traffic signals as examples of the disruptions these attacks can cause [36][37]. Cyberattacks on critical urban services—electricity, water, transportation, and emergency systems—undermine public safety, trust, and economic stability while disrupting vital operations [25][38][39]. With threats to intelligent surveillance, digital identity systems, and policy governance increasing, protecting data confidentiality, service integrity, and availability remains crucial to ensure the resilience of smart city infrastructure [39][40].

Robust security measures are crucial for protecting smart city networks from cyber threats and safeguarding the privacy and confidentiality of sensitive data [14]. Preventing disruptions, unauthorized access, or sabotage that could impact city-wide operations requires comprehensive protection [24]. Addressing these risks involves implementing strong cybersecurity protections, safeguarding privacy, fostering stakeholder coordination, and maintaining continuous monitoring. Standard protective techniques like encryption, biometrics, and anonymity are often used but fall short in the context of smart cities [35].

In response to these challenges, integrating AI and Blockchain technology offers promising solutions for managing complex interactions among citizens, government agencies, and private entities. AI enhances cybersecurity through anomaly detection, critical in identifying and mitigating cyber threats. AI analyzes large datasets using machine learning, deep learning, and natural language processing methodologies to detect irregularities and quickly address potential attacks. For instance, machine learning models can identify unusual patterns in network traffic indicative of cyberattacks. These capabilities are particularly advantageous in smart cities, where rapid detection and response are essential to prevent significant disruptions [10][25]. Blockchain technology addresses these challenges with decentralized, secure, and anonymous architecture. Blockchain stores data in cryptographically linked blocks within a peer-to-peer network as an immutable distributed ledger, ensuring data integrity, verifying identities, and enabling secure device communication [41]. Although initially used for fund transfers in trustless networks like Bitcoin, Blockchain has evolved to support applications such as self-executing smart contracts on platforms like Ethereum and Hyperledger [42]. By combining AI's data-driven adaptability with Blockchain's secure, decentralized framework, cities can build robust cybersecurity systems tailored to their needs [25].

This study critically surveys and analyzes existing literature on AI and Blockchain technologies to enhance cybersecurity in smart cities. It reviews key research to identify significant developments, emerging trends, and challenges applying these technologies to secure smart city infrastructures. Several studies have already explored the role of AI and Blockchain in improving cybersecurity for IoT-driven smart cities. For instance, Khan et al. [43] propose integrating secure remote sensing data with Blockchain distributed ledger technology for smart cities. Vempati and Nalini [44] examine the creation of digital twins by combining IoT, AI, and machine learning to strengthen cybersecurity. Despite these advancements, comprehensive research on integrating AI and Blockchain, explicitly addressing the unique cybersecurity challenges of smart cities, remains limited. This survey aims to narrow this gap by analyzing how the synergy of AI and Blockchain can bolster cybersecurity in smart cities and identifying potential future directions for these technologies in this context.

This survey makes several key contributions to the field of smart cities.

- It provides a comprehensive state-of-the-art overview, focusing on their evolution, characteristics, essential components, and system architecture.
- It examines emerging technologies shaping the future of smart cities and the cyber-attacks, threats, and vulnerabilities they face.
- The survey highlights the principles, services, and importance of cybersecurity in ensuring the safety and stability of urban infrastructure.
- It also explores advancements in cybersecurity technologies for smart cities, emphasizing the potential of AI and Blockchain to enhance security measures.
- Finally, it states future research directions in this rapidly evolving domain.

This study is motivated by the pressing need to improve cybersecurity in smart cities by leveraging the potential of AI and Blockchain technologies. Smart cities aim to integrate technology and sustainability to create more resilient, efficient, and responsive communities to residents' needs. However, these advancements have significant challenges, including privacy breaches and security threats. Protecting data is critical to preserving individual privacy and maintaining public trust in these innovative systems. To achieve this, conducting a thorough survey of existing cyber-attacks, threats, vulnerabilities, and security measures is essential, ensuring smart city initiatives' secure and successful deployment.

The survey is organized into several sections: Section 2 presents the methods and materials, while Section 3 reviews the state-of-the-art. Section 4 highlights emerging technologies in smart cities, and Section 5 examines cyber-attacks, threats, and vulnerabilities specific to these environments. Section 6 focuses on cybersecurity strategies for smart cities, followed by Section 7, which addresses technological advancements in this field. Section 8 explores the use of AI and Blockchain to enhance cybersecurity, and Section 9 discusses integrating these technologies for improved security in smart cities. Section 10 proposes future research directions, and Section 11 concludes the survey.

2. MATERIALS AND METHODS

This survey investigates how AI and Blockchain technologies can enhance cybersecurity measures for smart cities. The study utilizes a comprehensive literature review, data collection from academic and industry sources, and qualitative analysis of various case studies, frameworks, and applications. The research focuses on studies published between January 2021 and December 2024, aiming to identify, evaluate, and summarize key research on AI, Blockchain, cybersecurity, and smart city technologies. The primary sources for this study include research articles, conference proceedings, book chapters, and websites related to AI, Blockchain, and cybersecurity in the context of smart cities. To ensure thorough coverage, the researchers searched multiple scientific databases, including ACM Digital Library, Wiley Online Library, Taylor & Francis, Springer, ScienceDirect, MDPI, IEEE Xplore Digital Library, IGI Global, and Google Scholar. They used specific search terms such as "Artificial Intelligence" OR "Blockchain" AND "Cybersecurity" AND "Smart Cities," "Machine Learning" OR "Blockchain Applications" OR "Smart Cities Cybersecurity," and "Deep Learning" AND "Decentralized Security Solutions in Smart Cities," as well as keywords like "Artificial Intelligence in cybersecurity," "Blockchain for smart cities," "Cybersecurity frameworks in smart cities," and "AI and Blockchain in smart city security." Boolean operators like "AND" and "OR" refined the search results to include only relevant papers, and the researchers adjusted keywords to match the search features of each database. The researchers selected these databases because they extensively cover peer-reviewed computer science, engineering, and cybersecurity publications.

The authors independently gathered relevant research papers from selected databases using predetermined criteria. These criteria included the title, authors, publication year, study objectives, research questions, research design, analysis methods, results, conclusions, and key topics related to smart cities. The researchers focused on smart city features and system architecture, emerging technologies, cyber-attacks, threats, vulnerabilities within smart city environments, and cybersecurity principles and services. They also examined the application of AI and Blockchain technologies for cybersecurity in smart cities and explored future research directions.

To ensure consistency and accuracy, the authors systematically organized the collected information. They then applied specific inclusion and exclusion criteria to select relevant review materials. They carefully filtered the literature to include only high-quality studies focusing on AI and Blockchain applications in smart city cybersecurity. The researchers included research studies written in English that focused on AI and Blockchain applications in cybersecurity for smart cities. Eligible studies consisted of peer-reviewed journal articles, conference papers, book chapters, or magazines that presented transparent methodologies and well-defined results. We considered works published between 1 January 2021 and 30 December 2024. The exclusion criteria eliminated studies in languages other than English, those outside the scope of AI and Blockchain in smart city cybersecurity, non-peer-reviewed works, studies with unclear methodologies or ambiguous results, and articles published before 1 January 2021.

The researchers removed any duplicates by checking all initial database results. They then evaluated the abstracts and titles for relevance and reviewed the full text of each relevant article to ensure it met the eligibility criteria. A team of six independent reviewers completed the screening and selection process, with a seventh reviewer resolving any inconsistencies. The team used a test-retest approach to minimize biases in the exclusion criteria, randomly selecting papers from the original research and reviewing them multiple times for accuracy.

The study evaluated one hundred thirty-eight relevant research publications, including one from ACM Digital Library, two from Wiley Online Library, one from Taylor & Francis, six from Springer, twenty-four from ScienceDirect, thirty-six from MDPI, thirty-three from IEEE Xplore Digital Library, three from IGI Global, and thirty-two from Google Scholar. The researchers examined, appraised, and categorized these studies based on their relevance to AI and Blockchain applications in cybersecurity for smart cities. Fig. 1 depicts the digital databases used to retrieve the selected research papers for the survey.

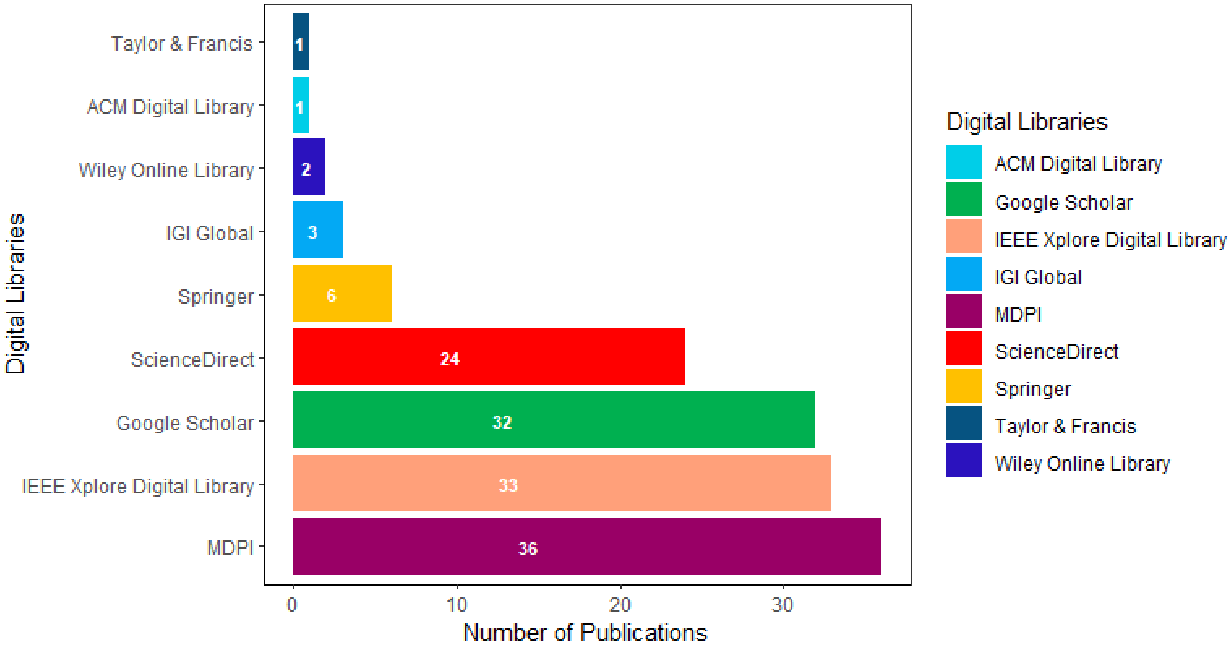

Fig. 1. Depicts the digital databases used to retrieve the selected research papers for the survey.

Fig. 2 shows the distribution of selected papers by digital libraries based on the paper type.

Fig. 3 depicts the distribution of selected papers by digital libraries based on the year of publications.

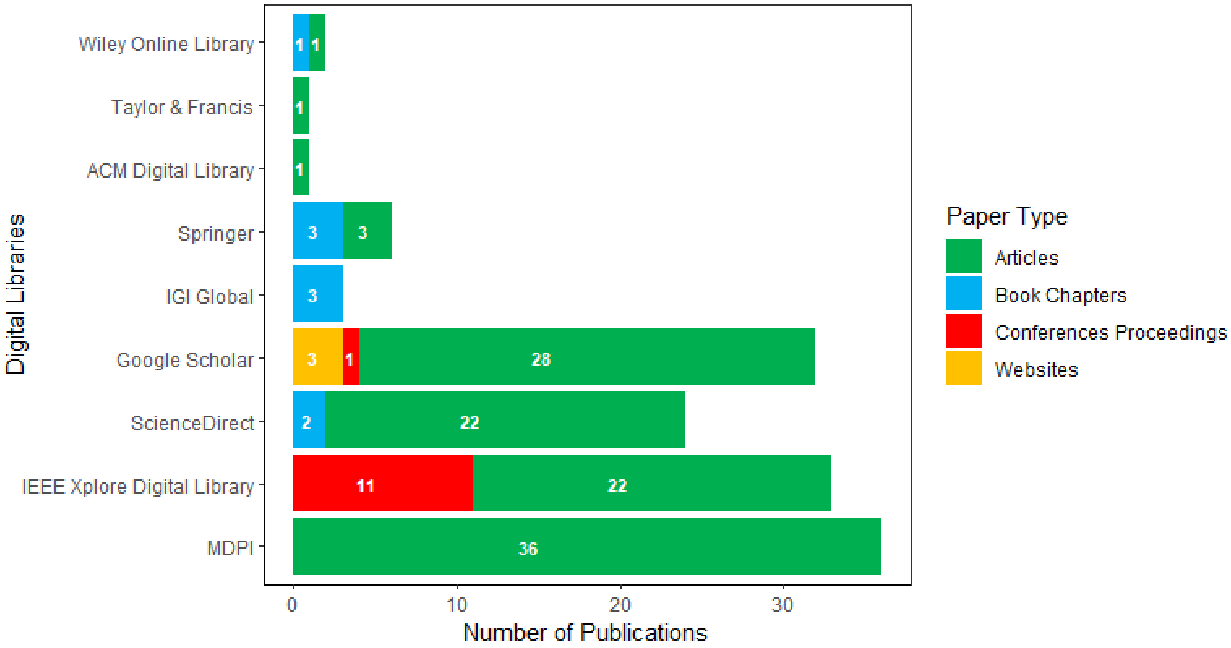

Fig. 2. Shows the distribution of selected papers by digital libraries based on the paper type.

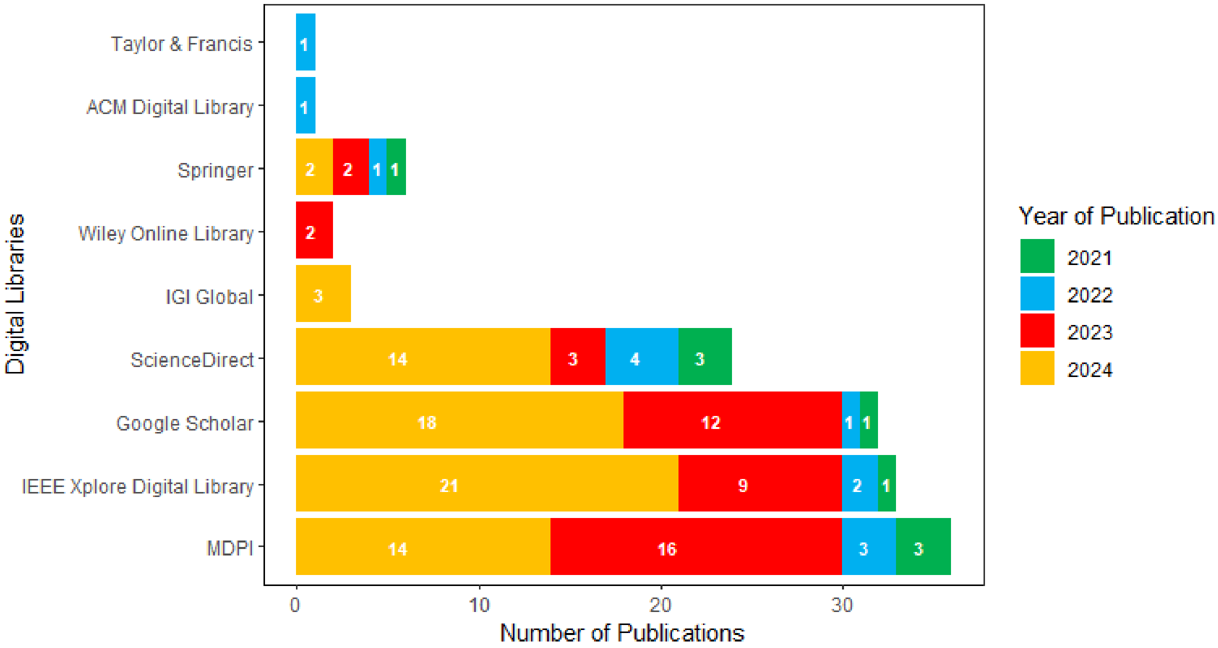

Fig. 3. Depicts the distribution of selected papers by digital libraries based on the year of publications.

The researchers systematically extracted data from each included study to gather relevant information for theme synthesis. They collected data on publication details, study focus, technologies like AI and Blockchain, cybersecurity domains, specific applications within smart city frameworks, and methodologies. They categorized the research into various application areas and cybersecurity domains using thematic analysis. They further classified the studies based on their technological approaches, such as AI, Blockchain, or cybersecurity.

The researchers adopted a qualitative approach to synthesize the findings, categorizing the results into thematic areas based on typical applications, challenges, and solutions identified across the studies. Key themes included AI-driven anomaly detection in IoT devices, Blockchain for data integrity and access control in smart city networks, and the integration of AI and Blockchain for automated security responses and threat mitigation. The researchers compared the effectiveness of AI and Blockchain applications, individually and when integrated, in addressing cybersecurity challenges. They focused on scalability, resource consumption, security levels, and performance in real-world scenarios.

The researchers critically analyzed gaps in existing research and applications, identifying potential areas for future research and technological development based on observed trends. To validate the survey findings, they consulted subject matter experts, cross-referenced results with existing literature, and critically assessed the strengths of the conclusions. They evaluated each paper for quality, considering the strength of the methodology, the reliability and validity of the findings, and their relevance to smart city cybersecurity. Due to its reliance solely on a literature search and lack of primary data gathering, the survey was exempt from ethical approval requirements. The researchers upheld the highest moral standards by adequately citing their sources and ensuring they did not plagiarize.

The researchers examined a subset of literature on methodology and performance measures relevant to smart cities, explicitly exploring the convergence of AI and Blockchain for cybersecurity. To evaluate the success of AI and Blockchain applications, they considered factors such as (1) the reduction in cyberattack incidents, including data breaches, DDoS attacks, and unauthorized access, (2) the ability of the solutions to scale with the growth of smart city infrastructure, (3) the evaluation of system resource consumption (e.g., computation and storage overhead) in AI and Blockchain applications, and (4) the ease of integrating these technologies into existing smart city infrastructures without significant disruptions.

The study also acknowledged potential limitations, noting the rapid advancements in AI, Blockchain, and cybersecurity technologies. It only considered studies published in English and available through major scientific databases, which might have excluded research in other languages or specialized publications. Moreover, as smart cities evolve, new uses and cybersecurity challenges may arise, affecting the relevance of the analysis.

3. PRESENT STATE-OF-THE-ART

The smart city concept originated in the United States in the 1990s, with the International Congress on ‘Smart Cities, Global Networks’ held in San Francisco in 1990. Since then, the definition of a smart city has evolved, requiring a multidisciplinary approach to understand its core elements fully. Scholars generally define a smart city from two perspectives: function and technology. Functionally, developing a smart city involves enhancing the coordination and mutual promotion of key urban sectors, such as the economy, government, people, transportation, environment, and daily life. Technologically, it arises from integrating advanced information technologies such as data storage, circulation, and utilization into existing urban systems [45]. Fig. 4 shows the bird’s-eye view of the smart city [17].

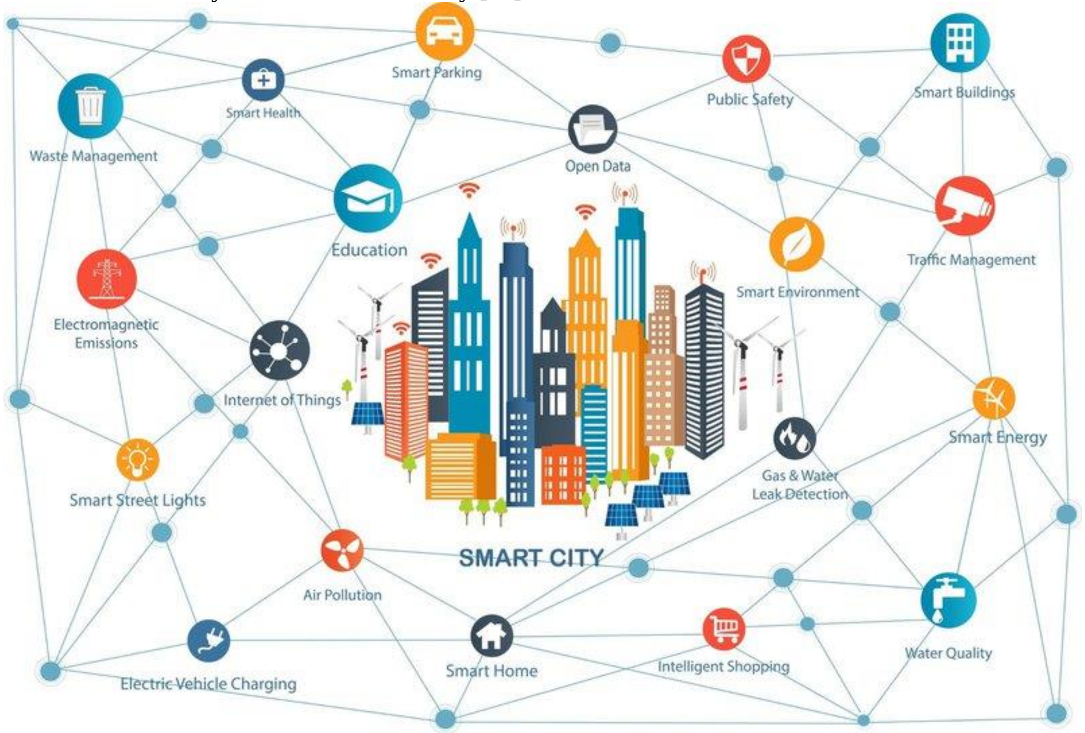

Fig. 4. Shows the bird’s-eye view of the smart city [17].

Smart cities use technological innovations, modern infrastructure, and efficient governance to transform urban spaces into sustainable, inclusive, and well-functioning environments. By combining technology and data analytics, these cities proactively improve residents’ quality of life. They leverage IoT, big data, and advanced analytics to optimize urban operations, improve public services, and promote sustainable growth [46]. Through effective data sharing and utilization across sectors like the economy, governance, transportation, and environmental protection, smart cities increase efficiency, convenience, and intelligence, benefiting their inhabitants. By creating interconnected systems for real-time data exchange and responsive governance, they strive to make urban environments more efficient and livable [45].

3.1. Evolution of Smart City

The evolution of smart cities unfolds across five distinct phases, from Smart City 1.0 to Smart City 5.0. Each phase marks a significant technological, governance, and community engagement leap. These phases highlight how urban environments transform to serve their inhabitants [18] better.

3.1.1. Smart City 1.0: Basic digitization and infrastructure development

Smart City 1.0 marks the first phase of a city's journey toward becoming smart. During this stage, cities actively explore and implement digital technologies, data-driven solutions, and innovative strategies to handle urban challenges and improve the quality of life for residents. This phase focuses on launching essential initiatives, pilot projects, and proof-of-concept efforts to test the viability of new technologies in real-world urban settings. These early projects often address areas such as transportation, energy, waste management, safety, and healthcare to demonstrate their effectiveness and potential for scalability. During Smart City 1.0, cities prioritize building the foundational infrastructure, including high-speed Internet, smart lighting, and basic data collection systems. They also begin digitizing public services, enabling more efficient management of utilities like water and electricity. The main objective of this stage is to establish a connected infrastructure that will serve as the basis for more advanced smart city developments [18][47].

3.1.2. Smart City 2.0: Integration of information technology with urban management

"Smart City 2.0" represents an advanced stage in the evolution of smart cities, building upon the initial efforts of Smart City 1.0. It relies on data-driven approaches, advanced analytics, machine learning, and AI to derive actionable insights, improve operations, and inform strategic decision-making. The focus of Smart City 2.0 is on seamless integration, scalability, sustainability, inclusivity, resilience, and placing citizens at the core. It emphasizes the unified and scalable connection of various systems, technologies, and services across different sectors. By utilizing integrated platforms, APIs, middleware, and cloud solutions, cities ensure smooth connectivity and collaboration among stakeholders, devices, and systems. In addition to foundational infrastructure, it integrates information technology across urban management. Centralized data platforms aggregate information from multiple departments, enhancing coordination and decision-making. Traffic management systems leverage real-time data to ease congestion and boost transportation efficiency, while advanced surveillance and emergency response technologies improve public safety, making cities safer and more responsive [18][47].

3.1.3. Smart City 3.0: Citizen engagement and participatory governance

Smart City 3.0 focuses on innovation, resilience, and adaptability in response to emerging challenges and opportunities. Cities use emerging technologies like Blockchain, IoT, and autonomous systems to build more resilient and adaptive urban environments. Smart infrastructure, such as self-healing power grids and automated water management systems, enhances the reliability of essential urban services. Innovation ecosystems and digital hubs are key in fostering innovation and entrepreneurship. These hubs, which include co-working spaces, incubators, and accelerators, support startups and small businesses while integrating universities and research institutions into the urban innovation ecosystem. The third phase envisions a hyperconnected infrastructure, where technologies like 5G/6G, quantum computing, edge computing, and IoT enable seamless integration, real-time data sharing, and collaborative decision-making. Smart City 3.0 also prioritizes active citizen engagement and participatory governance by deploying digital platforms that allow residents to express opinions, report issues, and participate in decision-making. This inclusive approach fosters community and ensures urban development aligns with residents' needs. Governments use social media, mobile apps, and interactive websites to maintain communication with citizens, enhancing transparency and trust [18][47].

3.1.4. Smart City 4.0: Advanced technologies and data-driven services

Smart City 4.0 represents the next phase in the evolution of urban development, building on the foundations of previous phases and integrating emerging technologies like AI, 5G networks, and edge computing. This phase aims to create more intelligent, responsive, and interconnected urban environments, offering personalized and immersive experiences for both citizens and visitors. Virtual reality and augmented reality technologies will actively shape the development of smart spaces by enabling them to adapt to individual needs and preferences. In addition, Smart City 4.0 fosters greater collaboration between cities and private sector partners while adopting decentralized and distributed governance models. It focuses on the holistic integration and convergence of systems, technologies, sectors, and stakeholders, creating a unified, adaptive urban ecosystem. By leveraging advanced integration platforms, digital twins, and cyber-physical systems, cities will enable seamless collaboration and coordination across the urban landscape. This phase also sees cities use IoT, AI, and big data analytics technologies to offer more efficient and personalized services. Smart grids will optimize energy distribution based on real-time usage, AI-powered analytics will proactively predict and resolve infrastructure issues, healthcare systems will enhance patient care with telemedicine and data-driven diagnostics, and smart transportation networks will ensure seamless mobility by adapting dynamically to changing conditions [18][47].

3.1.5. Smart City 5.0: Sustainable, resilient, and human-centric urban environments

Smart City 5.0 envisions technologically advanced, sustainable, resilient, and human-centric cities. These cities prioritize environmental sustainability by adopting circular economy principles, reducing waste, and promoting renewable energy sources. Resilience is central, with systems in place to quickly recover from natural disasters and other crises. Urban development prioritizes human well-being by enhancing the quality of life for residents. It focuses on improving access to opportunities and resources, fostering social inclusion, and preserving natural areas [18][47].

The evolution from Smart City 1.0 to 5.0 represents a dynamic journey toward more intelligent, responsive, and sustainable urban environments. Each phase builds on the previous one, utilizing technological advancements and fostering greater community involvement to create efficient, innovative, inclusive, and resilient cities. Fig. 5 illustrates the evolution of smart cities from Smart City 1.0 to 5.0.

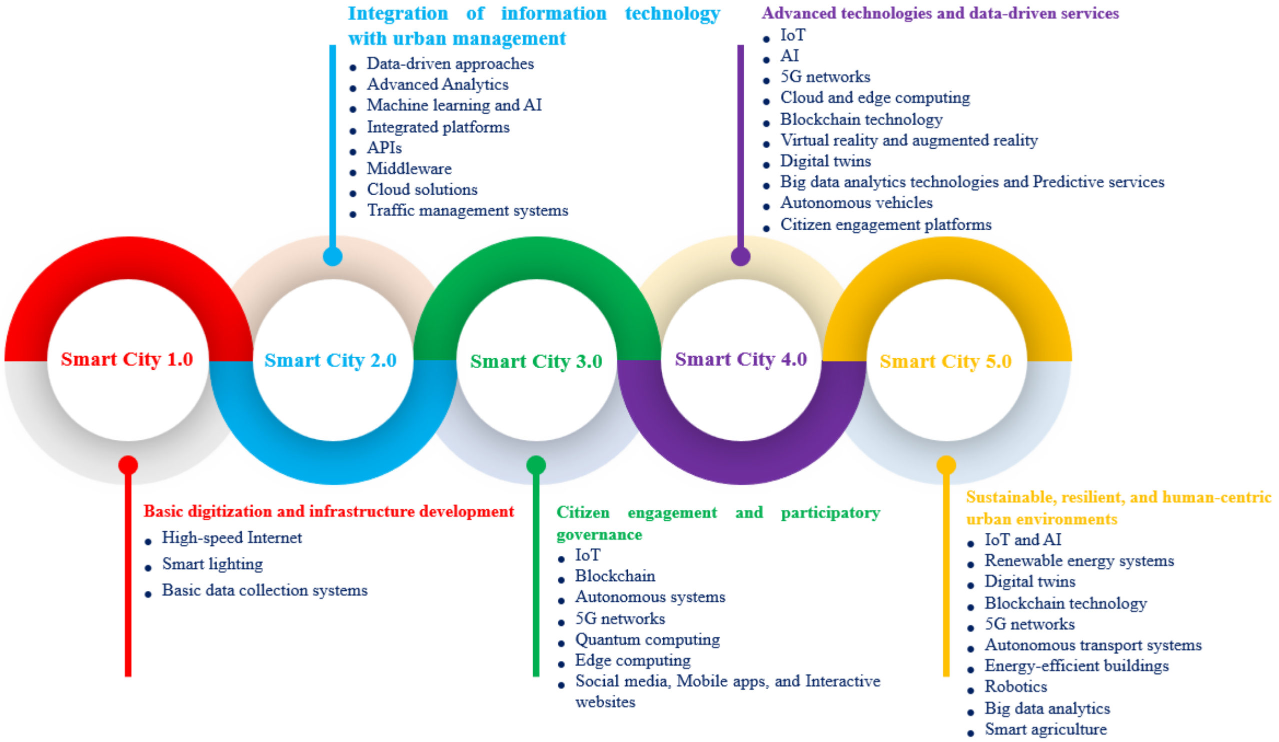
Integration of information technology with urban management
Data-driven approaches
Advanced Analytics
Machine learning and AI
Integrated platforms
APIs
Middleware
Cloud solutions
Traffic management systems
Advanced technologies and data-driven services
IoT
AI
5G networks
Cloud and edge computing
Blockchain technology
Virtual reality and augmented reality
Digital twins
Big data analytics technologies and Predictive services
Autonomous vehicles
Citizen engagement platforms
Smart City 1.0
Smart City 2.0
Smart City 3.0
Smart City 4.0
Smart City 5.0
Basic digitization and infrastructure development
High-speed Internet
Smart lighting
Basic data collection systems
Citizen engagement and participatory governance
IoT
Blockchain
Autonomous systems
5G networks
Quantum computing
Edge computing
Social media, Mobile apps, and Interactive websites
Sustainable, resilient, and human-centric urban environments
IoT and AI
Renewable energy systems
Digital twins
Blockchain technology
5G networks
Autonomous transport systems
Energy-efficient buildings
Robotics
Big data analytics
Smart agriculture

Fig. 5. Illustrates the evolution of smart cities from Smart City 1.0 to 5.0.

3.2. Characteristics of Smart Cities

Smart cities actively use technology and data to enhance quality of life, boost sustainability, and drive economic development. Table I summarizes their key characteristics.

TABLE I. SUMMARY OF KEY CHARACTERISTICS OF SMART CITIES.

S/No	Characteristics	Description	References
1	Heterogeneity	IoT-based systems are defined by their significant heterogeneity, characterized by their autonomous nature, distributed deployment, and use by diverse users. This diversity spans various elements, including IoT nodes, connectivity technologies, mobility options, hardware capabilities, and platforms. Each smart city adopts its own unique IoT architecture, with no universally accepted definition of a smart city.	[9]
2	Resource constraints	Smart cities typically rely on compact, cost-effective embedded devices, often lacking energy efficiency. These devices usually feature limited storage and random-access memory, equipped with 8-bit or 16-bit microcontrollers. Wireless networks using IEEE 802.15.4 radio technology further contribute to slow data transmission speeds, ranging from 20 to 250 kb/s, and restrict frame sizes to a maximum of 127 octets.	[9]
3	Smart mobility	Urban mobility is crucial to modern city development, covering the movement of people within cities and the transportation of goods. Smart city mobility leverages city-wide wireless communication, real-time traffic monitoring, and adaptive problem-solving to optimize transportation systems. It integrates intelligent transportation systems, electric vehicles, ride-sharing services, and autonomous	[9]

		transportation options to reduce traffic congestion, lower emissions, and enhance the overall transportation experience.	
4	Connectivity and scalability	Connectivity forms the backbone of a smart city ecosystem, enabling devices to integrate seamlessly and drive advancements in smart city initiatives. Smart cities leverage advanced communication technologies, including the IoT, 5G networks, and sensors, to collect and exchange data efficiently. As smart cities expand from small-scale projects to larger urban environments, the resulting surge in data and network traffic demands scalable systems.	[9][48]
5	User involvement	Smart city initiatives emphasize human aspects such as education, creativity, and learning. Engaging communities plays a crucial role in improving the quality and effectiveness of smart applications. For example, adequate security measures require a deep understanding of users' needs and concerns, underscoring the importance of early planning involvement.	[9]
6	Infrastructure and connectivity	Smart city infrastructure and connectivity form the technological foundation that empowers cities to collect, analyze, and use data to enhance quality of life, optimize services, and promote sustainability. These systems integrate technology into urban environments, driving innovation, improving efficiency, and supporting sustainable development.	[18][26]
7	IoT and Sensors	IoT connects devices and systems embedded with sensors, software, and technologies, facilitating data collection and exchange across various smart city sectors such as transportation, energy, healthcare, public safety, and waste management. These sensors actively gather real-time data on traffic patterns, air quality, energy consumption, water usage, and waste generation. This data empowers cities to make informed decisions, optimize resources, and enhance operational efficiency.	[18]
8	Data analytics and AI	Smart cities actively leverage data analytics, machine learning, and AI algorithms to analyze vast datasets collected from sensors, social media, and other sources. These technologies uncover urban trends, patterns, and anomalies, enabling cities to predict future scenarios, optimize services, and manage resources proactively.	[18]
9	Sustainable development	Smart city sustainable development involves cities adopting a strategic, holistic approach to foster economic prosperity, social inclusivity, and environmental sustainability while tackling the challenges posed by rapid urbanization and limited resources. By implementing energy-efficient solutions, promoting renewable energy sources, and focusing on waste reduction, smart cities actively improve environmental quality.	[18]
10	Public services and governance	Smart city public services and governance use technology, data, collaboration, and innovation to improve the delivery, accessibility, efficiency, transparency, and accountability of public services while promoting effective governance and citizen engagement. By leveraging digital technologies, smart cities enable citizen participation through e-governance platforms, digital service delivery, open data portals, smart healthcare systems, emergency response systems, and public safety initiatives. Smart governance actively fosters transparency, enhances civic engagement, and streamlines bureaucratic processes, utilizing e-participation, digital voting, and online platforms for community interaction. These efforts aim to create adaptive strategies for responsive, transparent, accountable, inclusive, equitable, and sustainable urban environments that meet the evolving needs and expectations of residents, businesses, and communities.	[18][26]
11	Innovation ecosystem	The smart city innovation ecosystem is an interconnected network of stakeholders, resources, organizations, policies, technologies, and initiatives that drive innovation, entrepreneurship, collaboration, and growth in urban areas. This ecosystem cultivates an environment where innovative solutions to urban challenges and opportunities can be developed, scaled, and implemented. By fostering research, development, collaboration, and investment in technology-driven solutions, smart cities encourage innovation and entrepreneurship. They actively support startups, incubators, accelerators, academic institutions, and industry partnerships, promoting economic growth, job creation, and advancements across various sectors.	[18]
12	Inclusive growth	Smart city inclusive growth focuses on the intentional and equitable development of urban areas, ensuring that all residents, regardless of their socioeconomic status, background, age, gender, ethnicity, or abilities, have access to opportunities, resources, services, and benefits that enhance their well-being, prosperity, and quality of life. These cities prioritize equitable access to technology, services, and opportunities for all, including marginalized and underserved communities. They address social disparities, promote digital literacy, improve accessibility, and foster social cohesion through inclusive policies and programs. By respecting diversity, promoting social justice, and creating shared value, they ensure that all residents benefit from innovation and progress, ultimately building a more resilient and inclusive future for all.	[18]
13	Security and safety	Smart cities leverage technology to improve public safety by using surveillance systems and crime prediction algorithms and enhancing emergency response coordination. Additionally, they implement robust cybersecurity measures to safeguard the city's digital infrastructure, ensuring excellent protection and resilience.	[26]

14	Data-driven decision making	Data collected from sensors, social media, and other sources is analyzed to guide policy decisions and improve services. This analysis helps optimize resource use, minimize inefficiencies, and enhance city management.	[26][49]
15	Citizen-centric services	Technology enhances services such as healthcare, education, and public safety. For instance, smart health monitoring systems, e-learning platforms, and real-time public safety alerts improve efficiency and accessibility. Additionally, citizens can actively engage with local governments through digital platforms, enabling them to report issues, suggest improvements, and access various public services.	[26]
16	Green spaces and urban biodiversity	Green spaces and urban biodiversity are crucial in enhancing city life by providing valuable ecosystem services, improving air quality, and offering recreational opportunities. IoT, AI, and Blockchain help monitor and manage these spaces in smart cities. IoT devices collect real-time environmental data, while AI analyzes this information to assess ecosystem health and recommend necessary interventions. AI also supports sustainable urban planning by simulating ecological impacts and guiding decision-making. Blockchain technology builds trust between residents and authorities by ensuring data transparency and authenticity. Together, these technologies foster biodiversity and sustainability in urban areas.	[31][50-54]
17	Air quality monitoring	Advanced technologies are transforming air quality monitoring by delivering critical data to improve public health. Smart cities now use sensor networks to instantly track particulate matter, nitrogen dioxide, sulfur dioxide, and ozone. AI analyzes this data to identify pollution patterns and sources, enabling city planners to implement targeted interventions. Machine learning models predict future pollution trends, allowing cities to take preventive actions. Blockchain technology safeguards the accuracy and integrity of air quality data, preventing tampering. By adopting this proactive approach, cities effectively address air quality issues and protect residents' health.	[24][51]
18	Digital twin technology	Digital twin technology is revolutionizing urban management by creating virtual models of physical spaces that allow city planners to simulate changes and assess their impacts before implementation. These models integrate real-time data from sensors and IoT devices to capture the essence of cities. They encompass infrastructure, monitor social dynamics, and reflect urban life. Planners can use digital twins to evaluate proposals, such as new transportation routes, and make well-informed decisions. Digital twins support disaster management by simulating emergency scenarios and developing strategies to strengthen urban resilience. This technology empowers planners to improve decision-making and optimize urban planning.	[50]
19	Emergency response systems	Smart cities leverage advanced emergency response systems powered by AI and Blockchain to enhance public safety and crisis management. AI actively analyzes data from sources like cameras, social media, and sensors to identify threats and improve coordination among emergency services quickly. By enabling faster and more effective responses, they significantly reduce the impact of disasters.	[49][50][55][56]

3.3. Key Components of Smart Cities

By integrating these elements, smart cities actively improve urban environments and ensure better resource management while working toward long-term sustainability. A smart city integrates several key components to enhance urban living, and these core components include:

3.3.1. Smart Infrastructure

Intelligent infrastructure, a cornerstone of smart cities, uses IoT devices and sensors to monitor roads, bridges, and public transportation, ensuring safety and efficiency. Smart buildings actively use advanced technologies to optimize energy consumption, improve indoor air quality, and improve occupant comfort, promoting sustainability [57][58]. Sensors provide real-time data on traffic, structural integrity, and environmental conditions, enabling AI to predict maintenance needs, optimize schedules, and prevent costly repairs. Blockchain technology secures data sharing and makes maintenance records transparent, promoting trust and accountability among stakeholders. These innovations collectively drive urban development, improving infrastructure performance and extending lifespan [59][60].

3.3.2. Smart Grid

Smart grid technology improves energy distribution in smart cities by enhancing efficiency, reliability, and sustainability. It optimizes power generation, transmission, and distribution from various energy sources like wind, water, and atomic power [61]. The system integrates generation, transportation, and consumption with IoT sensors, enabling real-time management through cloud or edge computing platforms [62][63]. AI algorithms balance supply and demand, prevent blackouts, and improve system reliability by predicting demand and detecting anomalies [63]. Blockchain supports peer-to-peer energy trading, strengthens security, and creates a tamper-proof ledger for energy transactions [31][50].

3.3.3. Smart Economy

An innovative economy fosters competitiveness, innovation, and knowledge-based growth, adapting to challenges to increase productivity and internationalization [64]. It leverages IT to enhance efficiency, address issues, make informed decisions, and promote interdisciplinary collaboration. Environmental preservation, sustainability, and advanced research drive innovation and creativity. Smart cities use technology to offer cost-effective solutions and support sustainable entrepreneurship, circular economy models, and global financial networks [65]. This innovative economy improves productivity, fosters entrepreneurship, and enhances citizens' quality of life [9][66][67].

3.3.4. Smart Transportation

Intelligent transportation systems unify and automate data to enhance user experiences and efficiency. IoT devices collect real-time traffic, road, and passenger data, which AI analyzes to optimize traffic flow, adjust transit schedules, and offer live updates [11]. Predictive analytics forecast congestion, while Blockchain ensures secure agency data sharing [52]. Autonomous vehicles improve safety, and innovative mobility solutions reduce reliance on single-occupancy vehicles by promoting walking, biking, and public transit [17][61]. Innovations like ride-sharing and bike-sharing ease congestion, improve air quality, and create more intelligent, more sustainable urban mobility [9][57][64][68].

3.3.5. Smart Healthcare

Smart healthcare integrates IoT components like wearables and mobile Internet to connect people, materials, and institutions, improving accessibility, especially in remote areas [62]. It supports elderly individuals by enabling independence at home and reduces hospital resource strain through remote monitoring. AI, robots, and telemedicine enhance diagnosis, treatment, and affordability [11][61]. Blockchain ensures data security, while AI-driven solutions use health data for proactive care and public health management [17][63]. In smart cities, machine learning analyzes health records and predicts outbreaks, improving care and guiding policies [9][66][68].

3.3.6. Smart waste management

Smart waste management uses IoT, AI, and Blockchain to improve city waste collection and disposal. IoT sensors monitor bin fill levels, while AI optimizes collection routes, cuts fuel consumption, and reduces emissions. AI also predicts waste patterns, allowing for better resource allocation and reduction strategies [63]. Blockchain ensures transparency by securely tracking waste activities. These innovations enhance recycling, reduce landfill use, and help cities achieve sustainability goals while cutting costs and supporting circular economy efforts.

3.3.7. Smart Industry

Integrating cyber-physical systems with IoT in factories has led to faster advancements, improved efficiency, better quality, and fewer accidents [61]. However, smart industries face challenges in using IoT due to the complexity of managing diverse equipment and automation. Overcoming these challenges requires rapid deployment and flexible, connected systems. AI can accelerate Industry 4.0 by collaborating with IoT, using sensor data to enhance automation and decision-making. Researchers also suggest incorporating data for prescriptive analytics to improve smart industry operations [69].

3.3.8. Smart governance

Smart city applications in governance transform urban operations by enhancing transparency, accountability, and citizen participation [64]. Using IoT devices and sensors, smart cities collect real-time data to optimize infrastructure and resources, such as improving traffic flow and road safety. This technology also boosts public service efficiency and fosters greater citizen engagement through new communication channels [57]. Smart governance increases transparency and productivity, tailoring services to citizens' needs with open data and e-government services [9]. It strengthens administrative services, promotes sustainable development, and enhances social welfare by focusing on citizen-centric digital platforms [65][67].

3.3.9. Smart citizens

Smart citizens enhance their lives and contribute to their communities by leveraging digital literacy, education, and entrepreneurial skills in a technology-driven lifestyle. They actively embrace new technologies to solve local issues, improve their quality of life, and drive positive change within their communities [64][67]. Smart cities empower residents to engage in governance through mobile apps, AI, and Blockchain, enhancing communication and service delivery. These technologies analyze citizen feedback and optimize resource allocation, ensuring efficient city operations. Blockchain ensures data privacy and fosters transparency, while machine learning supports data-driven policies [11][17][50][52]. Smart citizens focused on sustainability are central to building communities prioritizing well-being, environmental preservation, and digital inclusion [9][65].

3.3.10. Smart water management systems

Smart water management systems use IoT devices to monitor water quality, detect leaks, and manage irrigation in real time, preventing waste and ensuring a reliable water supply. AI-driven sensors track water quality parameters, and machine learning algorithms predict and detect leaks in aging infrastructure. AI optimizes water distribution by adjusting flow to match real-time demand, preventing shortages. Blockchain ensures transparency by securely storing water data and providing reliable records to stakeholders. These technologies promote sustainability, conserve resources, and improve urban water services [55][70][71].

3.3.11. Smart parking solutions

Smart parking solutions enhance urban mobility by reducing congestion and improving the driving experience. AI optimizes parking management by analyzing usage patterns and predicting demand for better resource allocation. Blockchain ensures secure, transparent transactions, builds trust, and prevents fraud. These systems integrate with public transport and alternative transportation options, promoting sustainability. By managing parking and encouraging alternative transport, smart parking reduces emissions, improves air quality, and supports healthier urban living [24][31][50][52].

3.3.12. Smart lighting

Smart street lighting uses advanced technologies to optimize energy use, improve safety, and enhance the smart city experience. Sensors detect traffic, weather, and security threats, while AI adjusts brightness based on real-time data. Blockchain tracks energy use and costs transparently, and integration with urban services like traffic management and emergency response improves city efficiency. These systems, including cameras and electric vehicle charging stations, create a more connected urban environment. Together, they lay the foundation for a more intelligent city network [24][51][72][73].

3.3.13. Smart Agriculture

Smart agriculture boosts crop profits with minimal investment while promoting natural farming by avoiding chemicals [61]. It uses sensors in trees and farms to monitor factors, aiding decision-making and preventing pests and diseases. These sensors provide data for targeted crop care. Agriculture is key to food security, sustainability, and environmental health. AI-driven IoT technologies improve farming by analyzing farm conditions, diagnosing issues, and guiding decision-making [69].

3.3.14. Smart Education

Smart applications in education aim to improve learning outcomes, increase access to education, and enhance the student experience. Personalized learning platforms, for example, use AI and machine learning algorithms to adjust learning materials to fit each student's needs, boosting engagement and understanding. Learning analytics also play a key role in analyzing student performance data to uncover patterns, helping teachers provide targeted support. In smart cities, education is further enhanced through digital classrooms, online learning platforms, and skill development programs, ensuring equal access to quality education and preparing citizens for future opportunities [57].

3.3.15. Smart energy management

Sustainable energy management in smart cities focuses on optimizing energy use and minimizing environmental impact by integrating renewable sources and smart grids. These grids utilize digital tools and two-way communication to balance supply and demand efficiently. AI forecasts energy needs, manages peak loads, and integrates renewable energy through real-time adjustments [17][63]. Blockchain enables secure, transparent energy trading, while machine learning analyzes consumption patterns to optimize infrastructure [51][71]. ICT supports smart grids, ensuring reliable, scalable, and green energy integration across sectors, driving sustainable energy transformations [11][57].

3.3.16. Smart Environment

Smart environments enhance urban development and quality of life using IoT sensors and data analytics to monitor environmental factors like air quality, noise, and pollution [63][64]. These technologies enable quick detection of hazards such as floods or pollution, allowing authorities to take timely actions like road restrictions or evacuations [9]. By integrating with city systems, they optimize resource use and improve safety. They also promote sustainability through waste management and renewable energy initiatives [9][61]. Advancements in sensor technologies support real-time monitoring, leading to better decision-making and reduced environmental risks [57][65][74].

3.3.17. Smart Buildings

Smart buildings enhance energy efficiency and operational effectiveness by adjusting lighting and temperature based on occupancy and integrating smart devices to automate daily tasks. They monitor structural integrity and use sensors and grid technologies to communicate with building equipment, sending energy data to the smart grid and receiving feedback [9][75]. This integration helps optimize energy profiles, supporting demand response and peak load reduction. Smart building platforms combine operational technology to manage equipment and information technology to analyze data. These buildings also integrate with various sectors like security, logistics, and education, enhancing the energy grid's sustainability [68].

3.3.18. Smart public services

Smart cities enhance public services by using real-time data to improve efficiency and quality of life. IoT devices monitor services like waste management and water supply, optimizing routes and cutting costs. AI analyzes data for better decision-making, resource allocation, and timely interventions. AI-powered surveillance, facial recognition, and predictive analytics improve safety and crime prevention. Smart governance, with real-time data, strengthens crime prevention, emergency response, and municipal services [9][31][68][74][76].

3.3.19. Public safety and security

AI-powered surveillance systems enhance public safety by analyzing real-time footage to detect unusual behaviors, enabling quick responses from authorities. Predictive policing helps law enforcement allocate resources efficiently by identifying crime patterns. AI aids in emergency planning by predicting high-risk zones for strategic resource deployment. Blockchain ensures secure, transparent data sharing among agencies, fostering trust and accountability. Integrating AI, machine learning, deep learning, and Blockchain improves safety, efficiency, and public trust, while robust privacy safeguards are essential for protecting sensitive data in smart cities [17][51][58][63][77].

3.3.20. Smart living

Smart living represents a high quality of life in a safe, welcoming urban environment where everyone can access public services and educational, cultural, health, and social infrastructure [64]. It focuses on optimizing and managing facilities to enhance residents' quality of life, a key goal of sustainable and smart territories. Built on the pillars of civic safety, social cohesion, and tourist attraction, smart living maximizes city infrastructure while improving urban life. By enabling real-time control, forecasting, and efficient asset management, it offers practical solutions for modern cities. The innovative application of technology drives cities to become more intelligent and inspires individuals to embrace a better way of living [65][66].

3.3.21. Digital identity solutions

Digital identity solutions enhance security and privacy by leveraging Blockchain technology to manage personal data securely. Blockchain's decentralized nature makes it harder for hackers to access or manipulate sensitive information. These solutions simplify service access and reduce administrative tasks by enabling secure identity verification. Users gain control over their data, sharing what is necessary to prevent identity theft. AI plays a role in improving identity verification by analyzing biometric data such as fingerprints and facial recognition. By combining AI and Blockchain, the efficiency and security of smart city services are significantly boosted [25][50][51].

3.3.22. Smart utilities

Smart utilities focus on minimizing energy, gas, and water consumption, supporting economic growth and sustainability. They use smart grids, decentralized energy storage, and virtual power plants as key applications. These systems often integrate electric vehicles and decentralized electricity generation, with smart metering devices playing a crucial role. Additionally, smart utilities monitor water resources, control water pressure, and dynamically manage a mix of conventional and renewable energy sources to meet current and future electricity demands [9].

Smart cities integrate advanced technology and sustainable practices to transform urban spaces into more livable, resilient, and inclusive environments. They tackle challenges such as climate change, rapid urbanization, and resource scarcity, embodying a proactive and innovative approach to urban development.

3.4. Smart City Architecture

The architecture of a smart city operates through a multi-layered framework that efficiently manages resources, enhances residents' quality of life, and promotes sustainability. It integrates various technologies and components across distinct layers to optimize data flow and improve city management and service delivery. The design of this architecture is scalable and dynamic, enabling the system to adapt to the evolving functional and quality requirements of city services. By facilitating seamless integration, these layers make smart cities more responsive to citizens' needs, ensuring better management and service delivery in an ever-changing environment [78][79]. Below is a detailed explanation of the layers of the system architecture for smart cities. Fig. 6 shows the main layers in the smart city architecture.

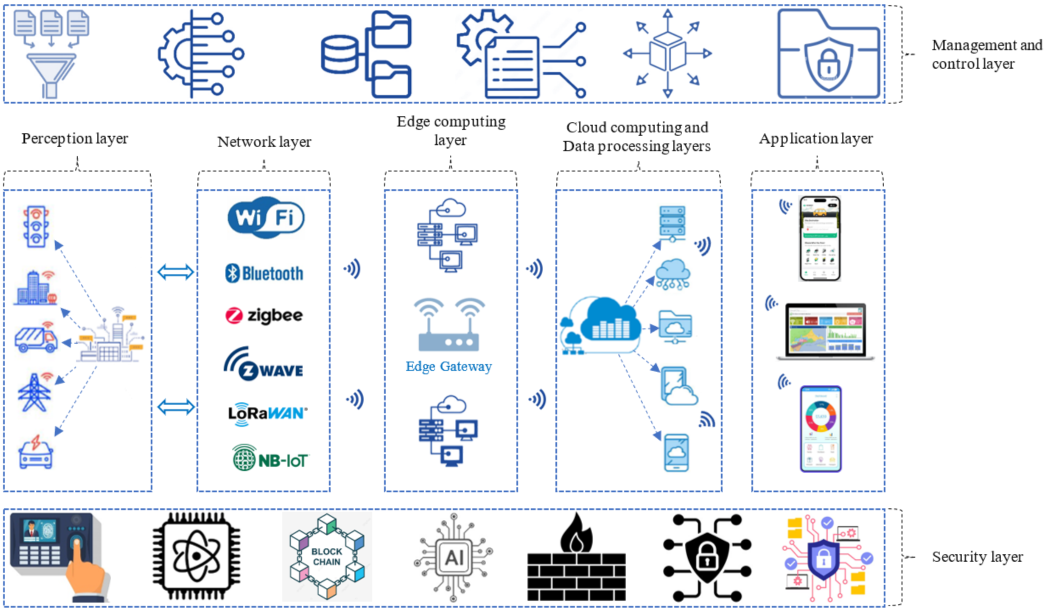

Fig. 6. Shows the main layers in the smart city architecture.

3.4.1. Perception layer

The perception or sensing layer plays a crucial role in smart city architecture by collecting real-time data from urban environments to support city management and decision-making. IoT sensors and devices, such as environmental sensors, motion detectors, smart meters, RFID tags, and GPS systems, gather vital information that helps improve public health, enhance security, and optimize resource use and transportation. Edge devices process this data locally, reducing latency, conserving bandwidth, and enabling quick responses to dynamic urban conditions, such as adjusting traffic signals or activating emergency alarms. Actuators then transform the data into actions, managing traffic signals, street lighting, and HVAC systems to enhance energy efficiency, safety, and comfort. Together, these integrated technologies form a responsive, data-driven urban ecosystem that fosters sustainability, resilience, and effective governance, making the perception layer increasingly essential as smart city initiatives continue to grow [19][58][71].

3.4.2.Network layer

The network layer is the communication backbone in smart city architecture, enabling seamless data transfer and connectivity between devices and systems. It ensures smooth information flow from data collection to processing and storage. Advanced wireless protocols, such as Wi-Fi, Bluetooth, Zigbee, and Z-Wave, support short-range communication, while cellular technologies like 4G LTE and 5G provide high-speed data transfer for real-time applications. Low-Power Wide-Area Networks (LPWANs), including LoRaWAN and NB-IoT, deliver energy-efficient, long-range connectivity for IoT devices. This layer supports scalability, security, and interoperability, enabling real-time analysis and decision-making while protecting data from cyber threats. Integrating innovative technologies enhances urban management and responsive smart city services [19][41][58][77].

3.4.3.Edge computing layer

Edge computing improves cloud computing by processing data closer to its source, which offers multiple benefits. It reduces latency, making it essential for applications that require real-time responses, such as traffic management and emergency services. By filtering and processing data locally, edge devices cut down on bandwidth usage and operational costs, boosting efficiency. Edge computing enhances traffic monitoring and emergency response capabilities, leading to better resource management. Furthermore, it supports localized processing, ensuring critical functions continue even in areas with limited cloud connectivity [80].

3.4.4.Cloud computing layer

Cloud computing plays a critical role in smart cities by providing the infrastructure to store, process, and manage massive amounts of data generated by IoT devices, sensors, and other sources. It offers scalable storage, computational power, and the flexibility to meet the dynamic needs of urban environments. Cloud platforms enable real-time data analysis, machine learning, and AI model training, which are essential for smart city applications. The scalability of cloud solutions allows cities to adjust resources based on fluctuating data volumes, such as during events or emergencies while ensuring secure storage and accessible data for analysis. Moreover, cloud computing reduces costs by minimizing the need for physical servers, allowing cities to pay only for the resources they use [19][50].

3.4.5. Data processing layer

The data processing layer is critical in smart city architecture as it transforms raw data from urban sensors into actionable insights. It leverages cloud and edge computing, big data analytics, and AI to process and analyze data, enabling real-time decision-making. Key functions include efficient data storage, predictive analytics for urban planning, and AI-driven optimization of operations such as traffic flow and resource allocation. Real-time processing tools allow for rapid responses to emergencies and dynamic urban challenges. This layer supports infrastructure development, enhances public safety, and helps city managers improve efficiency, sustainability, and residents' quality of life [55][58].

3.4.6. Application layer

The application layer directly serves smart city residents by transforming analyzed data from previous layers into practical services that address urban challenges and enhance quality of life. It applies AI-driven traffic management, energy optimization, and smart healthcare systems to improve efficiency, sustainability, and public safety. IoT-enabled waste management and smart water meters also ensure resource efficiency and cost-effectiveness. Residents can actively engage with services and participate in governance through user-friendly interfaces such as mobile apps and dashboards. This layer enables data-driven decision-making, allowing city officials to optimize urban planning and operations, fostering sustainability, operational efficiency, and stronger community connections [19][81].

3.4.7. Security layer

Smart city security integrates robust technologies and practices to ensure data integrity, privacy, and reliability. It employs data encryption to protect sensitive information, access controls such as role-based authentication, and Blockchain for transparent, tamper-proof data sharing. Data anonymization helps safeguard citizens' identities while still allowing for data analysis. Advanced threat detection systems monitor and respond to cyber risks in real time. At the same time, AI-powered algorithms improve threat detection by adapting to emerging risks for faster and more accurate responses. Smart cities foster trust and resilience in urban infrastructures by prioritizing security and ensuring sustainable and safe operations [56][71][77].

3.4.8. Management and control layer

The management and control layer is the backbone of smart city operations, ensuring seamless coordination across various components to optimize efficiency and performance. It enhances resource utilization and operational effectiveness by integrating advanced tools for data orchestration, real-time analytics, and automation. These tools enable smooth communication between sensors, processing units, and application interfaces, preventing bottlenecks and facilitating rapid responses to urban needs. Real-time data visualizations on analytics dashboards monitor city performance, supporting informed decision-making, while automation controllers handle routine tasks, improving efficiency in areas like energy management and traffic control. By promoting adaptability, the management and control layer enhances service delivery, urban resilience, and residents' quality of life, fostering sustainable development and addressing emerging challenges [53][82].

The system architecture of smart cities optimizes urban living by integrating IoT devices, data processing, AI, cloud computing, and security protocols. It improves city operations, enhances public services, and promotes sustainability, making cities more efficient, responsive, and resilient. This architecture addresses urbanization challenges and significantly enhances residents' quality of life.

4. EMERGING TECHNOLOGIES IN SMART CITIES

Emerging technologies transform smart cities by driving efficiency, sustainability, and citizen-focused urban development. Table II briefly gives an overview of key emerging technologies that are making an impact in smart cities.

TABLE II. BRIEF OVERVIEW OF KEY EMERGING TECHNOLOGIES MAKING AN IMPACT IN SMART CITIES.

S/No	Emerging Technologies	Brief Description	References
1	Internet of Things (IoT)	The IoT connects physical and virtual objects through interoperable technologies, forming a global infrastructure that supports advanced services and the information society. It integrates sensors, actuators, and communication capabilities into everyday devices like smart refrigerators and air conditioning units, enabling them to collect and share data online. IoT drives smart city development by powering real-time data collection on traffic, air quality, and energy use, allowing officials to optimize resources and improve urban functionality. Across sectors such as healthcare, transportation, and agriculture, IoT fosters innovation with smart grids, automated waste systems, and intelligent meters that cut costs and reduce environmental impact. However, its rapid growth amplifies cyber threats, compatibility issues, and data management challenges, demanding robust solutions to realize its full potential.	[9][11][26][50][83-86]
2	Artificial intelligence	Artificial intelligence designs computer systems to analyze data, follow programmed instructions, and perform tasks requiring human intelligence, such as learning, pattern recognition, natural language understanding, and decision-making. AI technologies like machine learning, deep learning, natural language processing, and robotics	[9][17][84][85][87-91]

		transform smart cities by enabling efficient urban management and sustainability. Middleware platforms, including CityPulse and OpenIoT, use machine learning for data quality monitoring, decision-making, and optimized digital responses. AI enhances urban systems by predicting traffic flow, energy demand, and urban growth, automating traffic control, public transit schedules, and waste management. It also strengthens public safety through predictive policing, real-time surveillance, and anomaly detection.	
3	Big data and analytics	Big data in smart cities comes from IoT devices, sensors, social media, public services, and other sources characterized by volume, velocity, variety, veracity, and value. Smart city middleware integrates and processes this data, addressing challenges like security, privacy, and real-time processing. Tools like Hadoop, Spark, and NoSQL databases enable efficient analysis, while Open Data initiatives enhance transparency by providing access to public service information. Advanced analytics help city planners identify patterns, predict traffic congestion, and optimize transportation routes. Real-time insights allow officials to monitor operations, resolve issues, and allocate resources effectively.	[84][85][92]
4	Blockchain technology	Blockchain technology enhances security, data integrity, and trust in smart cities through its decentralized, immutable, and transparent framework. It integrates seamlessly with IoT systems, enabling secure, tamper-proof data management via peer-to-peer networks and consensus protocols like Proof-of-Work (PoW) and Proof-of-Stake (PoS). Key features such as cryptographic security, smart contracts, and traceability streamline urban operations, including payments, identity management, and energy grid efficiency. By automating agreements and enhancing governance transparency, Blockchain safeguards digital identities, ensures transaction authenticity, and benefits supply chain tracking and environmental monitoring. Despite challenges like high energy demands in PoW, its integration with AI and IoT unlocks innovative solutions for sustainable and efficient smart city ecosystems.	[1][29][31][41][55] [62][72][85][93][94]
5	Fifth-generation (5G) networks and wireless communication technology	The rollout of 5G networks transforms smart cities by providing greater bandwidth, lower latency, and higher connectivity density, driving IoT adoption and enabling advanced AI applications. It enhances device and system communication, enabling real-time data sharing for applications like autonomous vehicles, remote healthcare, and augmented reality. 5G accelerates the deployment of smart city services, such as smart buildings, video surveillance, and holographic applications, while integrating edge computing to reduce delays and improve efficiency. It supports data-intensive applications by boosting IoT performance and enabling rapid decision-making. However, 5G faces challenges, including high infrastructure costs and increased security risks from expanded data flow and connected devices.	[65][84][94][95]
6	Augmented reality and virtual reality	Augmented and virtual reality enhance urban planning and community engagement by immersing stakeholders in interactive visualizations of proposed developments. Augmented reality overlays digital models onto the real world, helping residents and planners understand and discuss changes. These technologies improve smart city services, such as disaster response, medical aid, and navigation. Virtual reality provides immersive training for city officials and emergency responders, optimizing urban planning and crisis management. Bridging gaps in digital literacy, infrastructure, and community engagement is essential to ensure equal access.	[96]
7	Cryptography	Cryptographic algorithms secure smart application services by preventing unauthorized access during data storage, processing, and sharing. Traditional encryption faces challenges on resource-constrained devices due to high computational complexity and energy demands. Lightweight encryption techniques are essential for practical implementation in smart systems. Lightweight public key encryption, homomorphic encryption, and zero-knowledge proofs improve security in smart city applications, healthcare, and cloud computing.	[9]
8	Biometrics	Studies have identified biometrics as an effective solution to address key security and privacy concerns in smart cities. Biometrics is widely used in IoT-based systems to authenticate individuals through unique biological and behavioural traits, such as facial features, vocal patterns, and signatures. Brainwave-based authentication has emerged as a promising method, offering enhanced reliability and operational efficiency. Researchers have proposed standard authentication protocols to protect users' sensitive data on storage devices, reducing security risks and communication overhead. However, to prevent privacy breaches, developing privacy-preserving biometric techniques is crucial.	[9]
9	Unmanned Aerial Vehicles (UAVs)	UAVs provide significant flexibility, cost, and capability benefits, whether autonomous or remotely controlled, especially in smart city surveillance. They outperform traditional systems like CCTV cameras by covering large areas, operating at various altitudes, and transmitting real-time data. In disaster management, UAVs assist in damage assessment, search and rescue, and aerial mapping after natural disasters. They also support emergency responses by aiding police, monitoring traffic, and delivering medical supplies. Additionally, UAVs contribute to IoT, power efficiency,	[11][91][97]

		environmental sustainability, and infrastructure inspection, transforming urban service delivery and planning.	
10	Autonomous Systems	Artificial intelligence and robotics advances drive the development of autonomous systems in urban environments, such as self-driving cars, delivery drones, and robotic assistants, which will enhance city safety, efficiency, and mobility. These systems, often designed as robots, are set to play a crucial role in future urban landscapes. For instance, shifting from individually owned vehicles to shared autonomous transportation could transform commuting patterns. Additionally, autonomous systems can perform essential city tasks, including waste collection, street cleaning, and aerial surveillance, using drones to operate autonomously.	[9][94]
11	Autonomous vehicles	Autonomous vehicles transform urban transportation by enhancing efficiency and reducing congestion with advanced self-driving technology. They use sensors and communication tools to connect to cellular networks, enabling real-time traffic updates and emergency services. These vehicles interact with infrastructure like traffic signals for dynamic route optimization. Ride-sharing and driverless taxis further reshape mobility, while autonomous buses offer on-demand public transport. Despite regulatory challenges, collaboration between developers, regulators, and communities is crucial to creating adaptive policies for safe, sustainable innovation.	[98][99]
12	Sensor networks	Sensor networks form the backbone of smart city applications such as smart public services, environments, buildings, and mobility. These networks collect vital data to enable informed and automated decisions. For example, they support air quality monitoring, fire detection, CCTV systems, and traffic control via induction loops. Cities are expanding sensor coverage across urban areas, integrating data from consumer electronics like smartphones through participatory sensing. Additionally, sensors enhance location-based services, leveraging GPS, GLONASS, and Galileo receivers in portable devices.	[9]
13	Wearable devices	Wearable devices collect unique personal data, such as heart rate, blood pressure, and brain activity, and transmit it to medical professionals via communication technology, improving healthcare. These devices are useful in hospitals for whole-body monitoring and in homes to track the vital signs of those with chronic conditions. The U.S. Communications Commission has recognized these programs. Entertainment wearables, like smartwatches and fitness trackers, are becoming more popular. Additionally, smart nanotextiles with sensing, actuation, and communication features boost the adoption of environmental and health monitoring.	[9]
14	Cloud computing	Cloud computing revolutionizes how individuals and businesses access, store, and process data using Internet-hosted servers. It shifts IT costs from capital expenditures to recurring service usage fees. This technology supports smart cities by enabling scalable data analysis and managing IoT device integration for intelligent decision-making. Cloud platforms and services like CSaaS and CPaaS provide efficient, scalable solutions for city applications and reduce development time. These cloud-based solutions enhance scalability, flexibility, and cost-effectiveness while simplifying device management and software deployment.	[62]
15	Fog computing	Fog computing bridges the gap between edge and cloud by processing data at local nodes, such as gateways, for faster, more efficient handling. Technologies like FogFlow, SEDIA, and SmartCityWare use this model to optimize resource use and support smart city IoT services. Enabling real-time data processing helps manage traffic congestion and enhances public safety through rapid surveillance and threat detection. Its hierarchical architecture, with layers for monitoring, pre-processing, storage, and security, ensures efficient data flow. Fog computing boosts smart city functionality with flexible, dynamic applications that decouple software and hardware.	[62]
16	Edge computing	Edge computing is vital in addressing latency-sensitive applications and easing network demands in smart cities by processing data near its source, such as IoT devices. It enables real-time analysis and quick responses, benefiting applications like autonomous vehicles, industrial automation, and remote monitoring. Offloading tasks to edge devices reduces network congestion and dependency on cloud services and improves performance. Edge computing also filters and prioritizes data before sending it to the cloud, optimizing resource usage. Distributed edge computing, like MEC, offers scalable solutions that enhance real-time analytics and responsiveness in urban settings for time-sensitive applications.	[62][85][94]
17	Cyber-physical systems	Cyber-physical systems (CPS) integrate computational, networking, and physical processes to drive smart cities by optimizing resources, improving services, and enhancing quality of life. They enable the integration of ICT with urban infrastructure, helping manage energy, reduce emissions, and improve traffic control. Technologies like smart grids, autonomous vehicles, and medical monitoring demonstrate CPS applications in smart cities. Platforms like OpenIoT and middleware such as InterSCity simplify CPS integration and management. CPS also plays a crucial role in Industry 4.0, supporting automation, data exchange, and digital twins across the healthcare, transportation, and energy sectors.	[85][91]

18	Renewable Energy	The push for sustainability has ushered in a new era of urban development, with renewable energy playing a key role in smart city initiatives. As cities adopt digital technologies, they increasingly use renewable energy sources to minimize their environmental impact and enhance energy efficiency. Rapid urbanization drives higher energy demand, making the transition to cleaner alternatives essential. Solar, wind, hydro, and bioenergy replace fossil fuels, cutting emissions and improving air quality. This shift boosts energy security, resilience, and local economies by creating jobs and reducing dependence on external energy sources.	[91]
19	Smart grids technologies	Smart grid technologies modernize the electrical grid by integrating renewable energy, storage, and demand-response systems. These technologies enhance energy efficiency, reduce emissions, and improve grid reliability in smart cities. By incorporating solar and wind energy, smart grids reduce dependence on fossil fuels and support sustainability goals. They also provide real-time data to anticipate demand and prevent outages. However, their increased connectivity exposes the grid to cybersecurity risks, necessitating strong security measures like encryption and regular assessments to protect critical infrastructure.	[76][77][84]
20	Mobile crowd sensing and computing	Mobile Crowd Sensing and Computing (MCSC) utilizes mobile devices like smartphones, wearables, and in-vehicle systems to gather and analyze urban data. Integrated with smart city middleware, MCSC enhances traditional data sources, providing a fuller picture of urban dynamics. For example, OpenIoT's "Urban Crowdsensing Service" collects real-time air quality data via wearable sensors. S2NetM combines crowd-sourced data with IoT inputs for better decision-making. While MCSC focuses on crowd-sourced data and related challenges, edge computing emphasizes processing data at the source to ensure efficiency, integrity, and minimal delays.	[85]
21	Semantic web and ontologies	Semantic Web technologies and ontologies improve data representation, validation, and querying in smart city middleware. Resource Description Framework and Web Ontology Language provide standardized methods for sharing data, ensuring interoperability across smart city applications. For example, the ontology in S2NetM represents social relationships among IoT devices and incorporates ontology alignment and reasoning mechanisms for efficient data querying. Platforms like SGeoL and SEDIA use Semantic Web technologies for data annotation, validation, and inference, enhancing semantic searches and analysis. Middleware solutions like Snap4City apply the Km4City Ontology to represent city data, support sensor discovery, and offer personalized services using ontology-based reasoning.	[85]
22	Cybersecurity	As smart cities integrate ICT, cybersecurity becomes crucial to protect urban digital ecosystems. The reliance on digital technologies for city services exposes them to new risks, making robust security measures essential for public trust and sustainable development. Advanced security systems, like machine learning, are used to detect sophisticated cyber threats. The expansion of smart devices increases the attack surface, emphasizing the need for strong cybersecurity. Governments enforce cybersecurity standards to ensure the resilience and safety of urban systems, with technologies like encryption and Blockchain securing communication and data.	[85][91][92]

5. CYBER ATTACKS, THREATS, AND CHALLENGES IN SMART CITIES

Smart cities leverage advanced technologies to create interconnected urban environments, optimizing services and infrastructure. They enhance the quality of life, boost efficiency, and promote sustainability in the transportation, healthcare, energy, and public safety sectors. However, their reliance on digital systems exposes them to increasing cyber-attacks, threats, and vulnerabilities. Below is a detailed explanation of smart cities' key cyber-attacks, threats, and vulnerabilities.

5.1 Data privacy concerns

Smart cities use technologies like IoT, AI, and big data to enhance urban living but raise significant data privacy concerns. Surveillance cameras, sensors, and mobile apps collect extensive personal data, such as vehicle movements and household energy usage, often without clear safeguards [24][46][91]. Facial recognition technology heightens these risks, as seen in cases of exposed personal data and hefty fines for unauthorized data collection [30]. Data sharing among public and private stakeholders frequently lacks transparency, leading to unauthorized use and breaches. Cybersecurity threats, unregulated data usage, and poorly secured virtual reality systems expose cities to privacy violations and misuse [9].

5.2 Data breaches and unauthorized data access

Smart cities face significant risks from cyberattacks that exploit vulnerabilities in interconnected systems, often due to poor cybersecurity practices like weak passwords and outdated software [24]. Hackers have targeted critical infrastructure, such as the 2021 Oldsmar water treatment facility attack, where they attempted to alter water chemical levels—similarly, breaches like the 2019 compromise of a Singapore public transport app exposed sensitive user data. IoT devices, essential to smart cities, frequently lack robust security, as seen in the 2016 Mirai botnet attack, which disrupted numerous systems. These attacks compromise privacy, disrupt services, and erode public trust, highlighting the urgent need for stronger cybersecurity measures [28].

5.3 Ransomware and malware attacks

Ransomware and malware attacks threaten smart cities by targeting interconnected systems and causing widespread disruptions. Ransomware encrypts data and demands payment for releasing the decryption keys, while malware steals, corrupts, or deactivates data. High-profile attacks, such as the 2019 ransomware attack on Baltimore and the 2018 attack on Atlanta, disrupted city services and cost millions in recovery. Malware incidents like the 2016 Mirai botnet have paralyzed emergency responses, energy grids, and transportation [28][72]. Weak security practices, outdated software, and poor system updates amplify these vulnerabilities, emphasizing the urgent need for robust cybersecurity measures.

5.4 Insider threats

Insider threats pose a serious risk to smart cities, as individuals like employees or contractors can misuse their access to compromised systems or data. Malicious insiders may intentionally disrupt services or leak sensitive information, as seen in 2021 when a dismissed IT contractor planted ransomware on California municipal servers [28]. Negligent actions, such as downloading malware or mishandling information, also lead to breaches, exemplified by a 2020 European smart city employee exposing networks to phishing scams. Insiders often bypass traditional security measures to steal data, deactivate systems, or aid external attacks. For instance, a former Tesla employee leaked sensitive data in 2018, highlighting the potential devastation if similar actions targeted smart city infrastructure [76].

5.5 Replay attacks

Replay attacks are a serious cybersecurity threat to smart cities, where attackers intercept and reuse valid data transmissions to manipulate systems or gain unauthorized access [61]. These attacks exploit device vulnerabilities and real-time communication systems that control transportation, energy, and public safety. For instance, attackers can replay signals in smart transportation to evade tolls, manipulate traffic lights, or cause accidents. Similarly, they can falsify energy usage reports in smart grids or disrupt billing processes by resending old meter signals. By intercepting legitimate access signals, attackers can also breach building security or public transportation systems, endangering sensitive operations and data [31].

5.6 Social engineering attacks and phishing attacks

Social engineering and phishing attacks exploit human psychology to target smart cities, tricking individuals into revealing sensitive information or granting unauthorized system access [28]. These attacks disrupt operations, compromise data, and erode public trust in digital infrastructure. Hackers often impersonate trusted authorities, like IT administrators, to manipulate city employees or residents into resetting passwords or sharing access codes. In one case, attackers infiltrated a U.S. water treatment facility while phishing emails disguised as COVID-19 updates compromised devices in a European smart city [61]. Cybercriminals also exploit public Wi-Fi and fake apps, such as a fraudulent parking app that stole users' payment details, highlighting the need for secure platforms.

5.7 Denial of service (DoS) attacks

Denial of Service (DoS) attacks threaten smart cities by overwhelming systems and services with excessive traffic, rendering them inaccessible to legitimate users. These attacks disrupt critical services like transportation, healthcare, and public utilities, compromising safety and public trust. Hackers also target energy grids, with attacks on sensors and communication systems risking failures across essential services like hospitals and emergency responses. Vulnerable IoT devices, such as surveillance cameras and traffic sensors, have been exploited in DDoS attacks, as seen in 2019, when hackers deactivated a city's surveillance system, endangering public safety [9][61].

5.8 Distributed DoS (DDoS) attacks

Distributed DoS (DDoS) attacks threaten smart cities by flooding critical systems with traffic from compromised devices, rendering them inaccessible [100]. These attacks target interconnected services like transportation, energy, healthcare, and public safety, causing disruptions, financial losses, and eroding public trust [61]. In 2016, a Distributed DoS (DDoS) attack deactivated San Francisco's Municipal Transportation Agency ticketing machines, forcing free rides and disrupting operations. Hackers frequently exploit IoT devices, such as traffic cameras and public Wi-Fi, to create botnets, as seen in the 2016 Mirai botnet attack. Public transportation and energy grids are particularly vulnerable, with incidents like large-scale energy disruptions highlighting the risks [28]. Successful DDoS attacks can paralyze essential services, delay responses, and compromise public safety [101].

5.9 Man-in-the-Middle (MItM) attacks

Man-in-the-middle (MitM) attacks pose significant cybersecurity risks to smart cities by enabling attackers to intercept and modify communications between two parties. These attacks can result in data theft, service disruptions, and security breaches, particularly in systems managing sensitive data and critical services [61]. Hackers can exploit vulnerabilities in IoT devices, sensors, and servers, disrupting real-time communication. For example, attackers might tamper with traffic management systems to cause accidents or manipulate data in smart energy grids to alter billing or disrupt energy supply. Public Wi-Fi networks further expose smart cities, as rogue hotspots allow hackers to steal sensitive login credentials and payment details.

5.10 SQL injection attacks

SQL injection attacks pose a significant cybersecurity threat to smart cities by exploiting vulnerabilities in databases and applications. Malicious actors inject harmful SQL code into input fields, leading to unauthorized access, data corruption, or system compromise [61]. Smart cities, which depend on databases for transportation, utilities, and healthcare, are especially vulnerable. For example, attackers could target ticketing systems to steal personal data, alter fares, or modify schedules. Attackers might also alter medical records, compromising patient privacy and safety

5.11 Zero-day exploits

Zero-day exploits pose a serious cybersecurity risk to smart cities by targeting unknown vulnerabilities that have not yet been identified or patched. These vulnerabilities allow attackers to strike before developers respond, leading to potential disruptions [33]. Critical systems like energy grids, transportation, and healthcare are at risk in smart cities. For instance, attackers could manipulate power distribution, cause traffic accidents, or breach sensitive healthcare data. By bypassing security measures unnoticed, zero-day exploits threaten the safety and stability of smart city infrastructure [32].

5.12 Supply chain vulnerabilities

Supply chain vulnerabilities pose significant cybersecurity risks to smart cities, which rely on third-party vendors for critical services and components. A breach in any part of the supply chain can undermine the security and integrity of the entire system, leading to data theft, service disruptions, or damage to infrastructure. Attackers can exploit software vulnerabilities in IoT devices, like those used in transportation systems, to manipulate data or deactivate sensors [87]. The 2020 SolarWinds attack demonstrated how infiltrating a vendor’s software update process can impact vital city functions [87]. Additionally, compromised physical components, such as sensors or hardware, can provide attackers access to sensitive data and control over city systems.

5.13 Side-channel attacks

Side-channel attacks target physical traits or unintended emissions from hardware devices to access sensitive data without authorization. These attacks exploit vulnerabilities in smart city devices, such as power consumption, electromagnetic radiation, or sound. By analyzing these emissions, attackers can bypass traditional security, extract encryption keys, or disrupt critical systems [61]. For example, differential power analysis allows attackers to monitor power fluctuations and interfere with grid management in energy grids. Similarly, attackers can exploit electromagnetic emissions from IoT devices to disrupt traffic, steal data, or manipulate systems.

5.14 Advanced persistent threats (APTs)

Ali et al. [33] define APTs as prolonged, targeted cyberattacks that infiltrate networks and maintain unauthorized access to critical systems. These attacks can disrupt smart cities’ energy, transportation, healthcare, and public safety services. APTs can manipulate or deactivate systems, causing blackouts, altering traffic signals, or breaching healthcare data. They exploit vulnerabilities in IoT devices, which often lack strong security, to gain long-term network access, which risks city operations and sensitive data, potentially causing widespread damage.

5.15 Cryptojacking

Cryptojacking occurs when hackers exploit a system’s computing power to mine cryptocurrency without the owner’s consent [33]. In smart cities, attackers target interconnected devices and critical infrastructure like IoT devices, public services, and energy grids. These attacks drain resources, slow performance, and increase operational costs [33]. IoT devices, traffic systems, and energy grids are especially vulnerable to cryptojacking. The consequences include inefficiencies, power outages, and disruptions to essential services, with incidents spiking in 2018.

5.16 Black hole attacks

A black hole attack occurs when malicious actors intercept and discard data packets, disrupting device communication [32][102]. In smart cities, these attacks target the interconnected networks crucial for traffic, energy, and public safety. Attackers exploit protocol vulnerabilities to sever data flow, causing outages and delays. In smart traffic systems, they can cause traffic light malfunctions and congestion, while in smart grids, they may disrupt power management and cause outages. In healthcare, these attacks can compromise patient data, delay medical care, and endanger lives.

5.17 Gray hole attacks

Gray hole attacks are network threats where attackers selectively drop or alter specific data packets, making them harder to detect than black hole attacks, which discard all packets [32][102]. These attacks disrupt critical operations in smart cities, such as traffic control, energy management, and healthcare. For example, attackers can manipulate traffic data packets, causing signal adjustments and vehicle counting delays, leading to congestion. In energy grids, they may target power usage or fault detection packets, resulting in inefficiencies or blackouts. Healthcare systems also suffer, with attackers dropping patient information, delaying treatments, or causing misdiagnoses.

5.18 Sinkhole attacks

A sinkhole attack is a cyberattack where attackers manipulate routing protocols to redirect traffic to a compromised node, creating a "sinkhole" that traps data [61][102]. In smart cities, such attacks can disrupt communication networks essential for traffic control, energy distribution, and public safety. Attackers can target routing infrastructure, causing system failures, service outages, or manipulating critical functions. For example, sinkhole attacks can trigger traffic control failures, power outages, or incorrect medical diagnoses. These disruptions severely impact the safety and efficiency of smart city systems.

5.19 Wormhole attacks

Wormhole attacks exploit vulnerabilities in routing protocols to create shortcuts, redirecting communication and data between distant nodes. Attackers can capture and inject data into different network parts, disrupting operations, introducing delays, and spreading false information [61][102]. These attacks can severely impact smart cities by disrupting transportation, energy grids, healthcare, and public safety systems. For example, they can cause traffic delays, mismanage power distribution, alter medical data, or hinder emergency responses. Such disruptions pose significant risks to the safety and efficiency of interconnected networks.

5.20 Sybil attacks

Sybil attacks pose significant risks to smart cities by allowing malicious entities to create fake identities or nodes, disrupting network operations. Attackers flood systems with bogus nodes, manipulating data flow and decision-making processes [32][61][102]. These attacks can lead to system failures and security breaches, affecting services like traffic, energy, healthcare, and public safety. In traffic management, fake nodes can mislead algorithms, causing congestion. In smart grids, they can distort energy data, leading to outages or misdistribution.

5.21 Illusion attacks

Illusion attacks occur when attackers deceive systems into accepting false or misleading information, causing incorrect decisions [102]. These attacks can disrupt critical services in smart cities, such as traffic control, energy distribution, healthcare, and public safety. In transportation, attackers may distort traffic data, mismanage signals, and delay emergency vehicles. In energy grids, they can manipulate power data, causing misallocation and outages. Illusion attacks in healthcare can create false patient conditions, leading to dangerous medical errors, while they also threaten public safety by tampering with surveillance and emergency communication systems.

5.22 Sleep denial attack

A sleep denial attack targets low-power devices, like IoT sensors, by preventing them from entering sleep mode, causing excessive energy drain. These attacks disrupt smart city infrastructure, including traffic management, energy grids, and healthcare systems. By keeping devices active, they deplete batteries, degrade performance, and cause network congestion [61]. These attacks delay responses and compromise system reliability in critical areas like public safety and medical monitoring. Preventing devices from conserving energy leads to inefficiencies and failures, jeopardizing essential services.

5.23 Fake node injection

Fake node injection is a cyberattack where attackers introduce fraudulent nodes to disrupt networks, gain unauthorized access, or manipulate data [32][61]. This attack threatens services like transportation, energy, healthcare, and public safety in smart cities. It can distort traffic data, causing delays or congestion. Attackers can mislead energy grids, resulting in power misallocations or outages. In healthcare and public safety, fake nodes can cause misdiagnoses, delay treatments, and hinder emergency responses.

5.24 Buffer overflow

Buffer overflow attacks occur when attackers write more data to a buffer than it can hold, overwriting adjacent memory and potentially causing system crashes or enabling malicious code execution [32][61]. These attacks present serious risks to smart cities, which depend on interconnected devices and real-time data processing for essential infrastructure. Exploiting system vulnerabilities like traffic management, energy grids, healthcare devices, and surveillance networks can disrupt services and compromise data integrity. Attackers could manipulate traffic systems, mismanage power in smart grids, or interfere with healthcare devices. Such disruptions could lead to system failures, accidents, or fatalities.

5.25 Vulnerabilities in IoT devices and infrastructure

IoT devices and infrastructure vulnerabilities present significant security risks for smart cities, which depend on interconnected devices for critical services like transportation, energy, healthcare, and public safety [32][7]. Weak authentication and inadequate encryption open devices to attacks, while poor patch management and physical security issues add to the challenges. Unsecured communication protocols like Message Queuing Telemetry Transport (MQTT) can compromise data integrity and jeopardize public safety. Attackers can exploit these weaknesses to disrupt essential services, steal data, or gain unauthorized access [103]. These vulnerabilities can severely affect city operations [9][31][50].

5.26 Threats to critical infrastructure

Smart cities face significant threats to their critical infrastructure due to interconnected technologies and IoT devices. Cyberattacks targeting essential services like transportation, energy, healthcare, and communication can disrupt operations and endanger lives. Healthcare systems and IoT devices are prime targets, and attacks on communication networks can hinder emergency response. Natural disasters further expose vulnerabilities, complicating recovery efforts. To protect smart cities, strong cybersecurity measures like firewalls, intrusion detection systems (IDS), and regular vulnerability assessments are essential [50][76].

5.27 Artificial intelligence attacks

AI-driven systems in smart cities face growing cybersecurity risks as attackers exploit vulnerabilities like adversarial machine learning and data poisoning [32]. Malicious actors can manipulate traffic, energy grids, surveillance, and healthcare systems, causing service disruptions and safety hazards. They may also hijack autonomous vehicles, robots, and drones for harmful purposes. AI-powered virtual assistants and chatbots are vulnerable to social engineering attacks, undermining public trust. These threats underscore the need for stronger cybersecurity measures to safeguard smart city infrastructure [9].

5.28 Smart grid attacks

Smart grid systems, which distribute electricity through sensors, communication technologies, and data analytics, are vulnerable to cybersecurity threats. Malicious actors can exploit these weaknesses to disrupt power distribution, damage infrastructure, and jeopardize public safety. Attacks may target communication networks, manipulate control systems, or inject false data into algorithms, causing outages and equipment damage. Insider threats, DDoS attacks, and physical sabotage also pose risks. Integrating renewable energy sources increases these vulnerabilities, allowing attackers to manipulate solar or wind systems data and destabilize the grid [9].

5.29 Smart building security vulnerabilities

Smart buildings in smart cities face critical security risks, with cybercriminals increasingly targeting their IoT devices, sensors, and interconnected systems. Unsecured devices, weak protocols, and compromised building management systems offer attackers easy access [104][105]. Exploiting issues like default passwords, outdated firmware, and unencrypted data transmission, hackers can disrupt operations and steal sensitive information [104][105]. Vulnerabilities in physical security systems further expose buildings to risks, while privacy concerns arise from the vast amount of personal data collected [104][105]. Ransomware attacks, insider threats, and cyberattacks on smart systems are on the rise, stressing the need for stronger security measures.

5.30 Blockchain vulnerabilities

Despite their strong reputation for security, Blockchain networks are vulnerable to issues like smart contract bugs and 51% attacks, which can compromise their integrity [32]. In 2020, concerns emerged in Zug, Switzerland, about the risks of Blockchain-based voting systems. In 2016, attackers exploited flaws in Ethereum's smart contract code, causing the DAO hack and a loss of US$50 million in cryptocurrency. These vulnerabilities jeopardize the security of Blockchain systems. This is particularly concerning for smart city applications, such as voting, resource management, and financial transactions.

5.31 Vulnerabilities in connected vehicles

Due to technology vulnerabilities, connected vehicles pose significant risks to smart cities' safety, privacy, and efficiency. Their reliance on IoT, Vehicle-to-Everything (V2X) communication, and autonomous features exposes them to cyberattacks, threatening transportation systems and public safety [106]. Attackers can exploit weaknesses in V2X protocols, insecure IoT devices, and flawed over-the-air (OTA) updates to manipulate data, control vehicles, or inject malware. Collecting personal data also raises privacy concerns, making identity theft and surveillance possible. As autonomous vehicles become more common, the risks increase, demanding stronger security measures to protect smart cities.

5.32 Wi-Fi attacks

Wi-Fi attacks in smart cities present significant security risks, as attackers target widely used communication networks. They exploit vulnerabilities to disrupt services, steal data, or compromise systems [107]. For example, MitM attacks occur when hackers intercept device communication via rogue access points [108]. Attackers also crack weak Wi-Fi passwords or launch evil twin attacks to steal sensitive information [107]. The growing number of IoT devices, many of which lack strong security, amplifies the risks, along with threats like packet sniffing and Wi-Fi jamming, which can affect critical urban systems.

5.33 Physical security attacks

Physical security attacks in smart cities threaten critical infrastructure, IoT devices, and connected systems. As cities rely more on technology in transportation and utilities, attackers target assets such as data centers, smart sensors, and devices [32]. They tamper with IoT devices to alter or deactivate data, causing financial losses or disruptions [28][61]. Unauthorized access to critical facilities can lead to sabotage, data theft, or hardware implantation. Additionally, threats to communication infrastructure, autonomous vehicles, and drones further jeopardize urban security.

5.34 Radio-frequency interference/jamming

Radio-frequency (RF) interference and jamming attacks threaten smart cities by disrupting wireless communication channels that support critical systems [32]. Attackers can overpower legitimate signals, affecting smart traffic lights, public safety communications, and payment terminals, which can cause traffic accidents or delays in services like air quality monitoring and automated lighting. Critical infrastructure, like emergency response systems, is vulnerable, endangering lives. RF attacks can block payment systems and disrupt connectivity, leading to service outages and reduced reliability for businesses and residents [61].

5.35 Cloud malware injection attacks

Cloud malware injection attacks pose a significant security threat to smart cities, which depend on cloud computing for managing data from interconnected systems. Hackers exploit vulnerabilities in cloud infrastructure to inject malicious code, steal data, disrupt services, or compromise functionality [61]. For example, attackers can target cloud-based transportation systems, causing traffic gridlock, or manipulate Infrastructure as a Service (IaaS) platform to disrupt public services like water treatment or data encryption. IoT devices further expand the attack surface, allowing hackers to tamper with energy usage or billing in smart meters. These attacks can have immediate and widespread consequences in smart cities.

5.36 Signature wrapping attacks

A signature wrapping attack targets extensible Markup Language (XML)-based protocols like WS-Security by exploiting vulnerabilities in digital signature implementation [32]. In this attack, the attacker intercepts and alters a signed XML message, modifying its structure without invalidating the signature. This enables attackers to inject malicious content, compromising systems in smart cities. For example, they could disrupt energy allocation, alter transportation routes, or manipulate healthcare records, posing safety and service stability risks. Signature-wrapping attacks threaten the integrity of interconnected smart city systems [61].

5.37 Web browser attacks

Web browser attacks pose serious risks to smart cities, which depend on interconnected systems for management and communication. These attacks exploit browser vulnerabilities to steal data, disrupt operations, or compromise systems. Phishing emails may trick employees into revealing login credentials, while cross-site scripting (XSS) injects malicious code into websites [61]. Man-in-the-browser (MitB) attacks target sensitive transactions, altering payments or data. Additionally, drive-by download attacks and software vulnerabilities can infect systems with malware, disrupting vital city services.

5.38 Traffic analysis attacks

Traffic analysis attacks seriously threaten smart cities by exploiting communication patterns and metadata exchanged between connected devices. Adversaries can monitor network traffic to infer sensitive information without decrypting the content. These attacks jeopardize smart city infrastructures' privacy, security, and efficiency, which rely on constant data flow. For example, attackers could deduce occupancy patterns from smart energy meters or uncover routes and schedules of public transportation systems. Even encrypted surveillance feeds can reveal high-monitoring zones, making smart cities vulnerable to disruptions and security breaches [61].

5.39 RFID spoofing

Radio-frequency identification (RFID) spoofing poses a significant security risk in smart cities, where RFID is used for access control, transportation, and asset tracking. In such attacks, attackers mimic legitimate RFID signals to gain unauthorized access or deceive systems [32]. In public transportation, they clone RFID cards to bypass payments, while in smart parking systems, they manipulate restricted access. Spoofing also disrupts asset tracking, leading to misdirected equipment and system failures, and this emphasizes the need for strong security measures to prevent RFID spoofing and protect critical infrastructure [61].

5.40 Routing information assaults

Routing information attacks seriously threaten smart cities by targeting the protocols that manage data flow across networks. These attacks intercept, manipulate, or redirect traffic, compromising critical systems like transportation and infrastructure. For instance, MitM attacks can alter data in smart grid systems, risking power outages. Routing table poisoning misdirects data, disrupting traffic management or emergency services. DoS and Sybil attacks can overwhelm networks, causing delays or malfunctions in healthcare and smart water management [61].

5.41 Selective forwarding

Selective forwarding is a network attack that disrupts smart city communication by intentionally dropping or blocking specific data packets. This attack can impair systems like smart traffic management, causing delays or accidents by blocking critical traffic data. It also affects smart grids by preventing energy usage data from reaching operators and risking power outages. In healthcare, it delays vital medical information, endangering patient care. Additionally, attackers can block vehicle data in smart transportation, leading to delays and potential accidents, especially with autonomous vehicles making unsafe decisions [61].

5.42 Voice-based attacks

Voice-based attacks are becoming a growing threat in smart cities as more urban infrastructure integrates voice recognition and control systems. Attackers exploit vulnerabilities in technologies like smart assistants and security systems to bypass authentication and disrupt services [109]. Techniques like voice spoofing allow attackers to impersonate legitimate users and gain unauthorized access [110]. AI-powered voice synthesis and voice command injection can manipulate systems, causing accidents or breaches. Eavesdropping and vishing further compromise security, targeting residents and city employees for sensitive information [109][110].

5.43 GPS spoofing

Global positioning system (GPS) spoofing poses a significant cybersecurity threat to smart cities by feeding false signals to GPS receivers and disrupting location-based services [111]. It can mislead transportation systems, such as autonomous vehicles and drones, causing incorrect routing and unsafe decisions. Traffic management systems may miscalculate flow, leading to congestion and accidents. GPS spoofing can also affect smart grids, triggering energy imbalances or blackouts and compromising the efficiency of emergency vehicles [112]. Additionally, it can disrupt waste management, surveillance systems, and city services, undermining safety and operations.

5.44 API vulnerabilities

Application programming interfaces (APIs) are crucial for smart cities, enabling communication between systems and devices, but If not properly secured, they present significant security risks. Common API attacks include injection, DDoS, MItM, credential stuffing, and insecure key generation [113]. Vulnerabilities such as poor authentication, data exposure, lack of encryption, improper input validation, and inadequate rate-limiting can be exploited by attackers [113]. These weaknesses allow unauthorized access, data manipulation, and disruption of services like transportation or healthcare. Insecure third-party integrations and outdated APIs further heighten the risks to smart city infrastructure.

5.45 Cyber espionage

Cyber espionage in smart cities involves covert cyberattacks targeting government bodies, organizations, and critical infrastructure to steal sensitive data for political, economic, or strategic purposes. Smart cities generate massive data through their interconnected systems and IoT devices, which makes them prime targets for cyberattacks. Attackers exploit vulnerabilities in energy grids, water supply systems, and transportation networks to manipulate and disrupt these infrastructures [114]. They also target data from urban planning, traffic management, and governance for business intelligence or to incite unrest. Social engineering, spear-phishing, supply chain attacks, and zero-day exploits access these systems.

5.46 Insecure communication protocols

Insecure communication protocols in smart cities pose significant cybersecurity risks as they rely on interconnected systems across transportation, energy, and healthcare sectors. Weak or outdated protocols, unencrypted data transmission, and unsecured networks expose critical data to interception and unauthorized access. These vulnerabilities can cause privacy breaches, service disruptions, and operational failures. Poorly configured APIs and insecure devices increase the risk of cyberattacks. To protect smart city infrastructure, strong cybersecurity measures, standardized protocols, and increased awareness are essential [31].

5.47 Lack of standardized protocols

Smart cities face significant challenges due to the lack of standardized protocols, which affect system integration, interoperability, and security. Without common standards, devices and platforms like sensors, energy grids, and healthcare networks struggle to communicate, causing inefficiencies and delays, which leads to emergency response, traffic management, and system scalability issues. Inconsistent security protocols increase the risk of cyberattacks, jeopardizing public safety. The lack of standardized data formats also hampers data analysis, impeding decision-making and snowballing operational costs [39].

Smart cities face cyberattacks and threats that jeopardize their functionality and safety. To address these challenges, cities must develop robust cybersecurity strategies.

6. CYBERSECURITY IN SMART CITIES

Cybersecurity in smart cities focuses on protecting digital infrastructure, data, and systems from cyberattacks as cities increasingly rely on technology and interconnected networks. Smart cities integrate IoT devices, sensors, and AI-driven systems to enhance transportation, energy management, public safety, and waste management, but these advancements also introduce vulnerabilities that cybercriminals can exploit. For example, compromised IoT systems like smart traffic lights or water management sensors can disrupt essential services, as seen in Johannesburg's 2019 ransomware attack that affected electricity and water supplies. Similarly, a 2020 breach in a Florida water treatment facility revealed how hackers attempted to manipulate chemical levels, highlighting the need for secure access controls and monitoring. While improving decision-making and predictive analytics, AI also creates opportunities for attacks, such as disabling surveillance systems or injecting false data to compromise public safety. Smart cities must adopt multi-layered security strategies to mitigate these risks. Cities like Singapore set a global example by enforcing strict data protection regulations and cybersecurity frameworks to safeguard infrastructure. Ultimately, cybersecurity is not just a technical concern but a critical aspect of smart city governance, requiring proactive strategies, risk assessments, and community involvement to ensure technological advancements benefit citizens safely and securely.

6.1. Cybersecurity Principles in Smart Cities

Protecting smart cities requires strong cybersecurity principles, as interconnected systems rely on data, sensors, and AI to improve urban living. The key principles confidentiality, integrity, availability, and resilience—ensure the security and reliability of smart city infrastructure. By implementing these principles, cities can safeguard their systems against threats and maintain seamless operations.

6.1.1. Confidentiality

Confidentiality protects sensitive information from unauthorized access, which is vital in smart cities where personal and government data are constantly collected [32-34]. Smart traffic networks gather real-time data to optimize routes, while smart meters track detailed energy consumption in residential areas. Hackers who gain access to this information could misuse it to monitor individual movements, cause disruptions, or violate privacy. Organizations must implement encryption and role-based access controls to prevent such risks and regularly update these protocols to counter evolving threats. Recent studies emphasize the importance of safeguarding personal and critical government data to ensure the confidentiality and security of smart city applications [54][115].

6.1.2. Integrity

Integrity is vital for preserving the accuracy and trustworthiness of data, which is essential for the effective functioning of smart city systems [32-34]. These systems, such as smart energy grids, rely on accurate data to adjust power distribution based on demand predictions. If hackers tamper with this data, it can lead to outages, overloads, or inefficient energy use, disrupting critical services. Data accuracy and reliability from sensors and devices are vital for informed decision-making by city planners and emergency responders. Organizations must use techniques like hashing and digital signatures to effectively verify data integrity, fostering trust in the systems supporting urban infrastructure. For example, tampered data from traffic sensors can hinder traffic management, potentially causing congestion or accidents. Therefore, protecting data integrity is a technical necessity and vital for public safety.

6.1.3. Availability

Availability is crucial to ensuring that critical systems and services in smart cities remain operational when needed. Emergency response networks, public surveillance, and healthcare monitoring must always be accessible. For instance, a cyberattack on a smart healthcare system could delay access to medical data during emergencies, risking lives. Prioritizing availability helps protect against such failures, ensuring timely services and continuous operations. Ensuring authorized users can access information when necessary is vital to maintaining services like traffic flow and emergency responses [32-34]. Organizations must implement resilient backup systems and redundancy measures to reduce the risks of system failures. For example, a backup protocol in a traffic management system ensures safety during a cyberattack by enabling alternative traffic control measures. Additionally, regular stress testing helps identify vulnerabilities and strengthen resilience, providing critical services to remain operational during disruptions.

6.1.4. Resilience

Resilience refers to a system's ability to recover from cyberattacks or disruptions quickly. Smart cities must implement robust recovery plans and redundancies to minimize downtime. For instance, if a smart water management system is compromised, built-in backups or manual overrides can restore its functionality while the attack is addressed. Resilient systems ensure public safety and maintain citizen trust, even with cyber threats [34][29].

As smart cities integrate IoT, AI, and cloud systems, adhering to strong cybersecurity principles becomes crucial to protect against malicious actors who could exploit vulnerabilities to disrupt public services or endanger citizens. By implementing robust encryption, performing regular software updates, and maintaining continuous monitoring, smart cities can secure their infrastructure and ensure they provide safe, efficient urban experiences.

6.2. Cybersecurity Services in Smart Cities

Smart cities use advanced technologies to improve urban living by enhancing efficiency, sustainability, and residents' quality of life. As these cities become more connected, they grow increasingly vulnerable to cybersecurity threats, making tailored and robust cybersecurity services essential. These services safeguard the technological infrastructure, ensuring the cities remain secure and resilient against evolving risks. Cybersecurity services in smart cities focus on three key areas: prevention, protection, and monitoring with response. Together, these services create a comprehensive defense against potential cybersecurity threats.

6.2.1. Preventive services

Preventive services play a crucial role in smart city cybersecurity by proactively identifying and addressing vulnerabilities before attackers can exploit them. These services conduct risk assessments, penetration testing, and vulnerability scans to detect network, device, and application weaknesses. They also enforce secure software development practices, implement strong encryption protocols, and establish robust access controls to protect data and systems. Firewalls filter data based on predefined security rules to control network traffic. Next-generation firewalls enhance this process by incorporating application awareness and intrusion prevention. Regular firewall updates ensure resilience against evolving threats [71]. Intrusion detection and prevention systems (IDPS) monitor network traffic in real-time, using signature-based and anomaly-based methods to detect and mitigate threats. Machine learning algorithms integrated into IDPS strengthen their ability to identify unknown threats by analyzing patterns in network behavior. Together, firewalls and IDPS safeguard interconnected systems, minimize attack surfaces, and reduce the risk of cyber threats, ensuring the resilience and safety of urban services in smart cities.

6.2.2. Protective services

Protective services in smart cities play a vital role in securing critical systems, data, and infrastructure against cyber threats, forming the backbone of a strong cybersecurity framework. These services focus on threat prevention using access control mechanisms like role-based access control (RBAC) and multi-factor authentication (MFA). At the same time, endpoint security measures protect devices from malware and unauthorized access. System hardening ensures regular patch management and standardized configurations, and antivirus solutions are essential to defend against the heightened vulnerability of interconnected systems. Critical infrastructure, such as traffic management, public safety networks, and utility services, rely on digital platforms, making them prime targets for cyberattacks. The effectiveness of antivirus solutions depends on frequent updates to counter evolving malware strains. Experts advocate for a layered security approach that combines antivirus, firewalls, and IDS, while user education helps mitigate threats from human error. Encryption, mainly through the Advanced Encryption Standard (AES) and end-to-end encryption, safeguards sensitive data and builds trust in digital services [115]. Monitoring tools and behavioral analysis enhance the detection of suspicious activities, while physical security measures prevent tampering with critical systems. Structured incident response plans and disaster recovery measures ensure service continuity during cyberattacks or failures. By adopting these protective strategies, smart cities strengthen their defenses, ensure infrastructure reliability, and foster public trust in urban services.

6.2.3. Monitoring and response services

Monitoring and response services are crucial components of a comprehensive cybersecurity strategy for smart cities. As cities become more digital and interconnected, the volume and complexity of cyber threats grow, making proactive detection, assessment, and mitigation essential. Real-time network monitoring, powered by tools like IDS and security information and event management (SIEM) platforms, helps detect unusual traffic patterns and unauthorized access attempts [50][71][116]. AI-driven behavioral analysis and anomaly detection further identify potential threats by recognizing deviations from standard usage patterns, while endpoint monitoring ensures IoT devices and sensors are secure. Continuous vulnerability scanning identifies weaknesses in the city's digital infrastructure, helping prevent cyberattacks. Response services, including Incident Detection and Response (IDR), are equally vital for mitigating attack impacts and ensuring rapid service detection, isolation, and restoration. Well-defined incident response plans and playbooks guide actual actions, while threat intelligence sharing with other cities and organizations enables collaborative defense against emerging threats [115]. Forensic analysis and post-incident investigations uncover attack methods and exploited vulnerabilities, informing future security measures. Disaster recovery and business continuity planning ensure critical infrastructure remains operational during and after attacks [51][77]. By integrating these services, smart cities can quickly detect, mitigate, and recover from cyber threats, safeguarding public services and fostering trust in urban cybersecurity. Fig. 7 summarizes the cybersecurity services in smart cities.

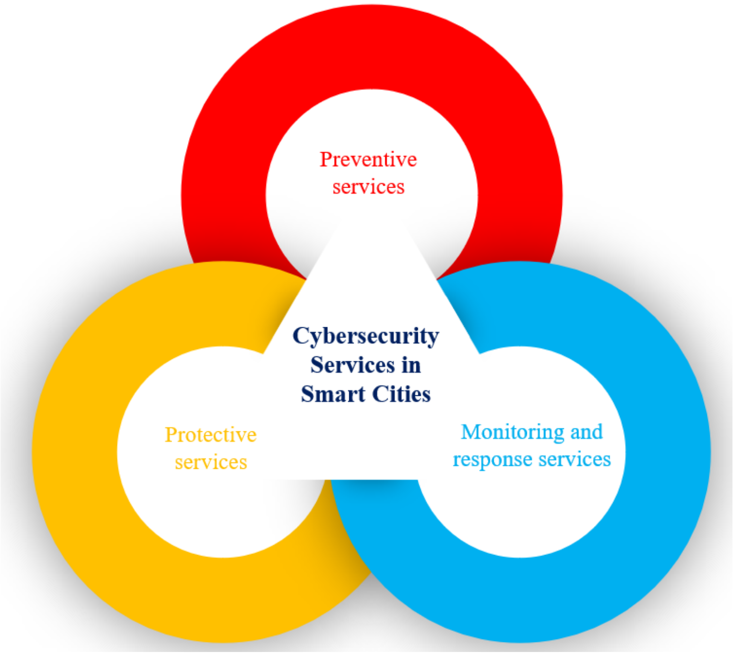
Preventive services
Cybersecurity Services in Smart Cities
Protective services
Monitoring and response services

Fig. 7. Summary of the cybersecurity services in smart cities.

6.3. Importance of Cybersecurity in Smart Cities

As smart cities integrate advanced technologies to improve infrastructure, services, and quality of life, ensuring robust cybersecurity becomes critical. Cybersecurity in smart cities offers several benefits, such as:

6.3.1. Protection of sensitive data

Smart cities collect and manage vast amounts of sensitive data, including personal and operational information from citizens, businesses, and critical infrastructure. Protecting this data is essential to prevent breaches resulting in financial losses, damage to reputation, and the misuse of private information [115][117]. As cyberattacks targeting critical infrastructure grow more sophisticated, implementing robust cybersecurity frameworks becomes increasingly essential [50]. Techniques such as data encryption, both at rest and in transit, along with stringent access control measures, are crucial for ensuring data integrity and confidentiality. Regular audits, updates, and patch management are necessary to address emerging threats and ensure security measures evolve with technological advancements.

6.3.2. Ensure business continuity and compliance

Strong cybersecurity practices are essential for maintaining business continuity in smart cities, where critical services such as transportation, public safety, and utilities rely on a constant data flow. Cybersecurity breaches could disrupt city functions, leading to operational failures and significant financial losses. Smart cities must actively manage complex legal and regulatory requirements, like GDPR, which enforces strict data protection standards. Failure to comply with these regulations can lead to penalties and diminish public trust. Research shows cities with robust cybersecurity frameworks are better positioned to meet these challenges and manage their legal obligations [111]. Cities must adopt dynamic cybersecurity strategies to stay ahead of the constantly evolving regulatory landscape. They can ensure compliance and effectively address emerging threats by staying proactive and adaptable, safeguarding their infrastructure and data.

6.3.3. Maintaining public trust

Trust is essential for citizen engagement with smart city systems, as public confidence in the security of personal data and the reliability of city services drives the adoption of smart technologies. Citizens are more likely to use services prioritizing their privacy and security, making effective cybersecurity a key factor in maintaining this trust [46]. Transparent communication about security measures and clear data usage policies strengthen public confidence. Research shows that when cities openly share their security protocols, citizens are more willing to participate in initiatives like digital health platforms and smart transportation systems [115]. By fostering a sense of security, robust cybersecurity encourages greater participation and support for smart city projects [50].

6.3.4. Protection of critical infrastructure

Smart cities rely on interconnected infrastructures like energy grids, water supply systems, and transportation networks, making them particularly vulnerable to cyberattacks that can disrupt services and cause widespread harm. Cybersecurity measures such as real-time monitoring, threat detection, and secure communication protocols are critical in protecting these systems. Research shows that implementing multi-layered cybersecurity architectures reduces the risk of targeted attacks and enhances the resilience of essential services [118]. Furthermore, adopting Blockchain-based solutions creates immutable records of system operations, boosting transparency and accountability within these infrastructures [50].

6.3.5. Defense against sophisticated cyberattacks

As smart cities evolve, they face increasing threats from sophisticated cyberattacks, including DDoS attacks, ransomware, and insider threats, jeopardizing public safety and financial stability. Urban planners and cybersecurity experts prioritize integrating advanced machine learning algorithms and AI for real-time threat identification and mitigation to counter these risks. By leveraging predictive analytics and anomaly detection systems, smart cities proactively address vulnerabilities before attackers can exploit them [119]. Additionally, Blockchain technology bolsters data integrity and minimizes the risk of tampering with critical information, ensuring a robust defense against emerging cyber threats.

6.3.6. Securing the IoT ecosystem

The proliferation of IoT devices in smart cities expands the attack surface for cybercriminals, as these devices—ranging from traffic-monitoring sensors to energy-managing smart meters—often lack robust security features, making them susceptible to exploitation. Cybersecurity measures must prioritize securing IoT devices from the outset by implementing regular security patches, secure communication protocols, and robust device authentication to protect against breaches. As IoT integration in urban services grows, cybersecurity solutions must continuously evolve to address the dynamic challenges of this expanding ecosystem [117].

6.3.7. Enhancing incident response and recovery

Responding rapidly and effectively to cybersecurity incidents is crucial for minimizing damage and swiftly restoring services in smart cities. These cities rely on vast, interconnected systems that demand advanced incident response frameworks capable of quickly identifying breaches, mitigating impacts, and recovering operations. Effective cybersecurity frameworks for smart cities integrate disaster recovery plans and contingency protocols to maintain business continuity during cyber incidents. Research highlights that implementing well-structured response plans, coupled with AI-driven automation tools, significantly enhances the speed and efficiency of incident management [59][80].

6.3.8. Supporting public-private partnerships

Public and private sector collaborations are essential to address the complexity and scope of cybersecurity threats in smart cities. Public-private partnerships enable both sectors to pool resources, expertise, and technology, strengthening cybersecurity frameworks and enhancing the overall security posture of smart city ecosystems. By actively sharing threat intelligence and best practices, they can better protect critical sectors like healthcare, transportation, and utilities. Researchers emphasize the need for regulatory frameworks that foster such collaboration, highlighting its vital role in building resilient cities capable of withstanding cyber threats [51].

6.3.9. Privacy preservation

Smart cities collect, store, and analyze vast amounts of personal data to enhance services like traffic management, healthcare, and energy efficiency, which raises significant privacy concerns. Organizations must handle personal data carefully to maintain citizen trust and comply with the GDPR. They should actively employ strong data anonymization and pseudonymization techniques and adopt privacy-enhancing technologies to safeguard personal information against unauthorized access or misuse. Transparent policies and precise consent mechanisms reassure citizens that their data is used ethically and securely [115].

6.3.10. Securing smart mobility solutions

As smart cities increasingly adopt autonomous vehicles, connected transportation systems, and intelligent traffic management solutions, securing these systems against cyberattacks becomes critical. These technologies rely heavily on real-time data and communication networks, vulnerable to threats that could disrupt traffic, cause accidents, or jeopardize public safety. To safeguard smart mobility systems, stakeholders must implement continuous monitoring, establish secure communication channels, and integrate AI for threat detection. Additionally, deploying robust encryption and multi-factor authentication mechanisms ensures secure interactions between vehicles and infrastructure, enhancing overall cybersecurity [81].

6.3.11. Cybersecurity as a catalyst for innovation

Strong cybersecurity in smart cities safeguards critical systems and fosters innovation by instilling confidence in citizens and businesses to adopt new technologies and engage with digital services. Secure systems drive advancements in digital health, smart grids, and autonomous transportation. As emerging technologies like AI, Blockchain, and IoT expand, cybersecurity becomes the foundation for sustainable growth and the successful implementation of smart city initiatives [46][49]. Additionally, AI-driven security measures actively uncover system optimization and resource management opportunities.

6.3.12. Collaborative threat intelligence sharing

In cybersecurity, collaboration is crucial as threat actors often target multiple cities at once. Sharing threat intelligence across cities and organizations allows for more effective detection and mitigation of attacks. Cities can strengthen their defenses by creating a global network of cities and cybersecurity agencies that exchange information on vulnerabilities, attack patterns, and defense strategies. Public-private partnerships, international cooperation, and data-sharing protocols enable rapid response and prevention, allowing smarter cities to learn from each other's experiences and stay ahead of cybercriminals [80].

6.3.13. Securing citizen participation and digital identity

Smart cities rely on citizen engagement, with residents using digital platforms to interact with urban services. Securing these platforms and protecting citizens' digital identities is crucial to building trust in smart city initiatives. Residents must safeguard their data and credentials to protect against identity theft, fraud, and unauthorized access, whether using government services or participating in smart mobility systems. Blockchain and decentralized identity solutions are emerging as promising technologies to secure digital identities. By implementing strong encryption, MFA, and biometric verification, cities can create safer digital environments, encouraging greater citizen participation in smart city initiatives.

6.3.14. Smart healthcare and data protection

Smart cities are integrating smart healthcare systems that use connected medical devices, electronic health records, and telemedicine platforms to enhance public health services. While these technologies can improve care delivery and health outcomes, they also create significant cybersecurity risks, particularly in protecting sensitive medical data from breaches. Cyberattacks on healthcare infrastructure can severely impact patient care and violate data privacy. A strong cybersecurity framework is necessary to safeguard healthcare systems, incorporating end-to-end encryption, secure data-sharing protocols, and regular audits of health-related IoT devices. Although data protection laws like the U.S. HIPAA set guidelines for securing health data, smart cities must continuously adapt to emerging threats.

6.3.15. Regulatory compliance and cybersecurity standards

As smart cities grow worldwide, governments increasingly enforce regulations to protect critical infrastructure and ensure citizens' privacy. Cities must comply with national and international cybersecurity standards, such as the European Union's GDPR and the NIST Cybersecurity Framework, which offer structured approaches to managing cybersecurity risks to meet these goals. Compliance with these regulations and certifications, like ISO/IEC 27001, helps implement best practices and robust security measures, fostering confidence in the resilience of smart city systems. Additionally, adherence to these standards ensures that data privacy and security meet legal and ethical requirements, reducing the risk of legal consequences from potential breaches.

6.3.16. Continuous improvement through cybersecurity testing

Cybersecurity in smart cities is an ongoing process that requires continuous attention. Regular penetration testing, vulnerability assessments, and red team exercises simulate real-world attacks to evaluate the effectiveness of security systems. These tests help identify weaknesses in defenses and highlight areas that need improvement. Cities must also invest in cybersecurity research and development to stay ahead of emerging threats. Smart cities can remain agile and effectively address evolving cyber risks by fostering a culture of continuous improvement and innovation [50][117].

7. TECHNOLOGICAL ADVANCEMENTS IN CYBERSECURITY FOR SMART CITIES

Technological advancements in cybersecurity play a crucial role in safeguarding the safety and integrity of smart cities, which depend on an interconnected network of devices and systems. Protecting the large volumes of data generated and transmitted across these networks is vital to prevent cyberattacks that could disrupt essential services such as transportation, energy supply, and healthcare. This section explores how technological advancements transform cybersecurity practices in smart cities, highlighting key research findings and practical applications.

7.1. Encryption technologies

Encryption technologies are vital in protecting sensitive data in smart cities. AES, a symmetric encryption method, secures data efficiently, though key management can be challenging in large systems. RSA, an asymmetric encryption method, enables secure key exchange but performs slower. Researchers are developing strong key management practices and hybrid models, crucial for smart cities that rely on secure data transmission and storage across interconnected networks [31].

7.2. Post-quantum cryptography

The rise of quantum computing has accelerated research into post-quantum cryptography, aiming to create quantum-resistant algorithms to protect data from potential vulnerabilities [29]. This research is essential for ensuring the long-term security of smart city applications by addressing data integrity and confidentiality risks. Quantum key distribution uses quantum mechanics to secure communications [29]. Consequently, investing in post-quantum cryptography is crucial for enhancing smart city cybersecurity against future threats.

7.3. Intrusion detection and prevention systems

IDPS plays a vital role in cybersecurity for smart cities by actively monitoring network traffic. They detect and prevent cyberattacks in real-time. As urban environments grow with more connected devices, the risk of cyber threats increases. IDPS can identify known threats and flag unusual behaviors by combining signature-based and anomaly-based detection methods, enhancing security. They can automatically block malicious traffic or alert cybersecurity teams for quick action, minimizing damage to critical services. By constantly updating threat databases and learning from new incidents, IDPS evolve to keep pace with the changing cyber threat landscape [14][120][121].

7.4. Security Information and Event Management (SIEM)

SIEM systems enhance cybersecurity in smart cities by monitoring networks and supporting compliance reporting. They gather and analyze data from various sources to detect and address security incidents, protecting public safety and trust [7]. Machine learning integration improves threat detection by analyzing large datasets for patterns and anomalies. These systems proactively identify issues and adapt to new threats, improving response times and agility [117]. Additionally, SIEM systems help cities comply with regulations like GDPR and HIPAA, ensuring data protection and fostering public trust [55].

7.5. Endpoint security solutions

Endpoint security is crucial in safeguarding networks as remote work and connected devices in smart cities increase. It protects laptops, smartphones, and IoT devices that connect to the network. Traditional security methods often fail to address advanced threats, making dynamic approaches like heuristic and behavior-based detection essential. These methods analyze user and application behavior to detect suspicious activities, even with unknown malware [46]. In smart cities, compromised endpoints can lead to more significant attacks, so implementing multi-layered security strategies, including network monitoring and SIEM, is key to protecting critical infrastructures and staying ahead of threats [80].

7.6. Firewalls

Next-generation firewalls integrate application awareness and intrusion prevention capabilities to provide advanced protection for smart city networks. Unlike traditional firewalls that rely solely on packet filtering, Next-generation firewalls inspect data packets for malicious content and identify specific applications. This feature is vital in smart cities, where various interconnected applications and devices operate. Next-generation firewalls effectively block unauthorized access and reduce the risk of cyberattacks, ensuring critical service security and continued operation [115][120].

7.7. Honeypots

A honeypot is a cybersecurity method that traps attackers in a decoy system, allowing analysis of their tactics and vulnerabilities to improve security. In smart home systems, the YAKSHA honeypot monitors YAKSHA installations, providing insights into attacks on home networks. Various honeypots, such as Honey, honeydv6, and SHaPe, secure smart grids and industrial control systems by identifying attack methods. ZigBee honeypots are used in smart health, energy, agriculture, and home systems to protect wireless technologies. Additionally, honeypots simulate services in water systems, offering different interaction levels to detect cyber threats [13][120].

7.8. Multi-Factor Authentication (MFA)

Multi-factor authentication boosts security by necessitating users to provide several verification factors before accessing sensitive services in smart cities. This layered approach strengthens authentication methods, making it harder for attackers to breach them and reducing the risk of unauthorized access. As smart cities offer various services that require citizen engagement, implementing MFA protects user data and builds trust in digital services. It is crucial to ensure that authentication processes remain user-friendly, encouraging adoption while maintaining strong security standards [117].

7.9. Cloud security technologies

As smart cities increasingly adopt cloud-based solutions, securing these environments has become a top priority. Cloud access security brokers enforce policies across cloud services, protecting sensitive data stored in the cloud. Research highlights the importance of data encryption for safeguarding information at rest and in transit. As cities transition to cloud-based infrastructures, developing strong cloud security frameworks will protect data and ensure compliance with regulatory standards [122].

7.10. Artificial intelligence and machine learning

In smart cities, AI and machine learning are used for threat detection and incident response automation, enabling proactive and adaptive security measures. These technologies enable organizations to analyze patterns and detect anomalies instantly, enhancing their ability to respond quickly and effectively to potential threats while minimizing the impact of cyber incidents [59]. Integrating AI and machine learning into cybersecurity frameworks significantly advances safeguarding urban infrastructures against emerging threats [7][103]. Various machine learning methods, including K-nearest neighbor, Extreme Gradient Boosting, decision trees, and random forests, are crucial in threat detection. These techniques actively identify potential threats by analyzing patterns and data. K-nearest neighbor classifies based on proximity, while decision trees make decisions through hierarchical structures. Random forests combine decision trees to improve accuracy. Extreme Gradient Boosting optimizes performance by iterating on model improvements [123].

7.11. Quantum key distribution

Quantum key distribution (QKD) uses quantum mechanics to secure communication by generating encryption keys that alert users if intercepted. Unlike traditional cryptography, QKD ensures privacy by detecting disturbances from eavesdroppers [124]. This technology is vital for secure data transmission in smart cities, where sensitive information flows across networks. Despite challenges like expensive hardware and infrastructure needs, research is focused on making QKD more accessible and compatible with existing systems [118]. As QKD advances, it promises to strengthen cybersecurity in key sectors like transportation, healthcare, and public safety [78].

7.12. Blockchain technology

Blockchain technology provides innovative cybersecurity solutions, particularly in decentralized identity management and secure transaction processing. Research shows that Blockchain empowers users by giving them control over their identities, enhancing privacy and security. In smart cities, Blockchain enables secure data sharing among stakeholders while ensuring data integrity. This decentralized model reduces the risks of centralized data storage, making Blockchain appealing for strengthening cybersecurity in smart urban environments [72].

7.13. Demilitarized Zone

A demilitarized zone (DMZ) acts as a perimeter network that shields an organization's internal LAN from untrusted traffic. It separates the internal network from external threats, especially as networks expand. The DMZ hosts resources like web servers, email servers, and DNS, which are accessible via the public network. This setup makes it harder for hackers to target internal systems and sensitive data. In smart cities like the Aspern smart city project, DMZs protect sensitive information by isolating public resources from internal networks, preventing unauthorized access [120].

7.14. Threat intelligence platforms

Threat intelligence platforms enhance smart cities' cybersecurity by integrating with existing security tools for seamless coordination. They automatically update firewalls, IDS, and endpoint security solutions to actively detect and respond to new threats by monitoring and analyzing the activities on devices connected to the network. These platforms provide insights into vulnerabilities, helping officials prioritize patches and upgrades [125]. Predictive analytics assist resource allocation and cybersecurity investments. Sharing threat intelligence among cities strengthens collective security and fosters collaboration in tackling evolving cyber threats [126].

Ongoing technological advancements in cybersecurity play a vital role in protecting smart cities from the evolving cyber threat landscape. As cities adopt advanced technologies like AI, Blockchain, 5G, edge computing, and quantum encryption, it is essential to implement robust cybersecurity measures that can adapt to the growing complexity of these interconnected urban environments.

8. APPLICATION OF ARTIFICIAL INTELLIGENCE IN CYBERSECURITY

Artificial intelligence is revolutionizing cybersecurity in smart cities by strengthening the protection of critical information and infrastructure. Below is an exploration of the key applications of AI in cybersecurity for smart cities:

8.1. Threat and anomaly detection

AI integration revolutionizes cybersecurity in smart cities by enhancing efficiency and enabling resilient urban infrastructures to adapt to evolving threats. AI systems actively analyze network activities in real-time, providing rapid insights to detect and respond to incidents and safeguarding critical services like transportation, healthcare, and energy [87]. These systems monitor traffic, flag abnormal activities, and mitigate breaches swiftly, significantly improving the speed and accuracy of threat detection. By identifying vulnerabilities and processing vast data, AI strengthens urban security, prevents risks, and improves situational awareness for city officials and cybersecurity teams. As smart cities grow, leveraging AI ensures safety, reliability, and sustainable development.

8.2. Automate incident response and remediation

AI-driven automated incident response transforms cybersecurity in smart cities by swiftly minimizing cyber threat impacts on urban operations. Using frameworks like Security Orchestration, Automation, and Response (SOAR), AI integrates with cybersecurity tools to detect, investigate, and resolve incidents efficiently. These systems proactively isolate affected devices, block unauthorized access, and restore compromised systems to secure states, reducing response times and human reliance. By executing predefined playbooks, AI quickly contains threats, such as locking compromised accounts, notifying users, and initiating password resets. This approach strengthens city resilience, safeguards essential services, and allows cybersecurity teams to focus on strategic priorities.

8.3. Enhanced surveillance and video analysis

AI-powered surveillance enhances public safety in smart cities by optimizing monitoring processes with advanced algorithms. Facial recognition enables real-time identification from CCTV footage, helping law enforcement quickly apprehend suspects and deter crime. AI detects suspicious objects, such as unattended bags or unauthorized vehicles, and alerts security personnel instantly, reducing response times. It analyzes behavior to identify unusual activities like loitering or crowd formations, allowing timely interventions. AI-driven analytics are vital in creating safer urban environments by improving response speed and reducing crime rates.

8.4. Identity and access management

AI improves smart city identity and access management systems by integrating advanced biometric authentication and adaptive access control. AI-driven biometrics, including fingerprint, facial, and voice recognition, improve accuracy, reduce errors, and secure sensitive areas and data. These systems adjust user permissions in real-time, detecting anomalies like unfamiliar login attempts and triggering additional verification steps. By automating permission management and monitoring access logs, AI helps organizations comply with data protection laws, avoiding penalties and building public trust [127]. This proactive approach ensures smart cities remain secure, resilient, and efficient while protecting residents and their data.

8.5. Malware detection and prevention

Artificial intelligence revolutionizes malware and phishing detection by analyzing vast data sets and adapting to evolving cyber threats. Machine learning identifies malicious software by examining behavior rather than relying on known signatures, enabling it to detect sophisticated and emerging malware, including zero-day exploits. Natural language processing (NLP) enhances phishing prevention by analyzing emails, URLs, and metadata to detect unusual sender behaviors and deceptive language patterns, blocking harmful messages in real-time. These AI-driven methods improve accuracy and enable faster responses by adapting to new cybercriminal tactics. As smart cities and digital ecosystems grow, AI protects critical infrastructure and sensitive data through dynamic, behavior-based defense mechanisms [87].

8.6. Data encryption and privacy enhancement

Artificial intelligence optimizes cryptographic algorithms to secure data transmission across smart city devices and networks. It automates key management, strengthens encryption protocols, and reduces human error, minimizing the risk of breaches and unauthorized access. AI enhances privacy through techniques like differential privacy, data anonymization, and masking of personal data to enable safe information sharing. AI preserves public trust and protects privacy by ensuring sensitive details remain undisclosed during data analysis. AI assists organizations in adhering to data protection laws, such as GDPR, by automating the anonymization of sensitive data and accurately identifying personally identifiable information.

8.7. Fraud detection

AI is key in detecting and preventing fraud in financial systems, e-commerce, and online transactions. It analyzes transaction data to identify unusual patterns, such as large or geographically unlikely purchases. Credit card companies use AI algorithms to detect and block real-time fraudulent transactions. These algorithms often alert users instantly. As a result, AI enhances security and helps prevent financial fraud [87].

8.8. Phishing detection

AI detects phishing attempts by analyzing email content, URLs, and sender metadata. It uses NLP to assess the language and structure of emails, identifying patterns indicative of phishing. AI-powered email filters actively spot and quarantine malicious emails. These systems help minimize the risk of phishing attacks [87].

8.9. Threat intelligence and proactive defense

Artificial intelligence enhances smart city cybersecurity by analyzing data from social media, dark web forums, and cybersecurity reports to detect emerging threats. It uses predictive analytics on historical data to forecast future trends, enabling urban administrators to anticipate cyberattacks and strengthen defenses. By integrating AI, cities proactively identify vulnerabilities and optimize security protocols to counter evolving cyber threats. AI enables organizations to stay ahead of cybercriminals by forecasting potential attacks before they happen. By identifying vulnerabilities early and addressing them proactively, AI strengthens the safety and resilience of interconnected urban systems, ensuring they can adapt to and withstand evolving cyber threats.

8.10. Critical infrastructure protection

Cybersecurity is crucial for protecting critical infrastructure in smart cities, such as energy grids and utility systems, with AI playing a key role in enhancing this protection. AI continuously monitors data from sensors and control systems, identifying vulnerabilities and recommending actions to defend against DDoS attacks and ransomware. It also enables real-time threat assessment, allowing smart cities to evaluate risks to their infrastructure rapidly. This capability provides valuable insights into potential threats and helps prioritize areas requiring immediate attention, strengthening overall security [128].

8.11. Vulnerability assessment

AI-driven tools revolutionize vulnerability assessment and penetration testing for smart city systems. These advanced tools enhance vulnerability detection, streamline testing, and protect infrastructure from threats. They automate scans to identify security weaknesses, analyze risk profiles, and simulate cyberattacks to test defenses. By proactively identifying and addressing vulnerabilities, AI strengthens smart city resilience against emerging threats. Continuous security evaluations provide actionable insights, recommend improvements, and reduce risks by addressing compliance gaps and enhancing existing measures.

8.12. Cybersecurity training and awareness

Cybersecurity training is vital for personnel securing smart cities, and AI-powered platforms enhance this effort by simulating realistic cybersecurity incidents. These platforms allow staff to practice responses in controlled environments, improving reaction times and boosting confidence. AI customizes training to focus on role-specific cybersecurity topics, strengthening employees' skills. This targeted approach helps them stay ahead of evolving threats. By integrating AI, organizations build a more knowledgeable workforce, improving smart city security through dynamic scenarios like phishing simulations and AI-driven virtual assistants.

8.13. Enhancing endpoint security

AI-powered endpoint protection platforms monitor the behavior of applications and processes on devices like laptops, mobile phones, and IoT devices to defend against cyber threats. They actively detect suspicious activities like unauthorized data access or ransomware encryption attempts. These platforms block malicious actions in real-time to prevent damage. They analyze device behavior to identify potential risks and respond quickly to ensure robust protection against cyberattacks [87].

8.14. User authentication and access control

AI enhances user authentication by analyzing behavioral biometrics like typing speed, mouse movements, and touchscreen interactions. It continuously verifies users through these behaviors and assesses login attempt risks based on location, device, and behavior. AI adapts security measures when needed to ensure safe access. By integrating these methods, AI strengthens traditional authentication processes, which improves accuracy and security [87].

8.15. Protection of IoT devices

The IoT faces significant security challenges due to the large number of devices and their limited security features. AI helps tackle these issues by continuously monitoring IoT devices for abnormal behavior or communication patterns that could indicate a security breach. In smart homes, AI identifies unauthorized access attempts on IoT devices. It then isolates these devices from the network to prevent further compromise. This approach enhances the overall security of IoT systems [87].

8.16. Combating advanced persistent threats

AI detects and mitigates APTs, advanced attacks that often go unnoticed for long periods. It identifies subtle system activity deviations to spot potential APTs. AI continuously monitors file access patterns in sensitive databases. It can detect unauthorized data exfiltration. This proactive approach helps prevent security breaches [87].

8.17. Enhancing cybersecurity with threat hunting

AI aids cybersecurity teams in detecting hidden threats by actively hunting for potential risks. It provides analysts with valuable insights, visualizes data, and uncovers risks that may go unnoticed by humans. AI-driven SIEM systems improve threat hunting by correlating events across vast datasets, enhancing the process's effectiveness and efficiency. As a result, analysts can respond more proactively to emerging threats [87].

AI improves cybersecurity by learning from experience and adapting to new threats. It enhances threat detection and automates responses. AI streamlines security measures and speeds up response times. Organizations can strengthen their defenses using AI to help them stay ahead of increasingly sophisticated cybercriminals.

9. APPLICATION OF BLOCKCHAIN IN CYBERSECURITY

Blockchain technology enhances smart city cybersecurity with its decentralized, immutable architecture, safeguarding data integrity, preventing unauthorized manipulation, and building user trust. It securely facilitates data sharing, ensures transparent transactions, and verifies user identities with tamper-proof methods for improved access control [41]. By creating auditable supply chain records, Blockchain mitigates risks associated with third-party vendors. Integrating into urban infrastructure strengthens cybersecurity while promoting transparency and accountability in data management. Below are some key areas where Blockchain can improve cybersecurity in smart cities:

9.1. Data integrity and secure data sharing

Blockchain enhances data integrity in smart cities by securing data against tampering and unauthorized modifications through consensus-based mechanisms. It enables stakeholders, including city services, law enforcement, and healthcare, to share data securely while maintaining privacy, reducing the risk of breaches during transfers. By protecting sensitive information like medical records and financial transactions, Blockchain ensures data authenticity and detects attempted alterations. It strengthens supply chain management by tracking and verifying product integrity at every stage, from origin to delivery. This transparency minimizes counterfeit risks and builds trust among stakeholders [33].

9.2. Identity and access management

Decentralized digital identities transform identity and access management, particularly in smart cities. Blockchain technology securely stores identities on decentralized ledgers, enhancing security, streamlining verification, and reducing identity theft risk. Self-Sovereign Identity (SSI) permits individuals to control their data, deciding who can access it without relying on centralized authorities. Blockchain enables smart cities to build secure, efficient, and user-centered digital identity ecosystems that foster trust and encourage participation in digital services. Unlike traditional systems prone to breaches, Blockchain-based solutions minimize single points of failure and allow users to share information with trusted parties selectively.

9.3. Enhancing IoT security

Securing IoT devices is crucial for maintaining the efficiency and resilience of smart city infrastructure. Blockchain technology enhances security by authenticating devices, encrypting communication channels, and blocking unauthorized access. It verifies device identities, controls access, and safeguards confidential data, minimizing the risk of cyberattacks and tampering [82]. These measures strengthen trust in interconnected systems and ensure the safe operation of smart cities. As IoT adoption grows, integrating Blockchain will play a vital role in securing communication, protecting data, and supporting robust urban systems.

9.4. Smart contracts for automated services

Smart contracts automate utility billing and traffic management, boosting efficiency and reliability in city operations. These self-executing contracts, coded with predefined terms, automatically act when conditions are met, reducing errors, fraud, and reliance on human intervention. They verify all conditions before processing transactions, ensuring safe and transparent public service payments that build resident trust. By automating security protocols and enforcing compliance in cloud computing, smart contracts strengthen cybersecurity and streamline urban service delivery. For instance, they can trigger alarms for unauthorized access or implement security measures, creating secure, responsive, and citizen-friendly urban systems.

9.5. Critical infrastructure protection

Protecting critical infrastructure is essential for smart cities as cyber threats grow, and Blockchain technology offers a powerful solution. By decentralizing operations, Blockchain reduces vulnerabilities found in centralized systems, enhancing resilience to cyberattacks. It enables real-time urban infrastructure monitoring, allowing rapid issue detection and automated responses to counter threats [129]. This proactive integration strengthens the security and reliability of essential services, ensuring urban environments remain safe and functional. By adopting Blockchain, smart cities build adaptive frameworks that address emerging threats and foster trust among residents.

9.6. Securing financial transactions and payments

Smart cities increasingly use Blockchain technology to secure digital payments and cryptocurrency transactions. Blockchain minimizes fraud risks and builds user trust in cashless systems by providing a transparent ledger. It enables asset tokenization, ensuring secure and transparent ownership transfers in sectors like real estate. Converting physical assets into digital tokens simplifies transactions while maintaining immutable ownership records. This innovation fosters financial inclusivity, streamlines interactions, and promotes economic growth in smart cities.

9.7. Blockchain-based e-voting systems

Blockchain-based e-voting systems enhance election integrity and transparency in smart cities by preventing vote tampering and ensuring accurate results through a secure, decentralized ledger [53]. These systems create an immutable record of the electoral process, fostering trust among voters. Blockchain also supports decentralized governance, enabling residents to participate in policy-making securely via online platforms. This technology empowers citizens, enhances transparency, and reduces corruption in local governments. By integrating Blockchain, smart cities modernize civic engagement and protect democratic integrity.

9.8. Supply chain and logistics management

Supply chain and logistics management ensure the efficient operation of smart cities by providing the seamless movement of goods and services. Blockchain enhances supply chain tracking and traceability through real-time monitoring of goods' origins, routes, and delivery status, reducing fraud, improving efficiency, and ensuring timely deliveries. It strengthens public transportation security by encrypting data and protecting against cyber threats, fostering trust in urban mobility. As smart cities increasingly depend on interconnected logistics networks, Blockchain becomes vital for improving transparency, security, and efficiency. Creating an immutable ledger prevents tampering, ensures safety standards, and combats counterfeit drugs in the pharmaceutical industry.

9.9. Ownership of data and intellectual property

In smart cities, data ownership and intellectual property are crucial as privacy and creative work protection gain importance. Blockchain technology empowers individuals and organizations to control access to their data, enhancing privacy and trust amid frequent breaches. It secures intellectual property by creating immutable ownership records, preventing unauthorized use, and encouraging innovation. Blockchain fosters a secure and innovative urban environment by safeguarding data and creative contributions. This technology enables individuals and businesses to thrive in a dynamic, data-driven digital ecosystem.

9.10. Securing healthcare data

In smart cities, securing healthcare data is vital as the demand for managing electronic health records (EHRs) grows. Blockchain technology ensures the secure sharing and management of EHRs among healthcare providers, granting access only to authorized personnel. It improves interoperability between healthcare systems, enhancing patient care. Additionally, Blockchain secures communication between medical devices, safeguarding patient data and ensuring accurate records for better treatment. Blockchain fosters a secure healthcare ecosystem, building trust between patients and providers while strengthening public health infrastructure.

9.11. Secure communication

Blockchain strengthens communication security by employing public-key cryptography to protect messages and ensure data immutability once recorded. It integrates with secure protocols to prevent MItM attacks, safeguarding message transmission. By securing messaging platforms, Blockchain blocks unauthorized access to communications. It maintains user confidentiality throughout the exchange. These features enhance messaging security [130][131].

9.12. Mitigation of DDoS

Blockchain helps mitigate DDoS attacks by decentralizing traffic across multiple nodes. This approach prevents attackers from targeting a single failure point, making it challenging to overwhelm a server or network. A Blockchain-based DDoS protection system reroutes incoming traffic through distributed nodes. It filters out malicious requests, reducing the attack's impact. This method enhances network security by spreading the load and blocking harmful traffic [130].

9.13. Incident response and forensics

Blockchain offers a transparent and traceable record of events, enabling cybersecurity professionals to conduct more efficient investigations. It securely records every action or transaction in an immutable ledger, which helps forensic investigators reconstruct event timelines, trace breach origins, and identify affected systems. As a result, response times are faster, and investigations after security breaches are more efficient. Blockchain enhances the security investigation [132-135].

9.14. Privacy protection in Cloud computing

Blockchain enhances privacy in cloud computing by giving users control over their data while utilizing cloud services. It stores data off-chain and ensures secure, transparent access without compromising privacy. Blockchain enforces consistent data access permissions across multiple cloud providers, which prevents unauthorized access to sensitive information [130][131].

Blockchain strengthens cybersecurity by addressing key challenges like data breaches, weak authentication, fraud, and IoT vulnerabilities. It helps organizations fortify their digital infrastructure and protect sensitive information. Blockchain solutions improve security across networks, preventing unauthorized access and fraud. These technologies enable more potent authentication methods. By adopting blockchain, organizations can enhance trust and reliability in a connected world.

10. INTEGRATION OF ARTIFICIAL INTELLIGENCE AND BLOCKCHAIN FOR CYBERSECURITY IN SMART CITIES

AI and Blockchain can strengthen cybersecurity in smart cities, which rely on interconnected systems. These cities face threats like data breaches, fraud, and attacks on critical infrastructure. AI helps analyze large data volumes to identify patterns and insights. Blockchain provides a secure, transparent framework for defense. Together, they create a powerful solution to counter emerging cybersecurity challenges. Below are the key applications of AI and Blockchain technologies in the cybersecurity for smart cities:

10.1. Enhanced threat intelligence

AI analyzes data to identify insights and anomalies that signal cyber threats. By integrating AI with Blockchain, cities can establish a real-time threat intelligence framework that encourages stakeholder collaboration. AI algorithms monitor data from IoT devices and network traffic, detecting patterns of potential attacks. Once a threat is identified, the information is recorded on the Blockchain, ensuring data integrity and secure access for authorized parties. This system enables rapid responses to emerging cyber threats.

10.2. Smart contracts for security compliance

Smart contracts are self-executing agreements stored on the Blockchain, automatically triggering actions when predefined conditions are met. In smart cities, they enforce security protocols across systems and devices. During a cyber attack, a smart contract can isolate compromised networks, revoke identities, or lock access points without human intervention. By integrating AI, cities can dynamically adjust security measures in response to evolving threats. AI analyzes real-time data and updates smart contracts to address emerging challenges, reduce human error, and ensure ongoing compliance.

10.3. Resilience against cyber threats

AI and Blockchain can strengthen a smart city's defense against cyber threats. AI enables cybersecurity teams to simulate various attack scenarios, preparing them for potential breaches. Blockchain ensures that simulation results and corrective actions are securely stored and immutable. For instance, Blockchain preserves the outcomes and lessons from a ransomware attack simulation, which creates a trustworthy reference for future training and incident response planning [75].

10.4. Data integrity and security

Integrating AI with Blockchain enhances data integrity and security in smart cities, where accurate information is crucial for decision-making. Blockchain ensures that AI-processed data remains secure, trustworthy, and immutable. It records sensor data, like air quality and traffic information, while AI analyzes it for trends and anomalies. Blockchain's immutability protects against tampering, and AI authenticates data before it's stored. This combination strengthens data security, reduces fraud risks, and fosters public trust in data-driven urban decisions.

10.5. Identity management and authentication

Blockchain and AI are transforming identity management by enhancing security and giving users more control. Blockchain permits individuals to manage their digital identities without relying on centralized authorities, reducing security risks and ensuring data ownership. AI strengthens authentication with biometric methods like facial recognition and fingerprint scanning while analyzing user behavior to detect unusual activity [51]. In smart cities, Blockchain secures access to transportation and healthcare, safeguarding data privacy. AI monitors user behavior in real-time, enforcing security measures when abnormal actions are detected [50].

10.6. Smart contracts for automated security protocols

AI is revolutionizing smart contract security by proactively enhancing vulnerability detection and addressing issues, ensuring reliable automated actions [31]. It strengthens contracts, boosting confidence in their deployment. AI also automates threat responses, enabling smart contracts to take immediate action when cybersecurity threats are detected, reducing response times and damage [76]. By integrating AI, organizations build a more resilient cybersecurity framework. This evolving approach prevents vulnerabilities and protects digital assets in a constantly changing threat landscape.

10.7. Threat intelligence and anomaly detection

Integrating Blockchain and AI enhances smart cities' threat intelligence and anomaly detection by enabling secure data sharing among stakeholders. Blockchain promotes collaboration and provides a comprehensive view of potential risks, while AI analyzes large datasets to detect patterns and emerging threats [52]. Machine learning models in AI continuously monitor smart city data, identifying unusual activities and logging incidents securely in real-time [59]. This combination strengthens cybersecurity by proactively addressing evolving threats. Together, Blockchain and AI improve the safety and resilience of digital infrastructure in complex urban environments.

10.8. IoT device security and infrastructure management

As IoT devices and infrastructure expand, securing communication becomes essential. Blockchain enhances security by encrypting data and preventing unauthorized access or manipulation. AI monitors communications, detecting irregularities and learning behavior patterns to identify security breaches [50][136]. Blockchain supports AI by providing immutable, auditable records of device behavior [77]. Together, they create a robust security framework, enabling secure interactions, better infrastructure management, and enhanced user trust in IoT networks.

10.9. AI-improved Blockchain consensus methods

AI enhances Blockchain consensus methods by improving efficiency and security through adaptive techniques and robust fraud detection. It optimizes transaction speed and reduces energy use by instantly predicting network states and adjusting parameters, addressing sustainability concerns [78]. Machine learning detects transaction anomalies and prevents fraud, ensuring system integrity. This collaboration between AI and Blockchain creates more efficient, secure, and resilient networks. It builds user trust and expands Blockchain applications across various industries.

10.10. Data privacy and encryption

AI enhances data privacy and encryption by anonymizing sensitive information before storing it on the Blockchain, enabling secure data sharing and supporting regulatory compliance. It improves encryption algorithms, boosting data security while maintaining processing speed and transaction efficiency. In smart cities, AI-powered Blockchain solutions control residents' data and define access permissions. Blockchain-based privacy solutions enable individuals to manage data sharing with services like healthcare and public transportation. Smart contracts ensure secure data-sharing with explicit consent, while AI monitors access policies to protect privacy across city departments.

10.11. Fraud detection and prevention

AI and Blockchain work together to enhance fraud detection and prevention. AI models use machine learning to analyze transaction patterns and quickly identify suspicious activity. Blockchain adds security by immutably recording fraud incidents, ensuring evidence remains tamper-proof. Its transparency guarantees trustworthy transaction records for AI systems to detect discrepancies. This integration improves detection speed and accuracy, boosting trust and accountability in fraud prevention.

10.12. Predictive analytics and proactive defense

AI-driven predictive analytics are integral to modern cybersecurity strategies for smart cities, leveraging historical data to identify patterns and forecast potential cyber threats. This proactive approach strengthens defenses and mitigates risks before they occur. Blockchain technology enhances security and complements AI, enabling real-time vulnerability detection and quick responses to emerging threats. Together, these technologies help protect critical services and safeguard urban environments. As a result, they inspire public trust in digital systems while addressing evolving cyber threats [51][76][80][115].

10.13. Integration with quantum-resistant security protocols

As quantum computing advances, it threatens traditional encryption methods, making the integration of quantum-resistant security protocols crucial. AI plays a key role in developing these cryptographic algorithms, ensuring compatibility with existing Blockchain systems to enhance security in a quantum-driven future [52]. Additionally, AI optimizes Blockchain consensus mechanisms, improving efficiency and scalability for real-time operations in smart cities. AI-driven protocols strengthen cryptographic methods and consensus processes by securing interconnected systems like traffic, energy, and public safety. This creates a robust framework that protects smart cities from emerging threats and supports a secure digital future [31].

10.14. AI-powered threat detection and prevention

AI continuously analyzes real-time data across a smart city's infrastructure to detect cyber threats like DDoS attacks, unauthorized access, or malware. Machine learning algorithms identify patterns and flag anomalies in network traffic, smart grid data, vehicle communications, and public transportation systems, which enables real-time threat detection and proactive risk mitigation. Blockchain securely stores AI analysis results, ensuring an immutable, tamper-proof record. This process enhances transparency and accountability in security operations.

10.15. Secure data storage and sharing

Smart cities generate vast amounts of sensitive data from traffic sensors, healthcare systems, and surveillance cameras, making data protection crucial. Blockchain technology creates an immutable ledger to record data transactions, ensuring verifiable changes and preventing manipulation. AI actively monitors and analyzes this data for signs of corruption, inconsistencies, or unauthorized access. If suspicious activity is detected, AI notifies administrators or triggers Blockchain-based protocols for verification. This system ensures the integrity and confidentiality of the city’s data.

10.16. Secure public infrastructure

Securing smart city infrastructure, like water, electricity, and transportation, is essential to prevent cyber threats from causing widespread harm. Blockchain stores critical configuration and operational data on an immutable ledger, ensuring secure communication between components like energy grids and water treatment plants. It prevents unauthorized modifications by safeguarding data integrity. AI algorithms analyze past cyberattacks to identify vulnerabilities and forecast potential threats. Additionally, AI simulations test the effectiveness of Blockchain-based security systems in different scenarios.

10.17. Securing smart traffic and transportation systems

In smart cities, real-time data optimizes transportation systems, including autonomous vehicles, traffic management, and public transit. Blockchain secures this data, preventing tampering and ensuring system integrity. Decentralizing control protects traffic signals and routing systems from cyberattacks. AI analyzes traffic data to detect patterns, predict incidents, and identify threats. When AI spots anomalies, it activates Blockchain protocols to secure or isolate compromised nodes.

10.18. DDoS attack mitigation

DDoS attacks often target smart cities by flooding their network infrastructure with high traffic. Blockchain helps mitigate these attacks by distributing the load across multiple nodes, making it harder for attackers to find a single weak point [130]. AI plays a key role in identifying the nature and source of a DDoS attack. It can then dynamically reroute traffic to secure nodes or activate emergency protocols. This combination of Blockchain and AI strengthens the system against such threats.

10.19. Cybersecurity Governance

Blockchain and AI work together to enhance cybersecurity governance in smart cities by improving transparency, accountability, and efficiency. AI monitors city operations for regulatory compliance, while Blockchain ensures an immutable audit trail of actions [50]. This combination simplifies audits and inspections, streamlining compliance processes. It also enables decentralized decision-making, reducing corruption risks in centralized systems [115][137]. By leveraging these technologies, smart cities strengthen governance, build trust, and align with legal and ethical standards in a complex digital landscape [122].

AI and Blockchain technology address the complex cybersecurity challenges of smart cities. AI enhances threat detection, accelerates response times, and adapts security measures. Blockchain manages secure data and protects identities with a decentralized, immutable, and transparent system. Together, these technologies create a robust security framework. They safeguard interconnected systems, public services, infrastructure, and citizens' privacy against evolving cyber threats.

11. FUTURE RESEARCH DIRECTIONS

Current research and survey findings show promising areas for integrating AI and Blockchain in cybersecurity for smart cities. These technologies offer potential solutions to enhance security measures. Researchers are exploring their application to improve data integrity and privacy. AI and Blockchain can collaborate to provide more robust defenses against cyber threats. Integrating AI and Blockchain in cybersecurity for smart cities highlights several promising areas for future exploration, including the following.

- Researchers are advancing privacy-preserving AI techniques like federated learning and differential privacy, enabling model training without exposing raw data. Integrating zero-knowledge proofs with Blockchain allows sensitive transactions to be verified without revealing details. AI-driven encryption improves key management and data exchange security. Combining federated learning with Blockchain ensures decentralized data and enhances transparency, creating a secure environment for smart cities.
- Research on user-centric security models personalizes protocols based on individual behaviors and risk profiles, using AI to adapt to deviations in residents’ actions, enhancing protection and satisfaction. Blockchain enables residents to control data-sharing through transparent, immutable records, granting or revoking access as needed, which fosters trust with authorities while ensuring privacy compliance. These technologies create a secure, adaptable security environment for smart city residents [126].
- Future research should focus on developing scalable, lightweight Blockchain architectures for smart cities, emphasizing cross-chain communication for interoperability. It should explore consensus algorithms like Proof-of-Stake variants or Directed Acyclic Graphs to balance scalability, energy efficiency, and security. Enhancing scalability with layer-2 solutions, such as state channels and sidechains, will improve transaction speed and reduce costs. Sharding techniques and interoperability frameworks will strengthen security and enable seamless integration of Blockchain and AI technologies.
- Researchers should work with policymakers to create standardized frameworks for interoperability, data privacy, and security in AI Blockchain systems. They must assess legal and ethical implications and propose guidelines for responsible use. Analyzing emerging regulations like the EU’s AI Act will guide smart city cybersecurity strategies. Research should also focus on governance models that align with ethical guidelines and compliance frameworks, ensuring transparency, accountability, and public trust.
- Enhancing security and trust through user behavior analytics and fraud detection mechanisms is a promising future direction for smart cities. Smart cities can improve security and trust using AI-driven user behavior analytics and fraud detection. AI algorithms analyze interaction patterns to create dynamic security profiles that adapt to individual behaviors. These systems can detect fraudulent activities and identify unauthorized access or manipulation. Integrating Blockchain technology ensures data integrity, strengthens security, and boosts public confidence in digital safety.
- Future research in smart cities should focus on creating energy-efficient Blockchain protocols and using AI to optimize resource allocation and reduce computational overhead. Exploring renewable energy sources to power AI and Blockchain nodes in urban infrastructure is essential. Integrating AI and Blockchain technologies will enhance resource management and create secure, efficient energy trading systems. Additionally, assessing the environmental impact of these technologies is crucial for developing sustainable cybersecurity solutions that balance security and energy consumption.
- Design hybrid AI-Blockchain models to enhance data security and access control in multi-cloud environments. Use federated learning across cloud platforms for collaborative threat intelligence. Leverage Blockchain to establish a unified security layer across different cloud services. Integrate AI and Blockchain to strengthen security and streamline threat detection.
- Develop AI systems that assist human analysts by providing insights and recommendations, with final decisions remaining with humans. Study how explainable AI enhances trust and usability in cybersecurity. Develop training programs to help cybersecurity professionals use AI and Blockchain tools effectively. Focus on increasing the impact of AI in the cybersecurity field.
- As quantum computing advances, researchers must focus on developing post-quantum cryptographic algorithms to protect AI and Blockchain technologies in smart cities. They must also design quantum-resilient AI systems integrating Blockchain

to secure training datasets and decision-making. These efforts aim to safeguard urban infrastructures from quantum threats. Researchers should prioritize these solutions to ensure smart cities' long-term security and efficiency.

- Future research should integrate QKD protocols into smart city infrastructures to enhance secure communications. Combining QKD with AI and Blockchain can significantly improve data protection. As quantum computing advances, evaluating post-quantum cryptographic algorithms is essential, particularly for IoT devices and sensitive data exchanges. Researchers must develop and rigorously test robust cryptographic solutions to withstand quantum attacks in urban environments [138].
- Researchers are developing lightweight cryptographic techniques for IoT devices in smart cities to optimize security and performance. Current protocols strain these devices' limited resources, prompting studies on efficient solutions that preserve data integrity. Efforts also focus on frameworks for integrating lightweight cryptography into smart city ecosystems. Structured implementation guides are needed to address smart city challenges effectively.
- Homomorphic encryption can significantly improve secure data processing in smart cities by enabling computations on encrypted personal data, such as health and financial records. Research should explore specific use cases to ensure privacy-preserving analytics. Future studies must assess homomorphic encryption's performance and feasibility, addressing computational overhead, latency, and scalability for real-time applications. The importance of balancing security and performance to implement this technology successfully must be stressed [78].

AI and Blockchain technology can transform cybersecurity in smart cities with innovative security solutions. Future research should address challenges in scalability, privacy, and integration. Collaboration among academia, industry, and policymakers is essential. These efforts will build resilient, secure, and adaptive smart city ecosystems against evolving cyber threats.

12. CONCLUSIONS

In recent years, smart cities have become a focal point for urban development, utilizing advanced technologies to enhance citizens' quality of life and streamline city management. However, as these cities become more interconnected and increasingly dependent on digital systems for critical infrastructure, they face growing cybersecurity risks. The expanding complexity and scale of smart city networks make them prime targets for cyberattacks, raising concerns about safeguarding sensitive data, protecting privacy, and maintaining the integrity of essential services.

Artificial intelligence and Blockchain technologies have significant potential in addressing these cybersecurity challenges. As smart city infrastructures become more complex, securing data and ensuring trust in vital systems becomes more critical. AI is essential in meeting these challenges by instantly processing and analyzing vast amounts of data. It helps detect, predict, and mitigate cybersecurity threats by identifying anomalies and conducting intelligent risk assessments, thus improving the responsiveness and efficiency of security measures.

Blockchain offers a decentralized and immutable solution for securing transactions and data exchanges, ensuring transparency, integrity, and resilience against cyberattacks. Together, AI and Blockchain create a powerful, multi-layered defense system. By combining AI's predictive capabilities with Blockchain's secure ledger, this hybrid approach effectively addresses cybersecurity challenges in smart cities. The synergy between these technologies helps reduce vulnerabilities, protect privacy, and foster trust within the ecosystem.

Despite their potential, challenges remain. Further research is needed to examine AI and Blockchain technologies' scalability, interoperability, and ethical implications. Integrating these technologies also raises issues related to computational resources, privacy concerns, and regulatory frameworks. Cooperation among governments, businesses, and technology providers will be essential to developing and implementing solutions that balance innovation and robust security as smart cities evolve.

In conclusion, AI and Blockchain offer promising solutions to enhance cybersecurity in smart cities. These technologies provide innovative and resilient approaches that can safeguard the digital transformation of urban environments. The continued advancement of AI and Blockchain, along with careful implementation and regulation, will be critical in realizing the full potential of secure and intelligent urban ecosystems.

Funding:

This research was conducted independently without the aid of any external funding bodies, public or private grants, or institutional sponsorships. All expenditures were borne by the authors.

Conflicts of Interest:

The authors declare no potential conflicts of interest.

Acknowledgment:

The authors are thankful to their institutions for offering unwavering support, both in terms of resources and encouragement, during this research project.

References

[1] S. Khawaja, and V. Javidroozi, "Blockchain technology as an enabler for cross-sectoral systems integration for developing smart sustainable cities," *IET Smart Cities*, vol. 5, no. 3, pp. 151–172, 2023. https://doi.org/10.1049/smc2.12059

[2] H. Omrany, K. M. Al-Obaidi, M. Hossain, N. a. M. Alduais, H. S. Al-Duais, and A. Ghaffarianhoseini, "IoT-enabled smart cities: a hybrid systematic analysis of key research areas, challenges, and recommendations for future direction," *Discover Cities,* vol. 1, no. 2, pp. 1–35, 2024. https://doi.org/10.1007/s44327-024-00002-w

[3] O. Wehbi, S. Arisdakessian, M. Guizani, O. A. Wahab, A. Mourad, H. Otrok, H. A. Khzaimi, and B. Ouni, "Enhancing mutual trustworthiness in federated learning for Data-Rich smart Cities," *IEEE Internet of Things Journal,* pp. 1–14, 2024. https://doi.org/10.1109/jiot.2024.3476950

[4] Á. Veloso, F. Fonseca, and R. Ramos, "Insights from Smart City Initiatives for Urban Sustainability and Contemporary Urbanism," *Smart Cities,* vol. 7, no. 6, pp. 3188–3209, 2024. https://doi.org/10.3390/smartcities7060124

[5] J. Liu, X. Liu, and J. Yang, "TOE Configuration analysis of smart city construction in China under the concept of sustainable Development," *Sustainability*, vol. 16, no. 23, pp. 1–15, 2024. https://doi.org/10.3390/su162310708

[6] S. Kahawala, N. Madhusanka, D. De Silva, E. Osipov, N. Mills, M. Manic, and A. Jennings, "Hypervector approximation of complex manifolds for artificial intelligence digital twins in smart cities," *Smart Cities*, vol. 7, no. 6, pp. 3371–3387, 2024. https://doi.org/10.3390/smartcities7060131

[7] V. S. 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, pp. 1–15, 2024. https://doi.org/10.1016/j.jss.2024.112161

[8] B. Anthony, "Artificial intelligence of things and distributed technologies as enablers for intelligent mobility services in smart Cities-A survey," *Internet of Things*, pp. 1–22, 2024. https://doi.org/10.1016/j.iot.2024.101399

[9] M. Houichi, F. Jaidi, and A. Bouhoula, "Cyber Security within Smart Cities: A Comprehensive Study and a Novel Intrusion Detection-Based Approach," *Computers, Materials & Continua*, vol. 81, no. 1, pp. 393–441, 2024. https://doi.org/10.32604/cmc.2024.054007

[10] H. Zeng, M. Yunis, A. Khalil, and N. Mirza, "Towards a conceptual framework for AI-driven anomaly detection in smart city IoT networks for enhanced cybersecurity," *Journal of Innovation & Knowledge*, vol. 9, no. 4, pp. 1–12, 2024. https://doi.org/10.1016/j.jik.2024.100601

[11] E. H. Houssein, M. A. Othman, W. M. Mohamed, and M. Younan, "Internet of Things in Smart Cities: Comprehensive review, open issues and challenges. *IEEE Internet of Things Journal*, vol. 11, no. 21, pp. 34941–34952, 2024. https://doi.org/10.1109/jiot.2024.3449753

[12] V. Demiroglou, S. Skaperas, L. Mamatas, and V. Tsaoussidis, "Adaptive Multi-Protocol communication in smart city networks," *IEEE Internet of Things Journal*, vol. 11, no. 11, pp. 20499–20513, 2024. https://doi.org/10.1109/jiot.2024.3372624

[13] A. M. Escolar, Q. Wang, and J. M. A. Calero, "Enhancing honeynet-based protection with network slicing for massive Pre-6G IoT Smart Cities deployments," *Journal of Network and Computer Applications*, vol. 229, pp. 1–15, 2024. https://doi.org/10.1016/j.jnca.2024.103918

[14] Y. Djenouri, and A. N. Belbachir, "Empowering Urban Connectivity in Smart Cities using Federated Intrusion Detection," *2022 IEEE 9th International Conference on Data Science and Advanced Analytics (DSAA),* Thessaloniki, Greece, 09-13 October 2023, pp. 1-9. https://doi.org/10.1109/dsaa60987.2023.10302528

[15] Y. Fang, Y. Deng, and X. Chen, "Resources on the move for Smart City: a disruptive perspective on the grand convergence of sensing, communications, computing, storage, and intelligence," *IEEE Communications Magazine,* pp. 1–7, 2024. https://doi.org/10.1109/mcom.001.2400084

[16] R. Salama, F. Al-Turjman, S. Alturjman, and A. Altorgoman, "An overview of artificial intelligence and blockchain technology in smart cities," In *Computational Intelligence and Blockchain in Complex Systems* (pp. 269–275). ScienceDirect, 2024. https://doi.org/10.1016/b978-0-443-13268-1.00018-2

[17] M. A. Fadhel, A. M. Duhaim, A. Saihood, A. Sewify, M. N. Al-Hamadani, A. Albahri, L. Alzubaidi, A. Gupta, S. Mirjalili, and Y. Gu, "Comprehensive systematic review of information fusion methods in smart cities and urban environments," *Information Fusion*, vol. 107, pp. 1–34, 2024. https://doi.org/10.1016/j.inffus.2024.102317

[18] A. Hassebo, M. Tealab, and M. Hamouda, "From a traditional city to a Smart City: The Measurement of Cities' Readiness for Transition, Egypt as a case study," *Urban Science,* vol. 8, no. 4, pp. 1–38, 2024. https://doi.org/10.3390/urbansci8040212

[19] H. Li, D. He, P. Vijayakumar, F. Alqahtani, and A. Tolba, "A certificateless and KGA-secure searchable encryption scheme with constant trapdoors in smart city," *Digital Communications and Networks*, pp. 1–13, 2024. https://doi.org/10.1016/j.dcan.2024.08.005

[20] L. Yang, Z. Luo, S. Zhang, F. Teng, and T. Li, "Continual Learning for Smart City: a survey," *IEEE Transactions on Knowledge and Data Engineering*, vol. 36, no. 12, pp. 7805–7824, 2024. https://doi.org/10.1109/tkde.2024.3447123

[21] B. U. I. Khan, K. W. Goh, A. R. Khan, M. F. Zuhairi, and M. Chaimanee, "Integrating AI and blockchain for enhanced data security in IoT-Driven smart Cities," *Processes*, vol. 12, no. 9, pp. 1–29, 2024. https://doi.org/10.3390/pr12091825

[22] T. Bergur, "*Size of smart cities market worldwide in 2019 and 2030*," Statista. https://www.statista.com/aboutus/our-research-commitment/3204/bergur-thormundsson (accessed December 3, 2024).

[23] T. Bergur, "*Projected revenue generated by companies in the global Smart City from 2020 to 2028*,"*. Statista. https://www.statista.com/aboutus/our-research-commitment/3204/bergur-thormundsson (accessed December 3, 2024).

[24] F. Almeida, "Prospects of cybersecurity in smart cities," *Future Internet*, 15, no. 9, pp. 1–22, 2023. https://doi.org/10.3390/fi15090285

[25] M. Alaeddini, M. Hajizadeh, and P. Reaidy, "A Bibliometric Analysis of Research on the Convergence of Artificial Intelligence and Blockchain in Smart Cities," *Smart Cities*, vol. 6, no. 2, pp. 764–795, 2023. https://www.mdpi.com/2624-6511/6/2/37#

[26] G. Dhiman, and N. S. Alghamdi, "SMOSE: Artificial Intelligence-Based Smart City Framework using Multi-Objective and IoT Approach for Consumer Electronics application," *IEEE Transactions on Consumer Electronics*, vol. 70, no. 1, pp. 3848–3855, 2024. https://doi.org/10.1109/tce.2024.3363720

[27] A. Matei, and M. Cocoşatu, "Artificial internet of things, Sensor-Based Digital twin urban computing vision algorithms, and blockchain cloud networks in sustainable smart city administration," *Sustainability*, vol. 16, no. 16, pp. 1–20, 2024. https://doi.org/10.3390/su16166749

[28] R. Salama, S. Al-Turjman, C. Altrjman, F. Al-Turjman, O. Vikash, S. P. Yadav, and S. Vats, "The Main Threat to Computer Network Security in Smart Cities. *2023 3rd International Conference on Advancement in Electronics & Communication Engineering (AECE)*, Ghaziabad, India, 23-24 November 2023, pp. 419–425. https://doi.org/10.1109/aece59614.2023.10428154

[29] W. Robert, A. Denis, A. Thomas, A. Samuel, S. P. Kabiito, Z. Morish, and G. Ali, "A Comprehensive Review on Cryptographic Techniques for Securing Internet of Medical Things: A State-of-the-Art, Applications, Security Attacks, Mitigation Measures, and Future Research Direction," *Mesopotamian Journal of Artificial Intelligence in Healthcare*, vol. 2024, pp. 135–169, 2024. https://doi.org/10.58496/MJAIH/2024/016

[30] F. Wahida, M. Chamikara, I. Khalil, and M. Atiquzzaman, "An Adversarial Machine Learning based approach for privacy preserving face recognition in distributed smart city surveillance," *Computer Networks*, vol. 254, pp. 1–12, 2024. https://doi.org/10.1016/j.comnet.2024.110798

[31] A. Algarni, Z. Ahmad, and M. A. Ala'Anzy, "An edge computing-based and threat behavior-aware smart prioritization framework for cybersecurity intrusion detection and prevention of IEDs in smart grids, integrating modified LGBM and one class-SVM models," *IEEE Access*, vol. 12, pp. 104948-104963, 2024. https://doi.org/10.1109/ACCESS.2024.3435564

[32] G. Ali, M. M. Mijwil, A. B. Bosco, M. Abotaleb, and I. Adamopoulos, "A Survey on Artificial Intelligence in Cybersecurity for Smart Agriculture: State-of-the-Art, Cyber Threats, Artificial Intelligence Applications, and Ethical Concerns," *Mesopotamian Journal of Computer Science*, vol. 2024, pp. 71–121, 2024. https://doi.org/10.58496/MJCSC/2024/007

[33] G. Ali, M. M. Mijwil, B. A. Buruga, and M. Abotaleb, "A Comprehensive Review on Cybersecurity Issues and Their Mitigation Measures in FinTech," *Iraqi Journal For Computer Science and Mathematics*, vol. 5, no. 3, pp. 45–91, 2024. https://doi.org/10.52866/ijcsm.2024.05.03.004

[34] G. Ali, and M. M. Mijwil, "Cybersecurity for Sustainable Smart Healthcare: State of the Art, Taxonomy, Mechanisms, and Essential Roles," *Mesopotamian Journal of CyberSecurity*, vol. 4, no. 2, pp. 20–62, 2024. https://doi.org/10.58496/MJCS/2024/006

[35] S. Sharma, and N. Mishra, "Analyzing the Potential of Smart Cities: Technologies, Frameworks, Vulnerabilities, Threats, and Information Security Solutions. *2024 ASU International Conference in Emerging Technologies for Sustainability and Intelligent Systems (ICETSIS)*, Manama, Bahrain, 28-29 January 2024, pp. 1570–1574. https://doi.org/10.1109/icetsis61505.2024.10459607

[36] A. Post, "*The cybersecurity risks of smart city technologies: What do the experts think?,*" CLTC. https://cltc.berkeley.edu/publication/smart-cities/ (accessed December 3, 2024).

[37] M. Alauthman, A. Aldweesh, and A. Al-Qerem, "IoT Security Challenges in Modern Smart Cities. *2024 2nd International Conference on Cyber Resilience (ICCR)*, Dubai, United Arab Emirates, 26-28 February 2024, pp. 1–6. https://doi.org/10.1109/iccr61006.2024.10533174

[38] I. Priyadarshini, "Anomaly detection of IoT cyberattacks in smart cities using federated learning and split learning," *Big Data and Cognitive Computing*, vol. 8, no. 3, pp. 1–15, 2024. https://doi.org/10.3390/bdcc8030021

[39] N. C. Chouraik, N. R. El-Founir, and N. K. Taybi, "Cyber-securing Morocco's smart cities: A case review," *International Journal of Science and Research Archive*, vol. 13, no. 1, pp. 102–112, 2024. https://doi.org/10.30574/ijsra.2024.13.1.1619

[40] Y. Mothanna, W. ElMedany, M. Hammad, R. Ksantini, and M. S. Sharif, "Adopting security practices in software development process: Security testing framework for sustainable smart cities," *Computers & Security*, vol. 144, pp. 1–9, 2024. https://doi.org/10.1016/j.cose.2024.103985

[41] K. S. Kumar, J. A. Alzubi, N. Sarhan, E. M. Awwad, V. Kandasamy, and G. Ali, "A secure and efficient BlockChain and distributed Ledger technology-based optimal resource management in digital twin beyond 5G networks using hybrid energy valley and levy Flight Distributer Optimization algorithm," *IEEE Access*, vol. 12, pp. 110331–110352, 2024. https://doi.org/10.1109/access.2024.3435847

[42] T. Hemalatha, K. Sangeetha, K. S. K. Rani, K. Kanimozhi, M. Lawanyashri, K. Santhi, and R. Deepalakshmi, "CPS in block chain smart city application based on distributed ledger based decentralized technique," *Measurement Sensors*, vol. 30, pp. 1–6, 2023. https://doi.org/10.1016/j.measen.2023.100906

[43] A. A. Khan, A. A. Laghari, R. Alroobaea, A. M. Baqasah, M. Alsafyani, R. Bacarra, and J. a. J. Alsayaydeh, "Secure remote sensing data with blockchain distributed ledger technology: a solution for smart cities," *IEEE Access*, vol. 12, pp. 69383–69396, 2024. https://doi.org/10.1109/access.2024.3401591

[44] S. Vempati, and N. Nalini, "Securing Smart Cities: A cybersecurity perspective on integrating IoT, AI, and machine learning for digital twin creation," *Journal of Electrical Systems*, vol. 20, no. 3, pp. 1420–1429, 2024. https://doi.org/10.52783/jes.3052

[45] Y. Zhuang, J. Cenci, and J. Zhang, "Review of big data implementation and expectations in smart cities," *Buildings*, vol. 14, no. 12, pp. 1–27, 2024. https://doi.org/10.3390/buildings14123717

[46] E. Ismagilova, L. Hughes, N. P. Rana, and Y. K. Dwivedi, "Security, privacy and risks within smart cities: Literature review and development of a smart city interaction framework," *Information Systems Frontiers*, vol. 24, pp. 393–414, 2022. https://doi.org/10.1007/s10796-020-10044-1

[47] D. E. Okonta, and V. Vukovic, "Smart cities software applications for sustainability and resilience," *Heliyon*, vol. 10, no. 12, pp. 1–20, 2024. https://doi.org/10.1016/j.heliyon.2024.e32654

[48] J. T. Costa, and R. P. C. D. Nascimento, "ICT governance practices and industry 4.0 technologies in support of Decision-Making in Brazilian smart cities in the face of the COVID-19 pandemic," *IEEE Transactions on Computational Social Systems*, vol. 11, no. 6, pp. 8213–8226, 2023. https://doi.org/10.1109/tcss.2023.3306707

[49] C. Davies, “Big Data Analytics for Smart Cities,” *International Journal of Computing and Engineering*, vol. 6, no. 1, pp. 14–29, 2024. https://doi.org/10.47941/ijce.2057

[50] A. A. Varfolomeev, and L. H. Al-Farhani, “Blockchain based digital identity management system for smart city services,” *2023 International Conference on Information Technology, Applied Mathematics and Statistics (ICITAMS)*, Al-Qadisyia, Iraq, 20-22 March 2023. *https://doi.org/10.1109/ICITAMS57610.2023.10525393*

[51] A. H. Ameen, M. A. Mohammed, and A. N. Rashid, “Dimensions of artificial intelligence techniques, blockchain, and cyber security in the Internet of medical things: Opportunities, challenges, and future directions,” *Journal of Intelligent Systems*, vol. 32, no. 1, pp. 1-18, 2023. https://doi.org/10.1515/jisys-2022-0267

[52] V. Bhatia, and B. Bhatia, “Machine learning-based solutions for Internet of Things-based applications,” In *A. K. Tyagi (Ed.),* (pp. 295-318). Wiley, 2023. https://doi.org/10.1002/9781394213948.ch15

[53] R. Fatih, S. Arezki, and T. Gadi, “A review of blockchain-based e-voting systems: Comparative analysis and findings,” *International Journal of Interactive Mobile Technologies*, vol. 17, no. 23, pp. 49–67, 2023. https://doi.org/10.3991/ijim.v17i23.45257

[54] S. Lysenko, N. Bobro, K. Korsunova, O. Vasylchyshyn, and Y. Tatarchenko, “The role of artificial intelligence in cybersecurity: Automation of protection and detection of threats,” *Economic Affairs*, vol. 69, no. 1s, pp. 43–51, 2024. https://doi.org/10.46852/0424-2513.1.2024.6

[55] D. Bastos, N. Costa, N. P. Rocha, A. Fernández-Caballero, and A. Pereira, “A comprehensive survey on the societal aspects of smart cities,” *Applied Sciences*, vol. *14*, no. 17, pp. 1-39, 2024. https://doi.org/10.3390/app14177823

[56] H. Kaur, and M. Bhatia, “Scientometric analysis of digital twin in Industry 4.0,” *IEEE Internet of Things Journal (*Early *Access)*, vol. 99, 1–1, 2024. https://doi.org/10.1109/JIOT.2024.3459965

[57] J. S. Gracias, G. S. Parnell, E. Specking, E. A. Pohl, and R. Buchanan, “Smart Cities—A structured literature review,” *Smart Cities*, vol. 6, no. 4, pp. 1719–1743, 2023. https://doi.org/10.3390/smartcities6040080

[58] B. P. Balasaheb, and M. S. Kumar, “Review of IoT-enabled Smart Cities: Cybersecurity Threat Detection using Cloud Computing,” *2024 15th International Conference on Computing Communication and Networking Technologies (ICCCNT)*, Kamand, India, 24-28 June 2024, pp. 1–11. https://doi.org/10.1109/icccnt61001.2024.10725673

[59] M. M. Rashid, J. Kamruzzaman, M. M. Hassan, T. Imam, S. Wibowo, S. Gordon, and G. Fortino, “Adversarial training for deep learning-based cyberattack detection in IoT-based smart city applications,” *Computers & Security*, vol. *120*, pp. 102783, 2022. https://doi.org/10.1016/j.cose.2022.102783

[60] O. Cheikhrouhou, I. Amdouni, K. Mershad, M. Ammi, and T. N. Gia, “Blockchain for the cybersecurity of smart city applications,” arXiv (Cornell University), pp. 1-65, 2022. https://doi.org/10.48550/arXiv.2206.02760

[61] A. Muniswamy, and R. Rathi, “A detailed review on enhancing the security in Internet of Things-Based Smart City Environment using Machine learning algorithms,” *IEEE Access*, vol. 12, pp. 120389–120413, 2024. https://doi.org/10.1109/access.2024.3450180

[62] S. A. Ali, S. A. Elsaid, A. A. Ateya, M. ElAffendi, and A. a. A. El-Latif, “Enabling Technologies for Next-Generation Smart Cities: A Comprehensive Review and research Directions,” *Future Internet*, vol. 15, no. 12, pp. 1–43, 2023. https://doi.org/10.3390/fi15120398

[63] A. Gelbukh, M. T. Zamir, F. Ullah, M. Ali, T. Taiba, M. Usman, N. Hafeez, L. Dudaeva, and C. Fasoldt, “State-of-the-Art Review in Explainable Machine Learning for Smart-Cities Applications,” In *Studies in Big Data* (Vol. 148, pp. 67–76). Springer, 2024. https://doi.org/10.1007/978-3-031-54277-0_3

[64] M. Tutak, and J. Brodny, “A smart city is a Safe City: Analysis and evaluation of the state of crime and safety in Polish cities,” *Smart Cities*, vol. 6, no. 6, pp. 3359–3392, 2023. https://doi.org/10.3390/smartcities6060149

[65] A. Ullah, S. Quddusi, and I. Haider, “Incorporation of artificial intelligence in enhancing quality of life in smart cities,” *American Journal of Artificial Intelligence*, vol. 8, no. 2, pp. 48–54, 2024. https://doi.org/10.11648/j.ajai.20240802.13

[66] V. Demertzi, S. Demertzis, and K. Demertzis, “An overview of cyber threats, attacks and countermeasures on the primary domains of smart cities,” *Applied Sciences*, vol. 13, no. 2, pp. 1–36, 2023. https://doi.org/10.3390/app13020790

[67] Z. A. Kaiser, “Smart governance for smart cities and nations,” *Journal of Economy and Technology*, vol. 2, pp. 216–234, 2024. https://doi.org/10.1016/j.ject.2024.07.003

[68] A. K. Dwivedi, and S. K. Prasad, “Exploring Smart Cities: Definitions, Advantages, Challenges, and Security Considerations for Urban Transformation,” *2023 2nd International Conference on Futuristic Technologies (INCOFT)*, Belagavi, Karnataka, India, 24-26 November 2023, pp. 1–6. https://doi.org/10.1109/incoft60753.2023.10425193

[69] C. Hazman, A. Guezzaz, S. Benkirane, and M. Azrour, “Enhanced IDS with Deep Learning for IoT-Based Smart Cities Security,” *Tsinghua Science & Technology*, vol. 29, no. 4, pp. 929–947, 2024. https://doi.org/10.26599/tst.2023.9010033

[70] B.-I. Pahonțu, D.-A. Arsene, A. Predescu, M. Mocanu, and A. Gheorghiță, “Blockchain-based decision support system for water management,” *Studies in Informatics and Control*, vol. *32*, no. 3, pp. 131–140, 2023. https://doi.org/10.24846/v32i3y2023012

[71] R. K. Mahmood, A. I. Mahameed, N. Q. Lateef, H. M. Jasim, A. D. Radhi, S. R. Ahmed, and P. Tupe-Waghmare, “Optimizing network security with machine learning and multi-factor authentication for enhanced intrusion detection,” *Journal of Robotics and Control*, vol. 5, no. 5, pp. 1502-1524, 2024. https://doi.org/10.18196/jrc.v5i5.22508

[72] H. N. Fakhouri, S. Alawadi, F. M. Awaysheh, I. Bani Hani, M. Alkhalaileh, and F. Hamad, “A comprehensive study on the role of machine learning in 5G security: Challenges, technologies, and solutions,” *Electronics*, vol. *12*, no. 22, pp. 1-44, 2023. https://doi.org/10.3390/electronics12224604

[73] S. Kouah, A. Saighi, M. Ammi, A. N. S. Mohand, M. I. Kouah, and D. Megías, “Internet of Things-Based Multi-Agent system for the control of smart street lighting,” *Electronics*, vol. 13, no. 18, pp. 1–40, 2024. https://doi.org/10.3390/electronics13183673

[74] H. Ali, O. M. Elzeki, and S. Elmougy, “Smart Attacks Learning Machine Advisor System for Protecting Smart Cities from Smart Threats,” *Applied Sciences*, vol. 12, no. 13, pp. 1–24, 2022. https://doi.org/10.3390/app12136473

[75] P. K. Dutta, S. M. El-kenawy, G. Ali, and K. Dhoska, “An Energy Consumption Monitoring and Control System in Buildings using Internet of Things,” *Babylonian Journal of Internet of Things*, vol. 2023, pp. 38–47, 2023. https://doi.org/10.58496/BJIoT/2023/006

[76] L. Chen, Z. Chen, Y. Zhang, Y. Liu, A. I. Osman, M. Farghali, J. Hua, A. Al–Fatesh, I. Ihara, D. W. Rooney, and P.-S. Yap, “Artificial intelligence-based solutions for climate change: a review,” *Environmental Chemistry Letters*, vol. 21, no. 5, pp. 2525-2557, 2023. https://doi.org/10.1007/s10311-023-01617-y

[77] M. H. B. Ibrahim, Y. Al Moaiad, W. Abu-Ulbeh, H. Al-Wahshat, W. A. H. M. Ghanem, and R. R. Mohamed, “Security frameworks for IoT devices in smart cities,” *Journal of Jilin University (Engineering and Technology Edition)*, vol. 43, no. 6, pp. 206-230, 2024. https://doi.org/10.5281/zenodo.12529126

[78] Z. Zhang, H. A. Hamadi, E. Damiani, C. Y. Yeun, and F. Taher, “Explainable artificial intelligence applications in cyber security: State-of-the-art in research,” *IEEE Access*, vol. *10*, pp. 93104–93139, 2022. https://doi.org/10.1109/ACCESS.2022.3204051

[79] M. M. Alshahrani, “A secure and intelligent Software-Defined networking Framework for future smart cities to prevent DDOS attack,” *Applied Sciences*, vol. 13, no. 17, pp. 1–16, 2023. https://doi.org/10.3390/app13179822

[80] O. Fadi, K. Zkik, A. El Ghazi, and M. Boulmalef, “A survey on blockchain and artificial intelligence technologies for enhancing security and privacy in smart environments,” *IEEE Access*, vol. 10, pp. 93168 – 93186, 2022. https://doi.org/10.1109/ACCESS.2022.3203568

[81] M. Elassy, M. Al-Hattab, M. Takruri, and S. Badawi, “Intelligent transportation systems for sustainable smart cities,” Transportation *Engineering*, vol. *16*, pp. 1-18, 2024. https://doi.org/10.1016/j.treng.2024.100252

[82] R. Wolniak, and K. Stecuła, “Artificial intelligence in smart cities Applications, barriers, and future directions: A review,” *Smart Cities*, vol. *7*, no. 3, pp. 1346–1389, 2024. https://doi.org/10.3390/smartcities7030057

[83] M. M. Mijwil, I. Bala, G. Ali, M. Aljanabi, M. Abotaleb, R. Doshi, . . . E.-S. M. El-Kenawy, “Sensing of Type 2 Diabetes Patients Based on Internet of Things Solutions: An Extensive Survey,” In K. K. Hiran, R. Doshi, & M. Patel (Eds.), *Modern Technology in Healthcare and Medical Education: Blockchain, IoT, AR, and VR* (pp. 34-46). IGI Global, 2024. https://doi.org/10.4018/979-8-3693-5493-3.ch003

[84] M. Ryalat, N. Almtireen, H. Elmoaqet, and M. Almohammedi, “The Integration of Two Smarts in the Era of Industry 4.0: Smart Factory and Smart City,” *2024 IEEE Smart Cities Futures Summit (SCFC)*, Marrakech, Morocco, Marrakech, Morocco, pp. 9–12. https://doi.org/10.1109/scfc62024.2024.10698351

[85] C. Goumopoulos, “Smart City Middleware: A survey and a Conceptual framework,” *IEEE Access*, vol. 12, pp. 4015–4047, 2024. https://doi.org/10.1109/access.2023.3349376

[86] E. Dritsas, and M. Trigka, “Machine Learning for blockchain and IoT systems in smart Cities: a survey. *Future Internet*, vol. 16, no. 9, pp. 1–15, 2024. https://doi.org/10.3390/fi16090324

[87] M. Ozkan-Okay, E. Akin, Ö. Aslan, S. Koşunalp, T. Iliev, I. Stoyanov, and I. Beloev, “A Comprehensive Survey: Evaluating the Efficiency of Artificial Intelligence and Machine Learning Techniques on Cyber Security Solutions,” *IEEE Access*, vol. 12, pp. 12229–12256, 2024. https://doi.org/10.1109/access.2024.3355547

[88] G. Ali, M. M. Mijwil, I. Adamopoulos, B. A. Buruga, M. Gök, and M. Sallam, “Harnessing the Potential of Artificial Intelligence in Managing Viral Hepatitis,” *Mesopotamian Journal of Big Data*, vol. 2024, pp. 128–163, 2024. https://doi.org/10.58496/MJBD/2024/010

[89] I. Bala, M. M. Mijwil, G. Ali, and E. Sadıkoğlu, “Analyzing the Connection Between AI and Industry 4.0 from a Cybersecurity Perspective: Defending the Smart Revolution,” *Mesopotamian Journal of Big Data*, vol. 2023, pp. 63–69, 2023. https://doi.org/10.58496/mjbd/2023/009

[90] M. M. Mijwil, O. Adelaja, A. Badr, G. Ali, B. A. Buruga, and Pudasaini, P. “Innovative Livestock: A Survey of Artificial Intelligence Techniques in Livestock Farming Management,” *Wasit Journal of Computer and Mathematics Science*, vol. 2, no. 4, pp. 99–106, 2023. https://doi.org/10.31185/wjcms.206

[91] A. Adel, “Unlocking the Future: Fostering Human–Machine Collaboration and Driving Intelligent Automation through Industry 5.0 in Smart Cities,” *Smart Cities*, vol. 6, no. 5, pp. 2742–2782, 2023. https://doi.org/10.3390/smartcities6050124

[92] I. a. T. Hashem, R. S. A. Usmani, M. S. Almutairi, A. O. Ibrahim, A. Zakari, F. Alotaibi, S. M. Alhashmi, and H. Chiroma, “Urban Computing for Sustainable Smart Cities: recent advances, taxonomy, and open research challenges,” *Sustainability*, vol. 15, no. 5, pp. 1–32, 2023. https://doi.org/10.3390/su15053916

[93] A. E. Bekkali, M. Essaaidi, and M. Boulmalf, “A Blockchain-Based architecture and framework for cybersecure smart cities,” *IEEE Access*, vol. 11, pp. 76359–76370, 2023. https://doi.org/10.1109/access.2023.3296482

[94] M. Padhiary, P. Roy, and D. Roy, “The future of urban connectivity,” In *Advances in electronic government, digital divide, and regional development book series* (pp. 33–66). IGI Global, 2024. https://doi.org/10.4018/979-8-3693-6740-7.ch002

[95] W. Rafique, J. Barai, A. O. Fapojuwo, and D. Krishnamurthy, “A survey on Beyond 5G network slicing for smart cities applications,” *IEEE Communications Surveys & Tutorials*, pp. 1–35, 2024. https://doi.org/10.1109/comst.2024.3410295

[96] R. Sabitha, S. Gowriswari, S. Yuvaraj, G. M. Devi, R. Babuji, and S. Murugan, “Augmented reality for public engagement in sustainable city planning: Cloud and machine learning integration,” *2024 International Conference on Advances in Modern Age Technologies for Health and Engineering Science (AMATHE)*. Shivamogga, India, 16-17 May 2024, pp. https://doi.org/10.1109/AMATHE61652.2024.10582095

[97] K. Al-Dosari, and N. Fetais, “A new shift in implementing Unmanned Aerial Vehicles (UAVs) in the safety and security of smart Cities: A Systematic literature review,” *Safety*, vol. 9, no. 3, pp. 1–22, 2023. https://doi.org/10.3390/safety9030064

[98] M. Kovačić, M. Mutavdžija, and K. Buntak, “New Paradigm of Sustainable Urban Mobility: Electric and Autonomous Vehicles—A Review and Bibliometric Analysis,” *Sustainability*, vol. 14, no. 15, pp. 1–23, 2022. https://doi.org/10.3390/su14159525

[99] N. O. H. Orieno, N. N. L. Ndubuisi, N. V. I. Ilojianya, N. P. W. Biu, and N. B. Odonkor, “The Future of Autonomous Vehicles in the U.S. Urban Landscape: A Review: Analyzing Implications for Traffic, Urban Planning, and the Environment,” *Engineering Science & Technology Journal*, vol. 5, no. 1, pp. 43–64, 2024. https://doi.org/10.51594/estj.v5i1.721

[100] L. Almuqren, S. S. Aljameel, H. Alqahtani, S. S. Alotaibi, M. A. Hamza, and A. S. Salama, “A White Shark Equilibrium Optimizer with a Hybrid Deep-Learning-Based Cybersecurity Solution for a Smart City Environment,” *Sensors*, vol. 23, no. 17, pp. 1–15, 2023. https://doi.org/10.3390/s23177370

[101] J. Fan, W. Yang, Z. Liu, J. Kang, D. Niyato, K. Lam, and H. Du, “Understanding security in smart city domains from the ANT-Centric perspective,” *IEEE Internet of Things Journal*, vol. 10, no. 13, pp. 11199–11223, 2023. https://doi.org/10.1109/jiot.2023.3252040

[102] M. Kalinin, V. Krundyshev, and P. Zegzhda, “Cybersecurity risk assessment in smart city infrastructures,” *Machines*, 9, no. 4, pp. 1–19, 2021. https://doi.org/10.3390/machines9040078

[103] H. M. K. K. M. B. Herath, and M. Mittal, “Adoption of artificial intelligence in smart cities: A comprehensive review,” International *Journal of Information Management Data Insights*, vol. *2*, no. 1, pp. 1-21, 2022. https://doi.org/10.1016/j.jjimei.2022.100076

[104] B. Sándor, and Z. Rajnai, “Cyber Security Analysis of Smart Buildings from a Cyber Security Architecture Point of View,” *Interdisciplinary Description of Complex Systems*, vol. 21, no. 2, pp. 141–147, 2023. https://doi.org/10.7906/indecs.21.2.2

[105] S. Mulero-Palencia, and V. M. Baeza, “Detection of vulnerabilities in smart buildings using the Shodan tool,” *Electronics*, vol. 12, no. 23, pp. 1–30, 2023. https://doi.org/10.3390/electronics12234815

[106] N. E. Vellinga, “Connected and vulnerable: cybersecurity in vehicles,” *International Review of Law Computers & Technology*, vol. 36, no. 2, pp. 161–180, 2022. https://doi.org/10.1080/13600869.2022.2060472

[107] E. Chatzoglou, G. Kambourakis, and C. Kolias, “How is your Wi-Fi connection today? DoS attacks on WPA3-SAE,” *Journal of Information Security and Applications*, vol. 64, pp. 1–21, 2022. https://doi.org/10.1016/j.jisa.2021.103058

[108] M. Thankappan, H. Rifà-Pous, and C. Garrigues, “Multi-Channel Man-in-the-Middle attacks against protected Wi-Fi networks: A state of the art review,” *Expert Systems With Applications*, vol. 210, pp. 1–29, 2022. https://doi.org/10.1016/j.eswa.2022.118401

[109] T. Arif, A. Javed, M. Alhameed, F. Jeribi, and A. Tahir, “Voice spoofing countermeasure for logical access attacks detection,” *IEEE Access*, vol. 9, pp. 162857–162868, 2021. https://doi.org/10.1109/access.2021.3133134

[110] C. Yan, X. Ji, K. Wang, Q. Jiang, Z. Jin, and W. Xu, “A survey on Voice Assistant Security: Attacks and Countermeasures,” *ACM Computing Surveys*, vol. 55, no. 4, pp. 1–36, 2022. https://doi.org/10.1145/3527153

[111] S. Z. Khan, M. Mohsin, and W. Iqbal, “On GPS spoofing of aerial platforms: a review of threats, challenges, methodologies, and future research directions,” *PeerJ Computer Science*, vol. 7, pp. 1-35, 2021. https://doi.org/10.7717/peerj-cs.507

[112] A. Altaweel, H. Mukkath, and I. Kamel, “GPS Spoofing Attacks in FANETs: A Systematic Literature review,” *IEEE Access*, vol. 11, pp. 55233–55280, 2023. https://doi.org/10.1109/access.2023.3281731

[113] F. Qazi, “Application Programming Interface (API) security in cloud applications,” *EAI Endorsed Transactions on Cloud Systems*, vol. 7, no. 23, pp. 1–14, 2023. https://doi.org/10.4108/eetcs.v7i23.3011

[114] N. I. a. I. Ahmad, N. a. C. Anyanwu, N. S. Onwusinkwue, N. S. O. Dawodu, N. O. V. Akagha, and N. E. Ejairu, “Cybersecurity Challenges in Smart Cities: A Case Review of African Metropolises,” *Computer Science & IT Research Journal*, vol. 5, no. 2, pp. 254–269, 2024. https://doi.org/10.51594/csitrj.v5i2.756

[115] K. Kim, I. M. Alshenaifi, S. Ramachandran, J. Kim, T. Zia, and A. Almorjan, “Cybersecurity and Cyber Forensics for Smart Cities: A Comprehensive literature review and survey,” *Sensors*, vol. 23, no. 7, pp. 1–25, 2023. https://doi.org/10.3390/s23073681

[116] I. Gligorea, M. Cioca, R. Oancea, A.-T. Gorski, H. Gorski, and P. Tudorache, “Adaptive learning using artificial intelligence in e-learning,” *Journal of Education Sciences*, vol. *13*, no. 12, pp. 1-27, 2023. https://doi.org/10.3390/educsci13121216

[117] L. Ismail, and R. Buyya, “Artificial intelligence applications and self-learning 6G networks for smart cities digital ecosystems: Taxonomy, challenges, and future directions,” *Sensors*, vol. 22, no. 15, pp. 1-30, 2022. https://doi.org/10.3390/s22155750

[118] J. Telo, “Smart city security threats and countermeasures in the context of emerging technologies,” International *Journal of Intelligent Automation and Computing*, vol. *6*, no. 1, pp. 31–45, 2023. https://orcid.org/0009-0004-5101-8064

[119] Y. Maleh, Y. Baddi, M. Alazab, L. Tawalbeh, and Romdhani, I. “Artificial intelligence and blockchain for future cybersecurity applications,” In *Studies in Big Data* (1st ed.). Springer, 2021. https://doi.org/10.1007/978-3-030-74575-2

[120] K. Kalinaki, N. N. Thilakarathne, H. R. Mubarak, O. A. Malik, and M. Abdullatif, “Cybersafe capabilities and utilities for smart cities,” In *Advanced sciences and technologies for security applications* (pp. 71–86). Springer, 2023. https://doi.org/10.1007/978-3-031-24946-4_6

[121] P. Manickam, M. Girija, S. Sathish, K. V. Dudekula, A. K. Dutta, Y. A. Eltahir, N. M. Zakari, and R. Gilkaramenthi, “Billiard based optimization with deep learning driven anomaly detection in internet of things assisted sustainable smart cities,” *Alexandria Engineering Journal*, vol. 83, pp. 102–112, 2023. https://doi.org/10.1016/j.aej.2023.10.039

[122] U. Majeed, L. U. Khan, I. Yaqoob, S. M. A. Kazmi, K. Salah, and C. S. Hong, “Blockchain for IoT-based smart cities: Recent advances, requirements, and future challenges,” *Journal of Network and Computer Applications*, vol. 181, pp. 103007, 2021. https://doi.org/10.1016/j.jnca.2021.103007

[123] Z. Noor, S. Hina, F. Hayat, and G. A. Shah, “An intelligent context-aware threat detection and response model for smart cyber-physical systems,” *Internet of Things*, vol. 23, pp. 1–20, 2023. https://doi.org/10.1016/j.iot.2023.100843

[124] U. Ghosh, D. Das, P. Chatterjee, and S. Shetty, “Quantum-Enabled Blockchain for Data Processing and Management in Smart Cities,” *2023 IEEE 24th International Symposium on a World of Wireless, Mobile and Multimedia Networks (WoWMoM),* Boston, MA, USA, 12-15 June 2023, pp. 425–430. https://doi.org/10.1109/wowmom57956.2023.00075

[125] K. D. O. Ofoegbu, O. S. Osundare, C. S. Ike, O. G. Fakeyede, and A. B. Ige, “Data-driven cyber threat intelligence: Leveraging behavioral analytics for proactive defense mechanisms,” *Cybersecurity and Information Technology Research Journal*, vol. 4, no. 3, pp. 502-524, 2023. https://doi.org/10.51594/csitrj.v4i3.1501

[126] M. A. Mansoor, M. Ali, A. Mateen, M. Kaleem, and S. Nazir, “Blockchain technology for land registry management in developing countries,” *2023 2nd International Conference on Emerging Trends in Electrical, Control, and Telecommunication Engineering (ETECTE)*, Lahore, Pakistan, 27-29 November 2023, pp. 1–6. https://doi.org/10.1109/ETECTE51838.2023.1005678

[127] S. O. Olabanji, O. O. Olaniyi, C. S. Adigwe, O. J. Okunleye, and T. O. Oladoyinbo, “AI for Identity and Access Management (IAM) in the Cloud: Exploring the Potential of Artificial Intelligence to Improve User Authentication, Authorization, and Access Control within Cloud-Based Systems,” *Asian Journal of Research in Computer Science*, vol. 17, no. 3, pp. 38–56, 2024. https://doi.org/10.2139/ssrn.4706726

[128] K. Wang, Y. Zhao, R. K. Gangadhari, and Z. Li, “Analyzing the adoption challenges of the internet of things (IoT) and artificial intelligence (AI) for smart cities in China,” *Sustainability*, vol. 13, no. 19, pp. 1–35, 2021. https://doi.org/10.3390/su131910983

[129] H. Malik, T. Anees, M. Faheem, M. U. Chaudhry, A. Ali, and M. N. Asghar, “Blockchain and Internet of Things in smart cities and drug supply management: Open issues, opportunities, and future directions,” *Internet of Things*, vol. 23, pp. 1-33, 2023. https://doi.org/10.1016/j.iot.2023.100860

[130] C. Kontos, T. Panagiotakopoulos, and A. Kameas, “Applications of blockchain and smart contracts to address challenges of cooperative, connected, and automated mobility,” *Sensors*, vol. 24, no. 19, pp. 1–30, 2024. https://doi.org/10.3390/s24196273

[131] I. Ehsan, M. I. Khalid, M. Helfert, N. Yaqub, and M. Ahmed, “Integrating Privacy and Security in Smart Cities: A Blockchain-based IPFS Framework,” *Companion Proceedings of the 17th IFIP WG 8.1 Working Conference on the Practice of Enterprise Modeling Forum, M4S, FACETE, AEM, Tools and Demos*, Stockholm, Sweden, 3-5 December 2024, pp. 1-13. https://ceur-ws.org/Vol-3855/aem3.pdf

[132] N. S. Johri, “Strengthening Digital Forensics with Blockchain Technology and Algorithms,” *World Journal of Advanced Research and Reviews*, vol. 24, no. 2, pp. 459–467, 2024. https://doi.org/10.30574/wjarr.2024.24.2.3317

[133] H. F. Atlam, N. Ekuri, M. A. Azad, and H. S. Lallie, “Blockchain Forensics: A systematic literature review of techniques, applications, challenges, and future directions,” *Electronics*, vol. 13, no. 17, pp. 1–37, 2024. https://doi.org/10.3390/electronics13173568

[134] A. K. Tyagi, B. F. Balogun, and S. Tiwari, “Role of Blockchain in Digital Forensics: A Systematic Study,” In *Global Perspectives on the Applications of Computer Vision in Cybersecurity* (pp. 197–222). IGI Global, 2024. https://doi.org/10.4018/978-1-6684-8127-1.ch008

[135] 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. https://doi.org/10.1016/j.aej.2023.12.021

[136] C. Ma, “Smart city and cyber-security; technologies used, leading challenges and future recommendations,” *Energy Reports*, vol. 7, pp. 7999–8012, 2021. https://doi.org/10.1016/j.egyr.2021.08.124

[137] A., Sharma, E. Podoplelova, G. Shapovalov, A. Tselykh, and A. Tselykh, “Sustainable smart cities: Convergence of artificial intelligence and blockchain,” *Sustainability*, vol. *13*, no. 23, pp. 1-16, 2021. https://doi.org/10.3390/su132313076

[138] D. Zeng, Z. Cao, and D. B. Neill, “Artificial intelligence–enabled public health surveillance: From local detection to global epidemic monitoring and control,” In L. Xing, M. L. Giger, & J. K. Min (Eds.), Artificial Intelligence in Medicine (pp. 437–453). Elsevier, 2021. https://doi.org/10.1016/B978-0-12-821259-2.00022-3