Review

Emerging Authentication Technologies for Zero Trust on the Internet of Things

Chanapha Bast and Kuo-Hui Yeh *

Posted Date: 1 July 2024

doi: 10.20944/preprints202407.0053.v1

Keywords: Authentication; Internet of Things (IoT); Security; Zero Trust

Review

Emerging Authentication Technologies for Zero Trust on the Internet of Things

Chanapha Bast [1] and Kuo-Hui Yeh [2,*]

[1] Chanapha Bast is with Information System and Business Computer Department, Management Science Faculty, Udon Thani Rajabhat University, Thailand. Email: chanapha.b@udru.ac.th
[2] Kuo-Hui Yeh is with Institute of Artificial Intelligence Innovation, National Yang Ming Chiao Tung University, 300 Hsinchu, Taiwan, and also with department of Information Management, National Dong Hwa University, 974 Hualien, Taiwan. Email: khyeh@nycu.edu.tw
* Correspondence: khyeh@nycu.edu.tw

Abstract: The large and interconnected nature of the Internet of Things (IoT) presents unique security challenges, even as it revolutionizes various sectors. With numerous devices, often limited in resources, traditional perimeter-based security methods struggle to keep pace. The "never trust, always verify" principle of zero trust security offers a viable solution. Zero trust security is a concept which has become increasingly popular, using key exchange techniques to ensure secure and authenticated communication within the network, especially in managing risks in critical infrastructure. Authentication is a process to identify an entity, a prerequisite for authorization, and essential for granting access control. It fundamentally relies on trust management and various methods to generate and manage cryptographic keys for authentication. The aim of this study is to enhance zero trust security in the context of the Internet of Things by investigating authentication methods and discussing several potential solutions for successful implementation. This study also presents the performance evaluation criteria for authentication in IoT and introduces advanced approaches for different scenarios, including lightweight cryptography, mutual authentication, and blockchain technology. Finally, we address challenges related to implementation and future directions for research.

Keywords: authentication; Internet of Things (IoT); security; zero trust

1. Introduction

The Internet of Things (IoT) has transformed numerous industries, but ensuring the security of its expanding network offerings has presented significant challenges. Traditional security methods that rely on firewalls and predefined access controls (ACLs) are inadequate for the IoT due to several factors: 1) scalability; 2) limited resources; 3) heterogeneity; and so forth, as noted in [1]. The IoT analytics market, predicted to grow at an annual rate of 60% over the next five years, will drive the adoption of technologies for continuously analyzing event streams. According to [2], through 2025, decision management systems will experience a 745% compound annual growth rate (CAGR) due to increased demands for decision consistency and knowledge retention. By 2025, 75% of users will interact regularly with services based on cognitive computing. Although big data is not a new concept, its importance has reached a tipping point as more people digitize their lives, effectively turning themselves as "walking sensors". However, as the number of connected devices continues to multiply, so does the attack surface for malicious actors, raising serious security concerns.

In the IoT environment, traditional authentication methods are often inadequate, leaving systems more vulnerable to phishing, brute-force, and man-in-the-middle attacks. The cybersecurity model known as "zero trust security" poses a significant opportunity for advancement to the perimeter-based approach. A critical component of zero trust security is the implementation of robust authentication procedures to ensure that only authorized individuals can access resources, thereby preventing unauthorized access. However, traditional authentication methods are hampered by the unique characteristics of the IoT ecosystem, which include heterogeneity, limited resources, and

doi:10.20944/preprints202407.0053.v1

scalability requirements. On the other hand, cryptographic authentication methods enhance security by utilizing encryption and precise algorithms. By enabling continuous authentication on IoT devices, Federated Identity and Access Management (FIdAM) solutions promote interoperability across systems. Additionally, emerging technologies which can further improve security, trust, and the tamper resistance of IoT authentication procedures are being explored. These technologies include blockchain-based authentication and Physical Unclonable Functions (PUFs) [3]. In addition, the authors presented the advantages of Zero Knowledge Proofs (ZKPs) and discussed the application of zero-knowledge authentication across various IoT networks. Additionally, they provided an overview of the properties of zero-knowledge authentication in the IoT environment. These state-of-the-art technologies provide innovative solutions to the unique challenges posed by the IoT environment, paving the way for more reliable and secure authentication systems. Furthermore, the National Institute of Standards and Technology (NIST) has introduced the concept of Zero Trust Architecture (ZTA) to address these issues. Trust in an object can only be established through identity verification and trust assessment. Once the system grants the necessary permissions, the object can perform relevant tasks. In [4], He et al. describe the adoption and migration to ZTA as facing various hurdles, including the complexity of security management, risk assessments, configurations, and life-cycle change management. Authority is obtained by providing the access agent with authorization data through the access control engine, which integrates outcomes (people and devices) at varying security levels. Users must adhere to applicable security policies to access resources across domains. The technological pillars of ZTA include identity authentication, access control, and trust evaluation algorithms. Particularly, authentication in IoT with Zero Trust security involves sensitive data, such as passwords, personal identification numbers (PINs), facial recognition, and fingerprints. Soewito et al. [5] present a data transmission system combining data encryption and authentication. Their experiments involved thirty text data samples, each measured for performance in both encryption and authentication processes. The proposed method showed a speed of processing suitable for the security of data transmission systems, with authentication performance around 5ms from the client-server side.

Security assurance is increasingly crucial for the IoT, which has become pervasive in our lives. Using passwords, token keys, systems, and other authentication techniques on IoT devices and networks introduces numerous risks and concerns. Recognizing and evaluating conventional authentication methods within IoT ecosystems is essential when exploring new authentication solutions with zero trust security. Patel et al. [6] provided a comprehensive review of the zero-trust security architecture, emphasizing its essential ideas, real-world applications, and its impact on cybersecurity as a paradigm shift in information systems. ZTA not only revisits previous concepts but also integrates additional foundations such as data, device, user, network, environment, visibility, analytics, application, workload, automation, and orchestration. Ahmadi et al. [7] introduced the concept of zero trust micro-segmentation, which manages traffic entering or leaving a network, enhancing security through detailed segmentation.

This study aims to evaluate the efficacy of the latest advancements in biometrics, blockchain, artificial intelligence (AI), and other cutting-edge techniques in authentication enhancing IoT security and resilience. It also explores how zero trust security and authentication methods interrelate within the IoT and examines the integration of zero trust security principles into IoT authentication frameworks. We will discuss how a robust security paradigm can be employed to mitigate cyber threats and enhance IoT ecosystems. By thoroughly examining recent research, case studies, and real-world implementations, this study also provides significant insights into the evolution of IoT security and authentication.

The organization of this study is as follows: Section II delves into new authentication methods designed for the IoT, focusing on their integration with zero trust security and providing a comprehensive overview of how authentication is evolving in IoT settings. In Section III, we will examine implementation challenges, security issues, and real-world deployment scenarios to help inform decisions and promote the adoption of reliable and secure IoT authentication solutions.

Section IV outlines future research directions, aiming to contribute to the ongoing discourse on enhancing the security posture and resilience of IoT systems.

2. Emerging Authentication Technologies for Zero Trust on the IoT

Zero trust is an emerging cybersecurity concept that adheres to the principle of "never trust, always verify." It mandates continuous identification and validation of access authorization, treating all users, devices, and networks as potentially compromised, as elaborated in [2,8]. The core principles of zero trust can be summarized as follows:

1) Every data source and computing service is regarded as a corporate asset that requires protection.

2) All communications are considered insecure, regardless of the network location specified in the access request. No entity seeking access is automatically trusted.

3) Resource access is granted on a session-by-session basis.

4) Device characteristics, along with behavioral and environmental factors, are considered in access decisions.

5) The principle of least privilege is applied.

6) Access is granted intermittently, not automatically.

7) Enhancements to security in communications, network infrastructure, and assets are continuously applied.

Thus, zero trust integrates the highest level of security into devices and assets, protecting against external threats. The elements of authentication offer enhanced security for data and resources against intrusions; access segmentation prevents malware and attackers; and DDoS attacks are thwarted before they can damage resources. This approach allows for more granular access control; suspicious activity and attacks can be identified and mitigated more swiftly. Furthermore, traditional authentication methods in IoT ecosystems are now being reevaluated for the integration of authentication technologies with zero trust security in the IoT:

1) Resource Restrictions enable the implementation of sophisticated authentication techniques and cryptography in IoT devices, which are often constrained by memory and energy capacities. Conventional authentication methods may impose a large overhead, potentially affecting the performance and battery life of these resource-limited devices. A significant portion of the IoT ecosystem is composed of devices with limited processing and memory capacities, complicating the implementation of secure authentication. The impracticality of traditional cryptographic protocols, which are often computationally expensive, further hampers secure authentication in these devices. This is similar to [9], which highlighted device-to-device (D2D) authentication as more feasible compared to user authentication methods, considering the memory and processing capacity limitations of deployed IoT devices. These devices often focus on authentication systems that are computationally impractical for certain usage scenarios. Additionally, [10] underscored the critical importance of resource security in cloud networks and examined the roles of authentication and access control within zero trust architectures. When applying distinct guidelines and standardized techniques to enforce access restrictions across a distributed network, the reliability of requests must be based on historical data. This involves establishing servers in the restricted visibility buffer zone as the outer layer of the primary network.

2) "Heterogeneous" refers to a variety of devices, ranging from low-power IoT sensors to high-performance servers and gateways. Although unique requirements have been developed for the integration and compatibility of authentication, the heterogeneity in communications, software, and hardware makes it much more severe. The heterogeneity of IoT devices ranges from robust smart appliances to sensor nodes with limited computing capabilities. Due to the varied nature of this environment, different computational budgets and security requirements cannot be met by a single authentication method as presented in [11] , who discussed the level of granularity and complexity of the ZTA in an end-to-end infrastructure, security controls, heterogeneity, and legacy issues. The technology's ability to promote unity and safeguard digital identities across numerous platforms and networks was also discussed in [12], including the use of blockchain technology and the issue of heterogeneous identity trust.

3) Scalability refers to the ability to manage the login credentials of connected devices created by IoT deployments. Authentication technology often relies on centralized systems or physical provisioning processes due to the exponential growth in the number of devices, as in [13]. As they highlighted, this ensures that telemetry data, control directives, and sensitive information are protected from unauthorized access or alteration. Furthermore, certificate-based authentication enables scalable and manageable authentication for large-scale drone deployments. Potential attacks on the scheme's security services were suggested by [14], who also examined both official and informal defenses against these threats. The Hypertext Transfer Protocol (HTTP) with internal authentication measures was identified, highlighting the protocol's high load, limited capacity for storing requests on devices with constrained resources, and scalability challenges in the IoT.

4) IoT devices are often placed in open or uncontrolled environments facing issues such as safe update mechanisms and physical accessibility. If an attacker gains physical access to a device, the authentication, which relies on stored credentials, is compromised. It may be necessary to update authentication systems to maintain security and respond to breaches. Devices are vulnerable to hacking due to manufacturer pre-configured passwords or credentials. Conventional methods lack dynamic credential management and secure key rotation across many devices. Unfortunately, as shown in [15] , several trusted and up-to-date IoT devices still use outdated login credentials. Zanasi et al. [15] unveiled a security architecture designed to meet the stringent specifications of IIoT systems, incorporating a software-defined network (SDN) and a centralized security management layer, which can be integrated publicly via the Internet to facilitate the initial enrollment process for new resources.

5) Since IoT devices typically lack traditional user interfaces, it may be necessary to establish authentication methods for interaction with humans. As demonstrated in [16], these methods can operate without explicit user input. The trust algorithm used in this process makes decisions based on input from a policy database, user roles, and behavioral data. Another implementation is the integration of IoT devices in healthcare applications, as seen in [17]. In healthcare IoT systems, anticipatory risk mitigation and adaptive responses based on real-time data trends are crucial for identifying security measures and implementing proactive security. Additionally, risk assessments, user behavior, and access patterns are considered when tailoring security measures. Similarly, Butpheng et al. [18] integrated IoT technology into an e-health system to provide real-time, on-demand services. Network-connected devices communicate and share data through a unique user interface that collects information from sensors and equipment on the network. Saravanan et al. [19] developed and implemented a zero-trust framework paradigm that combines behavioral analysis, device health assessment, and multi-factor authentication (MFA) with user identity verification. Users must authenticate using credentials, such as their username and password, for their identity to be verified.

6) IoT devices often use wireless networks for communication, making authentication techniques vulnerable to eavesdropping and man-in-the-middle attacks, among other threats. Ensuring the authenticity and security of authentication is challenging. To demonstrate zero trust security in IoT networks, Nawshin et al. [20] introduced AI-enabled Android malware detection, requiring apps to be validated and authorized before being distributed to networks. They also stated that identity verification is necessary for all communication networks, whether internal or external to network perimeters, in line with the zero-trust security concept.

7) In IoT environments, where devices may operate autonomously and generate vast amounts of data, the lack of accountability and auditability in authentication methods makes it difficult to track and investigate security or unauthorized access. Security struggles to provide real-time visibility into devices and access, as well as granular control. Identifying and addressing potential security issues is challenging due to this lack of detailed oversight. Additionally, [21] explored the role of trust, detailing trust algorithms. The method included certification, competency testing, and ensuring appropriate collaboration and accountability.

8) Zero Trust is an advanced form of network security that can be swiftly implemented to handle distrust. It requires requests, evaluations, and approvals each time to safeguard resources, as

described in [8]. According to [22] , the zero trust security concept asserts that no implicit trust is placed in any network asset or user account; access to resources is only granted after a thorough authentication and authorization process has verified the identity of the user, device, asset, and workload. Similarly, [23] , based on the principle of "Never Trust, Always Verify," aims to defend the modern environment and facilitate digital transformation by utilizing robust authentication methods, employing network segmentation, preventing threats, and streamlining granular policy. It represents a comprehensive approach to information security that does not trust any user, transaction, or network traffic unless it has been validated.

Additionally, the importance of security measures is increasing with the use of IoT devices, networks, and authentication methods. It is crucial to recognize and address the inadequacies of authentication techniques, as outlined below:

1) Vulnerabilities: Passwords are the primary means for confirming user identities and granting access to IoT devices under authentication methods. Alquwayzani et al. [13] listed seven criteria for evaluating zero trust: vulnerability, access control, security defects, network security, password detection, high-risk ports, and secured sensitive data. Moreover, IoT devices are particularly vulnerable to hacking and unauthorized access, as demonstrated in [3].

2) Multi-factor Authentication (MFA): MFA is a security feature for IoT devices and applications that combines several factors, such as passwords, biometrics, and token keys, to verify user identity before granting access to IoT resources. MFA-authorized solutions require an additional device and a high level of user involvement, as seen in [19]. Additionally, [24] examined various MFA models in the context of the Industrial Internet of Things (IIoT), which necessitate strong identity verification for users and devices accessing IIoT resources. Methods used included strong authentication techniques, biometric authentication, digital certificates, and secure device attestation to verify the security and integrity of network connections.

3) Blockchain Technology: Currently immature for use due to its reliance on a consensus mechanism to generate identities and manage access control for all IoT devices, as presented in [1]. Furthermore, Rivera et al. [25] introduced distributed authentication as a network of authenticators to enhance the process's reliability, integrating blockchain to mitigate single points of failure and centralized servers for authentication.

4) Device Capabilities: The authentication systems manage a multitude of IoT devices with diverse identities and access requirements. Centralized management solutions can result in identity granularity issues, discrepancies, threat detection challenges, and potential security vulnerabilities, as demonstrated in [9].

5) User Authorization and Access Control: Unauthorized users may gain advanced access to data and control devices in IoT environments due to the absence of fine-grained access restrictions and pre-established policies. IoT ecosystems face the risk of device breaches, unauthorized privilege escalation, and data manipulation. Moreover, issues such as access control, confidentiality, privacy, and security, along with protection limitations and device reliability in utilizing IoT authentication services, were also addressed in [26]. Additionally, Dhiman et al. [10] provided methods for biometric authentication that capitalize on the durability and uniqueness of physiological traits to verify user identities.

6) Predisposition Attacks and Spoofing: The authentication protocols used in the IoT aim to prevent predisposition attacks. IoT devices may be vulnerable to identity spoofing attacks, where malicious actors mimic authentic devices to deceive authentication systems and infiltrate the network, compromising the data confidentiality of resources, as used in [11].

As mentioned above, the emerging authentication technologies with zero trust security address these challenges and provide secure and reliable authentication for IoT environments. By utilizing authentication technologies such as blockchain, AI-driven anomaly detection, and continuous verification, security in IoT environments can be improved, and risks related to authentication vulnerabilities can be reduced. In the next part, we will explore new authentication mechanisms in the context of the IoT and zero trust security, along with the cybersecurity of networked IoT. As shown in Figure 1., we categorize the essential elements of authentication technologies for zero trust in the IoT environment.

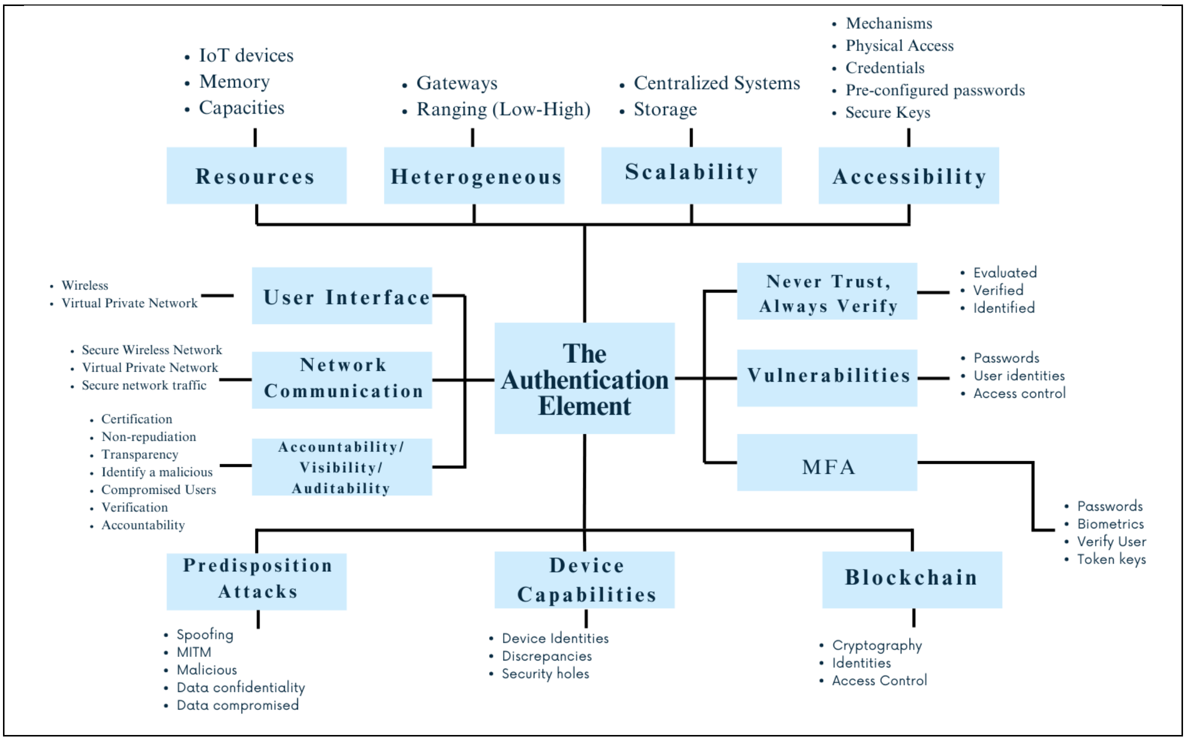

Figure 1. The essential elements of authentication technologies for zero trust in IoT environment.

Despite the detailed "never trust, always verify" principle of zero trust security, it necessitates robust authentication to secure communication and access control in constrained IoT environments. We summarize the contributors to various emerging authentication technologies for zero trust in the IoT, along with their challenges, as shown in Table 1.

Table 1. Summary of existing authentication technologies for IoT with zero trust.

Author(s)	Implementation	Authentication Technology	Advantages/ Challenges
[3] (2023)	Using factors as PIN password, verification, facial recognition.	Biometric Authentication	• Strong authentication based on unique biological or behavioral traits.
[9] (2021)	Identifying device fingerprints authentication for users and providing entry-point security, identity the subject, and accessing the device.		• Enhances user for memorizing passwords or token. • Potential privacy concerns.
[26] (2019)	Specifying biometric scanner collects unique biological data from users and matches the stored data.		• Increasing device costs.
[5] (2020)	Using for verification and calculating the discrete algorithm problem.	Cryptographic Authentication	• Offers mathematically security. • Supports secure key exchange.
[10] (2024)	Taking uniqueness and persistence of physiological characteristics and user identity.		• Non-repudiation, data integrity, and cryptographic primitives.

Author(s)	Implementation	Authentication Technology	Advantages/ Challenges
[21] (2022)	Protecting the system by manufacturers.		• Computationally intensive for constrained IoT devices. • Requires secure communication channels for key exchange.
[25] (2023)	Securing protocols for data storage and transmission and using to the confidentiality, integrity, and availability.		
[26] (2019)	Using to morph actual messages during communication in an insecure network.		
[27] (2023)	Offering higher confidence over authenticator and verifying an authentication key.		
[28] (2019)	Using as a key requirement within the scheme to fulfil the cryptographic checksum needed.		
[6] (2024)	Ensuring only authorized users, devices, and applications can access networks.	Federated Identity and Access Management (FIdAM)	• Enables seamless authentication across multiple IoT. • Reduce complexity • Supports various authentication methods. • Required trust establishment.
[11] (2023)	Providing the requested security services, access control, and management of configuration updates.		
[29] (2023)	Adding security for all resource authentication and authorization and strictly enforced.		
Author(s)	**Implementation**	**Authentication Technology**	**Advantages/ Challenges**
[1] (2020)	Proposing an anonymous access system and computing the divided identity block data.	Blockchain-based Authentication	• Provide a decentralized. • Enables secure and editable identity management. • Supports distributed trust. • Scalability limitations. • Requires design and implementation to ensure privacy and security.
[10] (2024)	Presenting blockchain technology for zero trust networks and comparing techniques used by different platforms. Presenting a possible approach for trusted transactions.		
[11] (2023)	Securing data storage, sensitive data and distributing data across multiple nodes.		
[25] (2024)	Protecting sensitive information and combining blockchain and trust assessment.		

Author(s)	Implementation	Authentication Technology	Advantages/ Challenges
[27] (2023)	Presenting blockchain technology with zero trust.		
[28] (2019)	Presenting the potential to increase privacy and security in blockchain applications.		
[9] (2021)	Designing characteristics that are used in one piece of hardware.	PUFs, or physically unclonable functions	• Unique physical properties. • Offers tamper resistance and counterfeiting capacities.
[20] (2024)	Linking between malware on Android devices and zero trust security.		

As shown in Table 1., and Figure 2., the FIdAM provides security access control. Emerging authentication technologies in IoT environments offer numerous benefits and trade-offs. The concepts of trust and interference resistance are enhanced by PUFs, blockchain technology, and authentication protocols. Consequently, the selection of an authentication combination will depend on specific components, feature requirements, limitations, and threat models. Therefore, robust authentication in an IoT environment should consider the device's capabilities, scalability, and security. These synthesized ideas could improve the effectiveness of blockchain technology in IoT environments.

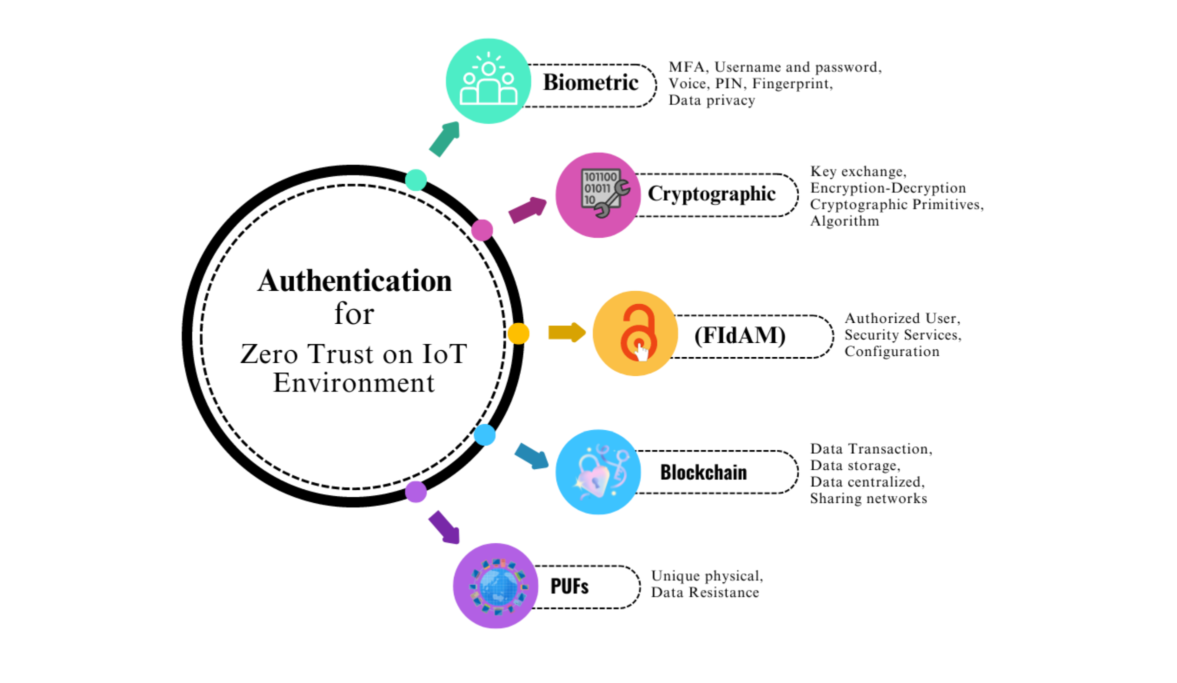
Authentication for Zero Trust on IoT Environment
Biometric
MFA, Username and password, Voice, PIN, Fingerprint, Data privacy
Cryptographic
101100 01011 10
Key exchange, Encryption-Decryption Cryptographic Primitives, Algorithm
(FIdAM)
Authorized User, Security Services, Configuration
Blockchain
Data Transaction, Data storage, Data centralized, Sharing networks
PUFs
Unique physical, Data Resistance

Figure 2. Authentication for Zero Trust in the IoT Environment.

The robust authentication methods align well with zero trust security principles. Figure 3. illustrates key considerations for developing and implementing secure authentication solutions in an IoT environment. This framework offers a roadmap for integrating emerging authentication techniques with zero trust security to establish robust protection across IoT layers. It ensures the reliable operation of interconnected IoT devices through mutual device authentication and confidential network communications. The framework encompasses user authenticity checks to ensure that only authorized devices can access networks and employs encryption to secure service access while protecting against various attacks, such as DoS attacks, MITM attacks, and sniffing attacks.

The safeguarding of user authentication data is vital for protecting the user's identity. Counterfeit attempts can lead to identity theft, spoof attacks, or situations where an attacker uses a counterfeit biometric to mimic a genuine user and gain unauthorized access. The framework advocates for user context recognition based on zero trust, fine-grained data access authentication control, and comprehensive monitoring of network traffic to identify and prevent potentially dangerous data access. It calls for regular reviews and updates to adapt to emerging threats and evolving requirements.

Moreover, it emphasizes adopting a zero-trust strategy that involves rigorous user verification and authentication, inherently distrusting any user, and assigning minimal access privileges to each user. To ensure access control security, it integrates continuous identity authentication and multifactor authentication. Biometric data, such as fingerprints and voiceprints, are collected by sensors via IoT devices and retained within edge devices, reducing the risk of data interception by attackers during network transmission.

This framework provides a structured approach to deploying emerging authentication technologies in an IoT environment guided by zero trust security principles. It emphasizes asset identification, risk assessment, technology selection, secure communication, continuous monitoring, incident response, secure updates, compliance, and continuous improvement. By adhering to this framework, organizations can enhance the security posture of their IoT ecosystems, mitigate risks associated with authentication challenges, and align with the core principles of zero trust security.

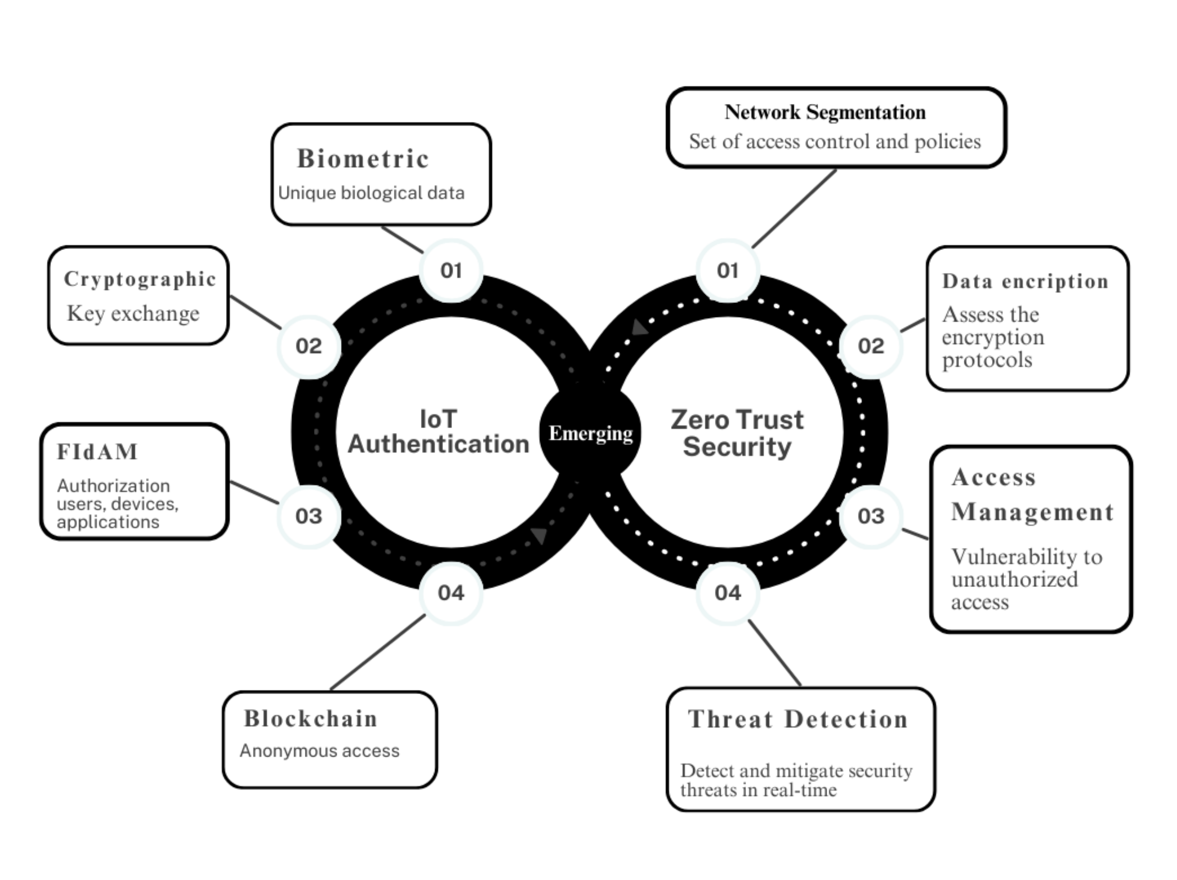

Figure 3. Key Considerations of Authentication for Zero Trust in the IoT Environment.

These emerging authentication techniques are integrated with the core principles of zero trust security in the IoT environment. By combining effective authentication with access control, risks associated with unauthorized access and malicious activities can be mitigated. Zero trust security provides a robust approach to securing communication and access control in the resource-constrained world of IoT devices. Next, we will explore the evaluation and implementation considerations for deploying zero trust security in IoT environments.

3. The Performance Evaluation Criteria for Authentication Zero Trust in the IoT

This section may be divided by subheadings. It should provide a concise and precise description of the experimental results, their interpretation, as well as the experimental

The "never trust, always verify" philosophy is personified in zero trust security, which addresses the lack of trustworthiness and enduring evaluation. Communication security and access control in IoT environments require securing authentication, which is a required strategy. Thus, zero trust security and emerging authentication are essential elements of the IoT ecosystem's security. Next, we may sum up the category of exiting authentication technology and performance evaluation as indicated in Table 2. Correspondingly, Yeoh et al. [30] introduced multifactor authentication, which can safeguard applications by confirming identity and validity prior to granting access, and others as follows:

Table 2. The category of exiting authentication technology and performance evaluation.

Feature	Mutual Authentication	Cryptographic Authentication	Multi-Factor Authentication (MFA)	Blockchain-based Authentication	Ref.
Security	High	Moderate	High	High	[25,30,31]
Processing	Low, Moderate	Low	Low, Moderate	Moderate, High	[32,33]
Scalability	Moderate	High	High	Scalability limitations	[28,29,34,35]
Resource	Moderate	Low	Low, Moderate	Moderate, High	[30,36]
Complexity	Moderate	Low	Moderate	High	[21,29,34]
Suitability	Moderate	High	Moderate	Limited	[2,28,31,37]

The authentication technology provides robust security by verifying devices, managing keys such as token keys, and creating digital certificates that can be scaled significantly. However, cryptography might not offer the same level of security in resource-constrained IoT devices. Nevertheless, MFA can enhance security by combining user verification with rigorous security checks. Blockchain technology provides robust mechanisms for identity verification and access control policies, though its implementation can be complex and challenging due to limited scalability on a large scale.

Complementing risk assessments with zero trust security for analysis and evaluation to find potential security and weaknesses in IoT environments. Likewise, evaluate the potential of the identified threats by using threat modeling to identify critical assets such as IoT devices, authentication, unauthorized access, and denial-of-service attacks. The progression of the system's ability to identify security is guided by the principle of zero trust security. Previously, continuous improvement in threat detection enhanced overall security and potential risks effectively. Nevertheless, cryptographic methods and blockchain authentication are adolescent for using a consensus mechanism, making them less attractive than centralized systems. The evaluation techniques should be considered several factors that we can conclude such as 1) security requirements: the security needed protection and reserved data, 2) device capabilities: processing, memory constraints, devices, 3) scalability: as long as a number of devices and the anticipated growth of IoT devices exist; 4) management: managing credentials with unique techniques; and 5) privacy concerns: sort of user privacy, data collection, and storage requirements. Additionally, [33] tested and simulated zero trust and perimeter-based IoT security systems. By applying a modeling and simulation tool to evaluate the effects of the zero-trust policy decision point (PDP) and policy enforcement point (PEP) functions on the overall networks, improved cybersecurity is the result of zero trust and security on networks.

The evaluation of emerging authentication zero trust security on IoT has different emerging authentications such as authentication, multifactor authentication, and blockchain authentication based on security features as presented in Table 3. At that point, consider the specific requirements of the IoT environment, such as low battery life, resource constraints, and selecting suitable devices. Consequently, the testing of proof-of-concept is necessary to assess the performance and security effectiveness of authentication in a controlled environment. As presented by [19], Saravanan et al. presented a measure and analyzed the authentication process in enforcing stringent access control with user identity verification and integration of MFA.

Table 3. The evaluation benefit of emerging authentication.

Evaluation Features	Benefits	Ref.
IoT Device Identification	• Identify all IoT devices connected to the networks. • Vulnerabilities security.	[5,24,32,38]
Network Segmentation	• Analyze network segmentation.	[7,10,39]
Access Management	• Determine authentication methods. • Vulnerability to unauthorized access.	[11,29]
Data Encryption	• Assess the encryption protocols. • Use data transmission within IoT environment.	[5,14]
Threat Detection	• Evaluate mechanisms and analyze effectiveness.	[20,30]
Penetration Testing	• Conduct hacking and simulated attacks to assess the authentication mechanisms. • Test against various attacks (spoofing, man in the middle). • Identify and exploit potential vulnerabilities.	[2,10,29,31,40,41]
Formal Verification	• Use techniques and mathematical models to confirm the security characteristics of cryptography and authentication. • Ensure established security guarantees.	[5,12,39]
Simulation and emulation	• Simulate the IoT and authentication to evaluate performance and scalability. • Identify resource constraints and interoperability.	[29,33]
Compliance Testing	• Assess authenticity to security standards. • Ensure compliance with legal data protection and data privacy.	[10,23,27]

These assessments of developing authentication methods, which can be successfully applied in IoT environments while adhering to zero trust security principles, encompass security analysis and evaluation. This method ensures authentication, risk mitigation, confidentiality, integrity, and availability. Zero trust security can be tailored and integrated with authentication to specify access control, user identity, and verification requirements within the IoT environment. Implementing zero trust authentication for IoT involves careful planning and consideration, including:

1) Uniformity: Establish newly developed authentication protocols.
2) Provisioning Devices: Distribute credential keys.
3) Monitoring: Identify inconsistencies and categorize threats.
4) Automatic: Utilize pre-established security measures.
5) Control and Management Access: Oversee and regulate access.

6) Cryptography: Explore cryptographic algorithms to provide sustained security.

7) User Experience: Enhance acceptability and usability.

The comprehensive implementation of zero trust security can effectively mitigate cybersecurity risks and enhance data protection, including ensuring the integrity of the IoT environment. As illustrated in Table 4, we present a comparison of the evaluation and implementation of Zero Trust in the IoT environment. The methods involve collaboration between IoT devices, communication networks, zero trust security, and others to ensure a comprehensive and effective zero trust security strategy for IoT environments. This includes:

1) Establishing strict access control for IoT devices, users, and applications.

2) Implementing network segmentation strategies to isolate IoT devices within networks.

3) Utilizing threat detection systems to identify potential incidents in real-time.

4) Applying data encryption to secure communication protocols for data transmission between IoT devices and authentication elements.

5) Integrating IoT security into the existing zero trust security framework and principles.

Table 4. Comparison of the evaluation and implementation of Zero Trust in the IoT environment.

Evaluation/ implementation	[11]	[12]	[15]	[20]	[24]	[34]	[36]	[38]	[42]	[43]	[44]
Stringent access controls	×	×	×	✓	✓	×	×	✓	✓	✓	×
Micro-segmentation strategies	✓	×	✓	×	✓	×	✓	✓	✓	×	✓
Threat detection systems	✓	✓	✓	✓	✓	✓	✓	✓	×	×	✓
Data Encryption	×	✓	✓	✓	✓	×	×	✓	×	×	×
Zero Trust policies across the IoT environment	×	×	×	×	×	×	✓	×	✓	×	✓
Integrating IoT security	×	✓	×	✓	✓	×	✓	✓	×	×	×
Developing IoT environments under Zero Trust principles	✓	×	✓	✓	×	×	×	✓	×	✓	✓

The evaluation and implementation of zero trust security in IoT environments entail assessing the appropriateness and practicability of protecting IoT devices and deploying the necessary techniques, security models, and mechanisms to enforce Zero Trust principles. These evaluations are critical for the successful implementation of zero trust security in IoT settings. By considering security requirements, device capabilities, and potential challenges, we can select the most suitable authentication technology and establish robust security measures.

4. Future Direction and Suggestions

New authentication systems provide ways to improve IoT environments' zero trust security. presented an efficient and safe authentication and key agreement (AKA) system, examined its performance, and contrasted it with alternative protocols [45]. They suggested improved security for smart devices is anticipated as IoT development progresses. In summary, the idea, tenets, and cutting-edge developments of zero trust in cybersecurity and important IoT contexts were put forth by [46]. It has been noted that the application of zero trust in the Internet of Things will incorporate both theoretical ideas to guarantee data privacy and security, averting unlawful access and data leakage. Similarity: Zero trust architecture is significant for fusion if it demonstrates a remarkable balance between strict security and user-friendliness, as suggested by [47]. Additionally, Chen et al. [48] presented the evaluating cross-chain trust, a software-defined zero trust architecture was created for the developing security 6G networks, allowing cooperative defense against network threats. Wu et al. [49] analyzed the key connotation of zero trust and IoT security and evaluated and simulated the stochastic Petri net, the model can effectively address network security problems. However, adoption and implementation will require consideration of factors such as scalability, interoperability, performance evaluation, and the specific requirements and constraints of IoT devices and systems. By exploring in this research, the future directions and adopting innovative authentication technologies that can strengthen security, manage risk, and ensure the trustworthiness of IoT environments within a zero-trust principle and zero trust policy, continuous research, development, and collaboration will be critical to addressing emerging threats and challenges in the evolving landscape of IoT security.

As shown in Table 5, there are various future directions and suggestions for emerging authentication technologies in zero trust and the IoT environment. For instance, behavioral biometrics utilize keystroke dynamics and voice recognition to authenticate users based on their behavioral patterns. Secure Multi-Party Computation (SMPC) and homomorphic encryption are used to ensure authentication and data processing in the IoT environment. This technology enables the secure computation and processing of encrypted data without decryption. Quantum-resistant cryptography is a proactive approach to cryptographic algorithms and protocols for authentication and secure communication in IoT environments and long-term security against potential threats from quantum computing. Lastly, collaboration and standardization are needed to develop the standardized authentication protocols and best practices for zero trust security, zero trust principles, and zero trust policies in IoT ecosystems. Interoperability in authentication is essential for seamless integration and security.

Table 5. Future directions for authentication with zero trust in the IoT environment.

Future Directions	Suggestions
Continuous Adaptive Risk and Trust Assessment (CARTA)	CARTA frameworks are endlessly adapted based on context, behavior, and risk factors for IoT devices [50–54].
Blockchain-based Authentication	Develop blockchain technologies for decentralized, tamper-proof authentication and access control in IoT ecosystems. This technology addresses scalability limitations on a large scale [55,56].
Quantum-resistant cryptography	Investigate quantum-resistant cryptographic algorithms as the protocols to secure IoT authentication against and prepare for potential vulnerabilities from future quantum computing threats[57].
Federated Identity and Access Management (FedIAM)	Implement FedIAM solutions to enable secure and seamless authentication across multiple IoT service providers. This reference implements a standardized authentication protocol to facilitate it across IoT platforms[51,52].
Integration of AI and Machine Learning (ML)	Develop AI/ML techniques for real-time anomaly detection and adaptive authentication mechanisms in IoT environments. To analyze user and device patterns in real-time, dynamically adjust access control policies based on risk assessment[54,58].
Privacy-preserving Authentication	Explore authentication schemes that protect user privacy and sensitive data in the IoT environment.

Future Directions	Suggestions
	Develop for user control and usage associated with authentication[53,59].
Secure Firmware and Hardware Roots of Trust	Integrate secure hardware and trusted execution environments for IoT device authentication and integrity[60,61].
Future Directions	**Suggestions**
Standardization of Authentication Protocols for Interoperability	Participate in standards and ensure interoperability among different IoT authentication solutions. Develop open-source libraries and references for standardized authentication protocols[51,56].
User-centric Authentication for Improve Usability	Discover user-centric authentication, user preferences, user-friendly interfaces, and workflows such as biometrics and behavioral patterns for secure and convenient IoT access control in an IoT environment[52].
Emerging Technologies	Investigate the security implications of emerging technologies and networks on authentication processes within the IoT environment[57,59,62].

This table outlines future directions and suggestions for emerging authentication technologies, covering areas such as continuous trust assessment, decentralized authentication, quantum-resistant cryptography, federated identity management, machine learning, privacy techniques, lightweight protocols, trust security, theories, standardization, and user authentication methods. By following these guidelines, we can create a more secure and resilient framework for the interconnected IoT environment.

5. Conclusion

This study explores evolving authentication methods in the IoT through zero trust security. We have delved into emerging technologies such as cryptography and multi-factor authentication, highlighting their integration with zero trust principles. Our research has provided a comprehensive understanding of the transformative changes within IoT authentication, transitioning from perimeter-based models to a continuous verification approach that is better suited for the IoT environment. The study critically examines implementation challenges, security considerations, device limitations, potential privacy concerns, and deployment scenarios. Additionally, we have provided insights that can guide decision-making for the adoption of reliable and secure IoT authentication solutions. Recognizing the importance of enhanced IoT security, we have identified its contributions to robust security. This includes the efficient and scalable application of authentication technology, the adoption of standardized network protocols, and the exploration of cryptography for long-term security. In conclusion, by integrating emerging authentication methods with zero trust principles, we aim to move toward a more secure future, underscoring the importance of robust authentication capable of effectively addressing emerging threats and vulnerabilities. This study also offers a framework for understanding these advancements and promotes a more secure and trustworthy IoT environment in our increasingly connected world.

References

1. Dhar, Suparna; Indranil Bose. Securing IoT Devices Using Zero Trust and Blockchain. *Journal of Organizational Computing and Electronic Commerce* **2020**, *31*(1), p. 18-34.
2. Kummar, Puneet; Satis Jumar; Wasik Iqbal; Apurva Goyal. *Emerging Technology and Management Trends*. Gautam Vihar Delhi, Manglam, India, 2023, p. 98-124.
3. Chen, Zhigang; Yuting Jiang; Xinxia Song; Liqun Chen. A Survey on Zero-Knowledge Authentication for Internet of Things. *Electronics* **2023**, *12*(5), p. 1-20.
4. He, Yuanhang; Daochao Huang; Lei Chen; Yi Ni; Xiangjie Ma. A Survey on Zero Trust Architecture: Challenges and Future Trends. *Wireless Communications and Mobile Computing* **2022**, *1*, p. 1-13.
5. Soewito, Benfano; Yonathan Marcellinus. IoT security system with modified Zero Knowledge Proof algorithm for authentication. *Egyptian Informatics* **2020**, *22*(3), p. 269-276.
6. Patel, Rajesh; Klaus Muller; Giorgi Kvirkvelia; John Smith; Emily Wilson. Zero Trust Security Architecture Raises the Future Paradigm in Information Systems. *Informatica and Digital Insight* **2024**, *1*(1), p. 24-34.
7. Ahmadi, Sina. Zero Trust Architecture in Cloud Networks: Application, Challenges and Future Opportunities. *Journal of Engineering Research and Reports* **2024**, *26*(2), p. 215-228.
8. Buck, Christoph; Christian Olenberger; André Schweizer; Fabiane Völter; Torsten Eymann. Never trust, always verify: A multivocal literature review on current knowledge and research gaps of zero trust. *Computers & Security* **2021**, *110*, p. 1-26.
9. Shah, Syed W.; Naeem F. Syed; Arash Shaghaghi; Adnan Anwar; Zubair Baig; Robin Doss. LCDA: Lightweight Continuous Device-to-Device Authentication for a Zero Trust Architecture (ZTA). *Computers & Security* **2021**, *108*, p. 1-44.
10. Dhiman, Poonam; Neha Saini; Yonis Gulzar; Sherzod Turaev; Amandeep Kaur; Khair U. Nisa; Yasir Hamid. A Review and Comparative Analysis of Relevant Approaches of Zero Trust Network Model. *Sensors (Basel)* **2024**, *24*(4), p. 1-19.
11. Federici, Fabio; Davide Martintoni; Valerio Senni. A Zero trust Architecture for Remote Access in Industrial IoT Infrastructures. *Electronics* **2023**, *12*(3), p. 1-20.
12. Nita, Stefania Loredana; Marius Iulian Mihailescu. A Novel Authentication Scheme Based on Verifiable Credentials Using Digital Identity in the Context of Web 3.0. *Electronics* **2024**, *13*(6), p. 1-49.
13. Alquwayzani, Alanoud Abdullah; Abdullah Abdulrahman Albuali. A systematic Literature Review of Zero Trust Architecture for UAV Security Systems in IoBT. *Computer Scient and Mathematics* **2024**, *1*(1), p. 1-33.
14. Hasan, Mohammad Kamrul; Zhou Weichen; Nurhizam Safie; Fatima Rayan; Awad Ahmed; Taher M. Ghazal. A Survey on Key Agreement and Authentication Protocol for Internet of Things Application. *IEEE Access* **2024**, *12*, p. 61642-61666.
15. Zanasi, Claudio; Silvio Russo; Michele Colajanni. Flexible zero trust architecture for the cybersecurity of industrial IoT infrastructures. Ad Hoc *Networks* **2024**, *156*, p. 1-15.
16. Syed, Naeem Firdous; Syed W. Shah; Arash Shaghaghi; Adnan Anwar; Zubair Baig; Robin Doss. Zero Trust Architecture (ZTA): A Comprehensive Survey. *IEEE Access* **2022**, *10*, p. 57143-57179.
17. Elsayed, Zag; Nelly Elasyed; Sajjad Bay. A Novel Zero Trust Machine Learning Green Architecture for Healthcare IoT Cybersecurity: Review. Analysis and Implementation in Southeast Conference 2024, Atlanta, GA, USA, (May 18 - May 22, 2024).
18. Butpheng, Chanapha; Kuo-Hui Yeh; Jia-Li Hou; Azees M. A Secure IoT and Cloud Computing-Enabled e-Health Management System. *Security and Communication Networks* **2022**, *2022*, p. 1-14.
19. Saravanan, K., R.; Anitha, P. Kamarajapandian; Thomas Paul Roy Arockiadoss; K. Sambath Kumar; R. Hariharan. Design and Elevating Cloud Security Through a Comprehensive Integration of Zero Trust Framework. *Intelligent systems and application in engineering* **2024**, *12*, p. 214-219.
20. Nawshin, Faria; Devrim Unal; Mohammad Hammoudeh; Ponnuthurai N. Suganthan. AI-powered malware detection with Differential Privacy for zero trust security in Internet of Things networks. Ad Hoc *Networks* **2024**, *1*, p. 161-178.
21. Neale, Christopher; Ian Kennedy; Blaine Price; Yijun Yu; Bashar Nuseibeh. The case for Zero Trust Digital Forensics. *Forensic Science International: Digital Investigation* **2022**, *40*, p. 1-13.
22. Liu, Chunwen; Ru Tan; Yang Wu; Yun Feng; Ze Jin, Fangjiao Zhang; Yuling Liu; Qixu Liu. Dissecting zero trust: research landscape and its implementation in IoT. *Cybersecurity* **2024**, *7*(20), p. 1-28.
23. Raheman, Fazal. From Standard Policy-Based Zero Trust to Absolute Zero Trust (AZT): A Quantum Leap to Q-Day Security. *Journal of Computer and Communications* **2024**, *12*(03), p. 252-282.
24. Cena, Joshua. Multi-Factor Authentication Paradigms for Securing Industrial Internet of Things (IIoT) Assets, in Electrical Energy and Power Systems Group (EEPS), Doctoral Degree, 2024, The University of Manchester: Manchester, Lancashire, United Kingdom. p. 12.
25. Rivera, Javier Jose Diaz; Afaq Muhammad; Wang-Cheol Song. Securing Digital Identity in the Zero Trust Architecture: A Blockchain Approach to Privacy-Focused Multi-Factor Authentication. *IEEE Open Journal of the Communications Society* **2024**, *5*, p. 2792-2814.

26. Nandy, Tarak; Mohd Yamani Idna Bin Idris; Rafidah Md Noor; Laiha Mat Kiah; Lau Sian Lun; Nor Badrul Annuar Juma'at; Ismail Ahmedy; Norjihan Abdul Ghani; Sananda Bhattacharyya. Review on Security of Internet of Things Authentication Mechanism. *IEEE Access* **2019**, *7*, p. 151054-151089.
27. Kawalkar, Sachin A.; Dinesh B. Bhoyar. Design of an Efficient Cloud Security Model through Federated Learning, Blockchain, AI-Driven Policies, and Zero Trust Frameworks. *Intelligent systems and application in engineering* **2023**, *12*(10), p. 378-388.
28. Walshe, Marcus; Gregory Epiphaniou; Haider Al-Khateeb; Mohammad Hammoudeh; Vasilios Katos; Ali Dehghantanha. Non-interactive zero knowledge proofs for the authentication of IoT devices in reduced connectivity environments. Ad Hoc *Networks* **2019**, *95*, p. 1-12.
29. Ali, Belal Ebrahim Mohamed Alshiec. Efficient Trust-Aware Authentication and Task Offloading in Multi-Access Edge Computing Using a Dual Fuzzy Method based Zero Trust Security Framework, Doctoral Degree, College of Science, Technology, Engineering and Maths. 2023, Royal Melbourne Institute of Technology: Royal Melbourne Institute of Technology, Australia.
30. Yeoh, William; Marina Liu, Malcolm Shore; Frank Jiang. Zero trust cybersecurity: Critical success factors and A maturity assessment framework. *Computers & Security* **2023**, *133*, p. 1-13.
31. Singhal, Nikita; Deepak Tyagi. Cybersecurity in the Era of Emerging Technology, in Emerging Technology and Management Trends, P. Kumar, et al., Editors. 2023, Manglam: K-129, Gali Pusta, Shiv Om Jewellers, Gautam Vihar Delhi, India, p. 98-124.
32. Kim, Hokeun; Edward A. Lee. Authentication and Authorization for the Internet of Things. *IEEE Computer Society* **2017**, p. 27-33.
33. Capili, Mirene. Simulation-Based Evaluation of Perimeter-Based and Zero Trust Security Implementation on Internet of Things, in Systems Engineering. Doctoral Degree, 2024, The George Washington University: The school of Engineering and Applied Science of The George Washington University, p. 1-24.
34. Cambou, Bertrand; Christopher Philabaum; Jeffrey Hoffstein; Maurice Herlihy. Methods to Encrypt and Authenticate Digital Files in Distributed Networks and Zero trust Environments. *Axioms* **2023**, *12*(531), p. 1-23.
35. Mehraj, Saima; M. Tariq Banday. Establishing a Zero Trust Strategy in Cloud Computing Environment, International Conference on Computer Communication and Informatics (ICCCI-2020), University of Exeter: Coimbatore, India, 22-24 January 2020, p. 1-6.
36. Zhang, Han; Ziyan Zhang; Liquan Chen. Toward zero trust in 5G industrial internet collaboration systems. *Digital Communications and Networks* **2024**, *1*, p. 2022-3357.
37. Olaoye, Godwin Oluwafemi; Ayuns Luz. Future trends and emerging technologies in cloud security,Telecommunication Engineering Centre. Doctoral Degree, 2024, Ladoke Akintola University of Technology: Ladoke Akintola University of Technology, India. p. 1-24.
38. Cena, Joshua. Zero trust Architecture for Robust IIoT Security, in Electrical Energy and Power Systems Group (EEPS). Doctoreal Degree, 2024, The University of Manchester: The University of Manchester.
39. Adhikari, Tapomoy. Advancing Zero Trust Network Authentication: Innovations in Privacy-Preserving Authentication Mechanisms. *Computer Science and Engineering* **2024**, *1*(1), p. 1-22.
40. Chuan, Tao; Yao Lv, Zhenfei Qi; Linjiang Xie; Wei Guo. An Implementation Method of Zero trust Architecture. *Journal of Physics: Conference Series* **2020**, *1651*(1), p. 1-7.
41. Bhattacharya, Saurav; Sriram Panyam; Gaurav Deshmukh; Sudha Gatala; Vamsi Vemoori; Dhruv Seth. Integrating User Experience and Acceptance in Authentication: A Synthesis of Technology Acceptance Model and User-Centered Design Principles. *International Journal of Computer Trends and Technology* **2024**, *72*(4), p. 15-23.
42. Aki, Sai Ranga Subhash. Zero Trust Securityin Wireless and communication Networks. *Computer Security and Reliability* **2024**, *1*(1), p. 1-24.
43. Tang, Fei; Chunliang Ma; Kefei Cheng. Privacy-preserving authentication scheme based on zero trust architecture. *Digital Communications and Networks* **2023**, *23*, p. 1-15.
44. Xu, Mingyang; Junli Guo; Haoyu Yuan; Xinyu Yang. Zero trust Security Authentication Based on SPA and Endogenous Security Architecture. *Electronics* **2023**, *12*(782), p. 1-21.
45. Chen, Chien-Ming; Xuanang Li; Shuangshuang Liu; Mu-En Wu; Saru Kumari; Youwen Zhu. Enhanced Authentication Protocol for the Internet of Things Environment. *Security and Communication Networks* **2022**, *2022*, p. 1-13.
46. Kang, Hongzhaoning; Gang Liu; Quan Wang; Lei Meng; Jing Liu. Theory and Application of Zero Trust Security: A Brief Survey. *Entropy* **2023**, *25*(1595), p. 1-26.
47. Khan, Muhammad Jamshid. Zero trust architecture: Redefining network security paradigms in the digital age. *World Journal of Advanced Research and Reviews* **2023**, *19*(3), p. 105-116.
48. Chen, Xu; Wei Feng; Ning Ge; Yan Zhang. Zero_Trust_Architecture_for_6G_Security. *IEEE Network* **2023**, *1*(1), p. 1-8.

49. Wu, Kehe; Rui Cheng; Huiyan Xu; Jie Tong; Baseem Khan. Design and Implementation of the Zero Trust Model in the Power Internet of Things. *International Transactions on Electrical Energy Systems* **2023**, *2023*, p. 1-13.
50. Su, Runbo; Arbia Riahi; Enrico Natalizio; Pascal Moyal; Amaury Saint-Jore; Ye-Qiong Song. Assessing intra- and inter-community trustworthiness in IoT: A role-based attack-resilient dynamic trust management model. *Internet of Things* **2024**, 26, p. 1-21.
51. Azad, Muhammad Ajmal; Sidrah Abdullah; Junaid Arshad; Harjinder Lallie; Yussuf Hassan Ahmed. Verify and trust: A multidimensional survey of zero trust security in the age of IoT. *Internet of Things* **2024**, *27*, p. 1- 27.
52. Itodo, Cornelius; Murat Ozer. Multivocal literature review on zero trust security implementation. *Computers & Security* **2024,** *141*, p. 1-27.
53. Sumanprakash, P.; K. Seshadri Ramana; Renzon Daniel Cosmepecho; M. Janardhan; Meryelem Tania Churampi Arellano; J. Mahalakshmi; M. Bhavsingh; K. Samunnisa. Learning-driven Continuous Diagnostics and Mitigation program for secure edge management through Zero trust Architecture. *Computer Communications* **2024**, *220*, p. 94-107.
54. Zhang, Jingci; Jun Zheng; Zheng Zhang; Tian Chen; Yu-An Tan; Quanxin Zhang; Yuanzhang Li. ATT&CK-based Advanced Persistent Threat attacks risk propagation assessment model for zero trust networks. *Computer Networks* **2024**, *245*, p. 1-20.
55. Krishnan, Prabhakar; Kurunandan Jain; Shivananda R. Poojara; Satish Narayana Srirama; Tulika Pandey; Rajkumar Buyya. eSIM and blockchain integrated secure zero-touch provisioning for autonomous cellular-IoTs in 5G networks. *Computer Communications* **2024**, *216*, p. 324-345.
56. Mekala, Sri Harsha; Zubair Baig; Adnan Anwar; Sherali Zeadally. Cybersecurity for Industrial IoT (IIoT): Threats, countermeasures, challenges and future directions. *Computer Communications* **2023**, *208*, p. 294-320.
57. Kaur, Manpreet; Vinod Kumar Verma. Cooperative-centrality enabled investigations on edge-based trustworthy framework for cloud focused internet of things. *Journal of Network and Computer Applications* **2024**, *226*, p. 1-15.
58. Ni, Lina; Xu Gong, Jufeng Li; Yuncan Tang; Zhuang Luan; Jinquan Zhang. rFedFW: Secure and trustable aggregation scheme for Byzantine-robust federated learning in Internet of Things. *Information Sciences* **2024**, *653*, p. 1-20.
59. Cao, Yihao; Jianbiao Zhang; Yaru Zhao; Pengchong Su; Haoxiang Huang. SRFL: A Secure & Robust Federated Learning framework for IoT with trusted execution environments. *Expert Systems with Applications* **2024**, 239, p. 95-118.
60. Varela-Vaca, Ángel Jesús; Rafael M. Gasca; David Iglesias; J. M. Gónzalez-Gutiérrez, Automated trusted collaborative processes through blockchain & IoT integration: The fraud detection case. *Internet of Things* **2024**, 25, p. 1-25.
61. Arazzi, Marco; Serena Nicolazzo; Antonino Nocera. A novel IoT trust model leveraging fully distributed behavioral fingerprinting and secure delegation. *Pervasive and Mobile Computing* **2024**, *99*, p. 89-99.
62. Javeed, Danish; Muhammad Shahid Saeed; Muhammad Adil; Prabhat Kumar; Alireza Jolfaei. A federated learning-based zero trust intrusion detection system for Internet of Things. Ad Hoc *Networks* **2024**, *162*, p.150- 162.

Disclaimer/Publisher's Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.

Chanapha Bast graduated with a Ph.D. in Information Management from National Dong Hua University, Taiwan, in 2020. She earned her Master of Information Technology and Computer in 2007 from King Mongkut's University of Technology Thonburi in Bangkok, Thailand. Currently, she serves as a lecturer in the Business Computer Department at the Management Science Faculty of Udon Thani Rajabhat University, Thailand. Her primary research interests include IoT, security, privacy, cybersecurity, network security, and cloud computing. Additionally, she has conducted significant research in blockchain technology. Her contributions have been widely published in various peer-reviewed journals and conference proceedings, underscoring her expertise and commitment to advancing knowledge in these critical areas.

Kuo-Hui Yeh (SM’16) serves as a professor at the Institute of Artificial Intelligence Innovation, National Yang Ming Chiao Tung University, Hsinchu, Taiwan. Prior to this appointment, he was a professor in the Department of Information Management at National Dong Hwa University, Hualien, Taiwan, from February 2012 to January 2024. Dr. Yeh earned his M.S. and Ph.D. degrees in Information Management from the National Taiwan University of Science and Technology, Taipei, Taiwan, in 2005 and 2010, respectively. He has contributed over 150 articles to esteemed journals and conferences, covering a wide array of research interests such as IoT security, Blockchain, NFC/RFID security, authentication, digital signatures, data privacy and network security. Furthermore, Dr. Yeh plays a pivotal role in the academic community, serving as an Associate Editor (or Editorial Board Member) for several journals, including the Journal of Information Security and Applications (JISA), Human-centric Computing and Information Sciences (HCIS), Symmetry, Journal of Internet Technology (JIT) and CMC-Computers, Materials & Continua. In the professional realm, Dr. Yeh is recognized as a Senior Member of IEEE and holds memberships with (ISC)², ISA, ISACA, CAA, and CCISA. His professional qualifications include certifications like CISSP, CISM, Security+, ISO 27001/27701/42001 Lead Auditor, IEC 62443-2-1 Lead Auditor, and ISA/IEC 62443 Cybersecurity Expert, covering fundamentals, risk assessment, design, and maintenance specialties.