IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received 26 January 2024, accepted 11 April 2024, date of publication 25 April 2024, date of current version 7 May 2024.

Digital Object Identifier 10.1109/ACCESS.2024.3393567

SURVEY

A Survey on Key Agreement and Authentication Protocol for Internet of Things Application

MOHAMMAD KAMRUL HASAN[1], (Senior Member, IEEE), ZHOU WEICHEN[1], NURHIZAM SAFIE[2], (Associate Member, IEEE), FATIMA RAYAN AWAD AHMED[3], AND TAHER M. GHAZAL[1,4], (Senior Member, IEEE)

[1]Center for Cyber Security, Faculty of Information Science and Technology, Universiti Kebangsaan Malaysia (UKM), Bangi, Selangor 43600, Malaysia
[2]Center for Software Technology and Management, Faculty of Information Science and Technology, Universiti Kebangsaan Malaysia (UKM), Bangi, Selangor 43600, Malaysia
[3]Computer Science Department, College of Computer Engineering and Science, Prince Sattam Bin Abdulaziz University, Al-Kharj 16273, Saudi Arabia
[4]Centre for Cyber Physical Systems, Computer Science Department, Khalifa University, Abu Dhabi, United Arab Emirates

Corresponding authors: Mohammad Kamrul Hasan (hasankamrul@ieee.org) and Zhou Weichen (msjoycezhou@foxmail.com)

This work was supported by Universiti Kebangsaan Malaysia (UKM) under the Research Grant Scheme under Grant GUP 2023-010.

ABSTRACT The Internet of Things (IoT) represents a dynamic infrastructure, leveraging sensing and network communication technology to establish ubiquitous connectivity among people, machines, and objects. Due to its end devices' limited computing resources and storage space, it is not feasible to merely transpose traditional internet security technologies directly to IoT endpoints. Maintaining security while concurrently ensuring performance is a particularly challenging endeavor. This paper provides a review of key agreements and authentication protocols pivotal to the security of IoT. First, this survey discusses the applications that need authentication and key agreement to strengthen their security and current research on these application fields. Subsequently, this paper engages in an in-depth exploration of the phase involved in the scheme of authentication and key agreement, including an examination of the cryptographic techniques employed within these processes. This survey also thoroughly studies the scheme's security services, potential attacks, formal analysis and informal analysis to ensure resilience against such threats. This study aims to provide a profound understanding of the recent research on authentication and key agreement in IoT applications. It strives to contribute towards strengthening security systems for IoT applications, ensuring their sustainability in the face of evolving threats.

INDEX TERMS Cryptography, AKA protocol, Internet of Things, formal security analysis, security and privacy.

I. INTRODUCTION

Over the past several decades, the digital revolution has given rise to a transformative technological framework, the Internet of Things (IoT). This network of interconnected devices and systems facilitates effortless data exchange, marking a significant shift in the technological landscape [1]. The initial concept of IoT, introduced by Kevin Ashton in 1999, refers to a system where the Internet is connected to the physical world via ubiquitous sensors [2]. This idea has now grown beyond this initial concept, with the evolution of IoT being driven by technological advancements, shifting needs, and institutional impacts. IoT is characterized by its ability to generate, exchange, and consume data with minimal human intervention. Its concept becomes feasible due to a network of physical objects equipped with electronics, software, sensors, and wired or wireless network connectivity. The potential applications of IoT are vast, varied, and spanning multiple sectors. They include healthcare, smart-home environment, unmanned aerial vehicles, and manufacturing, among others. However, despite its significant benefits, the IoT presents various challenges, particularly regarding security. In order to ensure the legitimacy of each device, mutual authentication is a useful method to verify the identity of devices before them connect to the network [3]. Authentication acts as the first line of defense, protecting systems from unauthorized access

The associate editor coordinating the review of this manuscript and approving it for publication was Amir Masoud Rahmani.

TABLE 1. Comparison with existing surveys.

Paper	Attributes	-	Contributions
[47]	IoT layers, Attacks, Security features, Authentication mechanisms	-	Evaluated the authentication schemes based on different domains in IoT.
		-	Analyzed security features for authentication protocols.
[48]	Smart applications, Data Security, Attacks, Identity authentication, Edge computing	-	Described crypto-techniques, security analysis and performance for authentication based on edge-computing in smart applications.
[49]	Blockchain, Authentication mechanisms, Security requirements, Attacks, Countermeasures	-	Analyzed the security requirements, open issues and countermeasures when designing authentication scheme in IoT
[50]	Security requirements, Attacks, Countermeasures, Authentication mechanisms, Formal analysis	-	Presented different authentication scheme in IoT environment.
		-	Analyzed security threats, formal analysis and countermeasures.
[51]	Security Requirements, Attacks, Formal analysis, Crypto-techniques	-	Classified authentication schemes in wireless body area networks
		-	Analyzed tools and techniques used in authentication schemes.
		-	Analyzed security issues, adversary model and formal analysis.
[52]	IoT Architecture, Security challenges, authentication classification,	-	Discussed vulnerability based on IoT layers.
		-	Analyzed the security of authentication protocols based on classifications.
[53]	Certificate-less authentication schemes, Security issues, Crypto-techniques, authentication classification	-	Analyzed authentication mechanisms based on different classification of certificate-less authentication protocols.
Our Paper	AKA in different IoT applications, Authentication mechanisms, Crypto-techniques, IoT standards, Security services, Attacks, Formal analysis tools, Informal analysis and countermeasures	-	Authentication and key agreement schemes and security problems in different IoT applications.
		-	Phase of AKA protocols.
		-	Cryptography technology used in AKA protocols.
		-	Security services provided in AKA protocols.
		-	Potential attacks, formal analysis, informal analysis and countermeasures.

and providing a reliable foundation for subsequent stages of secure communication. Recent research has focused on developing advanced authentication mechanisms to address the security challenges of the IoT environment. State of the art for authentication in recent research includes but is not limited to:

Lightweight Authentication Protocols: Due to the limited resources of IoT devices, various fields such as medical IoT [4], [5], [6], 5G-enabled IoT [7], 6G-based cellular networks [8], and industrial IoT [9] need lightweight authentication and key agreement (AKA) protocols. Current AKA protocols provide lightweight authentication by minimizing the computational and communication overhead [10], [11], [12]. Key features of these protocols are lightweight cryptographic techniques, including hash function [13], [14], [15], symmetric encryption [16], elliptic curve cryptography (ECC) [17], and pre-shaded keys [18]. Despite their lightweight, these protocols ensure robust security [19], [20], [21].

Identity-based Authentication: Traditional certificate-based authentication is heavy in IoT scenarios for limited-resource IoT devices [22]. Identity-based authentication allows devices to use the user's identity as a public key and generate a private key [23]. Identity-based authentication combined with ECC to generate signatures is suitable for IoT due to its security and low computational cost [24], [25].

Group-Based Authentication: The IoT environment involves access requests from multiple devices. Group authentication allows multiple users to establish a shared key [26], [27], [28]. The users in the same group can encrypt and decrypt messages using the shared key so that they can communicate with each other securely [29], [29]. There are two steps in generating a group shared key: distributing the pre-shared key and generating the final key [30]. To enable users to switch to different groups, the dynamic joining and leaving processes can reduce the cost of the authentication process [31], [32]. Group-based authentication is suitable for distributed and scalable IoT environments [33], [34], [35].

Biometric Authentication: The evolution of modern technology brings the emergency of biometric identification [36]. This implementation relies on biometric sensors such as fingerprint scanners, facial recognition cameras, and voice recognition microphones to collect biometric data [37]. Biometric-based authentication mechanisms are being explored for scenarios where traditional password-based authentication is impractical or less secure [38], [39]. In choosing biometric templates, it should have sufficiently entropy to ensure security while offering user-friendliness [40]. In the meantime, tolerating noise and disturbances is important when using the biometric function [41], [42]. Traditional biometrics, such as iris [43], face, and fingerprint [44], are more stable than soft biometrics but consume more computing capacity and sensors [45].

Blockchain-Based Authentication: The decentralized and immutable nature of blockchain technology offers the potential for enhancing authentication in the IoT. Blockchain-based authentication protocols leverage distributed ledgers to verify IoT devices' authenticity, integrity, and interactions. By leveraging the consensus mechanisms and cryptographic principles of blockchain, these protocols ensure the integrity of authentication data and prevent unauthorized access to IoT networks and services [36], [43], [46].

In the field of IoT, the AKA remains a vital method to defend against unauthorized access and establish a secure communication channel. While existing review papers have addressed various problems, this survey offers a comprehensive exploration of the critical elements of authentication in IoT. A detailed comparative analysis is presented in Table 1. This paper covers the AKA protocols based on IoT

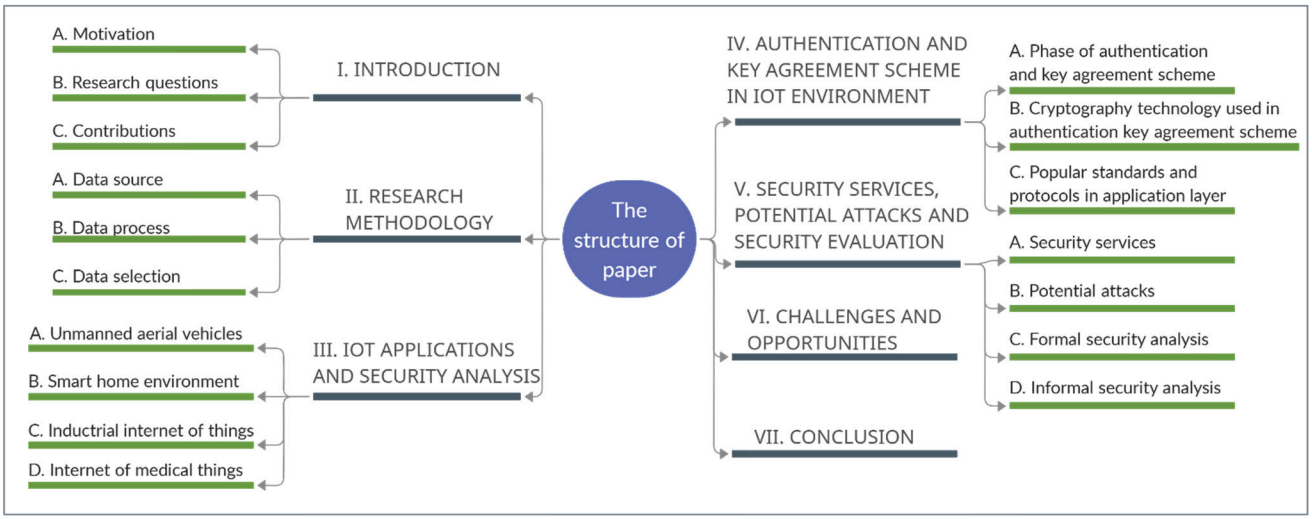


FIGURE 1. The structure of paper.

applications, the AKA process, cryptographic technology, security services, attacks in different IoT layers, formal analysis, informal analysis, and countermeasures. The distinct contributions of this survey offer a robust foundation for future research on designing AKA protocols.

The structure of this paper is outlined in Figure 1. The remainder of this section contains the motivation, research questions, and contribution. Section II discusses the research methodology. Then, section III presents the recent research on AKA protocol design based on IoT applications and their security analysis. Section IV explores the authentication and key agreement phase, cryptography technology, popular standards, and protocols in the Internet of Things. Section V investigates the security services, potential attacks, and security analysis tools. Finally, this survey presents the challenges, opportunities, and conclusions in sections VI and VII.

A. MOTIVATION

The motivation of this paper is driven by the rapid evaluation of IoT devices and their increasing integration into our daily lives. IoT devices, from smart home appliances to industrial sensors, transform how daily life interact with technology. However, this widespread adoption of IoT devices also brings various security challenges. Authentication and key agreement are fundamental components of secure communication in IoT networks. They ensure that the devices in a network can trust each other and securely exchange information. However, the unique characteristics of IoT devices, such as their resource constraints and the heterogeneity of IoT networks, make traditional key agreement and authentication protocols unsuitable. Moreover, the landscape of key agreement and authentication protocols for IoT is vast and rapidly evolving, with numerous protocols being proposed in the literature.

These protocols vary in their security properties, computational requirements, and suitability for IoT applications. The diversity of IoT applications makes it challenging for researchers and to design the appropriate protocol for their specific IoT applications. Therefore, there is a pressing need for a survey that provides a clear overview of the state-of-the-art key agreement and authentication protocols for IoT applications.

B. RESEARCH QUESTIONS

This paper will engage in a thorough examination and resolution of the subsequent research questions:

1) What types of IoT applications need authentication and key agreement?

2) What are the advanced cryptography technologies and solutions used for authentication and key agreement methods?

3) What are the security requirements, threats, and countermeasures in IoT applications?

4) What are the key performance metrics and standards requirements for modeling key agreement and authentication algorithms in IoT applications?

C. CONTRIBUTION

This survey makes several contributions to the literature. First, it identifies the types of IoT applications that necessitate authentication and key agreement mechanisms. This examination allows us to understand the unique security requirements across different IoT contexts. Second, it delves into advanced cryptographic technologies and solutions employed in current authentication and key agreement methods. Then, this paper illuminates the security services in IoT applications, as well as the potential threats during authentication and key agreement. Formal analysis and informal analysis in recent research are used for analyzing security, offering valuable insights into risk mitigation strategies within the IoT domain. Through these contributions, this paper aims to enrich the existing academic

discourse on IoT security and to provide tangible insights for practitioners and policymakers working on the frontlines of IoT implementation and regulation.

II. RESEARCH METHODOLOGY

A. DATA SOURCE

In order to make the review more aligned with cutting-edge research methods, research papers with the theme of IoT, authentication, and key agreement, and those published after 2023, have been selected. Meanwhile, articles irrelevant to the main theme have been excluded. The literature for this review was meticulously gathered from a variety of reputable digital libraries:

1) Science Direct
2) IEEE Xplore Digital Library
3) MDPI
4) Springer Link
5) ACM Digital Library

B. RESEARCH PROCESS

Employing our research methodology, this paper focus on keyword patterns related to the IoT, authentication, and key agreement. In order to uncover relevant research queries, this survey utilized Boolean operators and symbols such as ''AND'' and ''OR''. The target keywords included: (((Key agreement) AND (Authentication)) AND (IoT)).

C. DATA SELECTION

Data selection is the crucial procedure of determining the suitable data source and type, as well as selecting the optimal tools for data gathering. The act of choosing data takes place before the actual iterative process of data collection. The criteria for data selection were as follows:

1) Whether papers were published during 2023.

2) Whether papers were published in the well-known publisher such as: IEEE, Elsevier, Science Direct, ACM, Springer.

3) Whether papers focus on addressing key agreement and authentication problems.

III. IOT APPLICATIONS AND SECURITY ANALYSIS

The IoT is a network of interconnected devices that can communicate with each other through the Internet. IoT devices are everywhere, from Unmanned Aerial Vehicles (UAVs) to smart home environments, from Industrial Internet of Things (IIoT) to Internet of Medical Things (IoMT). UAVs can be used for crop monitoring, irrigation management, and pest control, helping farmers make more informed decisions and improve crop yields. A smart home represents devices such as smart thermostats, Smart Lighting, and security systems connected to the Internet, allowing people to interact with them remotely and promote life convenience. The IIoT means factories and industrial plants can use IoT devices for predicting maintenance, improving safety, and increasing efficiency. The IoMT enables remote patient monitoring. It can monitor patient vitals and health conditions in real-time, alerting healthcare professionals about serious health concerns. While IoT can bring about many benefits, it also opens up new avenues for security threats. IoT devices collect a massive amount of data, some of which can be sensitive. It is crucial to encrypt this data during transmission and at rest and to control who can access it. The device itself can be the point of vulnerability, so that must be designed with security in mind and the ability to update or patch their software securely. Physical access to an IoT device can lead to security breaches. Measures such as tamper detection and prevention mechanisms are essential in many contexts. Therefore, plenty of recent research focuses on improving and discussing the security performance and its efficiency in these applications.

A. UNMANNED AERIAL VEHICLES (UAVs)

Unmanned Aerial Vehicles in the IoT are devices that can collect and transmit data in real-time, move autonomously, and operate in various environments. They form part of the broader application of advanced technologies in IoT, as discussed in the paper [54]. UAVs in IoT can operate autonomously with mobility and have the capacity for real-time data collection and transmission. These characteristics make UAVs particularly useful in various applications, including smart farming, disaster management, and industrial operations. However, new security and privacy challenges are also present [55]. Authentication and key agreement are crucial for UAVs in IoT to ensure the security and integrity of the data they collect and transmit. These measures help prevent unauthorized data access and protect the network from security threats. For instance, A new scheme called HAKA (heterogeneous authenticated key agreement) protocol was proposed based on the combination of Identity-Based Cryptography (IBC) and Public Key Infrastructure (PKI) for providing a secure and efficient communication solution between unmanned aerial vehicles and ground stations. By combining the IBC and PKI, this scheme can reduce computational burden and communication costs while ensuring security [22].

B. SMART HOME ENVIRONMENT

A smart home is an environment where devices and appliances are interconnected and can be controlled remotely or via automation, often through a central system. It typically includes a smart gateway and resource-constrained smart devices [56]. The smart gateway has more computational capability, allowing it to perform relatively complex calculations before transmitting the data from the smart devices to the fog or cloud [57]. Despite the convenience and sophistication of smart homes, these environments are not without security risks, primarily due to the interconnected nature of IoT devices. Personal data privacy is a significant concern due to the vast amount of sensitive information collected by smart home devices [58]. Devices and the network to which they are connected can be compromised if they lack adequate security measures, providing an entry

point for attackers. By obtaining the operating hours of smart air conditioners, wrongdoers can analyze patterns of when users are at home and when they are away. Malware, cyberattacks, and software vulnerabilities on IoT devices pose additional threats. Paper [59] presents a scheme that enables mutual authentication between smart devices in the environment with forged smart devices or semi-trusted home gateways. Due to the limited computation capability of smart devices, an Software Defined Networking (SDN) based authentication mechanism was proposed. It is a lightweight protocol that enables anonymous security, was proved by BAN (Burrows–Abadi–Needham) logic and the ProVerif tool [60]. Fog computing is used in conjunction with blockchain technology [61]. This structure addresses the single-point failure and bottleneck problem of traditional central authority. Security and efficiency perform well in this authentication and key agreement protocol.

C. INDUSTRIAL INTERNET OF THINGS (IIoT)

The Industrial Internet of Things refers to the application of IoT technologies in industrial settings, such as smart grids, smart meters, and so on [62]. It involves the interconnection of machines, devices, sensors, and humans to enable advanced analytics, machine learning, and communication [63]. IIoT often operates on a much larger scale than consumer IoT, with more interconnected devices and larger volumes of data. The devices used in IIoT are also typically more diverse and complex, ranging from simple sensors to advanced industrial machinery. Furthermore, IIoT systems often require higher reliability, security, and real-time performance, as they are used in critical industrial processes [64]. However, the resource-constrained nature of many IIoT devices makes it challenging to implement complex security measures, as shown in Figure 2. There are also efficiency problems related to data processing and communication in large-scale IIoT systems [65]. In order to make communication in the IIoT environment more safety, a protocol was constructed between three components in the IIoT communication environment. Its cryptography technology is based on elliptic curve cryptography, which ensures more security but sacrifices some efficiency [38]. The scheme proposed in [66] focuses on authentication between the user/smartcard and smart device. They use a one-way collision-free hash function as the main cryptography technology, providing a lightweight and efficient authentication and key agreement scheme. Both schemes use fuzzy biometric extraction to increase security against key loss and stolen users' mobile devices. Paper [67] uses the same cryptography technology as [38] to propose a lightweight and robust scheme to defend it from all relevant malicious attacks. However, the workload of the sensor needs to be reduced by deploying a cloud server in further research. The battery of sensor nodes also needs to be taken into consideration. Paper [68] focuses on constructing an efficient and perfect forward secrecy symmetric-key authentication key agreement scheme in edge-cloud IIoT. A software-defined perimeter-based certificate-less anonymous key agreement (CL-AAKA) is proposed to solve the security problem of end devices in Power IoT. The protocol uses elliptic curve cryptography and software-defined perimeter structure to reduce computing and communication costs while maintaining anonymity and ensuring terminal identity privacy. The paper also demonstrates that the proposed protocol is safe and effective in practical applications by comparing the performance criteria of other similar protocols [69].

Fog-based IoT, or fog computing, extends the cloud computing paradigm to the network's edge. It benefits applications that require real-time analytics and low latency, such as health monitoring and emergency response. However, to fully unlock its potential, several challenges must be addressed.

One of these challenges involves the development of resource allocation strategies that effectively assign analytics application modules to respective edge devices, aiming to optimize latency and enhance throughput [70]. In order to enhance the communication process from the past work and solve problems caused by the requested IoT devices pre-selected from the start, a lightweight and anonymity authentication and key agreement scheme was proposed considering the social profile suitable for fog-based social IIoT [9]. A novel protocol for fog and dew computing scenarios was presented, offering the same security level as public-key-based protocols but at a lower cost. The protocol's security is verified through formal and informal analysis, and the protocol's performance is evaluated through computational, communication, and energy consumption metrics [71]. The fog-based protocol was proposed to ensure safety and anonymity between the user, fog node, and cloud service provider. It provides detailed analyses and comparisons of the protocol's resistance against various types of attacks, its security, and its efficiency. Future work includes research on blockchain-assisted access control for fog-driven IoT healthcare systems [72].

D. INTERNET OF MEDICAL THINGS (IoMT)

The Internet of Medical Things is a connected infrastructure of medical devices, software applications, health systems, and services. Essentially, it integrates multiple healthcare applications to create a fully interconnected network of medical devices and applications, paving the way for innovative healthcare delivery methods. With the emergence of cloud computing, 5G connectivity, and artificial intelligence, the scale and effectiveness of IoMT have been significantly improved, changing the landscape of healthcare and patient care [73]. The success of IoMT depends on ensuring the security of the network and data against potential cyber threats. To adequately address these problems, robust cryptographic algorithms and protocols ensure proper authentication and secure key agreement. A compromised device or unauthorized access could lead to

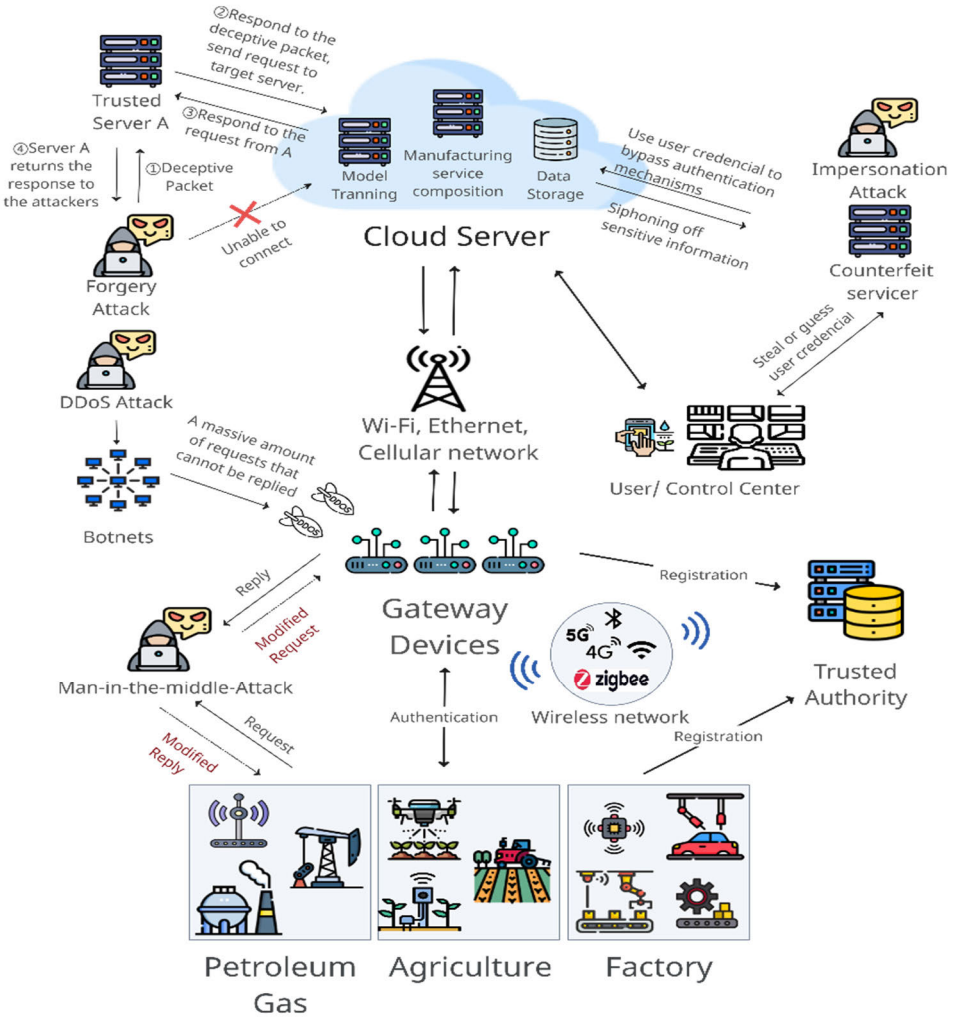


FIGURE 2. Authentication and key agreement scenario in Industrial Internet of Things (IIoT).

severe consequences, including data breaches, patient privacy violations, or even malfunctioning life-saving devices. Thus, the authentication and key agreement in IoMT are of utmost importance to ensure the success of this technology [10].

Three factors and hash functions are used in the Internet-of-Medical-Things. Although the computation cost of fuzzy extraction is high, their total computation cost reached an acceptable level. Compared with relative research, their scheme achieves better security and efficiency performance [74]. A group-based protocol was presented to improve the security between low-power IoT devices in medical applications. The authors discuss the challenges associated with IoT technology in the medical domain and how 5G technology can provide better network connectivity, data transmission, and secure verification for IoT devices [28]. A lightweight group authentication key agreement protocol was presented using symmetric binary polynomial and XOR operation for secure group communication in resource-constrained medical devices. The proposed scheme achieves efficient and low-cost communication, computation, and storage compared to other cryptographic protocols [6]. An improved lightweight user authentication scheme based on three-factor mutual authentication provides robust security while remaining computationally efficient [44]. In order to provide secure and privacy-preserving communication in remote patient data monitoring, which has become imperative in the COVID-19 pandemic era, an improved lightweight privacy-preserving authentication scheme was proposed. The scheme is proven resistant to attacks and reduces computational and storage overhead [4].

Healthcare in the Internet of Things integrates internet-connected devices and sensors into health-related services. Its devices can range from wearable fitness trackers to sophisticated medical imaging equipment. This technology will transform healthcare delivery by enabling remote patient monitoring, predictive analytics, and personalized medicine [75]. Due to the sensitive nature of private data, attackers try to intercept, manipulate, or misuse the data in each layer of IoT architecture, as shown in Figure 3. These threats may lead to severe consequences for patient safety and

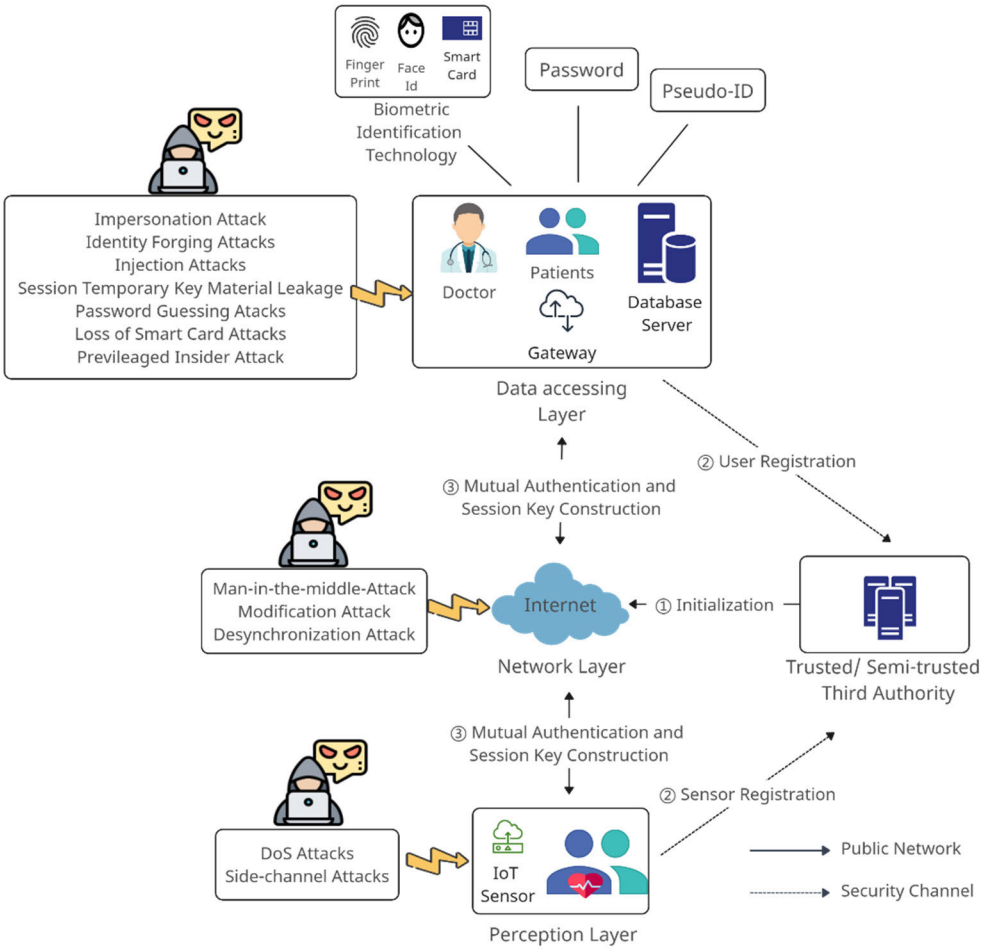


FIGURE 3. Authentication and key agreement scenario in Internet of Medical Things (IoMT).

privacy [76]. In order to protect security, robust security measures are necessary. When doctors, patients, or fog servers request health information in the sensor node, authentication ensures that the entities are who they claim to be, preventing unauthorized access to data. A key agreement allows entities to establish session keys for securing future communication. Authentication and key agreement in healthcare IoT can be achieved through various methods, including password-based, certificate-based, biometric-based, and multi-factor authentication. These methods provide varying levels of security and usability, and their selection should consider the specific requirements and constraints of the healthcare IoT system [77]. A lightweight user authentication protocol for the healthcare ecosystem in the Internet of Things was designed for post-quantum computing environments. The security has been validated by utilizing the random oracle model (ROM). Its performance has been found to be more efficient than other related protocols [5]. In paper [23], a novel pairing-free authentication and aggregation mechanism based on elliptic curve cryptography is proposed to protect data privacy and security in healthcare systems. The mechanism does not require pairing or ID-based cryptography. Its security was proved based on the ROM. A lightweight protocol in the IoMT field of the healthcare industry was proposed in the cloud and edge computing architecture. As trusted third authority, cloud and edge servers process and store patient health information, and allow authorized medical institutions to obtain the data [19]. Authors have proposed an improved certificateless authentication key agreement (CL-AKA) protocol based on the hash function and XOR operation. By analyzing the shortcomings of existing protocols and considering the needs of medical staff and patients, the proposed protocol ensures security and has high efficiency and applicability [78]. An authenticated key agreement protocol based on cross-server for DNA-based U healthcare services has been presented in the IoT. The designed protocol enables mutual authentication between two patients through the assistance of their respective servers, facilitating reliable shared E2E session key establishment while preserving privacy and security [41]. A secure and lightweight group key management protocol [32] was proposed for the IoHT. The

proposed protocol uses elliptic curve cryptography, one-way accumulation, and cryptographic accumulators to provide forward and backward secrecy. Session key establishment and group signature were used for secure communication. The proposed scheme reduces computation and communication overhead, making it suitable for resource-constrained sensor devices in healthcare environments. However, the authentication process for nodes in a group still imposes a burden on gateway devices.

IV. AUTHENTICATION AND KEY AGREEMENT SCHEME IN IOT ENVIRONMENT

A. PHASE OF AUTHENTICATION AND KEY AGREEMENT SCHEME

1) SYSTEM INITIALIZATION

This phase involves setting up the necessary parameters, generating cryptographic keys, and initializing the system components to enable full preparation for authentication and key agreement, as shown in Figure 4. During the system initialization phase, the following steps are typically performed:

a: PARAMETER SETUP

The AKA scheme requires various system parameters to be set up before the authentication process can begin. These parameters may include cryptographic algorithms, security levels, session lifetimes, and key sizes. These parameters should be selected and configured based on established cryptographic standards and best practices to ensure robust security. For example, the scheme may employ symmetric or asymmetric encryption algorithms such as elliptic curve cryptography and bilinear pairing.

b: KEY GENERATION

Cryptographic keys play a vital role in the security of the AKA scheme. During the initialization phase, the system generates the keys required for authentication and secure communication. This process may involve generating a primary key, shared secret key, or public-private key pairs. The key generation process should follow industry-standard cryptographic algorithms and random number generation techniques to ensure the keys' strength and unpredictability.

c: COMPONENT INITIALIZATION

Various system components, such as authentication servers, user devices, and network infrastructure, should be initialized during this phase. Initialization involves configuring these components with the necessary cryptographic parameters and keys. For example, the authentication server may set up a secure database to store user credentials, while user devices may securely generate and store their private keys. The initialization process should include security updates or patches to mitigate potential vulnerabilities.

2) USER REGISTRATION

This step involves enrolling new users into the system and securely storing their credentials. The user registration process establishes the initial trust relationship between the user and the authentication server, enabling subsequent authentication and secure communication. Here is an overview of the user registration phase:

a: USER ENROLLMENT

The user enrollment process involves collecting user information and generating the necessary credentials for authentication. During enrollment, the user typically provides identifying information, such as a username or email address, along with any additional required information. The authentication server verifies the provided information and assigns a unique identifier to the user. The process may also involve user verification mechanisms, such as email confirmation or identity verification, to ensure the authenticity of the user's identity.

b: CREDENTIAL GENERATION

Once the user is enrolled, the authentication server generates the necessary credentials for the user. This process typically includes the creation of a password or a cryptographic key pair. The password is securely hashed and stored in a database, while the key pair's private key is encrypted and stored on the user's device. Solid and secure hashing algorithms are essential to protect passwords against brute-force attacks. The private key generation process should adhere to established cryptographic standards, such as RSA or ECC, to ensure the key's strength.

c: CREDENTIAL STORAGE

The user's credentials, including the password or the private key, are securely stored by the authentication server and the user's device. The authentication server should employ secure database storage mechanisms, such as encryption or hashing, to protect the stored passwords from unauthorized access. Similarly, the user's device should store the private key in a secure storage area to prevent key leakage or tampering. Using secure storage mechanisms ensures the confidentiality and integrity of the user's credentials.

3) AUTHENTICATION AND KEY AGREEMENT

This step encompasses the authentication of communicating entities and the establishment of shared cryptographic keys for secure communication. Here is an overview of the authentication and key agreement phase:

a: MUTUAL AUTHENTICATION

Mutual authentication ensures that the user and the server authenticate each other's identities. The user sends their identity and any necessary credentials to the server, and the server verifies them, as discussed in the authentication phase. Simultaneously, the server presents its credentials or a

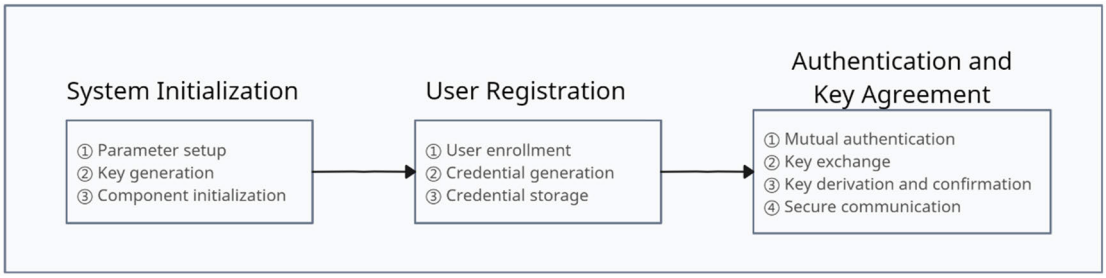


FIGURE 4. Phase of authentication and key agreement schem.

digital certificate to the user, which the user verifies using a trusted certificate authority or public key infrastructure. Mutual authentication builds trust between the entities and prevents impersonation attacks.

b: KEY EXCHANGE

After successful mutual authentication, the user and server should establish shared cryptographic keys for secure communication. This step can be achieved through a key exchange protocol. One widely used key exchange protocol is the Diffie-Hellman key exchange, which allows two entities to establish a shared secret over an insecure communication channel. The shared secret is then used to derive symmetric encryption keys for subsequent secure communication. Other key exchange protocols, such as the Elliptic Curve Diffie-Hellman (ECDH) or the RSA-based key exchange, may also be employed based on the AKA scheme's specific requirements and security considerations.

c: KEY DERIVATION AND CONFIRMATION

Once the shared secret is established through the key exchange protocol, the user and the server derive session keys for encryption and message authentication. These session keys are derived using a key derivation function (KDF), which inputs the shared secret and additional parameters. The KDF ensures that the derived keys are unique, secure, and suitable for the specific cryptographic algorithms employed in the AKA scheme. Additionally, the derived keys can be used to confirm the integrity and authenticity of subsequent communication through message authentication codes (MACs) or digital signatures.

d: SECURE COMMUNICATION

The user and the server can securely communicate with the session keys derived and authenticated. The session keys are used for symmetric encryption and decryption of the exchanged data, ensuring its confidentiality. Additionally, the MACs or digital signatures based on the derived keys provide data integrity and authentication, protecting against tampering or unauthorized modifications. Secure communication protocols such as Transport Layer Security (TLS) or the Secure Shell (SSH) can facilitate the secure data exchange between entities.

B. CRYPTOGRAPHY TECHNOLOGY USED IN AUTHENTICATION KEY AGREEMENT SCHEME

Cryptography, the art and science of secure communication in the presence of adversaries, plays a critical role in modern digital communication systems, providing essential services such as data confidentiality, data integrity, authentication, and non-repudiation. Authentication and key agreement (AKA) schemes form the cornerstone of such cryptographic systems. These mechanisms ensure that entities in a communication process are who they claim to be (authentication) and agree upon a secret key to secure subsequent communications (key agreement). Table 2 summarizes cryptography operations in recent research.

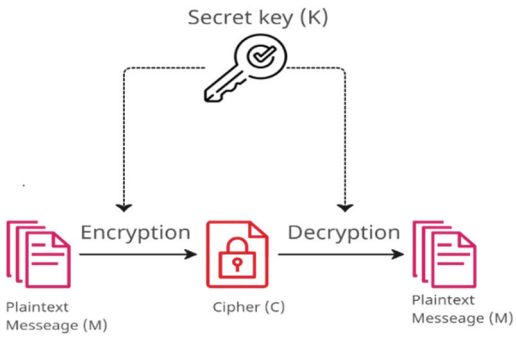


FIGURE 5. Diagram of the symmetric algorithm.

1) SYMMETRIC-KEY CRYPTOGRAPHY

This type of cryptography uses the same key for encryption and decryption. Its process is shown in Figure 5. Encryption is the process of converting plain text into ciphertext can be expressed in Eqn. (1):

$$C = E(K, P) \tag{1}$$

P is the plaintext message and C is the resulting ciphertext. The security of the system relies on the secrecy of the key K. Examples of symmetric key algorithms include AES (Advanced Encryption Standard) and DES (Data Encryption Standard). Symmetric-Key Cryptography can be divided into sub-categories: Block Ciphers and Stream Ciphers.

TABLE 2. Summary of application area, research goals and cryptography operations in recent research.

Paper	Application Area	Goals	Cryptography Operation					
			CO1	CO2	CO3	CO4	CO5	CO6
[22]	Unmanned aerial vehicles	- Secure and efficient communication between ground station and UAVs		✓	✓	✓		
[13]	Unmanned aerial vehicles	- To address security problems and improve efficiency based on [79]				✓	✓	✓
[80]	Smart Meters	- Lightweight and identity anonymity AKA scheme for smart meters	✓			✓		✓
[59]	Smart Home	- Acceptable efficiency authentication in Smart Home Environment		✓		✓		
[28]	IoMT with low power	- Group-based efficient authentication for low power IoMT			✓	✓		✓
[74]	IoMT	- Three factor-based security and efficient aka scheme for IoMT				✓	✓	✓
[6]	IoMT	- Lightweight membership authentication group key agreement			✓			✓
[44]	IoMT	- Three way and lightweight user authentication scheme				✓	✓	✓
[66]	IIoT	- Three factor-based lightweight AKA for IIoT				✓	✓	✓
[38]	IIoT	- Three factor-based security and privacy authentication	✓			✓	✓	
[68]	IIoT	- Efficient and perfect forward secrecy sysmmetric-key authentication			✓	✓		
[67]	IIoT	- Three factor and ECC based efficient authentication scheme	✓			✓		✓
[81]	IIoT	- ECC-based authenticated key exchange scheme between two Industrial IoT devices	✓			✓		✓
[5]	Healthcare	- Lightweight protocol in post-quantum computing environments using two factors				✓		✓
[23]	Healthcare	- Pairing-free authentication and aggregation mechanism	✓			✓		
[19]	Healthcare	- Secure and lightweight identity AKA protocol in the IoMT field of the healthcare industry.				✓		✓
[78]	Healthcare	- Certificateless and lightweight AKA protocol				✓		✓
[41]	Healthcare	- Three-way secure authentication key agreement scheme based on bio-hash and ECC for the healthcare	✓					
[32]	Healthcare	- Enabling forward and backward secrecy using lightweight primitives in group communication of IoHT	✓					
[9]	Fog-based SIIoT	- Lightweight and anonymity hash-based authentication key agreement for fog-based social IoT			✓	✓		✓
[72]	Fog-based IoT	- Privacy-preserving authenticated key agreement for fog-driven IoT				✓		✓
[71]	Fog and dew computing	- Authentication for fog and dew computing scenarios			✓	✓		✓

CO1: Elliptic Curve Cryptography; CO2: Bilinear Pairing; CO3: Symmetric Encryption; CO4: Hash Function; CO5: Fuzzy Extraction; CO6: XOR Operation.
✓: Yes

2) ELLIPTIC CURVE CRYPTOGRAPHY (ECC)

Elliptic curve cryptography is a type of asymmetric encryption algorithm. ECC-based systems rely on the mathematical properties of elliptic curves to provide security and efficiency. They involve operations on points in elliptic curve groups and utilize the difficulty of certain mathematical problems for cryptographic purposes. Compared to RSA, the advantage of ECC is that it can use shorter keys to achieve equivalent or higher security levels. An elliptic curve over a field is defined by Eqn. (2), where Eqn. (3) to avoid singularities [82].

$$y^2 = x^3 + ax + b \tag{2}$$

$$4a^3 + 27b^2 \neq 0 \tag{3}$$

$$y^2 mod\ p = \left(x^3 + ax + b\right) mod\ p \tag{4}$$

$$Q = dG \tag{5}$$

Cryptographic applications typically use a curve over a finite field (4), while p is a prime number. In an asymmetric encryption scheme, a random integer d is always chosen

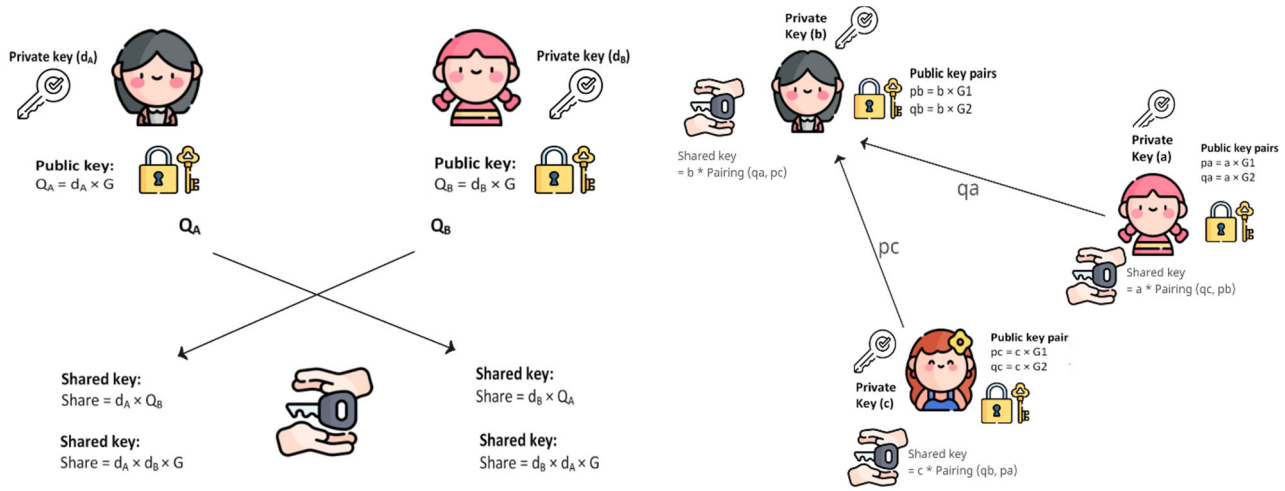


FIGURE 6. Elliptic curve Diffie Hellman cryptography (left) and generation of a shared key between three parties (right).

as a private key. Its public key is calculated in Eqn. (5), where G is the base point on the elliptic curve. Elliptic Curve Diffie-Hellman is a variant of the Diffie-Hellman protocol that uses ECC to generate a shared secret between two parties, as shown in Figure 6.

3) BILINEAR PAIRING

Bilinear pairing, also known as bilinear mapping, is a function that allows certain operations between elements from two different groups to be performed more efficiently. Bilinear pairings are defined by the set of three abelian groups $G_1, G_2 and G_T$ over a finite field Z_n together with a deterministic function e. Bilinearity means for all $P \in G_1, Q \in Q_2, and\ a, b \in Z$ presents in Eqn. (6):

$$e\left(P^a, Q^b\right) = e(P, Q)^{ab} \tag{6}$$

Bilinear Diffie-Hellman Problem (BDHP) utilizes the properties of Bilinear Pairing, shown in Figure 6. Given $P, aP, bP, cP \in G_1, computee\ (P, P)^{abc}$ cannot be solved in polynomial time if the discrete logarithm (DL) problem is hard in the Group G_1. Initially, bilinear pairing played a negative role in cryptography. In 2000, bilinear pairing was utilized to construct a three-party key exchange protocol [83]. Subsequently, in 2001, it was used to devise the first practical and provably secure Identity-Based Encryption (IBE) scheme [84]. Since then, bilinear pairing has received widespread application in cryptography. Bilinear pairing can also be used in Attribute-Based Encryption (ABE) and short signatures. The former can be based on a set of attributes, and the latter can be used to save bandwidth and computing power.

4) FUZZY EXTRACTION

It is a cryptographic primitive that involves constructing a stable and reliable cryptographic key from a noisy input, such as sensor data or biometric identifiers. Keys generated are usually distributed as random numbers [85]. This process is often used when the data inputs may not always be identical due to minor changes or errors during data capture. There are two steps in fuzzy extraction, the generate and the reproduce stages [86]. Generate (Gen) is a probabilistic algorithm generate two outputs from a noisy input: a public string and a secret key. Reproduce (Rep) is a reproduction function using the public string and a noisy version of the original input to reproduce the original secret key, as shown in Figure 7. The helper data should not reveal any information about the secret key. Fuzzy extraction was used in the biometric identification method in the authentication and user login process to prevent key loss and stolen users' mobile devices [38]. A biometric key was extracted from the user's biometrics to ensure the verification of the user's identity for the smart card [66].

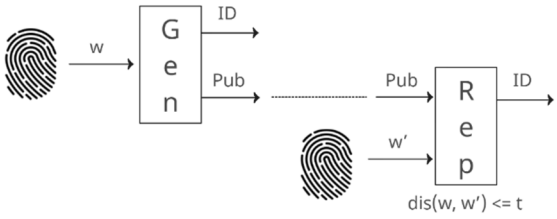


FIGURE 7. Typical scenario of a fuzzy extractor.

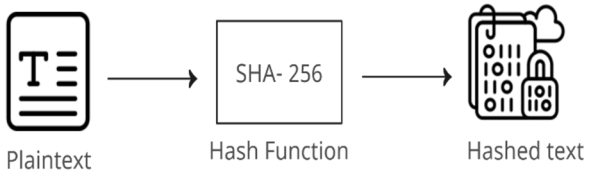


FIGURE 8. Cryptographic hash function.

5) HASH FUNCTION

It is a cryptographic algorithm that takes an input message and produces a fixed-size output, called a hash value or digest

TABLE 3. Comparison between application layer protocols.

Protocol	Standard	Transport	Architecture	Authentication Mechanism	Security Mechanism	Unauthenticated Attacks Recorded in NVD
HTTP	IETF	TCP/IP	Request - Response	TLS/SSL	HTTPS	CVE-2022-35136, CVE-2022-20916, CVE-2022-24562, CVE-2022-24796, CVE-2021-30302, CVE-2021-33221, et al.
MQTT	OASIS	TCP/IP	Publish – Subscribe	Username / Password; TLS; JWT [a]	TLS/SSL [b]	CVE-2023-22600, CVE-2022-45423, CVE-2021-44222
CoAP	IETF	UDP	Request – Response	DTLS	DTLS; IPSec [c]	CVE-2020-3162
AMQP	OASIS; ISO	TCP/IP	Publish – Subscribe; Request – Response	SASL	SASL and/or TLS	CVE-2019-0200, CVE-2018-11050, CVE-2018-1298, CVE-2017-15702, CVE-2017-15701
XMPP	IETF	TCP/IP	Request - Response	SASL	TLS / SSL/ SASL	CVE-2023-32315, CVE-2020-3160, CVE-2016-6445, CVE-2014-2744
DDS	OMG	UDP/IP unicast and TCP/IP multicast	Publish - Subscribe	Built-in plugins	TLS/ SSL/ DTLS	-
WebSocket	IETF	TCP/IP	Request - Response	HTTPS	HTTPS	CVE-2022-46901, CVE-2022-23128, CVE-2022-21667, CVE-2020-16839, CVE-2021-21588, CVE-2021-1403, CVE-2020-16101, CVE-2020-16100, CVE-2019-17654, CVE-2018-12678, CVE-2018-0278, CVE-2017-1000080
STOMP	IETF	TCP/IP	Publish - Subscribe	Login / Passcode	HTTPS	-

a JSON Web Tokens. *b* Transport Layer Security and/or Secure Socket Layer. *c* Internet Protocol Security

(Figure 8). This digest is used to verify the integrity of the data and prevent tampering. Hash function in cryptography has properties such as preimage resistance, which means given a hash value h, it should be computationally infeasible to find any input that hashes to h. Second preimage resistance is given an input m_1, it should be computationally infeasible to find another input, m_2 (not equal to m_1), such that the hash of m_1 is equal to the hash of m_2. Collision resistance is that it should be computationally infeasible to find any two distinct inputs m_1 and m_2 presents in Eqn. (7) [87].

$$\text{hash}(\text{m}_1) = \text{hash}(\text{m}_2) \tag{7}$$

These properties are the guarantee of the security of the hush function. The hash function is more suitable for constructing lightweight authentication and key agreement schemes for resource-limited edge devices in IoT applications.

6) BITWISE XOR OPERATIONS

It is a fundamental operation used in cryptographic algorithms. It stands for "exclusive or," meaning it returns true if exactly one of the operands (but not both) is true. This property is useful in cryptography because the operation is reversible. In cryptographic protocols, the XOR operation is beneficial due to its simplicity and reversibility.

$$A \; XOR \; B = C \tag{8}$$

Given any two of A, B, C in Eqn. (8), while A, B and C are binary digit 0 or 1, can determine the third. The role of XOR operation in AKA protocols can take various forms.

C. POPULAR STANDARDS AND PROTOCOLS IN IOT

The application layer interacts with the user directly, so that demands robust security mechanisms to secure the integrity and confidentiality of data. Authentication is a crucial method to verify the identities of devices and users. Current features of protocols in this layer are represented in Table 3.

1) PROTOCOLS WITH INNER AUTHENTICATION MECHANISMS

a: HTTP

The Hypertext Transfer Protocol (HTTP) is a request-response protocol for web-based communication. While HTTP is fundamental for web-based communication, its limitations become evident in IoT contexts. Recent studies indicate that HTTP's heavy load and limited capacity for retaining requests fall short of meeting the requirement for resource-limited devices and scalability in IoT [88]. The built-in authentication mechanisms are insufficient for IoT's security demands due to their simplicity and vulnerability to cyber-attacks [89]. Therefore, other security protocols and standards, such as HTTPS and OAuth 2.0, are often recommended in applications requiring a high degree of security.

b: MQTT

The default password-based authentication in MQTT, with plaintext transmission, is a notable security concern. Implementing TLS can encrypt the entire communication session but requires heavy resource consumption [90]. Under the same testing condition, the battery consumption in MQTT with SSL/TLS is four times that of without SSL/TLS [91]. Recent research focuses on optimizing authentication and key agreement for MQTT suitable for resource-constrained devices in IoT [92], [93], [94]. Cipher suites with Curve 25519 and RSA in TLS 1.3 protocol perform significantly better on computation than P-256 and ECDSA suites while providing the same security level [95].

2) PROTOCOLS WITHOUT INNER AUTHENTICATION MECHANISMS

a: CoAP

Constrained Application Protocol (CoAP) is a lightweight protocol for low-power devices. As HTTP is the most prevalent protocol on the internet, CoAP is designed to interact with it seamlessly. CoAP operates over UDP and relies on Datagram Transport Layer Security (DTLS) for security. DTLS's flexibility in authentication mechanisms such as Pre-Shared Key (PSK), Raw Public Key (RPK), and X.509 certificates align with IoT's diverse needs. The client and server negotiate session keys during the DTLS handshake phase.

b: AMQP

Advanced Message Query Protocol (AMQP) is a platform-agnostic protocol for heterogeneous networks but lacks native authentication, relying on additional security layers like SASL or TLS. While robust, these mechanisms increase the computational load for IoT devices [96].

c: DDS

As a scalable solution for machine-to-machine (M2M) communication in large-scale IoT, Data Distribution Service (DDS) incorporates unique security features through plugins. For example, the DDS: Auth: PKI-DH plugin leverages PKI and x.509 certificates for mutual authentication [97].

d: WebSocket

WebSocket protocol does not offer authentication but uses HTTP or TLS-based methods. Token-based authentication offers better security compared to traditional username-password methods [98].

V. SECURITY SERVICES, POTENTIAL ATTACKS AND SECURITY EVALUATION

A. SECURITY SERVICES

The Internet of Things has revolutionized how we interact with the world, connecting everyday objects to the Internet and allowing them to communicate. However, this interconnectivity has also brought significant security challenges, particularly in authentication and key agreement. Recent research in IoT security has focused on addressing these challenges, emphasizing enhancing security services such as un-traceability, anonymity, and so on [99]. (Table 4)

1) UN-TRACEABILITY AND ANONYMITY

They are two security services that protect the identities of users and devices in an IoT network. Un-traceability ensures that unauthorized entities cannot track the activities of a device, while anonymity protects the identity of the device or user. These services are essential in applications where user or device privacy is paramount, such as in healthcare or smart home environments [19]. Recent research has proposed various methods to enhance un-traceability and anonymity in IoT, such as using pseudonyms or advanced cryptographic techniques.

2) MUTUAL AUTHENTICATION

Mutual authentication ensures that both parties in communication are legitimate, preventing impersonation attacks. It is particularly important in IoT networks, where devices often communicate with each other without human intervention. It ensures confidentiality in the process of service providing using cryptography technology [100]. Recent research has proposed various mutual authentication protocols for IoT, many of which leverage public key cryptography to ensure the authenticity of devices.

3) SESSION KEY AGREEMENT

It is a security service that allows two or more devices to establish a secure communication session. Each session has a unique key used to encrypt and decrypt messages, ensuring the confidentiality and integrity of the data. Recent research has focused on developing efficient session key agreement protocols for IoT, considering the resource constraints of many IoT devices.

4) PERFECT FORWARD SECRECY

In the IoT environment, devices may be physically accessible to attackers. With perfect forward secrecy, even if an attacker manages to compromise a device and obtain a current session key, they cannot decrypt past messages.

B. POTENTIAL ATTACKS

Table 5 summarizes the potential attacks of the examined protocols. This table only encompasses attacks that authors have analyzed using formal or informal methods. When classifying IoT attacks, a hierarchical approach has become the norm. This structure usually involves three IoT levels: perception layer, network layer, data link, and application layer [101]. It is worth noting that certain attacks can impact multiple layers simultaneously. Moving forward, we will briefly overview of each layer's scope and discuss the most prevalent types of IoT attacks associated with them.

TABLE 4. Security services provided in recent research.

References	Un-traceability	Anonymity	Mutual Authentication	Session Key Agreement	Perfect forward secrecy
[22]	×	✓	✓	✓	✓
[80]	×	✓	✓	✓	×
[13]	✓	✓	✓	✓	×
[59]	×	✓	✓	✓	×
[66]	✓	✓	✓	✓	✓
[38]	✓	✓	✓	✓	✓
[68]	×	✓	✓	✓	✓
[81]	✓	✓	✓	✓	✓
[9]	×	✓	✓	✓	×
[71]	×	✓	✓	✓	✓
[72]	✓	✓	✓	✓	✓
[74]	×	✓	✓	✓	✓
[28]	✓	✓	✓	✓	✓
[6]	×	×	✓	✓	✓
[44]	×	✓	✓	✓	✓
[5]	×	✓	✓	✓	×
[23]	×	✓	✓	✓	✓
[19]	✓	✓	✓	✓	✓
[78]	✓	✓	✓	✓	✓
[41]	✓	✓	✓	✓	✓
[32]	×	✓	✓	✓	✓

✓: Yes. ×: Not shown in the paper.

1) PERCEPTION LAYER

a: STOLEN DEVICE ATTACK

This attack refers to situations where a malicious entity gains physical control of a device and uses it to access or compromise the network. Incorporating biometric authentication can protect against stolen device attacks in the authentication and key agreement scheme. If an attacker steals an IoT device, they still need specific biometric data (like fingerprint or face recognition) to access it.

b: LOSS OF SMART CARD ATTACK

Smart cards are often used in IoT devices for authentication and secure communication. However, if a smart card is lost or stolen, it poses a significant security risk as it could be used to gain unauthorized access to the system. One approach is to employ multi-factor authentication schemes, where a user is required to present two or more separate pieces of evidence for authentication. The loss of a smart card would not automatically lead to a security breach, as the attacker would still need to bypass the other authentication factors. In addition to multi-factor authentication, robust AKA schemes can further enhance the security of IoT devices against smart card loss attacks. An AKA scheme ensures that a unique secret key is generated and agreed upon by the IoT device and the network server for each session, minimizing the chance of unauthorized access.

2) NETWORK LAYER

a: MAN-IN-THE-MIDDLE (MITM) ATTACK

It refers to situations where the attacker positions themselves between two parties, such as an IoT device and a network server. The attacker can then eavesdrop, intercept sensitive information, or alter the data sent between the parties. Due to the generally weaker security protocols in many IoT devices and the amount of data they exchange, these devices are often attractive targets for MitM attacks. The implications of successful MitM attacks can lead to breaches of personal and financial data, alteration of data leading to incorrect device operation, and unauthorized access to networks or services. These attacks could cause substantial financial losses and damage the trust in IoT devices.

b: REPLAY ATTACK

It's a kind of man-in-the-middle attacks [102]. It involves the interception and replay of previously captured messages between IoT devices and the network. Attackers can capture valid data packets transmitted and replay them later to gain unauthorized access, deceive devices, or manipulate the system. Timestamps can detect reply attacks by checking

TABLE 5. Security attack prevented in the scheme of recent research.

Attacks	Authentication Scheme									
	[22]	[80]	[13]	[59]	[66]	[38]	[68]	[67]	[81]	[9]
Privileged Insider Attack					✓			✓		
Password Guessing Attack			✓		✓	✓				
Loss of Smart Card Attack					✓					
Stolen Device Attack			✓		✓	✓				
DoS/DDoS		✓				✓		✓		
Impersonation Attack	✓	✓	✓			✓	✓		✓	✓
Modification Attack	✓		✓			✓	✓			
Man-in-the-Middle Attack	✓	✓	✓		✓	✓	✓	✓	✓	✓
Desynchronization Attack					✓	✓				
Replay Attack	✓	✓	✓		✓	✓	✓	✓	✓	
Known Session Key Attack							✓	✓		✓
Unknown Key-share (UKS) Attacks		✓	✓							
Forgery Attack				✓	✓					
	Authentication Scheme									
	[71]	[72]	[74]	[28]	[6]	[44]	[5]	[78]	[41]	[32]
Privileged Insider Attack	✓	✓			✓	✓	✓		✓	
Password Guessing Attack			✓			✓			✓	
Loss of Smart Card Attack			✓				✓		✓	
Stolen Device Attack	✓	✓								
DoS/DDoS									✓	
Impersonation Attack		✓	✓	✓		✓		✓	✓	
Modification Attack										
Man-in-the-Middle Attack						✓	✓	✓	✓	✓
Desynchronization Attack	✓	✓							✓	
Replay Attack	✓			✓	✓	✓			✓	
Known Session Key Attack		✓				✓				
Unknown Key-share (UKS) Attacks										
Forgery Attack										

✓: Yes. ×: Not shown in the paper.

whether the message transmission time is in the normal range. One-time tokens are also a useful method. For each communication, a token can only be used only once. In this way, even if the attacker intercepts this token, a replay attack cannot be performed due to the rejection from the server.

3) DATA LINK AND SOFTWARE LAYER

a: PASSWORD GUESSING ATTACK

It occurs when an attacker repeatedly tries different passwords to gain unauthorized access to IoT devices or networks. Passwords with features such as weak or easily guessable are particularly vulnerable to these attacks. Biometrics information provides a more stable way to authenticate the actual user. Choosing suitable and applicable biometrics is necessary due to the situation that IoT devices are always resource-constrained.

4) MULTI-LAYER ATTACKS

a: DENIAL OF SERVICE (DOS)

This kind of attack in IoT involves overwhelming targeted devices or networks with a flood of requests or traffic, causing them to be unavailable for legitimate users. IoT devices are vulnerable to these attacks due to their limited processing power, memory, and network bandwidth. In wireless sensor networks, sensors are often clustered to improve scalability. Cluster heads typically experience a higher volume of traffic compared to other nodes. Their significant influence presents more attraction for attackers to launch DoS attacks. Setting low computing cost operations in the registration step as an access control or limiting the number of requests for the same user can effectively prevent DoS/DDoS attacks [38].

b: DISTRIBUTED DENIAL OF SERVICE (DDOS)

It refers to the malicious use of multiple internet-connected devices, known as a botnet, attempting to disrupt a network's normal functioning by overwhelming it with internet traffic. IoT devices such as smart thermostats, home security systems, or wearables are often manufactured with minimal security protocols. This limitation makes these devices perfect targets for hackers aiming to conduct DDoS attacks.

c: PRIVILEGED INSIDER ATTACK

It refers to someone who has authorized access to the system or its components and misuses their permissions to inflict harm. This attack can potentially exploit their access across multiple layers. In the network layer, the attacker could intercept or modify data in transit or manipulate the network configuration. In the application layer, the attacker could steal passwords and pretend to be other legitimate users. In the edge tier, a privileged insider could get key materials from the gateway database to generate a session key.

d: IMPERSONATION ATTACK

This attack appears in several layers of the IoT architecture, depending on the specifics of the attack. In the perception layer, a device might be physically tampered with to make it impersonate another device. The network layer is the most common layer for impersonation attacks. Attackers could impersonate a device or a node by their IP or MAC address in the network to gain unauthorized access. In the application layer, attackers could create a counterfeit server that behaves like a real one, stealing user credentials to bypass authentication mechanisms.

e: FORGERY ATTACK

This attack in IoT environments usually involves creating false data or altering existing data, making it appear as if it is from a trusted source. For instance, an attacker might alter sensor readings to manipulate the IoT system's actions or even fabricate a new device identity to gain unauthorized access to the network. These attacks can have numerous consequences, from causing incorrect system operations to providing unauthorized access to sensitive data. In healthcare, false readings from medical devices could lead to misdiagnosis or incorrect treatment plans.

f: MODIFICATION ATTACK

This attack refers to a malicious act where the attacker alters the content of the messages transmitted between IoT devices or changes the configuration or code of the IoT devices themselves. Such attacks can lead to false data being accepted as legitimate, potentially causing incorrect actions to be taken or sensitive data to be exposed.

g: DESYNCHRONIZATION ATTACK

It typically involves an attacker manipulating the sequence numbers in the packets of a TCP (Transmission Control Protocol) session between two devices. This manipulation can lead to both devices thinking that the other has lost data, forcing them to retransmit data packets. Repeated retransmission consumes network resources, slows communication, and may eventually lead to a denial of service due to resource exhaustion. The effects of desynchronization attacks can range from mild annoyances to severe system disruptions, depending on the importance of the affected services. It can cause delays in data transmission, impede real-time communication, and drain device and network resources. These delays could have significant real-world consequences like disrupting essential services or leading to inaccurate data-driven decisions in critical infrastructures like healthcare, transportation, or energy sectors.

h: KNOWN SESSION KEY ATTACK

This attack refers to an attacker obtaining a valid session key and using it to masquerade as a legitimate user or device, thereby gaining unauthorized access to information or potentially disrupting operations. Perfect Forward Secrecy (PFS) is a property that prevents the compromise of a long-term secret key from affecting the secrecy of past session keys.

5) ATTACK ASSESSMENT AND DETECTION

Various methods are available for assessing and detecting attacks to improve the security of the IoT. Attack graphs combined with other methods, such as game theory and machine learning, help assess the vulnerability of IoT networks [103]. Recent research focuses on using deep learning methods to design malware detection systems [104]. HSAS-MD Analyzer [105] employs a combination of model-checking technique (MCT) and deep learning (DL), particularly a convolutional neural network (CNN) model, to analyze and detect potential threats for IoT applications, which shows the best performance compared with other security analysis systems.

C. FORMAL SECURITY ANALYSIS

In recent research, formal analysis helps validate the security properties of AKA protocols. These properties include mutual authentication, secure session keys, and resistance to several attacks. Formal analysis systematically uses rigorous mathematical methods to analyze protocols and find the security limitations. Eight popular formal analysis tools in recent research have been highlighted in Table 6. It includes the Automated Cryptographic Protocol Verifier (ProVerif), Automated Validation of Internet Security Protocols and Applications (AVISPA), Scyther Tool, Burrows–Abadi–Needham Logic (BAN-logic), Real-Or-Random (RoR) model.

1) PROVERIF

ProVerif serves as an automated solution for validating the security of cryptographic protocols. Bruno Blanchet [106] developed this most powerful verifier to assess communication protocols and Web applications. The structure of ProVerif is represented in Figure 9 [107]. The input for ProVerif comprises two parts: the protocol written in Pi calculus with cryptography and the security properties that need to be proven. The general verification process with ProVerif is structured into three steps:

- The construction of models and security properties;
- The translation of these elements into a format that ProVerif can read;
- The verification of the protocol against the specified security requirements.

The output of ProVerif consists of three types: if the result is not derivable, it means the property is true and the desired security is proved. If the result is derivable, there may be an actual attack or a false attack. A ''false attack'' indicates it is unknown whether the property is true or false, caused by the abstraction inherent in Horn clauses, which represents a limitation of the ProVerif tool [108]. Researchers commonly use the ProVerif tool to validate multi-factors AKA protocols with security properties relevant to the password's security,

TABLE 6. Formal analysis tools used in recent research.

References	ProVerif	AVISPA	BAN logic	Scyther	ROM	ROR
[20]	✓					
[44]	✓					
[60]	✓		✓			
[114]	✓		✓			
[115]	✓					
[109]	✓		✓			
[17]		✓	✓	✓		
[15]			✓	✓		
[78]			✓	✓		
[9]			✓			
[41]			✓			✓
[28]		✓	✓			
[38]			✓			✓
[36]		✓				
[43]		✓				✓
[72]		✓			✓	
[29]					✓	
[13]					✓	
[23]					✓	
[116]					✓	
[74]					✓	
[117]						✓
[81]						✓
[5]					✓	
[66]						✓
[19]						✓
[68]					✓	

session key's security, and authentication process. This tool's shortcoming is that ProVerif does not extend its analysis for the property, such as node capture attack [109].

2) BAN LOGIC

BAN logic [110] focuses on the beliefs of participants. These beliefs are a key's trustworthiness or a message sender's authenticity. In BAN logic, a protocol is proved to be secure if it can defend against eavesdropping or if the message transmitted is trustworthy. The general procedure for validating a protocol using BAN logic consists of four steps: protocol idealization, protocol goal setting, protocol assumption setting, and protocol verification [17]. AKA protocols [9], [15], [38], [60], [60], [78], [109] applied BAN logic to prove that the communication parties achieve mutual authentication and the establishment of a shared key. GBEAKA [28] employed BAN logic to prove that the AKA scheme achieves subscription privacy, unlikability, perfect forward security, confidentiality, integrity, and resistance to replay and impersonation attacks.

3) AVISPA

AVISPA is a formal analysis tool for cryptography protocols [111]. As shown in Figure 10, the input of this tool is codes written in the language of High-Level Protocol Specification Language (HLPSL). This language allows users to describe the properties and behaviors of protocols expressly. After being translated by the HLPSL2IF translator, the codes will run in four verification back-ends. In the AVISPA framework, the adversary in the middle has total control over the network. The AVISPA tool aims to prove that the protocol achieves mutual authentication and is resistant to security attacks. To enable protocol designers to write HLPSL codes more precisely, an animator [112] was designed to provide more supports for AVISPA tool.

4) SCYTHER

Scyther [113] is a tool that combines black-box analysis with formal semantics. It supports a graphical user interface to improve the usability. This analysis tool supports an unbounded number of sessions, parallel execution of multiple

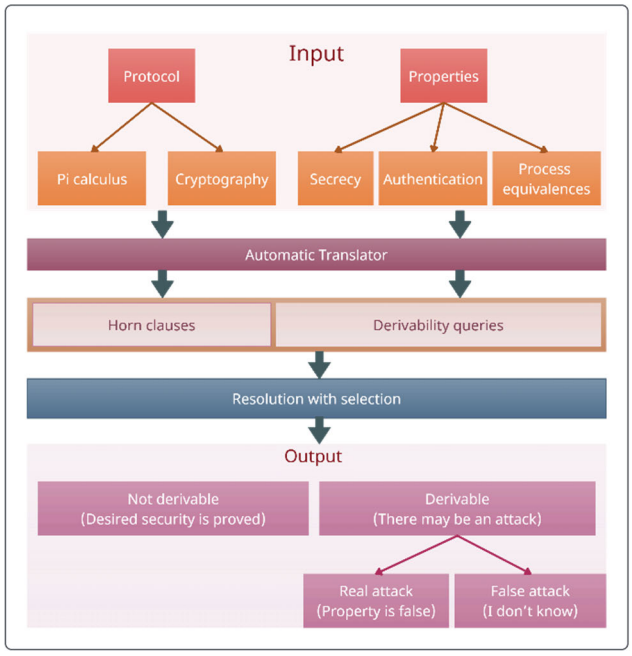


FIGURE 9. Structure of ProVerif [105].

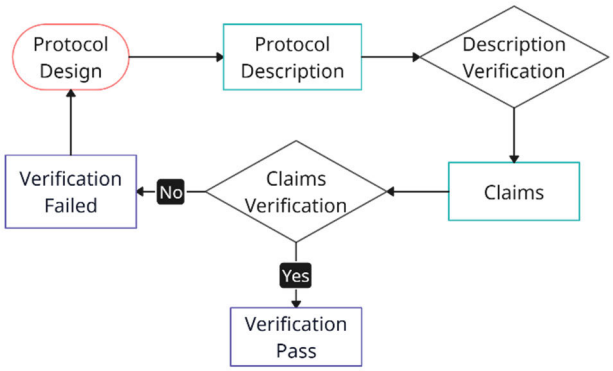


FIGURE 10. Structurer of AVISPA [111].

protocols, and multi-party authentication. The general verification step of the Scyther tool is represented in Figure 11 [27]. Key attributes of Scyther consist of Ni-synch, Ni-agree, Weak-agree, and Alive. Ni-synch ensures that the receiver successfully receives all messages from the sender and follows the protocol requirement. Ni-agree focuses on both parties consistently and accurately understanding the exchanged data Weak-agree provides resilience against impersonation attacks. Alive checks whether the partners are actively communicating with the planned sequence of events. These four claims are applied to detect man-in-the-middle and replay attacks.

5) ROM

ROM [118] is a hypothetical black box to model the ideal hash function as a random function. In this model, it generates random responses for each unique query. The reason behind adopting ROM is the practical limitations of achieving an ideal hash function due to constraints in

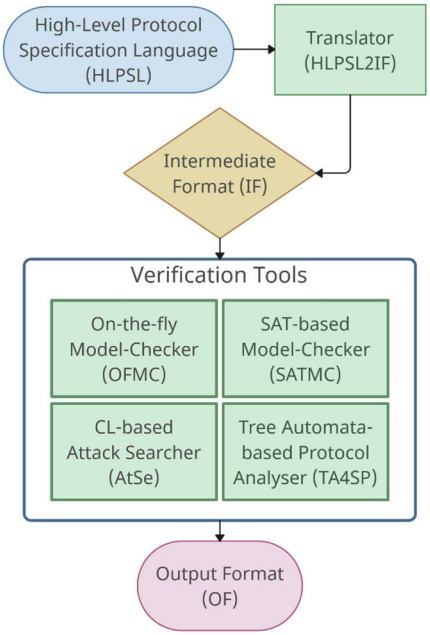


FIGURE 11. Verification steps of Scyther [27].

computational resources and storing capacity. During the protocol verification process under ROM, whenever a party needs to compute a hash function, it will call a third-party function called an oracle. The main principle is to assess whether an adversary can extract useful information from ciphertext within a limited time.

6) ROR

ROR [119] model was proposed by Abdalla et al. and used to analyze the security of encryption schemes. The basic assumption is that the encryption scheme can be considered secure if an adversary does not have a non-negligible advantage in telling the difference between real encryption and a random output produced by an oracle in polynomial time. The advantage of an adversary to win is represented in Eqn. (9) [119]. *SUCC* represents the event that the adversary successfully distinguishes between real and random ciphertext. The operation of rescales of the probabilities to eliminate the influence of simple guesses by an adversary.

$$\mathrm{Adv}_{\mathrm{P,D}}^{\mathrm{ftg-ake}}(\mathrm{A}) = 2\Pr[\mathrm{SUCC}] - 1 \tag{9}$$

D. INFORMAL SECURITY ANALYSIS

While formal analysis provides a rigorous method to prove the security of protocols, informal analysis serves as a supplement, addressing the distinct characteristics brought by AKA protocols. Unlike formal analysis, informal analysis employs a more flexible and responsive approach to evaluate how the protocol resists various security problems. In informal analysis, it is assumed that the attacker has accessed part of the key materials, then to deduce whether the scheme

designed can prevent the attacker from obtaining the shared session key.

As countermeasures against attacks, combining robust cryptographic techniques and encryption methods can enhance the security of AKA scheme designs, as shown in Table 7. The following sections will detail the methods used in recent research to defend against each type of attack.

1) PASSWORD GUESSING ATTACK

Recent advancements in password protection mechanisms have adopted a combination approach, integrating hashing functions with XOR operations. The collision resistance inherent in the hashing function makes it computationally infeasible to find two different inputs that produce the same hash output. The integration of an XOR operation introduces an additional layer of obfuscation. Moreover, implementing a biometric key, as highlighted in a three-factor AKA protocol [74], ensures that even if an attacker acquires the password, the absence of the secret value generated by the fuzzy extractor function makes it unfeasible to derive the pseudo password.

2) STOLEN DEVICE ATTACK

Local data stored in devices is vulnerable to threats posed by stolen device attacks. When a device falls into the hands of an attacker, the data stored in the device will be compromised. Implementing robust local data storage controls is essential to mitigate this risk. Techniques such as employing hash functions and XOR operations can effectively conceal plaintext information [13], [72], [120]. Attackers are unable to extract confidential data without the accurate secret value. To further enhance device security, the login process is a barrier against stolen user mobile device attacks. Without the correct user password or biometric key, attackers are blocked from further communication processes [38], [74]. Suppose the attacker has acquired a session key through a stolen device attack. Updating shared secret values dynamically can ensure each session's uniqueness and prevent the security of other session keys from being compromised [71].

3) IMPERSONATION ATTACK

a: SERVER IMPERSONATION

I n addressing server impersonation threats, a secret random number is generated during the initial phase of a communication session and functions as a unique session identifier. This measure ensures that only a server possessing the correct private key can decrypt the message and subsequently be authenticated by the client [9], [13], [38]. I n contrast, a malicious server lacks this secret random number and primary secret and cannot satisfy the client's verification criteria, effectively terminating further communication attempts.

b: USER IMPERSONATION

The adoption of multifactor authentication is helpful to mitigate user impersonation threats. This approach includes the use of user identification, biometric keys, and passwords [13], [38], [74]. The absence of any of these elements will fail verification processes. Furthermore, one-way collision-resistance hash functions ensure user information. Even when an attacker gains access to hashed data, extracting the underlying user information is impractical. Additionally, the integration of timestamps provides the timeliness of the message, thereby preventing attackers from executing replay attacks to conduct user impersonation attacks [9].

c: EDGE-DEVICES IMPERSONATION

To defend against edge-devices impersonation attacks, a signature-based authentication scheme [59] combined the secret parameters with the DL problem. This method relies on the secrecy of the secret parameters. An attacker can only pass the authentication process by knowing the accurate secret parameters [28], [80].

4) PRIVILEGED INSIDER ATTACK

In addressing privileged insider attacks, an AKA scheme generates unique parameters for each device [71]. These unique parameters establish a distinct set of credentials to ensure each device is independent and unlinked to other devices.

5) MAN IN THE MIDDLE ATTACK

A robust authentication mechanism among communication parties is essential to defend against MitM attacks. Recent research relies on the ECC [23], [80], digital signature [32], the Inverse Computational Diffie–Hellman (ICDH) problem, and the DL problem [22] as methods to mitigate this attack. The security parameters should be deployed in the registration phase using the secured channel in these methods. Only legitimate devices and servers hold the credentials for passing the authentication process [78], [81].

6) MODIFICATION ATTACK

The digital signature is an essential tool to ensure the integrity of the message. An AKA scheme for UAV [22] integrates an identity-based signature with a hash function, ensuring encryption and preventing messages from being tampered with by malicious attackers.

7) DOS ATTACK

Employing lightweight verification processes, such as hash functions and XOR operations, is helpful to safeguard against DOS attacks [38]. The integration of timestamps [80] provides further defense against this attack by verifying the freshness of each request before executing resource-intensive calculations.

8) REPLAY ATTACK

Methods such as timestamps [9], [22], [28], [38], [78], [80], [81] or counters [71] bind with long-term secret key and temporary secret parameters and offer countermeasures for a replay attack. The timestamp or counter ensures the freshness

TABLE 7. Countermeasures provided in the informal analysis.

Attacks	References [13]	[22]	[23]	[38]	[71]	[74]	[80]	[81]
Password guessing	Hash function; XOR operations	-	-	Biometric key	-	Biometric key; Hash function; XOR operations	-	-
Stolen device attack	Local data storage control	-	-	Biometric key; Password	Dynamic update of shared secret parameters	Biometric key; Hash function; XOR operations	-	-
Server impersonation	Pre-shared secret random number; Asymmetric encryption	-	Pre-shared secret value; Hash function; XOR operations	Pre-shared secret random number; Asymmetric encryption	-		-	-
User impersonation	User ID; Password	-	User ID; Hash function; Timestamp	Biometric key; User ID; Password; Hash function	-	Biometric key; Password; Hash function; XOR Operations	-	-
Privileged insider attack	-	-	-	-	Unique parameters; Primary key	-	-	-
DOS attack	-	-	-	Hash Function; Bitwise XOR Operations;	-	-	Timestamp	-
Edge-devices impersonation	-	-	-	-	-	-	ECC; Pre-shared secret value	Secret random parameters; DL problem; Tamper-resistant chip
Man in the middle attack	Hash function; XOR operations; Asymmetric encryption; User ID	ICDH problem; DL problem	Hash function; Timestamp; ECC	Timestamp; Hash function; XOR operations	-	-	ECC; Pre-shared secret value	Pre-shared secret parameters
Modification attack	-	Identity-based signature; Hash function	-	-	-	-	-	-
Replay attack	-	Timestamp	-	Timestamp	Secret random numbers; Counters	-	Timestamp; Secret random parameters; DL problem	Secret random numbers; Timestamps
De-synchronization attack	-	-	-	Secure channel; Real-time update	Counters; Key update	-	-	-
Known provisionally information attack	-	-	ECC; PKG; Hash function	-	Pre-shared secret random number; Hash function; update of secret value	-	Ephemeral key	-
Known session key attack	-	-	Ephemeral key	-	-	-	-	-

-: Not mentioned in the paper.

of each message and prevents the attacker from reusing the message. Additionally, incorporating random secret keys brings unpredictability for messages to enhance security.

9) DE-SYNCHRONIZATION ATTACK

Addressing de-synchronization attacks requires real-time information updates during the authentication scheme. Recent research uses secured communication channels [38], counters, and key updating mechanisms [71] to reduce the risk of de-synchronization attacks.

10) KNOWN PROVISIONALLY INFORMATION ATTACK

A pairing-free AKA scheme [23] describes an approach that integrates ECC with a Private Key Generator (PKG) to counter known providential information attacks. The mechanism is based on the fact that an attacker, without knowing the primary key of the PKG, the compromise of ephemeral keys does not lead to the disclosure of the session key. Furthermore, a symmetric-based AKA scheme [71] utilizes a pre-shared hashed secret value to derive a common shared key. This pre-shared key update after every authentication process enhances the security of the common shared key. As a result, even if an attacker can intercept information on the public channel, deriving the common shared key remains an impracticable task.

11) KNOWN SESSION KEY ATTACK

In addressing the known session key attack, employing temporary keys ensures each communication session is unique [23], [80]. Each session operates with a distinct key to isolate itself from other sessions. As a result, even the compromise of a session key in one communication session will not affect the security of other sessions.

VI. CHALLENGES AND OPPORTUNITIES

Recent research on authentication and key agreement protocols for IoT applications shows the ongoing tension between achieving robust security and maintaining acceptable efficiency. A recurrent theme is the potential of lightweight cryptographic algorithms. By significantly reducing computational overhead, they allow for the preservation of device resources while maintaining acceptable levels of security. However, choosing the right lightweight cryptography solution requires considering the specific application, its security requirements, and the resource constraints of the involved end devices. Furthermore, utilizing hybrid cryptographic techniques, leveraging the benefits of symmetric encryption with the high security provided by asymmetric encryption, thus offering a balanced solution. The increased application of authentication measures, such as biometrics and multi-factor authentication, underscores the industry's effort to enhance security without compromising usability. These strategies, however, are not devoid of their potential pitfalls. Incorporating biometrics introduces a new array of data security concerns, particularly regarding data privacy and the potential misuse of biometric information. Similarly, multi-factor authentication, while adding an additional layer of security, could inadvertently create new vulnerabilities if not implemented with care and diligence.

VII. CONCLUSION

The extensive literature review carried out in this study has elucidated the current state of research on authentication and key agreement protocols within the Internet of Things applications. With the accelerating growth of IoT and its increasing integration into our daily lives, it is paramount to ensure IoT networks' security. The paper identifies various types of IoT applications that require authentication and key agreement mechanisms. It is clear from our analysis that these mechanisms need to be tailored to suit the specific needs and resource constraints of each IoT context. Additionally, we delve into advanced cryptographic technologies and solutions currently employed in these mechanisms. Moreover, we explore the potential threats that IoT applications face and the security analysis tools to mitigate these risks. Securing IoT networks is one of the top research challenges and priorities for various significant applications. This paper presents the latest resources on authentication and key agreement fundamentals, protocols, and mechanisms to update the research communities for securing a sustainable IoT landscape

REFERENCES

[1] D. Miorandi, S. Sicari, F. De Pellegrini, and I. Chlamtac, "Internet of Things: Vision, applications and research challenges," *Ad Hoc Netw.*, vol. 10, no. 7, pp. 1497–1516, Sep. 2012, doi: 10.1016/j.adhoc.2012.02.016.

[2] K. Ashton, "That 'Internet of Things' thing," *RFID J.*, vol. 22, no. 7, pp. 97–114, 2009.

[3] R. M. Needham and M. D. Schroeder, "Using encryption for authentication in large networks of computers," *Commun. ACM*, vol. 21, no. 12, pp. 993–999, Dec. 1978, doi: 10.1145/359657.359659.

[4] R. Praveen and P. Pabitha, "Improved Gentry–Halevi's fully homomorphic encryption-based lightweight privacy preserving scheme for securing medical Internet of Things," *Trans. Emerg. Telecommun. Technol.*, vol. 34, no. 4, p. e4732, Apr. 2023, doi: 10.1002/ett.4732.

[5] A. A. Al-saggaf, T. Sheltami, H. Alkhzaimi, and G. Ahmed, "Lightweight two-factor-based user authentication protocol for IoT-enabled healthcare ecosystem in quantum computing," *Arabian J. Sci. Eng.*, vol. 48, no. 2, pp. 2347–2357, Feb. 2023, doi: 10.1007/s13369-022-07235-0.

[6] C. Hsu, L. Harn, Z. Xia, Z. Zhao, and H. Xu, "Fast and lightweight authenticated group key agreement realizing privacy protection for resource-constrained IoMT," *Wireless Pers. Commun.*, vol. 129, no. 4, pp. 2403–2417, Apr. 2023, doi: 10.1007/s11277-023-10239-0.

[7] S. Kumar, H. Banka, and B. Kaushik, "Ultra-lightweight blockchain-enabled RFID authentication protocol for supply chain in the domain of 5G mobile edge computing," *Wireless Netw.*, vol. 29, no. 5, pp. 2105–2126, Feb. 2023, doi: 10.1007/s11276-023-03234-7.

[8] A. S. Khan, M. I. B. Yahya, K. B. Zen, J. B. Abdullah, R. B. A. Rashid, Y. Javed, N. A. Khan, and A. M. Mostafa, "Blockchain-based lightweight multifactor authentication for cell-free in ultra-dense 6G-based (6-CMAS) cellular network," *IEEE Access*, vol. 11, pp. 20524–20541, 2023, doi: 10.1109/ACCESS.2023.3249969.

[9] A. Ben Amor, S. Jebri, M. Abid, and A. Meddeb, "A secure lightweight mutual authentication scheme in social industrial IoT environment," *J. Supercomput.*, vol. 79, no. 12, pp. 13578–13600, Mar. 2023, doi: 10.1007/s11227-023-05176-5.

[10] F. Wu, L. Xu, S. Kumari, X. Li, A. K. Das, and J. Shen, "A lightweight and anonymous RFID tag authentication protocol with cloud assistance for e-healthcare applications," *J. Ambient Intell. Humanized Comput.*, vol. 9, no. 4, pp. 919–930, Aug. 2018, doi: 10.1007/s12652-017-0485-5.

[11] B. Gong, G. Zheng, M. Waqas, S. Tu, and S. Chen, "LCDMA: Lightweight cross-domain mutual identity authentication scheme for Internet of Things," *IEEE Internet Things J.*, vol 10, no. 14, pp. 12590–12602, 2023, doi: 10.1109/JIOT.2023.3252051.

[12] W. Hou, Y. Sun, D. Li, Z. Guan, and J. Liu, "Lightweight and privacy-preserving charging reservation authentication protocol for 5G-V2G," *IEEE Trans. Veh. Technol.*, vol. 72, no. 6, pp. 7871–7883, 2023, doi: 10.1109/TVT.2023.3241324.

[13] D. Chaudhary, T. Soni, K. L. Vasudev, and K. Saleem, "A modified lightweight authenticated key agreement protocol for Internet of Drones," *Internet Things*, vol. 21, Apr. 2023, Art. no. 100669, doi: 10.1016/j.iot.2022.100669.

[14] B. D. Deebak and F. Al-Turjman, "A smart lightweight privacy preservation scheme for IoT-based UAV communication systems," *Comput. Commun.*, vol. 162, pp. 102–117, Oct. 2020, doi: 10.1016/j.comcom.2020.08.016.

[15] R. Krishnasrija, A. K. Mandal, and A. Cortesi, "A lightweight mutual and transitive authentication mechanism for IoT network," *Ad Hoc Netw.*, vol. 138, Jan. 2023, Art. no. 103003, doi: 10.1016/j.adhoc.2022.103003.

[16] Z. Ashraf, A. Sohail, and M. Yousaf, "Robust and lightweight symmetric key exchange algorithm for next-generation IoE," *Internet Things*, vol. 22, Jul. 2023, Art. no. 100703, doi: 10.1016/j.iot.2023.100703.

[17] P. Borgohain and H. Choudhury, "A lightweight D2D authentication protocol for relay coverage scenario in 5G mobile network," *Comput. Netw.*, vol. 225, Apr. 2023, Art. no. 109679, doi: 10.1016/j.comnet.2023.109679.

[18] S. Amanlou, M. K. Hasan, and K. A. A. Bakar, "Lightweight and secure authentication scheme for IoT network based on publish-subscribe fog computing model," *Comput. Netw.*, vol. 199, Nov. 2021, Art. no. 108465, doi: 10.1016/j.comnet.2021.108465.

[19] M. Abdussami, R. Amin, and S. Vollala, "Provably secured lightweight authenticated key agreement protocol for modern health industry," *Ad Hoc Netw.*, vol. 141, Mar. 2023, Art. no. 103094, doi: 10.1016/j.adhoc.2023.103094.

[20] Q. Jiang, S. Zeadally, J. Ma, and D. He, "Lightweight three-factor authentication and key agreement protocol for Internet-integrated wireless sensor networks," *IEEE Access*, vol. 5, pp. 3376–3392, 2017, doi: 10.1109/ACCESS.2017.2673239.

[21] Y. Chen, L. López, J.-F. Martínez, and P. Castillejo, "A lightweight privacy protection user authentication and key agreement scheme tailored for the Internet of Things environment: LightPriAuth," *J. Sensors*, vol. 2018, Sep. 2018, Art. no. e7574238, doi: 10.1155/2018/7574238.

[22] X. Pan, Y. Jin, and F. Li, "An efficient heterogeneous authenticated key agreement scheme for unmanned aerial vehicles," *J. Syst. Archit.*, vol. 136, Mar. 2023, Art. no. 102821, doi: 10.1016/j.sysarc.2022.102821.

[23] P. Verma and D. S. Gupta, "A pairing-free data authentication and aggregation mechanism for intelligent healthcare system," *Comput. Commun.*, vol. 198, pp. 282–296, Jan. 2023, doi: 10.1016/j.comcom.2022.12.009.

[24] J.-L. Tsai and N.-W. Lo, "Secure anonymous key distribution scheme for smart grid," *IEEE Trans. Smart Grid*, vol. 7, no. 2, pp. 906–914, Mar. 2016, doi: 10.1109/TSG.2015.2440658.

[25] L. Chen, J. Zhou, Y. Chen, Z. Cao, X. Dong, and K. R. Choo, "PADP: Efficient privacy-preserving data aggregation and dynamic pricing for vehicle-to-grid networks," *IEEE Internet Things J.*, vol. 8, no. 10, pp. 7863–7873, May 2021, doi: 10.1109/JIOT.2020.3041117.

[26] W. Yuan, X. Li, M. Li, and L. Zheng, "DCAGS-IoT: Dynamic cross-domain authentication scheme using group signature in IoT," *Appl. Sci.*, vol. 13, no. 10, p. 5847, May 2023, doi: 10.3390/app13105847.

[27] M. A. Mobarhan and M. Salamah, "REPS-AKA5: A robust group-based authentication protocol for IoT applications in LTE system," *Internet Things*, vol. 22, Jul. 2023, Art. no. 100700, doi: 10.1016/j.iot.2023.100700.

[28] G. Singh, "GBEAKA: Group-based efficient authentication and key agreement protocol for LPIoMT using 5G," *Internet Things*, vol. 22, Jul. 2023, Art. no. 100688, doi: 10.1016/j.iot.2023.100688.

[29] Z. Yang, Z. Wang, F. Qiu, and F. Li, "A group key agreement protocol based on ECDH and short signature," *J. Inf. Secur. Appl.*, vol. 72, Feb. 2023, Art. no. 103388, doi: 10.1016/j.jisa.2022.103388.

[30] W. Ali and A. Ahmed, "An authenticated group shared key mechanism based on a combiner for hash functions over the industrial Internet of Things," *Processes*, vol. 11, no. 5, p. 1558, May 2023, doi: 10.3390/pr11051558.

[31] M. Soni and D. K. Singh, "Blockchain-based group authentication scheme for 6G communication network," *Phys. Commun.*, vol. 57, Apr. 2023, Art. no. 102005, doi: 10.1016/j.phycom.2023.102005.

[32] C. Trivedi and U. P. Rao, "Secrecy aware key management scheme for Internet of Healthcare Things," *J. Supercomput.*, vol. 79, no. 11, pp. 12492–12522, Mar. 2023, doi: 10.1007/s11227-023-05144-z.

[33] J. Liu, J. Xie, J. Zhang, B. Liu, X. Chen, and H. Feng, "A secure secret key agreement scheme among multiple twinning superlattice PUF holders," *Sensors*, vol. 23, no. 10, p. 4704, May 2023, doi: 10.3390/s23104704.

[34] R. Subrahmanyam, N. R. Rekha, and Y. V. S. Rao, "Authenticated distributed group key agreement protocol using elliptic curve secret sharing scheme," *IEEE Access*, vol. 11, pp. 45243–45254, 2023, doi: 10.1109/ACCESS.2023.3274468.

[35] H. Tan, "An efficient IoT group association and data sharing mechanism in edge computing paradigm," *Cyber Secur. Appl.*, vol. 1, Dec. 2023, Art. no. 100003, doi: 10.1016/j.csa.2022.100003.

[36] A. Altameem, P. Prabu, T. Senthilnathan, R. C. Poonia, and A. K. J. Saudagar, "A hybrid AES with a chaotic map-based biometric authentication framework for IoT and Industry 4.0," *Systems*, vol. 11, no. 1, p. 28, Jan. 2023, doi: 10.3390/systems11010028.

[37] V. O. Nyangaresi, "Privacy preserving three-factor authentication protocol for secure message forwarding in wireless body area networks," *Ad Hoc Netw.*, vol. 142, Apr. 2023, Art. no. 103117, doi: 10.1016/j.adhoc.2023.103117.

[38] H. Xu, C. Hsu, L. Harn, J. Cui, Z. Zhao, and Z. Zhang, "Three-factor anonymous authentication and key agreement based on fuzzy biological extraction for industrial Internet of Things," *IEEE Trans. Services Comput.*, vol.16, no.4, pp. 3000–3013, 2023, doi: 10.1109/TSC.2023.3257569.

[39] R. M. A. Haseeb-Ur-Rehman, M. Liaqat, A. H. M. Aman, A. A. Almazroi, M. K. Hasan, Z. Ali, and R. L. Ali, "LR-AKAP: A lightweight and robust security protocol for smart home environments," *Sensors*, vol. 22, no. 18, p. 6902, Sep. 2022, doi: 10.3390/s22186902.

[40] A. Braeken, "Highly efficient bidirectional multi-factor authentication and key agreement for real-time access to sensor data," *IEEE Internet Things J.*, vol.10, no. 23, pp. 21089–21099, 2023, doi: 10.1109/JIOT.2023.3284501.

[41] T.-V. Le, "Cross-server end-to-end patient key agreement protocol for DNA-based U-healthcare in the Internet of Living Things," *Mathematics*, vol. 11, no. 7, p. 1638, Mar. 2023, doi: 10.3390/math11071638.

[42] B. Khalid, K. N. Qureshi, K. Z. Ghafoor, and G. Jeon, "An improved biometric based user authentication and key agreement scheme for intelligent sensor based wireless communication," *Microprocessors Microsyst.*, vol. 96, Feb. 2023, Art. no. 104722, doi: 10.1016/j.micpro.2022.104722.

[43] M. Savitha and M. Senthilkumar, "A unique secure multimodal biometrics-based user anonymous authenticated key management protocol (SMUAAKAP) based on block chain mechanism for generic HIoTNs," *Theor. Comput. Sci.*, vol. 941, pp. 77–90, Jan. 2023, doi: 10.1016/j.tcs.2022.09.020.

[44] K. Kim, J. Ryu, Y. Lee, and D. Won, "An improved lightweight user authentication scheme for the Internet of Medical Things," *Sensors*, vol. 23, no. 3, p. 1122, Jan. 2023, doi: 10.3390/s23031122.

[45] C.-W. Lien and S. Vhaduri, "Challenges and opportunities of biometric user authentication in the age of IoT: A survey," *ACM Comput. Surv.*, vol. 56, no. 1, pp. 1–37, Jan. 2024, doi: 10.1145/3603705.

[46] S. L. Nita and M. I. Mihailescu, "Elliptic curve-based query authentication protocol for IoT devices aided by blockchain," *Sensors*, vol. 23, no. 3, p. 1371, Jan. 2023, doi: 10.3390/s23031371.

[47] A. Kumar, R. Saha, M. Conti, G. Kumar, W. J. Buchanan, and T. H. Kim, "A comprehensive survey of authentication methods in Internet-of-Things and its conjunctions," *J. Netw. Comput. Appl.*, vol. 204, Aug. 2022, Art. no. 103414, doi: 10.1016/j.jnca.2022.103414.

[48] X. Li, T. Chen, Q. Cheng, S. Ma, and J. Ma, "Smart applications in edge computing: Overview on authentication and data security," *IEEE Internet Things J.*, vol. 8, no. 6, pp. 4063–4080, Mar. 2021, doi: 10.1109/JIOT.2020.3019297.

[49] F. H. Al-Naji and R. Zagrouba, "A survey on continuous authentication methods in Internet of Things environment," *Comput. Commun.*, vol. 163, pp. 109–133, Nov. 2020, doi: 10.1016/j.comcom.2020.09.006.

[50] M. Saqib and A. H. Moon, "A systematic security assessment and review of Internet of Things in the context of authentication," *Comput. Secur.*, vol. 125, Feb. 2023, Art. no. 103053, doi: 10.1016/j.cose.2022.103053.

[51] B. Narwal and A. K. Mohapatra, "A survey on security and authentication in wireless body area networks," *J. Syst. Archit.*, vol. 113, Feb. 2021, Art. no. 101883, doi: 10.1016/j.sysarc.2020.101883.

[52] M. El-hajj, A. Fadlallah, M. Chamoun, and A. Serhrouchni, "A survey of Internet of Things (IoT) authentication schemes," *Sensors*, vol. 19, no. 5, p. 1141, Mar. 2019, doi: 10.3390/s19051141.

[53] S. K. S. V. Naga, R. Yesuraj, S. Munuswamy, and K. Arputharaj, "A comprehensive survey on certificate-less authentication schemes for vehicular ad hoc networks in intelligent transportation systems," *Sensors*, vol. 23, no. 5, p. 2682, Mar. 2023, doi: 10.3390/s23052682.

[54] M. Chen, Y. Miao, Y. Hao, and K. Hwang, "Narrow band Internet of Things," *IEEE Access*, vol. 5, pp. 20557–20577, 2017, doi: 10.1109/ACCESS.2017.2751586.

[55] A. Rauf, R. A. Shaikh, and A. Shah, "Security and privacy for IoT and fog computing paradigm," in *Proc. 15th Learn. Technol. Conf. (L&T)*, Feb. 2018, pp. 96–101, doi: 10.1109/LT.2018.8368491.

[56] A. Zanella, N. Bui, A. Castellani, L. Vangelista, and M. Zorzi, "Internet of Things for smart cities," *IEEE Internet Things J.*, vol. 1, no. 1, pp. 22–32, Feb. 2014, doi: 10.1109/JIOT.2014.2306328.

[57] W. Yan, Z. Wang, H. Wang, W. Wang, J. Li, and X. Gui, "Survey on recent smart gateways for smart home: Systems, technologies, and challenges," *Trans. Emerg. Telecommun. Technol.*, vol. 33, no. 6, Jun. 2022, doi: 10.1002/ett.4067.

[58] M. Hussin and R. A. Raja Mahmood, "Privacy based classification model of public data by utilizing two-steps validation approach," *Asia–Pacific J. Inf. Technol. Multimedia*, vol. 11, no. 2, pp. 123–132, Dec. 2022, doi: 10.17576/apjitm-2022-1102-10.

[59] Q. Ma, H. Tan, and T. Zhou, "Mutual authentication scheme for smart devices in IoT-enabled smart home systems," *Comput. Standards Inter.*, vol. 86, Aug. 2023, Art. no. 103743, doi: 10.1016/j.csi.2023.103743.

[60] W. Iqbal, H. Abbas, P. Deng, J. Wan, B. Rauf, Y. Abbas, and I. Rashid, "ALAM: Anonymous lightweight authentication mechanism for SDN-enabled smart homes," *IEEE Internet Things J.*, vol. 8, no. 12, pp. 9622–9633, Jun. 2021, doi: 10.1109/JIOT.2020.3024058.

[61] X. Xu, Y. Guo, and Y. Guo, "Fog-enabled private blockchain-based identity authentication scheme for smart home," *Comput. Commun.*, vol. 205, pp. 58–68, May 2023, doi: 10.1016/j.comcom.2023.04.005.

[62] R. Hassan, F. Qamar, M. K. Hasan, A. H. M. Aman, and A. S. Ahmed, "Internet of Things and its applications: A comprehensive survey," *Symmetry*, vol. 12, no. 10, p. 1674, Oct. 2020, doi: 10.3390/sym12101674.

[63] R. Sanchez-Iborra and M.-D. Cano, "State of the art in LP-WAN solutions for industrial IoT services," *Sensors*, vol. 16, no. 5, p. 708, May 2016, doi: 10.3390/s16050708.

[64] J. Al-Jaroodi and N. Mohamed, "Blockchain in industries: A survey," *IEEE Access*, vol. 7, pp. 36500–36515, 2019, doi: 10.1109/ACCESS.2019.2903554.

[65] M. Younan, E. H. Houssein, M. Elhoseny, and A. A. Ali, "Challenges and recommended technologies for the industrial Internet of Things: A comprehensive review," *Measurement*, vol. 151, Feb. 2020, Art. no. 107198, doi: 10.1016/j.measurement.2019.107198.

[66] J. Cui, F. Cheng, H. Zhong, Q. Zhang, C. Gu, and L. Liu, "Multi-factor based session secret key agreement for the industrial Internet of Things," *Ad Hoc Netw.*, vol. 138, Jan. 2023, Art. no. 102997, doi: 10.1016/j.adhoc.2022.102997.

[67] S. Itoo, M. Ahmad, V. Kumar, and A. Alkhayyat, "RKMIS: Robust key management protocol for industrial sensor network system," *J. Supercomput.*, vol. 79, no. 9, pp. 9837–9865, Jun. 2023, doi: 10.1007/s11227-022-05041-x.

[68] Y. Zhang, D. He, P. Vijayakumar, M. Luo, and X. Huang, "SAPFS: An efficient symmetric-key authentication key agreement scheme with perfect forward secrecy for industrial Internet of Things," *IEEE Internet Things J.*, vol. 10, no. 11, pp. 9716–9726, Jun. 2023, doi: 10.1109/JIOT.2023.3234178.

[69] K. Wu, J. Zhang, X. Jiang, R. Cheng, X. Zhang, and J. Tong, "An efficient and provably secure certificateless protocol for the power Internet of Things," *Alexandria Eng. J.*, vol. 70, pp. 411–422, May 2023, doi: 10.1016/j.aej.2023.02.033.

[70] H. Gupta, A. Vahid Dastjerdi, S. K. Ghosh, and R. Buyya, "IFogSim: A toolkit for modeling and simulation of resource management techniques in the Internet of Things, edge and fog computing environments," *Software: Pract. Exper.*, vol. 47, no. 9, pp. 1275–1296, Sep. 2017, doi: 10.1002/spe.2509.

[71] A. K. Yadav, A. Braeken, and M. Misra, "Symmetric key-based authentication and key agreement scheme resistant against semi-trusted third party for fog and dew computing," *J. Supercomput.*, vol. 79, no. 10, pp. 11261–11299, Jul. 2023, doi: 10.1007/s11227-023-05064-y.

[72] M. Rana, K. Mahmood, M. A. Saleem, F. Al-Turjman, M. S. Kolhar, and C. Altrjman, "Towards a provably secure authentication protocol for fog-driven IoT-based systems," *Appl. Sci.*, vol. 13, no. 3, p. 1424, Jan. 2023, doi: 10.3390/app13031424.

[73] A. Hussain, R. Wenbi, A. L. da Silva, M. Nadher, and M. Mudhish, "Health and emergency-care platform for the elderly and disabled people in the smart city," *J. Syst. Softw.*, vol. 110, pp. 253–263, Dec. 2015, doi: 10.1016/j.jss.2015.08.041.

[74] C.-M. Chen, S. Liu, X. Li, S. H. Islam, and A. K. Das, "A provably-secure authenticated key agreement protocol for remote patient monitoring IoMT," *J. Syst. Archit.*, vol. 136, Mar. 2023, Art. no. 102831, doi: 10.1016/j.sysarc.2023.102831.

[75] S. M. R. Islam, D. Kwak, M. H. Kabir, M. Hossain, and K.-S. Kwak, "The Internet of Things for health care: A comprehensive survey," *IEEE Access*, vol. 3, pp. 678–708, 2015, doi: 10.1109/ACCESS.2015.2437951.

[76] A. Rejeb, K. Rejeb, H. Treiblmaier, A. Appolloni, S. Alghamdi, Y. Alhasawi, and M. Iranmanesh, "The Internet of Things (IoT) in healthcare: Taking stock and moving forward," *Internet Things*, vol. 22, Jul. 2023, Art. no. 100721, doi: 10.1016/j.iot.2023.100721.

[77] M. Li, S. Yu, N. Cao, and W. Lou, "Authorized private keyword search over encrypted data in cloud computing," in *Proc. 31st Int. Conf. Distrib. Comput. Syst.*, Jun. 2011, pp. 383–392, doi: 10.1109/ICDCS.2011.55.

[78] Y. Ma, Y. Ma, Y. Liu, and Q. Cheng, "A secure and efficient certificateless authenticated key agreement protocol for smart healthcare," *Comput. Standards Inter.*, vol. 86, Aug. 2023, Art. no. 103735, doi: 10.1016/j.csi.2023.103735.

[79] Y. Zhang, D. He, L. Li, and B. Chen, "A lightweight authentication and key agreement scheme for Internet of Drones," *Comput. Commun.*, vol. 154, pp. 455–464, Mar. 2020, doi: 10.1016/j.comcom.2020.02.067.

[80] S. Chai, H. Yin, B. Xing, Z. Li, Y. Guo, D. Zhang, X. Zhang, D. He, J. Zhang, X. Yu, W. Wang, and X. Huang, "Provably secure and lightweight authentication key agreement scheme for smart meters," *IEEE Trans. Smart Grid*, vol. 14, no. 5, pp. 3816–3827, 2023, doi: 10.1109/TSG.2023.3234000.

[81] C. Patel, A. K. Bashir, A. A. AlZubi, and R. Jhaveri, "EBAKE-SE: A novel ECC-based authenticated key exchange between industrial IoT devices using secure element," *Digit. Commun. Netw.*, vol. 9, no. 2, pp. 358–366, Apr. 2023, doi: 10.1016/j.dcan.2022.11.001.

[82] S. Ullah, J. Zheng, N. Din, M. T. Hussain, F. Ullah, and M. Yousaf, "Elliptic curve cryptography; applications, challenges, recent advances, and future trends: A comprehensive survey," *Comput. Sci. Rev.*, vol. 47, Feb. 2023, Art. no. 100530, doi: 10.1016/j.cosrev.2022.100530.

[83] A. Joux, "A one round protocol for tripartite Diffie–Hellman," in *Algorithmic Number Theory* (Lecture Notes in Computer Science), W. Bosma, Ed. Berlin, Germany: Springer, 2000, pp. 385–393, doi: 10.1007/10722028_23.

[84] D. Boneh and M. Franklin, "Identity-based encryption from the Weil pairing," in *Advances in Cryptology—CRYPTO 2001* (Lecture Notes in Computer Science), J. Kilian, Ed. Berlin, Germany: Springer, 2001, pp. 213–229, doi: 10.1007/3-540-44647-8_13.

[85] A. K. Das, "A secure and effective biometric-based user authentication scheme for wireless sensor networks using smart card and fuzzy extractor," *Int. J. Commun. Syst.*, vol. 30, no. 1, p. e2933, Jan. 2017, doi: 10.1002/dac.2933.

[86] Y. Dodis, L. Reyzin, and A. Smith, "Fuzzy extractors: How to generate strong keys from biometrics and other noisy data," in *Advances in Cryptology—EUROCRYPT 2004* (Lecture Notes in Computer Science), C. Cachin and J. L. Camenisch, Eds. Berlin, Germany: Springer, 2004, pp. 523–540, doi: 10.1007/978-3-540-24676-3_31.

[87] D. R. Stinson, "Some observations on the theory of cryptographic hash functions," *Des., Codes Cryptogr.*, vol. 38, no. 2, pp. 259–277, Feb. 2006, doi: 10.1007/s10623-005-6344-y.

[88] M. A. A. da Cruz, J. J. P. C. Rodrigues, P. Lorenz, V. V. Korotaev, and V. H. C. de Albuquerque, "In.IoT—A new middleware for Internet of Things," *IEEE Internet Things J.*, vol. 8, no. 10, pp. 7902–7911, May 2021, doi: 10.1109/JIOT.2020.3041699.

[89] P. J. Franks, "HTTP authentication: Basic and digest access authentication," Internet Eng. Task Force, Fremont, CA, USA, Tech. Rep. RFC 2617, 1999, doi: 10.17487/RFC2617.

[90] E. B. Sanjuan, I. A. Cardiel, J. A. Cerrada, and C. Cerrada, "Message queuing telemetry transport (MQTT) security: A cryptographic smart card approach," *IEEE Access*, vol. 8, pp. 115051–115062, 2020, doi: 10.1109/ACCESS.2020.3003998.

[91] I. L. B. M. Paris, M. H. Habaebi, and A. M. Zyoud, "Implementation of SSL/TLS security with MQTT protocol in IoT environment," *Wireless Pers. Commun.*, vol. 132, no. 1, pp. 163–182, Sep. 2023, doi: 10.1007/s11277-023-10605-y.

[92] S. Tian and V. G. Vassilakis, "On the efficiency of a lightweight authentication and privacy preservation scheme for MQTT," *Electronics*, vol. 12, no. 14, p. 3085, Jul. 2023, doi: 10.3390/electronics12143085.

[93] A. J. Hintaw, S. Manickam, S. Karuppayah, M. A. Aladaileh, M. F. Aboalmaaly, and S. U. A. Laghari, "A robust security scheme based on enhanced symmetric algorithm for MQTT in the Internet of Things," *IEEE Access*, vol. 11, pp. 43019–43040, 2023, doi: 10.1109/ACCESS.2023.3267718.

[94] Ö. Şeker, G. Dalkılıç, and U. C. Çabuk, "MARAS: Mutual authentication and role-based authorization scheme for lightweight Internet of Things applications," *Sensors*, vol. 23, no. 12, p. 5674, Jun. 2023, doi: 10.3390/s23125674.

[95] R. Salles and R. Farias, "TLS protocol analysis using IoTST—An IoT benchmark based on scheduler traces," *Sensors*, vol. 23, no. 5, p. 2538, Feb. 2023, doi: 10.3390/s23052538.

[96] L. Năstase, I. E. Sandu, and N. Popescu, "An experimental evaluation of application layer protocols for the Internet of Things," *Stud. Informat. Control*, vol. 26, no. 4, pp. 403–412, Dec. 2017, doi: 10.24846/v26i4y201704.

[97] C. Gao, G. Wang, W. Shi, Z. Wang, and Y. Chen, "Autonomous driving security: State of the art and challenges," *IEEE Internet Things J.*, vol. 9, no. 10, pp. 7572–7595, May 2022, doi: 10.1109/JIOT.2021.3130054.

[98] Websockets. *Authentication*. Accessed: Oct. 16, 2023. [Online]. Available: https://websockets.readthedocs.io/en/stable/topics/authentication.html

[99] P. M. Rao and B. D. Deebak, "A comprehensive survey on authentication and secure key management in Internet of Things: Challenges, countermeasures, and future directions," *Ad Hoc Netw.*, vol. 146, Jul. 2023, Art. no. 103159, doi: 10.1016/j.adhoc.2023.103159.

[100] F. Marino, C. Moiso, and M. Petracca, "Automatic contract negotiation, service discovery and mutual authentication solutions: A survey on the enabling technologies of the forthcoming IoT ecosystems," *Comput. Netw.*, vol. 148, pp. 176–195, Jan. 2019, doi: 10.1016/j.comnet.2018.11.011.

[101] P. Jayalaxmi, R. Saha, G. Kumar, N. Kumar, and T.-H. Kim, "A taxonomy of security issues in industrial Internet-of-Things: Scoping review for existing solutions, future implications, and research challenges," *IEEE Access*, vol. 9, pp. 25344–25359, 2021, doi: 10.1109/ACCESS.2021.3057766.

[102] F. F. Ashrif, E. A. Sundararajan, R. Ahmad, M. K. Hasan, and E. Yadegaridehkordi, "Survey on the authentication and key agreement of 6LoWPAN: Open issues and future direction," *J. Netw. Comput. Appl.*, vol. 221, Jan. 2024, Art. no. 103759, doi: 10.1016/j.jnca.2023.103759.

[103] O. S. M. B. H. Almazrouei, P. Magalingam, M. K. Hasan, and M. Shanmugam, "A review on attack graph analysis for IoT vulnerability assessment: Challenges, open issues, and future directions," *IEEE Access*, vol. 11, pp. 44350–44376, 2023, doi: 10.1109/ACCESS.2023.3272053.

[104] M. M. Shtayat, M. K. Hasan, R. Sulaiman, S. Islam, and A. U. R. Khan, "An explainable ensemble deep learning approach for intrusion detection in industrial Internet of Things," *IEEE Access*, vol. 11, pp. 115047–115061, 2023, doi: 10.1109/ACCESS.2023.3323573.

[105] A. A. Hamza, I. T. A. Halim, M. A. Sobh, and A. M. Bahaa-Eldin, "HSAS-MD analyzer: A hybrid security analysis system using model-checking technique and deep learning for malware detection in IoT apps," *Sensors*, vol. 22, no. 3, p. 1079, Jan. 2022, doi: 10.3390/s22031079.

[106] B. Blanchet, "Symbolic and computational mechanized verification of the ARINC823 avionic protocols," in *Proc. IEEE 30th Comput. Secur. Found. Symp. (CSF)*, Aug. 2017, pp. 68–82, doi: 10.1109/CSF.2017.7.

[107] B. Blanchet, "Modeling and verifying security protocols with the applied pi calculus and ProVerif," *Found. Trends Privacy Secur.*, vol. 1, nos. 1–2, pp. 1–135, Oct. 2016, doi: 10.1561/3300000004.

[108] B. Blanchet, "The security protocol verifier ProVerif and its horn clause resolution algorithm," *Electron. Proc. Theor. Comput. Sci.*, vol. 373, pp. 14–22, Nov. 2022, doi: 10.4204/eptcs.373.2.

[109] C. Wang, D. Wang, Y. Duan, and X. Tao, "Secure and lightweight user authentication scheme for cloud-assisted Internet of Things," *IEEE Trans. Inf. Forensics Security*, vol. 18, pp. 2961–2976, 2023, doi: 10.1109/TIFS.2023.3272772.

[110] M. Burrows, M. Abadi, and R. Needham, "A logic of authentication," *ACM Trans. Comput. Syst.*, vol. 8, no. 1, pp. 18–36, Feb. 1990, doi: 10.1145/77648.77649.

[111] D. von Oheimb, "The high-level protocol specification language HLPSL developed in the EU project AVISPA," in *Proc. APPSEM Workshop*, Jan. 2005, pp. 1–7.

[112] Y. Glouche, T. Genet, O. Heen, and O. Courtay, "A security protocol animator tool for AVISPA," in *Proc. Artist Secur. Workshop*, Jan. 2006, pp. 414–418.

[113] C. J. F. Cremers, "The Scyther tool: Verification, falsification, and analysis of security protocols," in *Computer Aided Verification* (Lecture Notes in Computer Science), A. Gupta and S. Malik, Eds. Berlin, Germany: Springer, 2008, pp. 414–418, doi: 10.1007/978-3-540-70545-1_38.

[114] Z. Chen, Z. Cheng, W. Luo, J. Ao, Y. Liu, K. Sheng, and L. Chen, "FSMFA: Efficient firmware-secure multi-factor authentication protocol for IoT devices," *Internet Things*, vol. 21, Apr. 2023, Art. no. 100685, doi: 10.1016/j.iot.2023.100685.

[115] J. Ryu, H. Lee, H. Kim, and D. Won, "Secure and efficient three-factor protocol for wireless sensor networks," *Sensors*, vol. 18, no. 12, p. 4481, Dec. 2018, doi: 10.3390/s18124481.

[116] A. A. Ahmed, S. J. Malebary, W. Ali, and A. A. Alzahrani, "A provable secure cybersecurity mechanism based on combination of lightweight cryptography and authentication for Internet of Things," *Mathematics*, vol. 11, no. 1, p. 220, Jan. 2023, doi: 10.3390/math11010220.

[117] R. Kumar, S. Singh, and P. K. Singh, "A secure and efficient computation based multifactor authentication scheme for intelligent IoT-enabled WSNs," *Comput. Electr. Eng.*, vol. 105, Jan. 2023, Art. no. 108495, doi: 10.1016/j.compeleceng.2022.108495.

[118] M. Bellare and P. Rogaway, "Random oracles are practical: A paradigm for designing efficient protocols," in *Proc. 1st ACM Conf. Comput. Commun. Secur.* New York, NY, USA: Association for Computing Machinery, Dec. 1993, pp. 62–73, doi: 10.1145/168588.168596.

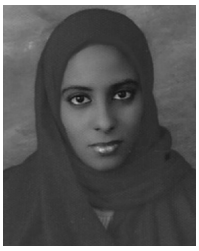
[119] M. Abdalla, P.-A. Fouque, and D. Pointcheval, "Password-based authenticated key exchange in the three-party setting," in *Public Key Cryptography—PKC 2005* (Lecture Notes in Computer Science), S. Vaudenay, Ed. Berlin, Germany: Springer, 2005, pp. 65–84, doi: 10.1007/978-3-540-30580-4_6.

[120] M. Hammad, A. Badshah, G. Abbas, H. Alasmary, M. Waqas, and W. A. Khan, "A provable secure and efficient authentication framework for smart manufacturing industry," *IEEE Access*, vol. 11, pp. 67626–67639, 2023, doi: 10.1109/ACCESS.2023.3290913.

MOHAMMAD KAMRUL HASAN (Senior Member, IEEE) received the Doctor of Philosophy degree in electrical and communication engineering from the Faculty of Engineering, International Islamic University, Malaysia, in 2016. He is currently an Associate Professor and the Head of the Network and Communication Technology Research Laboratory, Center for Cyber Security, Universiti Kebangsaan Malaysia (UKM). He is a certified Professional Technologist in Malaysia. He has published more than 300 indexed papers in ranked journals and conference proceedings. He specializes in elements pertaining to cutting-edge information centric networks, computer networks, data communication and security, mobile network and privacy protection, cyber-physical systems, the industrial IoT, transparent AI, and electric vehicles networks. He is a member of the Institution of Engineering and Technology and the Internet Society. He served as the Chair for the IEEE Student Branch, from 2014 to 2016. He has actively participated in many events/workshops/trainings for the IEEE Humanity Program. He is an Editorial Member in many prestigious high-impact journals, such as IEEE, IET, Elsevier, Frontier, and MDPI. He is the general chair, the co-chair, and a speaker of conferences and workshops for the shake of society and academy knowledge building and sharing and learning.

ZHOU WEICHEN received the Bachelor of Science degree from East China Jiaotong University, China, in 2018. She is currently pursuing the Master of Science degree in computer science (network technology) with the Faculty of Information Science and Technology, Universiti Kebangsaan Malaysia, Bangi, Malaysia. Her research interests include computer network security, authentication and key agreement protocols, blockchain, and artificial intelligence. She possesses strong coding skills in Python and Java.

NURHIZAM SAFIE (Associate Member, IEEE) received the Master of Information Technology degree from UKM, in 1999, the Master of Business Administration (MBA) degree from Anglia Ruskin University, U.K., in 2019, and the Ph.D. degree in management information systems (MIS) from Malaysian Ministry of Science, Technology, and Innovation (MoSTI). He was conferred the Professional Technologist credential from Malaysian Board of Technology (MBoT), in 2018. He is currently an Associate Professor and the Dean of the Faculty of Information Science and Technology. Before this position, he was a Research Fellow with United Nations University, a United Nations academic arm. During the Ph.D. degree, he was awarded the National Science Fellowship (NSF) Scholarship from MoSTI.



FATIMA RAYAN AWAD AHMED received the B.S. degree in computer science from Sudan University of Science and Technology, in 2004, and the M.S. and Ph.D. degrees in computer science from Al Neelain University, Sudan, in 2007 and 2012, respectively. In 2004, she joined Sudan Telecommunications Company, Sudan, as a Computer Programmer with the IT Department, where she analyzed, designed, and programmed a set of systems. She joined Sattam University, Saudi Arabia, in 2013, as an Assistant Professor with the Information Systems Department, from 2013 to 2016, and has been with the Computer Science Department, since 2017. Her research interests include artificial intelligence, systems and algorithms analysis and design, web applications, and E-learning.

TAHER M. GHAZAL (Senior Member, IEEE) received the Bachelor of Science degree in software engineering from Al Ain University, in 2011, the Master of Science degree in information technology management from The British University in Dubai, in 2013, associated with The University of Manchester and The University of Edinburgh, and the Ph.D. degree in information science and technology from Universiti Kebangsaan Malaysia, in 2023.

He is a seasoned academician with a comprehensive educational background. He possesses over a decade of multifaceted expertise, he has fulfilled various roles, including a Lecturer, an Instructor, a Tutor, a Researcher, a Teacher, an IT Support/Specialist Engineer, and a Business/Systems Analyst. He has contributed significantly across diverse departments, such as Engineering, Computer Science, and ICT, and the Head of STEM and Innovation. His professional engagements have extended to governmental and private educational institutions under the purview of KHDA, Ministry of Education, and the Ministry of Higher Education and Scientific Research, United Arab Emirates. His scholarly pursuits encompass a wide array of interests, including the IoT, artificial intelligence, cybersecurity, information systems, software engineering, web development, building information modeling, quality of education, management, big data, quality of software, and project management. He is actively engaged in community service through his involvement in impactful projects and research endeavors.