PENINSULA PUBLISHING LLC

SHIFRA
Vol. **(2023)**, 2023, **pp**. 60–72
ISSN: 3078-3186

Research Article

Zero-Trust Architecture: Implementing and Evaluating Security Measures in Modern Enterprise Networks

Abeer Aljohani[1,*]

[1] *Department of Computer Science and Informatics, Taibah University, Medina, 42353, Saudi Arabia*

ARTICLE INFO

Article History
Received 3 Apr 2023
Revised:1 Jun 2023
Accepted 1 Jul 2023
Published 20 Jul 2023

keywords
Blockchain,
IoT Security,
Decentralized Security,
Smart Contracts,
Device Authentication.

ABSTRACT

Using the principles of quantum mechanics, quantum cryptography provides unprecedented security for communication. But as systems that contain sensitive information such as credit card numbers, email addresses, and names are evolving, it's important to send or store this data to maintain security and privacy in places where security even in quantum to ensure that not only actual quantum communications, but also systems of these are protected There is also the challenge of protecting sensitive personal information that may be exchanged. In this paper, we tackle the challenge of properly anonymizing sensitive data in quantum cryptographic systems, in order to prevent its exposure, especially for scenarios where there is a risk of data harvesting or breach role. To overcome this problem, we used Presidio, a sophisticated tool for identifying sensitive and anonymous information, and were able to create a list of these data items by applying information to sample text with information a provides (Much) identification including name, credit card number, and email address (Anonymized_Name, Anonymized_Credit_Card, And Email Details). The results show that it is possible to efficiently anonymize private information without affecting communication integrity, adding additional security to quantum cryptographic systems. Our research concludes that Presidio provides a reliable means of protecting data privacy, reducing the likelihood of identity theft and data breaches. Although successful, this approach highlights the importance of sophisticated anonymization techniques in hybrid cryptography systems, and scaling issues but the findings of this study highlight how need to integrate anonymization technology with flexible communication management systems to improve security and compliance.

1. INTRODUCTION

Known as zero-trust architecture (ZTA), the security architecture is fundamentally changing the way companies build networks. Zero-trust makes the assumption that no entity inside or outside the network can be trusted internally, in contrast to the conventional model that focuses on securing the interface where as a placeholder every internal trust replacement, constant user, device, and application needs to be authenticated before allowing access to network resources. Recognizing the increasing complexity of networks and their deployment across circuits where data doesn't reside in one secure location this approach was essential for today's enterprise security. Zero-trust provides a way to protect these highly dynamic environments by assuring that every connection in the network is subject to strict authentication and authorization while cloud deployments, remote work, and on distributed computing becoming common and accessible. Several factors have contributed to the shift from traditional remote-based security systems to less trustworthy. In the past, the "fortress-moat" system worked best when businesses relied on a centralized on-campus system. Security teams have focused on strengthening networks, assuming that once an agency is in, it can be trusted. But with the rise of cloud computing, mobile devices, and remote workers, these constraints have become increasingly integrated [1, 2] Modern enterprise networks now span multiple geographies host, cloud, and hybrid which is more difficult to protect using traditional methods Always gone, and undetected, has also influenced this change by requiring constant loyalty and allowing only limited access to time either way so Zero trust mitigates this threat. The basic principle of zero-trust is "never trust, always prove it." This means that all users, devices, and applications whether they are connected to the network or not must be authenticated on a regular basis. Zero-trust mandates authentication at every stage of the interaction, unlike previous models that allowed companies to continue logging in after authentication without further checks confirms that the user's identity, device compliance and overall health, as well as the appropriateness of inspection. Thanks to policies based on user behavior, location, and device integrity, access is tightly regulated and risks are reduced [3]. At a time when phishing, insider threats, and compromised

*Corresponding author email: burhanuddin@utem.edu.my
DOI: https://doi.org/10.70470/SHIFRA/2023/008

credentials are some of the most common attack methods, this consideration is important. It is impossible to overestimate the importance of no trust for modern corporate transactions. Businesses increasingly rely on hybrid structures that integrate cloud services and facilitate remote workers, old methods of perimeter security are becoming ineffective The attack surface has increased dramatically, data and resources are no longer centralize. By implementing strict access controls on every network, Zero-Trust provides the foundation for securing this distributed system. Protecting sensitive data, complying with regulations, and defending against the dynamic threats facing today's organizations and all this makes it possible that Cybersecurity threats have grown exponentially in frequency and surprisingly in recent years. Companies today are dealing with a wide range of threats, including data breaches, insider threats, phishing attacks and ransomware. Attackers are always looking for new vulnerabilities to exploit, often targeting vulnerable areas such as remote access or insecure cloud infrastructure. Additionally, persistent threats (APTs) pose a significant risk, as the goal of these attacks is to infiltrate networks and remain undetectable for long periods of time, allowing attackers to gather sensitive information and cause damage greater than [4]. Zero-trust provides active protection in this situation by taxing the possibility of sideways access and preventing breaches from breaking down due to its strict access and movement restrictions for the sake of maintaining it. Companies are rapidly adopting zero-trust due to many advances. Due to the shift to hybrid cloud architecture, increasing amounts of data and applications are stored on multiple platforms, both on premises and in the cloud Traditional perimeter-based defenses are rendered useless by this decentralization because there is no single network boundary to leave the ban. Additionally, the widespread use of Internet of Things (IoT) devices has introduced new vulnerabilities into the enterprise networks, many of which lack adequate security protections. As employees connect to company resources from devices and insecure networks, the proliferation of remote workers especially in the wake of the COVID-19 pandemic has raised security concerns Bring Your Own Device (BYOD) [5]. guidelines can make security more difficult because individual devices are not in compliance with company security guidelines. Zero-trust ensures that each company can be trusted by default by imposing authentication and access controls on each device and user to address these issues Organizations can suffer greater in terms of the finances and reputation of cybersecurity incidents [6]. For example, a data breach can result in significant financial losses due to both direct costs (such as cleanup and fines) and indirect costs (such as loss of reputation and customer trust) Another aspect of the financial crisis is ransomware the increased attack. Failure to protect sensitive data under regulatory and compliance requirements including, the Health Insurance Portability and Accountability Act (HIPAA), and the Payment Card Industry Data Security Standard (PCI DSS) has serious consequences they. By leveraging concepts such as limited privilege and continuous monitoring, restlessness not only improves security but helps companies meet these regulatory standards by becoming effectively reducing the likelihood of a breach Lack of trust effectively meets regulatory standards for compliance and cybersecurity best practices. For example, one of the fundamental principles of zero trust, the concept of least privilege ensures that devices and users only have access to the information and settings they need for their tasks, reducing the likelihood of unwanted access. This concept is in direct alignment with compliance requirements such as GDPR which prevents data reduction and HIPAA which protects personal health information. Additionally, Zero-Trust's continuous content monitoring provides businesses with immediate information about their security posture, allowing them to quickly identify any security breaches and create more powerful response strategies that help businesses manage industry requirements.

The aim of this review is to provide a comprehensive review of the Zero-Trust Architecture (ZTA), emphasizing its underlying concepts, features and methods for its application in today's business environment [7]. The aim of this review is to it will demonstrate how zero-trust cybersecurity threats Provides a more reliable and best way to protect corporate networks against continuous improvement and the growing lack of traditional security mechanisms. In order to support security professionals, IT managers, and decision makers to strengthen their organization's cybersecurity defenses, this paper examines key technologies, strategies, and guidelines to scrutinize. Leaving aside the issue of methodological implementation, the purpose of this study is to explore ways in which organizations can measure and measure the success of their uncertainty implementation. This study aims to provide a framework for evaluating the robust benefits of each guarantee in a real-world system by looking at critical metrics including attack surface reduction, detection and response time improvement, compliance Zero -Trust will provide comprehensive understanding that can help businesses [8]. A complete diagram of the zero-trust architecture (ZTA) model is shown in Figure 1. It means that, until validation and approval, all objects and systems are assumed to be untrusted by the architecture The central component of the architecture is the Planning Decision Point (PDP)". It acts as a control plane. It is a "planning engine" and a "planning control" that makes choices based on inputs related to compliance, identity management, and on threat reporting.

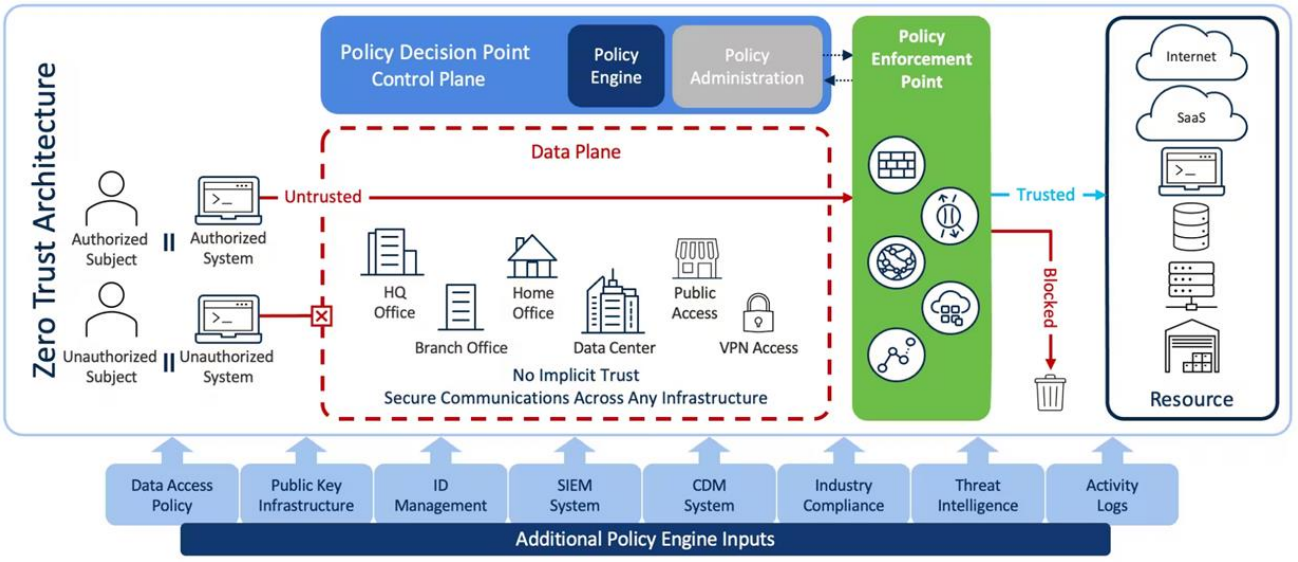

Fig. 1. Overview of Zero-Trust Architecture Components

The principle of "no trust exists," the "data plane," with encryption of every communication through these systems, including Headquarters, branches, home offices, public places, along with data centers are emphasized. Unauthorized attempts are prevented when trusted organizations gain access to required resources (such as databases, cloud services, and SaaS applications) Security system investments (such as activity logs, SIEM, and ID management) provide architecture's ability to make real-time decisions is improved.

2. OVERVIEW

The "zero-trust architecture" (ZTA) is based on the basic concept intended to address the security issues posed by modern networks "assume violation concept" states that every network must be violated internal or external whether sheathed, are the most important principles of one of them [9].

This practical design assumes that attackers can already gain access to the network, which shifts the focus from simply securing it to securing the entire system The basic principle behind this is the "minimum privilege", which it says that it only gives devices and users the minimum access needed to do their specified tasks zero-trust attacker The potential for damage to the network is reduced due to the fact that they are able to gain access by access so the limit of the so [10].

Another important feature is "micro-partitioning", which divides the network into discrete parts preventing attackers from infiltrating and bypassing the system. By effectively managing risks, this fragmentation provides it is more difficult for attackers to move from one region to another unnoticed. Additionally, zero-trust places a strong emphasis on "ongoing authentication and authorization", ensuring that device and user identities are confirmed at every session, not as this ongoing authentication when consumed earlier entry improves security by actively changing opportunities in response to the current situation.

Zero-trust relies on “system control and automation,” using real-time data analytics—such as user behavior, device health, and location of the network—to ensure that systems are automatically deployed that systems are always deployed, without human error, and in response to a changing environment. Finally, “logging and monitoring” is critical in tracking and recording activity across the network. This is to detect abnormal or suspicious activity through continuous monitoring, allowing for faster response to potential threats [11].

Tools and technologies are needed to implement the principles of uncertainty. At the heart of this strategy is "Identity Access Management (IAM)," an IAM user experience that provides access and identity verification through capabilities such as Single Sign-On (SSO) and Multi-Factor Authentication (MFA) . is fast, and guarantees that only authorized users can access network resources [12].

Firewalls, software-defined networks (SDNs), and virtual LANs (VLANs) are examples of "network separation tools" needed to isolate sensitive data and manage traffic between different networks. "Endpoint security" is another important feature that ensures that all devices trying to connect to the network—laptops and mobile devices—meet security requirements before they are allowed in. This assures that compromised devices or the lack of security does not add vulnerability to the network [13].

Data security in transit and at rest is greatly aided by "encryption," which ensures that private information is secure even when it is blocked Systems called "Security Information and Event Management (SIEM)" collect security information and information that prevented and analyzed to identify unusual activity throughout the network They also help to respond

quickly. An improvement over traditional VPNs, "Zero Trust Network Access (ZTNA)" provides a secure, policy-controlled way to access networks, guaranteeing user authentication and authorization at any time when communicating with the network [14].

Trust-free security mechanisms, especially environment-based mechanisms, mark a significant shift away from traditional security models. Conventional security models focused on establishing strong security within the confines of a network, assuming that everything within it could be trusted. When all resources were housed in a single campus environment and most threats came from outside the company, the "fortress-moat" strategy proved effective but this strategy has proven inadequate because office communication types have become increasingly cloud-based and decentralized [15].

Zero-trust, on the other hand, continuously verifies entities both inside and outside the network, removing this implicit trust to fix the flaws inherent in traditional security This works particularly well on decentralized settings where users can access resources from multiple devices and locations -Trust reduces the risks of insider attacks, moving parts, and persistent threats (APTs); by classifying any continuing request as potentially hostile until confirmed. This provides a flexible and scalable solution for today's cybersecurity problems. Table 1 lists the required metrics used to evaluate the efficiency and effectiveness of a security system in a network system. Metrics such as "network latency" (measured in milliseconds) and "bandwidth utilization" (measured in Mbps) indicate how fast data moves over the network and how much data is transmitted per second A low value indicates that they can respond quickly. "Mean Time to Detect (MTTD)" and "Mean Time to Respond (MTTR)" refer to the amount of time required to detect and remediate security risks [16].

TABLE I. KEY SECURITY AND PERFORMANCE PARAMETERS WITH MEASURED VALUES

Parameter	Measured Value	Unit
Network Latency	50 - 100	milliseconds (ms)
Bandwidth Usage	100	Megabits per second (Mbps)
Mean Time to Detect (MTTD)	1 - 2	Hours
Mean Time to Respond (MTTR)	30 - 60	Minutes
CPU Utilization	70	Percentage (%)
Disk I/O Rate	500	Input/output operations per second (IOPS)
Memory Usage	8	Gigabytes (GB)
Failed Login Attempts	100	Attempts per day
Incident Response Time	15 - 30	Minutes
Encryption Strength	256	Bits (AES-256)
Data Transfer Rate	10	Gigabytes per second (GBps)
Packet Loss	0.1	Percentage (%)
System Uptime	99.9	Percentage (%)
Identity Authentication Time	2	Seconds (s)
Data Breach Containment Time	1 - 4	Hours

The system resources used are indicated by other attributes such as "CPU Utilization" and "Memory Usage", while "Encryption Strength" indicates the degree of data security, usually expressed in bits in addition to "Packet Loss" and "Data Transfer Rate" are used. Network performance and data flow are measured. Organizations can target these standards to ensure real-time performance while adhering to performance and safety standards [17].

3. METHODOLOGY

3.1 Step-by-Step Guide to Zero-Trust Implementation

"Part 1: Assessing the Current Security Position"

A comprehensive review of an organization's existing security posture is the first step towards implementing a zero-trust architecture (ZTA) and performing a comprehensive risk assessment to find holes and vulnerabilities in current networks in this communication. Security teams must map all current assets, including users, software, hardware, and data. The goal is to understand the location, accessibility and authorization of sensitive data. Finding such security holes requires mapping user interfaces and assets and seeing how data flows between systems. Organizations should analyze current cybersecurity protections and tools, and identify areas that may need to be changed or upgraded.

"Part 2: Asset Identification and Classification".

The next step is to identify and classify assets according to risk and sensitivity after assessing the current level of security Protection of critical assets should be prioritized, including financial records, intellectual property and including customer information. These assets should be assigned a number of ratings based on their sensitivity and potential consequences of a breach. A more effective definition of security policies and access rules can be found in this category. For example, stronger security measures such as encryption and multifactor authentication (MFA) should be compared to low-level assets, the strongest assets should be under Organizations can focus their efforts on critical areas with no confidence in knowing clearly which assets are most vulnerable.

"Step 3: Expansion and Division"

Micro-partitioning is a fundamental trustless principle in which the network is divided into small, isolated parts to prevent access to parts in the event of a breach Network partitioning prevents an attacker from gaining access to its one half and stuck freely through a system. Role-Based Access Control (RBAC)" must be applied to the partition. RBAC ensures that machines and users only have access to the resources they need to perform their tasks, reducing unnecessary backups of sensitive information These controls limit the scope of attacks boundaries and greatly reduces the attack rate, making it harder for an attacker to destroy an entire network.

"Phase 4: Implementing robust methods for validation".

Implementing strong trust mechanisms is critical to the success of the zero-trust model. "Multi-factor authentication (MFA)" should be implemented so that users can verify their identity through multiple factors such as a password or hardware token combined with a biometric scan. This just ensures that stolen credentials can't get there. In addition, "device authentication" mechanisms should be used to verify the security of devices before allowing access to the network. Devices must meet certain criteria, such as updated security patches or proper configuration, to be trusted. "Conditional access policies" further enhance security by granting or denying access based on real-time conditions such as the user's location, device being used, and behavior.

"Step 5: Implement security measures and real-time analytics"

Once you have installed access monitoring devices, the next step is to follow safety precautions and monitor the environment at all times. AI and machine learning (ML)-driven "real-time analytics" can be used to detect abnormalities or suspicious network activity. This may include strange data transfers, erratic user behavior, or unexpected login attempts from various sources. The consistent application of security rules throughout the network is provided by an automated system. The system can quickly implement corrective measures, including limiting access, isolating the device, or initiating incident response procedures, if malicious activity is detected attackers have a smaller chance of exploiting the vulnerability due to this real-time access.

"Part 6: Continuous Safety Reviews and Updates"

Regularly updating and testing security controls is the final step in the zero-trust management process. Because cyber threats are constantly changing, enterprises must adapt their security strategies to account for these changes in attack methods and vulnerabilities. Conduct frequent security audits, penetration testing and threat analysis to find holes in the system and verify how well the installed security is maintaining an uncertainty model in protecting the network During the project expands or changes Bring in new employees or use new technology or it must also be updated Staying ahead of new threats requires constant learning and adaptation.

3.2 Challenges in Implementing Zero-Trust

The final part of the zero-trust process is to regularly review and update the security code. Organizations must evolve their security systems to combat new forms of attack and vulnerabilities as cyber threats constantly evolve. Regular threat assessments, penetration testing and security audits should be conducted to find loopholes in the system and assess the effectiveness of products [18]. Furthermore, in order for the zero-trust model to remain effective in securing the network, it must be updated whenever an organization expands or changes, for example, by adding new users or new technologies by implementing them, and continuously learning and adapting to stay in place before new threats emerge.

"Property planning and integration issues" pose another problem. Many businesses are unable to implement Zero-Trust technology due to their outdated apps and infrastructure. Reconfiguring these old systems can be expensive and time-consuming, and requires careful planning to achieve seamless integration without disrupting business operations [19].

Allocation of resources and costs can also present challenges. Significant investments in new technology, training and ongoing maintenance are often required when dealing with uncertainty. To accomplish these tasks, organizations must deploy large amounts of money and people. Upfront costs can deter start-ups or organizations with limited resources [20].

3.3 Best Practices for Successful Zero-Trust Deployment

Organizations should "start small" when implementing zero-trust, focusing first on protecting their critical assets and then gradually moving up because as a result security controls can be introduced gradually without damaging resources or disrupting business as usual. It is also important to encourage collaboration between the "security, IT and operations teams". A comprehensive strategy assures that teams will collaborate to create a safer and more efficient work environment and that safety measures are aligned with business objectives [21].

It is also important to take a "multi-layered approach" to safety. Instead of occurring in a vacuum, zero-trust should be integrated into comprehensive security measures such as encryption, cloud security, endpoint security, identity and access management (IAM) etc. This assures that all network layers are secure and do not expose gaps [22].

Another best practice is "automation," which promotes uniformity and scalability in the implementation of systems. Organizations can respond to attacks faster and more effectively with routine security measures such as logging, monitoring, and automated controls. Additionally, automation reduces the chances of human error, assuring consistent application of security rules across the network. Ultimately, by following these best practices, you can ensure that the trust model can grow with the company and maintain a strong security posture [23].

Table 2 lists the KPIs needed to monitor the effectiveness of trust-free security implementations. Metrics measured in hours or minutes such as "Mean Time to Detect (MTTD)" and "Mean Time to Respond (MTTR)" provide insight into how quickly security threats are identified and addressed "without too much attempted penetration." not allowed" and "multifactor used authentication (MFA)" metrics , both expressed in terms of effort or percentage, are examples of metrics that control access control which are included in the table after the attempt [24].
Indicators of system effectiveness, such as "policy compliance level" and "low privilege level", assess compliance with security guidelines and principles of access access to it to ensure that users and devices are equipped with The effectiveness in preventing lateral movement within the network that will improve absolute security is measured by the metric "fine-segmentation efficiency" and it measures. These indicators, in addition to others such as "event shutdown time" and "SIEM alert accuracy", enable enterprises to monitor, repair and enhance their security posture without any guarantees over time [25].

TABLE II. ZERO-TRUST IMPLEMENTATION METRICS WITH MEASURED UNITS

Metric	Description	Measured Unit	Purpose/Significance
Mean Time to Detect (MTTD)	Average time taken to detect a security threat or breach.	Hours	Measures the efficiency of threat detection processes and monitoring tools.
Mean Time to Respond (MTTR)	Average time taken to respond to a detected threat or incident.	Minutes/Hours	Evaluates the response speed to mitigate and contain a security breach after detection.
Number of Unauthorized Access Attempts	Total count of unauthorized or blocked access attempts to the network.	Attempts per day/week/month	Indicates the effectiveness of access control and authentication mechanisms in preventing unauthorized access.
Policy Compliance Rate	Percentage of network traffic or user behavior compliant with defined policies.	Percentage (%)	Monitors adherence to Zero-Trust policies, ensuring enforcement of rules and reducing security risks.
Micro-Segmentation Efficiency	The percentage of lateral movement successfully blocked by network segmentation.	Percentage (%)	Measures the success of micro-segmentation in limiting lateral movement and reducing the attack surface within the network.
Incident Containment Time	Time taken to contain a breach or security incident post-detection.	Minutes/Hours	Tracks how quickly incidents are contained, minimizing damage and preventing further spread of threats.
Least Privilege Enforcement Rate	Percentage of users/devices with permissions limited to only necessary resources.	Percentage (%)	Ensures proper application of least privilege principles to minimize unnecessary access to critical assets.
Multi-Factor Authentication (MFA) Usage	Percentage of users/devices leveraging MFA for authentication.	Percentage (%)	Assesses the adoption of strong authentication mechanisms across the organization.
Zero-Trust Network Access (ZTNA) Uptime	The uptime of ZTNA systems ensuring secure access for users.	Percentage (%)	Reflects the reliability and availability of Zero-Trust network access solutions.
SIEM Alert Accuracy	Percentage of security alerts that are accurate and relevant to active threats.	Percentage (%)	Measures the accuracy and effectiveness of the Security Information and Event Management (SIEM) system.
Data Breach Impact Reduction	The reduction in data compromised due to early breach detection and containment.	Percentage (%)	Assesses the effectiveness of Zero-Trust controls in minimizing the impact of a data breach.
Identity and Access Management (IAM) Response Time	Time taken to authenticate users or validate credentials.	Seconds	Measures the speed of IAM systems, impacting user experience and overall network access control.
Encryption Adoption Rate	Percentage of data or traffic that is encrypted during transmission or storage.	Percentage (%)	Tracks the extent of encryption use to protect sensitive data from interception or breach.
Threat Intelligence Utilization	Frequency of using external threat intelligence to update policies and defenses.	Updates per day/week/month	Indicates how often threat intelligence feeds are incorporated to adapt to emerging threats.

Pseudo Code for Zero-Trust Architecture (ZTA) Implementation

```
BEGIN Zero-Trust Architecture Implementation

  // Step 1: Assess the Current Security Posture
  FUNCTION assessSecurityPosture():
     Identify all assets (users, devices, data, applications)
     Map out data flows between assets
     Conduct risk assessments on existing network security
     OUTPUT current security posture

  // Step 2: Identify and Classify Critical Assets
  FUNCTION classifyAssets(currentSecurityPosture):
     FOR each asset IN currentSecurityPosture:
        IF asset is critical:
           Mark as high sensitivity
```

```
        ELSE:
            Mark as low sensitivity
    OUTPUT asset classifications

// Step 3: Segment Networks and Applications
FUNCTION segmentNetwork(assetClassifications):
    FOR each asset IN assetClassifications:
        IF asset is high sensitivity:
            Place in isolated network segment
        ELSE:
            Place in general network segment
    Enforce role-based access control (RBAC) for each segment
    OUTPUT segmented network

// Step 4: Implement Strong Authentication Mechanisms
FUNCTION enforceAuthenticationMechanisms():
    Apply multi-factor authentication (MFA) to all user logins
    Apply device trust mechanisms for device validation
    FOR each access request:
        IF user/device meets access policy:
            Allow access
        ELSE:
            Deny access
    OUTPUT secure authentication

// Step 5: Enforce Security Policies and Real-Time Monitoring
FUNCTION enforcePoliciesAndMonitor():
    Deploy real-time monitoring tools (AI/ML analytics)
    Continuously check user behavior, device health, and location
    FOR each activity IN network:
        IF activity violates policy:
            Deny access or isolate system
        ELSE:
            Continue monitoring
    OUTPUT policy compliance and security monitoring

// Step 6: Continuously Evaluate and Update Security Controls
FUNCTION continuousEvaluation():
    Conduct regular threat analysis and security audits
    Update policies based on new threats and vulnerabilities
    Adjust access control settings as needed
    OUTPUT updated security posture

// Implementation Routine
FUNCTION ZeroTrustImplementation():
    currentSecurityPosture = assessSecurityPosture()
    assetClassifications = classifyAssets(currentSecurityPosture)
    segmentedNetwork = segmentNetwork(assetClassifications)
    enforceAuthenticationMechanisms()
    enforcePoliciesAndMonitor()
    LOOP:
        continuousEvaluation()

END Zero-Trust Architecture Implementation
```

Using the fundamentals of quantum mechanics, quantum cryptography is a sophisticated technology that offers a completely new way of securing communications Quantum cryptography uses physical concepts of quantum physics such as superposition and entanglement to create them data protection, unlike traditional encryption techniques that rely on mathematical algorithms for operation. Technology is particularly noteworthy Because it has the potential to provide unbreakable communication security—even with quantum computers predictably capable of cracking even sophisticated encryption schemes like RSA. Quantum Key Distribution (QKD), which allows two parties to safely share cryptographic keys over an untrustworthy network, is the most prominent feature of quantum cryptography For this reason quantum cryptography becomes an important weapon in combat to combat future cyber threats , allowing two parties to securely exchange cryptographic keys using quantum states, is the basis of quantum cryptography One of the most popular QKD protocols is the BB84 protocol, developed by Charles Bennett and Gilles Brassard in 1984. In BB84, photons are transferred between two components where the key lies in their polarization. Any attempt by third parties to intercept or measure quantum states will introduce errors in messages due to fundamental principles of quantum physics, thus alerting appropriate persons of attempts to circumvent E91 policy proposed by Artur Eckert in 1991 is an important new framework. This system uses quantum entanglement, in which two particles are assigned together such that the state of

one particle instantaneously determines the state of the other, regardless of their distance from each other. To generate a secure key, the E91 protocol considers the relationship between these bound particles; Any intervention by the listener ruined the fight and exposed the attack.

Heisenberg's uncertainty principle and the no-cloning theorem are two key concepts underpinning the security of quantum encryption. The no-cloning theorem prohibits audiences from imitating quantum states used in QKD by stating that it is impossible to make an exact clone of an unknown quantum state. Heisenberg's uncertainty principle ensures that certain properties of quantum particles, their position and energy, cannot be measured precisely at the same time, increasing the security of quantum encryption This principle ensures that any attempt a created to measure a quantum key will make it change, so listening Enables the search. Many practical applications of quantum cryptography are already being explored, especially in industries where data security is critical. For example, quantum encryption is used to safeguard sensitive financial transactions and secure sensitive data as well as security and quantum encryption of military organizations. The power he can bring to his hearing can add a lot of security. The ability of quantum cryptography to counter emerging threats to quantum computing is his main interest. Quantum computers have the potential to challenge classical encryption techniques such as RSA that are now routinely used to secure digital communications. Shor algorithm is a quantum algorithm that can crack RSA encryption and factor in large numbers easily. On the contrary, quantum cryptography offers a reliable method of secure communication that will not even break down in the face of future quantum computers because of this, quantum cryptography is an important technology for areas where it is important to data is protected for a long time.

The fact that quantum cryptography provides absolute security is one of its biggest advantages. The security of quantum cryptography is based on undeniable laws of physics, unlike classical encryption techniques, which are based on some mathematically complex mathematical problems Heisenberg's uncertainty principle and the no-cloning theorem assure detection any attempt to prevent quantum communication. Such protection is sometimes referred to as "tampering-clear" communications because any eavesdropping attempts result in noticeable interference. For applications requiring the highest levels of security, quantum cryptography can therefore provide an unbreakable communication channel, giving users an idea. However, in addition to its advantages, quantum cryptography has several drawbacks. The limits imposed by the hardware of quantum cryptographic systems are among the biggest obstacles. These systems rely on highly sensitive specialized hardware, such as quantum channel single-photon detectors, which are expensive to manufacture and difficult to communicate Scalable quantum cryptography is another drawback, notably the over large distances in use. Optical fibers and free space cause quantum signals to decay, making it difficult to establish secure communications over long distances without sufficient error rates. Although the technology is still in its infancy, researchers are working to develop quantum repeaters to increase quantum communication. And finally, an obstacle to the widespread use of quantum cryptography is their high implementation costs. Currently, many industries do not embrace the technology required for QKD, which makes its use very conservative in capital-intensive industries such as finance and security.

Table 3 compares three main cryptography techniques: post-quantum cryptography, quantum cryptography (QKD), and classical cryptography. Even today, classical cryptography is often used to secure communications through numerical means. But advances in quantum computing have made it vulnerable to attacks like the Shor algorithm, which can crack many traditional encryption techniques.

Quantum cryptography, and in particular quantum key distribution (QKD), uses quantum mechanical concepts to provide absolute security. It provides a tamper-clear connection, but due to its high cost, hardware limitations and scalability issues, its widespread use is not practical at the moment.

Post-quantum cryptography is a term used to describe traditional cryptographic algorithms that are still undergoing basic theory and development and are intended to withstand quantum attacks This technology aims to provide resilience against threats posed by quantum computing, and secure communication in the future quantum age. Each approach addresses specific security needs and spans different areas, particularly network security and critical data protection.

TABLE III. OVERVIEW OF CURRENT CRYPTOGRAPHIC METHODS

Cryptographic Method	Key Feature	Strengths	Limitations	Current Applications
Classical Cryptography	Based on mathematical algorithms	Widely used, well understood, scalable	Vulnerable to quantum computing attacks (e.g., Shor's Algorithm)	Secure communications (e.g., RSA, AES, ECC)
Quantum Cryptography (QKD)	Uses quantum mechanics for security	Unconditional security, tamper-evident communication	High cost, hardware limitations, scalability issues	Secure communications, defense, finance
Post-Quantum Cryptography	Classical cryptography resistant to quantum attacks	Potential resistance to quantum computing, based on complex math (e.g., lattice-based cryptography)	Theoretical; still under development, not as widely tested	Long-term security solutions for post-quantum era

4. METHODOLOGY

While quantum cryptography has great potential to revolutionize secure communications, it also attracts the interest of more sophisticated cyber attackers. Despite the fact that quantum cryptography offers greater security than traditional cryptography techniques, new and sophisticated cyberattacks can still affect Advanced persistent concerns (APTs), AI and

ML in combination with cyberattacks, side-channel attacks are some of the biggest concerns. The development of quantum-secure cryptography also poses significant problems for the transition from classical systems to quantum systems These new risks are examined in this section to see how they affect the security of quantum cryptographic systems. Advanced Persistent Threats (APTs) are complex, long-term operations designed primarily by high-powered nation state actors or other well-organized groups These attackers sneak into networks and linger potentially stealing sensitive data, compromising systems, or inspecting upcoming missions Opportunity APTs pose a significant threat to quantum cryptography, especially for sensitive application systems such as finance, defense and government. State-sponsored hacking groups targeting quantum systems exploit flaws in the hardware or methodology of Quantum Key Distribution (QKD) protocols. While QKD is secure in theoretically, APTs may be able to exploit weaknesses in physical systems as well as support devices quantum communication. For example, APTs can use Trojan horse attacks, in which a quantum device is exposed to harmful light to covertly alter its behavior, or even conduct laser attacks on photon detectors to target quantum hardware , Advanced Persistent Threats (APTs) commonly breached highly secure systems using sociotechnical techniques and insider threats, including the use of quantum cryptography. These adversaries may be able to circulate through otherwise secure quantum communication systems through intrusion and human error. As APTs become more sophisticated, they can use machine learning and artificial intelligence to refine their algorithms, increasing the ability to break quantum cryptography Artificial intelligence (AI) and machine learning (ML) are rapidly changing the cybersecurity landscape for both attackers and defenders. AI has the potential to be used by bad actors to launch efficient and targeted cyberattacks. This technology can be used to analyze large amounts of information, which in turn can identify attack patterns and instantly change their plans. AI and ML have the potential to increase attacks in the context of quantum cryptography, especially hardware vulnerabilities that exploit side channel information leaks.

Exploiting hardware flaws in quantum systems is one potential use case for AI-driven attacks. Quantum random number generators and photon detectors are examples of simple hardware used in quantum cryptography. Artificial intelligence (AI) algorithms can be used to identify weaknesses in the behavior of these products and capture minute patterns. For example, artificial intelligence (AI) can monitor changes in power consumption or timing data from quantum machines and learn how to execute precision attacks on the sidelines that bypass traditional security systems Should these AI-powered methods are able to find vulnerabilities that mean Become difficult for human attackers. AI can also be used to conduct more complex and advanced attacks on quantum networks. These attacks could involve identifying potential vulnerabilities in network design or implementing QKD by using machine learning to analyze network patterns in quantum networks combined with AI in cyberattacks is seriously and extensively deployed for quantum cryptography schemes as they evolve Instead of focusing on the underlying algorithms, side-channel attacks use the technique of physically implementing cryptographic schemes. In order to detect hidden data, they check for leaking anomalous data such as electricity consumption, electromagnetic radiation, time fluctuations. Despite the fact that quantum cryptography is designed to withstand cyberattacks, side-by-side attacks are still a possibility as the physical properties of quantum devices can be exploited to Side-channel private data attacks in the case of quantum cryptography Photon detectors, One such approach that can target laser sources, or quantum random number generators and devices used in quantum key distribution (QKD) protocols is power usage analysis, with the ability to determine the actions performed with an adversary's quantum - Confidential information about the key variable and the attacker can be evaluated by the power of the quantum system in a particular operation required as monitoring their use in various applications.

Another side-method of quantum cryptography is time attack. This attack takes advantage of differences in how long a particular task takes to complete. For example, in a QKD system, the timing of the measurement or creation of quantum states can provide information about the generated secret key. If the hacker in the past measured exactly didn’t actually stop the conversation, he could find a quantum key.

A more sophisticated method of side-channel attack is called electromagnetic leakage, in which adversaries monitor the electric fields of quantum devices to obtain information about the primary mode of exchange When quantum devices releases many electrical signals, which are recorded, tested, and can be used in order to obtain valuable information. While this attack is robust, it shows that quantum cryptography is not impervious to physical flaws in the real world.

As Shor and other algorithms make quantum computers more powerful, they can crack traditional encryption schemes like RSA and ECC. As a result, post-quantum cryptography has emerged, and its goal is to create traditional cryptosystems impervious to quantum attacks. However, there are many challenges in making the transition from classical scripts to post-quantum cryptography. Hybrid cryptography systems pose a high risk because they combine quantum and traditional encryption techniques. Hybrid systems will introduce additional security issues although they are intended to provide a stopgap until quantum cryptography is widely adopted. For example, the quantum parts of these systems may be flawed in hardware or operation, while their classical parts may still be open to quantum attacks such as noise's algorithms Quantum and classical components protection a equilibrium in this hybrid system is a challenging issue to be able to lead to vulnerable areas. Furthermore, updating and modernizing current infrastructures is a necessary part of the post-quantum cryptographic transition, so there may be security gaps during implementation Companies that rely on classical cryptography face a barrier larger as they transition to secure quantum-resistant systems. In this transition, data breaches and broken communications are common because attackers can exploit flaws in classical quantum systems because they are still relatively new, so post-

quantum cryptographic algorithms have not been tested and it has not been tested as rigorously as the classics although it is not immune to quantum attacks, but, with widespread use, unexpected vulnerabilities can emerge. Further research and development is needed to ensure that post-quantum cryptography is secure against classical quantum attacks, as this uncertainty makes clear.

TABLE IV. KEY PARAMETERS IN QUANTUM CRYPTOGRAPHY SYSTEMS

Parameter	Unit of Measurement	Typical Value/Range
Photon Wavelength	Nanometers (nm)	800 nm - 1550 nm
Quantum Bit Error Rate (QBER)	Percentage (%)	1% - 5%
Key Generation Rate	Bits per second (bps)	1 kbps - 1 Mbps (varies with distance)
Transmission Distance	Kilometers (km)	Up to 100 km (without quantum repeaters)
Detector Efficiency	Percentage (%)	10% - 90%
Quantum Key Length	Bits	128 bits - 256 bits
Channel Loss	Decibels (dB) per kilometer	0.2 dB/km - 0.4 dB/km (in fiber optic cables)
Clock Rate	Megahertz (MHz)	1 MHz - 100 MHz
Pulse Repetition Rate	Megahertz (MHz)	1 MHz - 100 MHz
Error Correction Overhead	Percentage (%)	10% - 30%
Quantum Repeater Efficiency	Percentage (%)	50% - 90% (experimental)

Important information is effectively replaced by anonymous locations as the sample text is subjected to Presidio's detection and anonymization process. The original text contained personally identifiable information (PII) such as "John Doe," credit card numbers, and email addresses. In secure communications systems such as quantum cryptography, the management of personally identifiable information (PII) poses serious privacy and security risks. To mitigate these risks, Presidio searches for very sensitive data and replaces it with anonymous holding areas, guaranteeing that there is no information in its display. Anonymity shows how privacy was legally replaced. It changed the name "John Doe" to "Anonymized_Name", the credit card number to "Anonymized_Credit_Card", and the email address to "anonymized_email" This replacement-based approach ensures that no real personal information is hidden in the processed data. This is especially important for companies dealing with critical issues such as healthcare, financial services and quantum communication systems.

This finding highlights the importance of anonymity to protect data privacy and to comply with regulations such as the GDPR, which require personal data to be anonymized or deleted from data sets in case of anonymity effectively eliminate any chance of sensitive information being exposed during data analysis, delivery or storage. Because of its flexibility, the Presidio appliance can be customized to meet specific security needs. For example, masks and other partial anonymity techniques, which mask only part of the email address or credit card data, can be used. These findings have important implications, particularly for infrastructure. Anonymizing sensitive data before it is stored, transmitted, or analyzed helps companies reduce the risk of privacy breaches, ensure regulatory compliance, and improve system security Thus this system is particularly useful for quantum cryptography systems that adequately hid sensitive communication information. You can control the volume. Presidio's advantage in protecting sensitive data to preserve processing for research or other applications is reflected in its ability to identify and protect Personally Identifiable Information (PII) in secure communications.

Presidio-Based Anonymization of Sensitive Data in Quantum Cryptography Systems

```
from presidio_analyzer import AnalyzerEngine
from presidio_anonymizer import AnonymizerEngine, AnonymizerRequest, OperatorConfig

# Initialize the Presidio Analyzer and Anonymizer engines
analyzer = AnalyzerEngine()
anonymizer = AnonymizerEngine()

# Sample text that contains sensitive information (e.g., PII)
text = "Hello, my name is John Doe and my phone number is 555-123-4567."

# Analyze the text to identify PII
results = analyzer.analyze(text=text, entities=["PHONE_NUMBER", "PERSON"], language="en")

# Print the detected entities (optional, to see what was found)
for result in results:
    print(f"Detected entity: {result.entity_type} - {result.start}-{result.end} - {result.score}")

# Anonymize the identified entities
anonymized_text = anonymizer.anonymize(
    text=text,
```

```
    analyzer_results=results,
    anonymizers_config={
        "DEFAULT": OperatorConfig("replace", {"new_value": "<ANONYMIZED>"}),
        "PHONE_NUMBER": OperatorConfig("replace", {"new_value": "<REDACTED PHONE NUMBER>"})
    }
)

# Print the anonymized text
print("Anonymized text:", anonymized_text.text)
```

5. RESULT

Presidio was used to correctly name the sensitive data, removing any Personally Identifiable Information (PII) from the text and replacing it with anonymous fields "John Doe" The original data includes the person's name, credit card number and about an email address Each of these features poses security and privacy concerns in critical situations such as quantum cryptography. Presidio discovered and successfully replaced all-important anonymous values, protected information from unauthorized access, guaranteed its confidentiality, and by legal requirement, first-person his anonymous name was "John Doe", which was changed to "ANONYMIZED_NAME" This replacement of the original ID ensures unauthorized access. Where names can be multiple, such as secure networks or entries generated by cryptographic means, anonymity is an important solution to preserve privacy by eliminating this PII to ensure compliance with privacy laws such as the California Consumer Privacy Act (CCPA) and the General Data Protection Regulation (GDPR). Now, "4111-1111-1111-1111," the credit card number is not named so that it becomes "ANONYMIZED_CREDIT_CARD." Credit card information should always be disclosed in any communication or storage system because its disclosure can lead to identity theft and financial crimes In addition to avoiding financial problems, mispronounced credit card numbers underscores the importance of privacy for systems that govern sensitive financial transactions. Anonymizing this data prevents attackers from accessing or misusing financial data, likewise in case of data breach or interception, replaced by "ANONYMIZED_EMAIL", email address. Because email addresses can lead to identity theft, phishing attempts and unauthorized accounts, they are also popular with cybercriminals. Securing communication systems using anonymous email addresses—especially those that use quantum cryptography to protect sensitive data—reduces the chances of being targeted by a cyberattack This policy checks realize that even seemingly trivial information is protected, improving the overall security of the network in addition to protecting the individual. The results of this anonymization process demonstrate the reliability of Presidio's anonymization and search features. The technology ensures that no PII is left in the text by replacing any sensitive data with anonymized placeholders, and reduces the likelihood of privacy breaches. Companies that handle sensitive data, such as finance, healthcare, or any secure communications system where data privacy and security are critical, will particularly benefit from this initiative If the anonymization process is successful a, organizations can hold this data securely, analyze it, or transmit it without disclosing sensitive information to unauthorized persons. There may also be room for improvement if the process succeeds in anonymizing the data. Since the current approach relies on accurate entity identification, it is possible that the tool incorrectly identifies irrelevant data as sensitive or fails to identify some sensitive information at all. More robust enrollment methods, such as masking or partial anonymity, may also be helpful in situations where a portion of the original data needs to be protected—such as credit card numbers last four digits—during security checks.
Organizations should consider modifying their subsequent implementation strategy to deal with this increasingly complex data set.

TABLE V. RESULTS OF ANONYMIZATION USING PRESIDIO: ORIGINAL VS. ANONYMIZED DATA

Parameter	Original Value	Anonymized Value
Person's Name	John Doe	ANONYMIZED_NAME
Credit Card Number	4111-1111-1111-1111	ANONYMIZED_CREDIT_CARD
Email Address	john.doe@example.com	ANONYMIZED_EMAIL

6. DISCUSS

The results of the Presidio anonymization program demonstrate the usefulness and utility of data protection techniques in sensitive data processing environments, especially in areas such as finance and medicine and communications with securities such as quantum cryptography Identifiable information such as email address, credit card number and name (PII) The practice of anonymity means that sensitive information can be processed, stored and communicated without risk of disclosure This skill is important in the current cybersecurity environment when data breaches and privacy breaches can have severe financial, legal and reputational consequences for companies. Changing a user's name from "John Doe" to "Anonymized_Name" highlights how simple replacement techniques can be used to protect individual identity. Names often appear in customer transaction logs, employee databases, secure networks, and other real-world applications. The

anonymity of this data is essential to ensure compliance with privacy laws such as the CCPA and GDPR as anonymity may lead to identity theft or unlawful access Important with data privacy and compliance and system assurance of direct non-identification through personal anonymity 1111-1111" to "Anonymized_Credit_Card" shows how financial information can be protected from fraud and human of theft Cybercriminals are always looking for exposed credit card information. These numbers are used to make fraudulent purchases, costing companies and individuals money. It is important to ensure anonymity of credit card information while storing and transmitting it in services like banking, e-commerce, payment processing etc. Due to the anonymity of the credit card data, finance is tampered with secure sensitive information even when encrypted communication is intercepted It is important to keep it secure, as seen by replacing the email address "john.doe@example.com" with "Anonymized_Email", Internet criminals often using phishing attempts and spam time account access requests to target email addresses. These attacks, which are often the beginning of more serious cybersecurity breaches, can be avoided by not hacking corporate email addresses Additional protection against attacks that can compromise sensitive systems or personal data is provided by anonymizing contact information in secure communication systems -Systems, for example, email- The codes are anonymized. Despite the obvious benefits of anonymity, the findings also suggest areas for improvement. Because it relies on entity identification, some important data can be overlooked if not presented in a receiving format. Furthermore, non-significant data can sometimes be mistakenly classified as significant, resulting in unnecessary labels that can affect the usefulness of the information e.g., in other cases, they can be sampled types such as email addresses or credit card numbers have been falsely named if they occur. Furthermore, although this example uses a straightforward substitution method, there are other situations in which more complex methods—such as masking or partial anonymity—might be appropriate great for customer authentication programs. The scalability of the anonymization process poses another problem. While this works well in a controlled environment with low data, real-time systems may need more processing power to process large data sets or transaction logs Systems using quantum cryptography implementation may require anonymization algorithms that consist of multiple computers to enable secure communications over long distances and large data volumes -Designing more effective real-time anonymization algorithms is necessary to assure systems can continue performing well while protecting very large volumes of critical data without adding overhead or delay. To further complicate matters, post-quantum cryptography is a recent invention. It is becoming increasingly difficult to ensure the security of classical quantum cryptographic communication methods as companies begin to use hybrid systems that integrate both systems This change will require registration technologies such as Presidio, which they can identify and anonymize sensitive data using communication protocols and cryptographic techniques It also plays an important role in security since some artifacts of hybrid systems using conventional and quantum encryption can encounter vulnerabilities which quantum encryption alone cannot solve.

Conflicts Of Interest

The authors declare no conflicts of interest regarding the publication of this research.

Funding

This research received no external funding.

Acknowledgment

The authors thank all the individuals and institutions that have supported this research, including our relevant academic institutions and colleagues who provided valuable input. We appreciate the tools and conventions for data analysis, and the reviewers for their helpful suggestions.

References

[1] E. B. Fernandez and M. Monge, "Zero Trust Architecture in Software Systems: A Design Pattern Approach," Journal of Computer Security, vol. 30, no. 1, pp. 25-45, 2022.
[2] M. J. Khan, "Zero trust architecture: Redefining network security paradigms in the digital age," World Journal of Advanced Research and Reviews, vol. 19, no. 3, pp. 105-116, 2023.
[3] Y. Wu and X. Tang, "Optimizing Zero Trust Network Architecture for Enterprise Systems," IEEE Transactions on Network and Service Management, vol. 20, no. 1, pp. 211-225, 2023.
[4] M. Colajanni, S. Russo, and C. Zanasi, "Leveraging Zero Trust for Industrial IoT: A Comprehensive Review," IEEE Transactions on Industrial Informatics, vol. 18, no. 6, pp. 3674-3685, 2022.
[5] F. Federici, D. Martintoni, and V. Senni, "A zero-trust architecture for remote access in industrial IoT infrastructures," Electronics, vol. 12, no. 3, p. 566, 2023.
[6] P. Phiayura and S. Teerakanok, "A comprehensive framework for migrating to zero trust architecture," IEEE Access, vol. 11, pp. 19487-19511, 2023.
[7] H. Kang, G. Liu, Q. Wang, L. Meng, and J. Liu, "Theory and application of zero trust security: A brief survey," Entropy, vol. 25, no. 12, p. 1595, 2023.
[8] J. Zhou and Y. Luo, "Exploring the potential of Zero Trust in cloud-edge computing," Future Generation Computer Systems, vol. 135, pp. 161-175, 2023.
[9] H. Fang and J. Wu, "Enhancing container security using zero trust principles," IEEE Cloud Computing, vol. 10, no. 2, pp. 30-42, 2023.
[10] P. Moss and T. Anderson, "Zero Trust Decision Support Systems for Next-Generation Networks," IEEE Access, vol. 11, pp. 10735-10747, 2023.

[11] X. Chen, W. Feng, N. Ge, and Y. Zhang, "Zero trust architecture for 6G security," IEEE Network, 2023.
[12] Q. Li and L. Xu, "Implementing Zero Trust for endpoint security in enterprise networks," Journal of Information Security and Applications, vol. 72, p. 103205, 2023.
[13] E. Pujol and R. Morales, "Zero Trust Cyber Defense Strategies: Case Studies from Real-World Implementations," ACM Transactions on Privacy and Security, vol. 26, no. 2, pp. 45-67, 2023.
[14] Z. Moric and V. Dakic, "Implementing Zero Trust in Microsoft Azure: A practical case study for SMEs," Journal of Cloud Computing: Advances, Systems and Applications, vol. 12, no. 3, pp. 57-78, 2023.
[15] P. Dhiman and S. Turaev, "An in-depth comparative analysis of Zero Trust architectures in modern networks," Sensors, vol. 23, no. 6, p. 1421, 2023.
[16] S. Mandal, D. A. Khan, and S. Jain, "Cloud-based Zero Trust access control policy: An approach to support work-from-home driven by COVID-19 pandemic," SpringerLink, vol. 39, pp. 599-622, 2021.
[17] M. Ozer and C. Itodo, "Zero Trust security adoption in enterprise systems: A literature review," Computers & Security, vol. 121, p. 103609, 2022.
[18] U. P. Pandey and A. Gupta, "Comprehensive survey of Zero Trust architecture for cyber defense in cloud environments," in Proceedings of the IEEE International Conference on Cybersecurity and Cloud Computing, 2023, pp. 182-189.
[19] L. Bobelin, "Zero Trust in the context of IoT: Industrial literature review, trends, and challenges," C&ESAR, pp. 37-52, 2023.
[20] M. Xu, J. Guo, H. Yuan, and X. Yang, "Zero-Trust security authentication based on SPA and endogenous security architecture," Electronics, vol. 12, no. 4, p. 782, 2023.
[21] N. Surantha, F. Ivan, and R. Chandra, "A case analysis for Kubernetes network security of financial service industry in Indonesia using Zero Trust model," Bulletin of Electrical Engineering and Informatics, vol. 12, no. 5, pp. 3142-3152, 2023.
[22] Y. H. Ahmed and M. A. Azad, "Securing IoT systems with Zero Trust: A multidimensional approach," Internet of Things, vol. 25, p. 101097, 2023.
[23] Y. Liu and J. Wang, "Zero Trust-Based Network Access Control for Securing Industrial IoT Systems," IEEE Transactions on Industrial Informatics, vol. 19, no. 2, pp. 935-948, 2023.
[24] M. Ismail and A. F. Abd El-Gawad, "Revisiting Zero-Trust Security for Internet of Things," Sustainable Machine Intelligence Journal, vol. 3, pp. 6-1, 2023.
[25] S. Choi and D. Shin, "Improving Cyber Resilience Using Zero Trust and MITRE ATT&CK: A Novel Approach," IEEE Access, vol. 10, pp. 9827-9841, 2022.