Comparative Analysis of Multi-Factor Authentication Schemes for Internet of Things

HALVOR VADA, University of Twente, The Netherlands

The Internet of Things (IoT), with its numerous systems of interconnected devices gathering and analysing data about the world, is seeing adaptation in increasingly many areas of society, including smart homes, remote healthcare and autonomous industry. As these new areas of application are bringing with them new risks associated with illegal access and malicious behaviour, it is becoming increasingly important to ensure the security of IoT systems. While a variety of security challenges and solutions are present, one of the core features in ensuring the security of IoT systems is authentication. Traditionally, single-factor authentication has been used to secure computer systems. However, with the ability of a single factor to ensure security decreasing, multi-factor authentication (MFA) is emerging as the new standard. As IoT systems face challenges not present in traditional systems, such as using devices with limited power and memory, and a variety of IoT-specific schemes have been proposed in the literature, there is a need for an overview of MFA schemes applicable in IoT systems. In this paper, individual analyses of MFA schemes for IoT, as well as a comparative table of all the schemes, are presented. These contain the schemes' core features, strengths and weaknesses, and are brought together to form a comparative analysis focused on providing people wanting to implement MFA for IoT with the necessary understanding to make a well-informed decision.

Additional Key Words and Phrases: Internet of Things, IoT security, Authentication, Multi-factor authentication schemes, Comparative analysis

1 INTRODUCTION

The advancement of Internet of Things (IoT) has led to the emerging of many new areas of society where such systems bring value. Everything from smart homes to healthcare monitoring to autonomous industrial applications is now seeing advancements with the application of IoT systems [37, 55], but at the same time, is bringing new and significant risks associated with unintended access to or behaviour of the systems [10, 35]. As a result, security in IoT systems is increasingly important, with one of the core challenges being authentication [10, 20, 45]. For example, in 2017, security vulnerabilities that could lead to unauthorized access to and control over almost half a million pacemakers in use by patients were discovered [22], showing the degree of severity of consequences that unauthorized access to an IoT system can have.

The traditional, single-factor methods of authentication, such as using user-created, or default, passwords or scanning radio frequency identification (RFID) tags, can no longer provide the degree of security needed with regards to the potential consequences of unauthorized access [27]. Instead, multiple distinct factors must be applied through multi-factor authentication (MFA) to ensure the security needed. As IoT systems, compared to traditional computer systems, face implementation challenges related to their devices' limited power and storage capacity [21], MFA schemes for IoT have different requirements than those of traditional computer systems. A variety of IoT-based MFA schemes have been proposed in the literature, with differing factors, architectures and functionalities. As they all have their own strengths, weaknesses and degree of applicability, the requirements for implementing such schemes vary depending on their use-cases. As a result, there is a need for a comparative overview and analysis of the available schemes that can provide the knowledge necessary to make an informed decision of which factors or schemes to apply with regards to the use case.

To bring forth such an analysis, this paper first looks at the security challenges present in IoT systems to show both the variety of attacks and vulnerabilities IoT systems are at risk from, as well as display the importance of authentication in securing such systems. Then, MFA schemes for IoT systems found in the literature are presented individually through a short analysis covering its core features, strengths and weaknesses. Bringing together the individual analyses, all the schemes are presented in a benchmark that gives a comparative overview of their core details. Finally, taking into account the schemes presented and analysed, a comparative analysis related to the decision-making process is presented, providing both what is observed from analysing the schemes and recommendations on how to make a decision for implementation.

The remaining sections of this paper are as follows: Section 2 defines a common abstract architecture for IoT systems and presents the security challenges each layer of the architecture faces. Section 3 is a literature review consisting of a short analysis of each multi-factor scheme included in the comparative table at the end of the section. Section 4 contains a comparative analysis of the schemes and recommendations for people deciding on a scheme to implement, and section 5 concludes the findings of the research.

2 SECURITY CHALLENGES

As IoT systems consist of complex networks of devices that are applied in a variety of ways, they contain many core functionalities, such as physical sensing of the environment, network transportation of data, storage and processing of data, and presenting of data in user applications. In addition, the technological perspective needs to support security, scalability, and interoperability between heterogeneous devices [3]. As a result, different architectures have been suggested for IoT systems in order to optimally separate the various functionalities in an abstract way and make the distinguishing of requirements simpler [11, 34]. To identify the security challenges facing IoT systems, a reference architecture is needed to separate the functionalities and requirements into abstract layers where the challenges and solutions can be presented for each layer.

As various architectures exist, the identification of security challenges in this paper will make use of one such architecture, namely the 3-layer architecture [1, 11]. The 3-layer architecture, consisting of the perception layer, the network layer and the application layer,

TScIT 37, July 8, 2022, Enschede, The Netherlands

is the most basic architecture presented in the literature, and has been widely used as a reference for IoT systems [11, 16]. Various other architectures have been proposed, which implement additional layers to distinguish the aspects of IoT systems to a higher degree, with the most common general-purpose architectures being various forms of 4-layer (perception, network, service/support, application) [32, 34, 59] and 5-layer (perception, transport, processing, application, business) [3, 40, 54] architectures. Although these more specific abstractions exist, the 3-layer architecture covers all core aspects of IoT systems, and hence is sufficient for describing the core security challenges facing IoT, as well as their proposed solutions.

2.1 Perception layer

The perception layer consists of sensing devices that gather information about the physical environment, making them the end-nodes in the IoT network [1]. These devices make use of a variety of technologies, including RFID, near-field communication (NFC) and global positioning system (GPS), to gather data about their environment, such as temperature, pressure or the movement and location of physical objects [34, 46, 56]. The core functionality of this layer is to collect, and potentially digitize, data according to some defined task without significant processing or storage required. After data is collected by the perception layer, the network layer propagates the data through the network for communication and processing.

The limited, specific functionality of perception layer devices and the scale of their deployment in IoT systems commonly lead to them needing to be cheap and easily deployed. As these devices are normally battery-powered and limited in their processing power and storage capacity, they are called resource-constrained devices [21]. In addition to the challenges resulting from this, perception layer devices can be at risk of physical attacks stemming from their deployment. Attacks observed on the perception layer are:

Device subversion: When an attacker gains partial or full control over a device in the network, allowing the attacker to send faulty data from the device or make the device cease to function as it is supposed to. Control of multiple devices in the system gives the attacker more power to manipulate the functioning of the network as a whole. This could be achieved through node capture [46].

Device data access: When an attacker gains access to the data collected by the device. The data may be confidential information about a system or a person, compromising the security of the system. This could be achieved through eavesdropping, node capture or side-channel attacks. [34, 46].

Device degradation: When an attacker attempts to stop the device from functioning as it is supposed to by making the device unavailable, either by preventing access through a denial-of-service (DoS) attack, or by depleting the devices resources through DoS or a denial-of-sleep attack [18, 46].

Fake node attacks: When an attacker deploys an invalid node into the perception layer of an IoT network. Such a node can then be used to manipulate the functioning of the system, either by flooding real nodes with data to make them unavailable (DoS) or by sending fake data to other parts of the network [16].

Multiple solutions are presented to deal with the challenges facing the perception layer. Node authentication helps prevent fake node attacks and the ability for an attacker to execute denial-of-service attacks, and data encryption helps protect the data being collected by devices or passed between them, while maintaining the confidentiality of the data. One of the key challenges facing perception layer devices is their limited capacity when it comes to energy consumption, processing power and storage capacity, and hence a central requirement for the security of these devices is that the security schemes implemented are lightweight.

2.2 Network layer

The network layer consists of wired or wireless networks that transmit the data gathered by devices in the perception layer to the application layer. The layer makes use of a variety of network technologies (3G, 4G, 5G, Wi-Fi, Bluetooth, ZigBee, GSM, UMTS, etc.) to transmit data, in addition to being able to communicate with external services for data processing and storage (cloud-computing services, big data repositories) [40, 46]. The core functionalities of this layer are to transmit and aggregate data gathered in the perception layer and handle the communication across the whole IoT system.

As the network layer is in charge of transporting data throughout the IoT system and maintaining communication between the devices in the system, the main challenges facing this layer stems from overloading the network, manipulating the routing and communication of the network, and illegally gaining access to the data passed through the network [16, 34, 46]. Attacks observed on the network layer are:

Denial-of-service (DoS): When devices in the network layer are made unavailable by being flooded with packets, for example by using a fake node, or when the transmission of radio signals in the network are jammed by an adversary. Both methods lead to the unavailability of network layer services, and hence impact the functioning of the whole IoT system [34, 46].

Man-in-the-middle (MITM): When an attacker manipulates the network into thinking it is a part of it, and is able to intercept messages passing between two devices without impacting the functioning of the system. Through such an attack, the attacker can gain access to the data passed in the system [34].

Eavesdropping: When an attacker passively listens to the communications in the network layer and is able to access the data being transmitted. Such passive listening might provide the attacker with confidential information that can either inform it about the system or be used to execute other attacks [16, 34].

Routing attacks: When an attacker targets the routing and transmission of data throughout the network layer in order to disrupt the flow of information in the system. Such disruption can be done by dropping packets or redirecting them to unintended destinations, and can cause DoS attacks or hinder the system from functioning correctly. Examples of such attacks include black hole, gray hole and wormhole [34, 46].

To deal with the challenges facing the network layer, several key solutions present themselves. Firstly, data transmitted through the network must be encrypted to maintain confidentiality from eavesdropping or other access to the transmitted data. In addition, an identity management scheme, a secure routing protocol and point-to-point authentication are needed to ensure communication in the network is only done through authenticated devices and always follows the implemented routing protocol.

2.3 Application layer

The application layer consists of the applications that make use of the data from the perception layer to provide users with the desired services. The core functionality lies in providing user interfaces that either display information regarding the collected data in an understandable way or allow users to control devices in the perception layer or the system as a whole [28, 46].

As the application layer may depend on a variety of software providers, has the ability to control devices in the IoT system, and is where users provide input and interact with the system, the main challenges in this layer stem from unauthorized access to the system and illegally gaining access to the data stored on or passed through the layer [28, 41, 46]. Security challenges observed on the application layer are:

Data confidentiality and user privacy: The data stored in the application layer contains both user data and information about the system. Hence, an attacker gaining access to this data risks both the confidentiality of the system and the privacy of its users. In addition, the potentially different software providers make protecting data through all interactions extra challenging. Common attacks include injection attacks and malware [11, 28, 46].

Authentication and authorization: As users access the IoT system through the application layer and use this access to either control the system or access the data of the system, significant risks exist regarding unauthorized access in this layer. If an attacker is able to access the system, significant damage can be caused both in terms of the functioning of the system and the confidentiality of its data. Common attacks include various forms of injection attacks and social engineering [46].

Accessibility and availability: Since the correct functioning of the IoT system may depend on users being able to interact with and control the system at all times, an attacker causing the services of the layer to become unavailable is a significant security risk. Attacks that can affect this include DoS and malware [28].

As unauthorized access in the application layer presents great risks regarding both the functioning of the system and the confidentiality of user and system data, secure authentication schemes that protect access, user privacy and interaction between components in the layer are required to ensure security. In addition, to manage the various software and hardware components in the layer and ensure security is maintained across their potentially varying communication and authentication protocols, information security management schemes are needed.

As can be seen from the security challenges and solutions present in IoT systems, shown in table 1, authentication is of the utmost importance in securing IoT systems.

Table 1. Security challenges and solutions in 3-layer IoT architecture

Layer	Challenges	Solutions
Perception	Node capture Node impersonation Fake node attack Data confidentiality Node availability	Lightweight authentication Lightweight encryption
Network	Data confidentiality Routing attacks Network availability Impersonation attacks	Data encryption Point-to-point authentication Identity management scheme Secure routing protocol
Application	Data confidentiality User privacy User impersonation Application availability	Data encryption Authentication Information security management scheme

3 LITERATURE REVIEW

In this section, each scheme involved in the comparative analysis is presented individually through a short analysis covering the factors it uses, the architecture it is designed for, as well as the core strengths and weaknesses of both the scheme itself and the quality of the way the authors presented the scheme. The core features, strengths and weaknesses of each scheme are presented in table 2.

In [15], the authors proposed a three-factor authentication scheme that uses passwords, smart cards and biometrics as factors, and elliptic curve cryptography (ECC) as a lightweight approach to public-key cryptography. The scheme is made for medical professionals accessing patient sensor data stored in a centralized cloud environment in real-time. While both medical professionals and patients register with the system, only medical professionals authenticate with the cloud server to gain access to the data. The authors provided security and performance comparisons of their scheme with 11 relevant schemes, and showed that their scheme covers more security features while keeping performance close to the most lightweight schemes.

The authors in [31] presented a three-factor scheme that uses passwords, smart cards and biometrics as factors. The scheme is made for multi-gateway IoT environments using a control server for communication. Each gateway consists of an IoT network, and the gateways register with the control server and mutually authenticate with users wanting to access the data. While the authors looked away from the security and computation requirements of the control server, the architecture presented is still very relevant as it takes into account authentication between users and gateway networks.

The authors in [57] proposed a two-factor authentication scheme that uses passwords and smart cards as factors. The scheme is made for basic cloud IoT environments, only covering communication between users and a central server that provides the desired resources. While the architecture is basic, the authors included phases for changing both passwords and smart cards in their scheme, in addition to an extensive informal security analysis as well as formal verification using BAN-logic, random oracle model and AVISPA tool.

In [26], the authors proposed a three-factor AES-ECC-based authentication scheme for cross-platform cloud environments that uses passwords, smart cards and biometrics as factors. The scheme is designed for cloud environments where fog servers that users want to access may stem from different providers, while being connected to the same trusted cloud service provider. While they provided an extensive informal security analysis covering many security attacks and features, their comparison with other schemes was quite limited.

The authors in [63] analysed two recent multi-server authentication schemes and showed that a variety of vulnerabilities were present in both. To address the vulnerabilities, the authors proposed a two-factor ECC-based scheme applicable in generic multi-server IoT environments that uses passwords and smart cards as factors. The scheme consists of a trusted registration authority that registers both servers and users, before they are able to mutually authenticate each other and communicate.

In [48], the authors analyzed the most up-to-date USB-based authentication scheme for smart healthcare and found various vulnerabilities, as well as a lack of ability for users to change their password. They proposed an improved version of the scheme that uses passwords, USBs and biometrics as factors, covers the vulnerabilities found, and includes a change-password mechanism. The scheme consists of users and a central server, and while it was made for smart healthcare, the generic structure of the architecture makes it applicable in many fields.

The authors in [64] presented a two-factor scheme for multi-server smart healthcare environments that uses passwords and biometrics as factors, and includes a physically unclonable function (PUF) in the wireless body area network (WBAN) of a medical patient. Users, including both medical professionals and patients, can authenticate with both sensors and medical servers. The architecture and inclusion of both user-sensor and user-server authentication makes the scheme both sophisticated and relevant, and the authors also provided formal verification using BAN-logic, real-or-random (ROR) model and AVISPA tool.

In [36], the authors analysed a recent authentication scheme [14] for Internet-of-Multimedia-Things (IoMT) and found that the scheme violates user anonymity and user untraceability, and is vulnerable to multiple attacks. They then presented an improved three-factor ECC-based scheme that is secure against the issues they identified. The scheme uses passwords, smart cards and biometrics as factors, and while presented for IoMT, consists of a generic user-server architecture that is applicable in many environments. The authors only performed formal verification using a random oracle model, and provided a limited comparison where the accuracy of the computation cost is unclear.

In [33], the authors focused on wireless sensor networks (WSN) in IoT and the limitations of sensor nodes. They performed an in-depth analysis of an existing relevant scheme [24] and improved on the vulnerabilities found by creating a three-factor scheme that uses passwords, smart cards and biometrics as factors. The architecture consists of users, gateway nodes and sensor nodes, and the authors gave special attention to ensuring mutual authentication between users and sensors and using gateway nodes to reduce the work required by the sensors in order to increase their lifetime.

The authors of [6] proposed a three-factor authentication scheme for cloud IoT environments, consisting of a system administration node, users, gateway nodes and sensor nodes. The scheme is highly applicable in IoT environments, allowing users to directly authenticate with sensors through gateways. They included phases for changing passwords, smart cards and biometrics, as well as the dynamic adding of both gateways and sensors to the system, ensuring a highly sophisticated scheme. They also provided an extensive informal security analysis and formal verification using BAN-logic, ROR model and AVISPA tool.

In [65], the authors analysed a recent related scheme [38] and showed that both mutual authentication and anonymity is compromised in the scheme, before proposing an improved password, smart card and biometric-based scheme. The scheme is made for generic cloud IoT environments where users authenticate with registered cloud servers through a trusted central authority. Although the scheme appears quite efficient, the authors only compared their scheme to three others.

The authors of [5] presented the most up-to-date schemes for wireless health sensor networks and found vulnerabilities in the most up-to-date scheme [66]. They then presented a password, smart card and biometric-based scheme, with an extensive list of security attacks that it is secure against. The system consists of a system manager that registers users, sensors and gateway nodes, before allowing users to authenticate with sensors through the gateway to gain access to sensor data and data stored in the gateway. The scheme includes the secure addition of sensor nodes, but does not include password or smart card change.

In [30], the authors found vulnerabilities in a recent WSN-based authentication scheme [12] and proposed an improved scheme that uses passwords, smart cards and biometrics as factors. The scheme consists of users, gateway nodes and sensor nodes, with both users and sensors registering with the gateway before being able to mutually authenticate each other. Although the scheme does not include a phase for smart card change, the authors provided an in-depth and extensive informal security analysis and performed formal verification using BAN-logic, ROR model and AVISPA tool.

In [52], the authors performed an in-depth analysis of an existing authentication scheme [29], finding several vulnerabilities, before proposing a revised and improved version of the scheme. The revised scheme is based on ECC and uses passwords, smart cards with PUFs and biometrics as factors. While the PUF in the smart card improves the security of the scheme, the authors did not provide information relating to the feasibility of such a functionality. In addition, the scheme solely consists of users and a server, and hence does not specifically relate to any IoT environment, other than through its low computation costs. While the authors did provide an extensive informal security analysis, they only compared their scheme to the one they analysed and based their scheme on.

In [2], the authors proposed a two-factor authentication scheme for smart healthcare that uses passwords and smart cards as factors. The scheme consists of a trusted authority that registers users, servers and sensor hub nodes (personal digital assistants) before allowing users to log into a server and mutually authenticate with sensor hubs. Although the authors did not include phases for changing passwords and smart cards, they did perform formal verification using BAN-logic, ROR model and AVISPA tool. They also compared their scheme with 9 related schemes, and it appears to be both lightweight and secure.

In [49], the authors performed an in-depth analysis of a recent smart healthcare authentication scheme [53] and found that it does not ensure patient anonymity and has a flaw in the password change phase. They then proposed a three-factor ECC-based authentication scheme that uses passwords, smart cards and biometrics as factors. The scheme consists of a trusted registration center, users and telecare servers. Once users and telecare servers are registered, they can directly authenticate each other to give users access to the server's resources. Although the architecture is quite basic, the authors provided an extensive informal security analysis and performed formal verification using BAN-logic, ROR model and AVISPA tool.

In [50], the authors proposed an ECC-based scheme for generic IoT environments consisting of users, gateway nodes and sensor nodes. The scheme uses passwords, biometrics and smart devices with public key certificates as factors. The scheme requires users to register with a certificate authority before being able to register with gateway nodes, while sensor nodes can be registered using a pre-secret received from gateway nodes during deployment. The authors also made use of a symmetric key between gateway nodes and users, which is computed during registration. Once registered, users mutually authenticate with sensor nodes through a gateway node before being able to directly communicate with them.

The authors of [7] performed an analysis of, and found vulnerabilities in, a recent authentication scheme for generic IoT architectures [9] consisting of users, gateways and sensors. They then proposed a revised symmetric key-based scheme using passwords, smart cards and biometrics as factors. The scheme requires users and sensors to register with gateways before being able to mutually authenticate each other and communicate directly.

In [42], the authors proposed an ECC-based authentication scheme for generic IoT environments consisting of sensors, trusted gateways and users, using a private key generator to generate keys distributed through the trusted gateways. Once users and sensors have registered with a gateway, they can mutually authenticate with each other for direct communication. The scheme makes use of identity-based-cryptography for lightweight signing and encrypting of data, although because of the unclear performance analysis provided by the authors, it is difficult to compare the efficiency of the scheme to others.

The authors of [60] performed an in-depth analysis of a recent authentication scheme for generic IoT environments [4] consisting of users, servers and a trusted registration center. They then proposed an improved ECC-based scheme that uses passwords, smart cards and biometrics as factors. While the scheme does include a phase for changing passwords, it does not include one for changing smart cards. The authors provided an extensive informal security analysis.

The authors of [23] proposed a two-factor ECC-based authentication scheme for cloud environments consisting of a central cloud server that registers users and fog nodes. Once registered, users and fog nodes can mutually authenticate through the central cloud server. The scheme is quite sophisticated, having phases for password change, user revocation and re-registration (covering smart card change), and fog node revocation. However, the authors only performed formal verification using a modified three-party BRP model that they defined in the paper.

In [47], the authors proposed an authentication scheme for WSN, with users and sensor nodes having to register with a gateway node before being able to authenticate each other. The ECC-based scheme uses password and smart card for authentication, and while it has a phase for password change, it does not have one for smart card change. Surprisingly, although the authors included an informal security analysis covering the most common security features and attacks, they did not perform any form of formal verification for their scheme.

The authors of [39] performed an extensive analysis of a recent authentication scheme for WSN [58]. After showing the presence of a variety of vulnerabilities in the scheme, they proposed an improved scheme based on passwords, smart cards and biometrics that uses Chebyshev chaotic mapping to improve security. Once users register with the trusted gateway node, they can mutually authenticate with sensor nodes through the gateway. Although the authors did not include a smart card change phase in the scheme, they included both an extensive informal security analysis and an in-depth comparison with related schemes.

In [43], the authors provided an in-depth analysis of an authentication scheme made for smart home environments [62] consisting of a trusted registration authority, trusted home gateway, smart devices and users. The authors found a variety of vulnerabilities, and proposed an improved scheme that uses passwords and mobile phones as factors. As the home gateway is trusted, only smart devices and users need to register with the registration authority, before users can mutually authenticate with smart devices through the gateway. The authors provided a very extensive informal security analysis and formal verification using BAN-logic, ROR model and AVISPA tool. Although they did include a performance comparison with four other schemes, the computation cost analysis only included the total cost, and not the cost per entity in the scheme.

The authors of [17] proposed a lightweight two-factor authentication scheme for WSN, with a specific focus on healthcare. The scheme uses passwords and mobile devices as factors, and is designed for an environment with trusted gateway nodes that both users and sensors have to register with before being able to authenticate each other. While the authors stated that the scheme applies to healthcare and WBANs, the scheme's generic architecture makes it applicable in other fields as well. The authors provided an extensive informal security analysis and a solid comparison, and based on the results, the scheme appears highly efficient.

In [51], the authors performed an in-depth analysis of a recent authentication scheme for WSN [61], before proposing their own password and smart card-based scheme that is secure against the vulnerabilities they found. The scheme relies on trusted gateway nodes for authentication between users and sensors, and includes phases for both password and smart card change. While both the informal security analysis and the formal verification were sufficient, the authors only compared their scheme to three others, with one of them being the one already analysed.

The authors of [13] proposed a three-factor ECC-based authentication scheme for multi-gateway WSN as an improvement to a scheme they analysed [19]. The scheme uses passwords, smart cards and biometrics as factors. The architecture consists of trusted gateway nodes that users and sensors register with, and accounts for users being able to both register for multiple gateways as well as authenticate with the sensor of an unknown gateway by communicating through a known one.

The authors of [44] provided a short analysis of two authentication schemes for WSN [8, 25], before proposing an improved scheme that overcomes the security weaknesses they found. The scheme uses passwords, smart cards and biometrics as factors, and consists of an architecture containing a system administrator, gateways, sensors and users, where both users and sensors have to register with a gateway in order to be able to authenticate each other. The scheme lacks a phase for changing smart cards, and although the authors provided a good comparison with related schemes, the only formal verification they performed, using AVISPA, was not extensive.

4 COMPARATIVE ANALYSIS

From the individual analyses and the comparison in table 2, it is clear that MFA schemes for IoT exist in a variety of forms, with different strengths, weaknesses and levels of applicability. When considering which scheme to use or which qualities to seek out for implementation, the information provided in table 2 brings out several important features. One, while many schemes exist, there also exist many architectures to which they apply. While the general architecture is relatively similar, mostly consisting of a trusted central node that users and sensors connect to, smaller scheme-specific details also exist. Whether that is requiring an external trusted authority, having a static, predefined sensor network instead of a dynamic one, or only allowing users to authenticate with a server, and not sensors, these details strongly affect the applicability and functionality of schemes. Another noticeable feature affecting the functionality of the system, is whether the scheme has all the required phases or not. As noted above, many schemes lack the ability to change smart cards or dynamically add sensor nodes, and some even lack a phase for changing passwords. While not being able to change smart cards might not be a problem in all systems, it seems clear that a user-oriented IoT system would be less ideal if it lacked the ability for users to change their passwords.

Another aspect that stands out is the need to make trade-offs in deciding which scheme to use, especially when it comes to factors and performance. The vast majority of schemes use either a password and a smart card or a password, a smart card and an unspecified biometric factor as factors. The biometric factor increases the degree of security at the cost of efficiency, resulting in a choice that comes down to the feasibility of having biometric readers, the risk of only having passwords and smart cards, potentially combined with whether there are phases for changing them, and the degree to which the devices in the system require a highly lightweight scheme. As is clear from table 2, there exist many highly efficient schemes, and as the main differences in performance stem from which factors are used and what architecture it is made for, performance comes at a trade-off with both the degree of security and the simplicity of the system. If more specific performance requirements are present, they are most likely to exist in the sensor nodes, as the majority of architectures have relatively high-performing trusted central nodes that users communicate through. As this is a common problem, a variety of schemes have purposely sought to reduce the work required by sensor nodes at the cost of increasing the work of other nodes, a feature that would prove highly valuable in a system with tight performance requirements on its sensor layer devices.

The final aspect that stands out and impacts which scheme to use relates to the quality of the paper it was proposed in, especially when it comes to the informal analysis of security features and attacks and formal verification of the scheme. As is clear from the papers, there exists great variety in how thorough the authors were with the security analysis of their scheme. How thorough the analysis is can prove highly valuable, considering a vast number of previously proposed schemes are proven vulnerable, often to a variety of attacks, not long after they are proposed. Therefore, in order to increase the chance that a chosen scheme will prove resistant over time and ensure the most severe potential vulnerabilities are not present, it would be wise to consider both the quality and quantity of the authors' informal security analysis and formal verification.

5 CONCLUSION

This paper started with presenting the core security challenges and solutions for IoT systems based on a common architecture, making clear the importance of authentication in ensuring a high degree of security. Focusing on user-system authentication, an extensive group of multi-factor authentication schemes specifically made with IoT architectures and limitations in mind were presented and analysed. The individual analyses focused on the core features, architectures, strengths and weaknesses of the schemes, which were then brought together in a table providing an overview and comparison of the schemes. From the information gathered by analysing all the schemes, a comparative analysis was conducted, focusing on recommendations for people deciding on a scheme to implement. From this analysis, the core features that vary between schemes and lead to different levels of security and applicability are made clear, helping anyone wanting to either learn the current state of multi-factor authentication schemes for IoT or make a well-informed decision on which scheme to implement.

REFERENCES

[1] Mohammed ABDMEZIEM, D. Tandjaoui, and Imed Romdhani. 2015. Architecting the Internet of Things: State of the Art. *Studies in Systems, Decision and Control* (08 2015), 55–75. https://doi.org/10.1007/978-3-319-22168-7_3

[2] Abhay K. Agrahari, Shirshu Varma, and S. Venkatesan. 2022. Two factor authentication protocol for IoT based healthcare monitoring system. *J Ambient Intell Human Comput* (2022). https://doi.org/10.1007/s12652-022-03834-9

[3] Ala Al-Fuqaha, Mohsen Guizani, Mehdi Mohammadi, Mohammed Aledhari, and Moussa Ayyash. 2015. Internet of Things: A Survey on Enabling Technologies, Protocols, and Applications. *IEEE Communications Surveys Tutorials* 17, 4 (2015), 2347–2376. https://doi.org/10.1109/COMST.2015.2444095

[4] Rifaqat Ali and Arup Kumar Pal. 2018. An efficient three factor–based authentication scheme in multiserver environment using ECC. *International Journal of Communication Systems* 31, 4 (2018), e3484. https://doi.org/10.1002/dac.3484 arXiv:https://onlinelibrary.wiley.com/doi/pdf/10.1002/dac.3484

[5] Abdullah M. Almuhaideb and Kawther S. Alqudaihi. 2020. A Lightweight Three-Factor Authentication Scheme for WHSN Architecture. *Sensors* 20, 23 (2020).

https://doi.org/10.3390/s20236860

[6] Ahmed Yaser Fahad Alsahlani and Alexandru Popa. 2021. LMAAS-IoT: Lightweight multi-factor authentication and authorization scheme for real-time data access in IoT cloud-based environment. *Journal of Network and Computer Applications* 192 (2021), 103177. https://doi.org/10.1016/j.jnca.2021.103177

[7] Bander A. Alzahrani, Shehzad A. Chaudhry, Ahmed Barnawi, Wenjing Xiao, Min Chen, and Abdullah Al-Barakati. 2020. ILAS-IoT: An improved and lightweight authentication scheme for IoT deployment. *Journal of Ambient Intelligence and Humanized Computing* (2020). https://doi.org/10.1007/s12652-020-02349-5

[8] Ruhul Amin, SK Hafizul Islam, G.P. Biswas, Muhammad Khurram Khan, Lu Leng, and Neeraj Kumar. 2016. Design of an anonymity-preserving three-factor authenticated key exchange protocol for wireless sensor networks. *Computer Networks* 101 (2016), 42–62. https://doi.org/10.1016/j.comnet.2016.01.006

[9] Soumya Banerjee, Vanga Odelu, Ashok Kumar Das, Jangirala Srinivas, Neeraj Kumar, Samiran Chattopadhyay, and Kim-Kwang Raymond Choo. 2019. A Provably Secure and Lightweight Anonymous User Authenticated Session Key Exchange Scheme for Internet of Things Deployment. *IEEE Internet of Things Journal* 6, 5 (2019), 8739–8752. https://doi.org/10.1109/JIOT.2019.2923373

[10] Broadband Internet Technical Advisory Group (BITAG). 2016. Internet of Things Security and Privacy Recommendations. http://www.bitag.org/documents/BITAG_Report_-_Internet_of_Things_(IoT)_Security_and_Privacy_Recommendations.pdf

[11] Muhammad Burhan, Rana Asif Rehman, Bilal Khan, and Byung-Seo Kim. 2018. IoT Elements, Layered Architectures and Security Issues: A Comprehensive Survey. *Sensors* 18, 9 (2018). https://doi.org/10.3390/s18092796

[12] Yuwen Chen, Lourdes López, José-Fernán Martínez, and Pedro Castillejo. 2018. A Lightweight Privacy Protection User Authentication and Key Agreement Scheme Tailored for the Internet of Things Environment: LightPriAuth. *Journal of Sensors* 2018 (2018). https://doi.org/10.1155/2018/7574238

[13] Cong Dai and Zhongwei Xu. 2022. A secure three-factor authentication scheme for multi-gateway wireless sensor networks based on elliptic curve cryptography. *Ad Hoc Networks* 127 (2022), 102768. https://doi.org/10.1016/j.adhoc.2021.102768

[14] Parwinder Kaur Dhillon and Sheetal Kalra. 2017. Secure multi-factor remote user authentication scheme for Internet of Things environments. *International Journal of Communication Systems* 30, 16 (2017), e3323. https://doi.org/10.1002/dac.3323

[15] Parwinder Kaur Dhillon and Sheetal Kalra. 2018. Multi-factor user authentication scheme for IoT-based healthcare services. *J Reliable Intell Environ* 4 (2018), 141–160. https://doi.org/10.1007/s40860-018-0062-5

[16] Mohammed El-hajj, Ahmad Fadlallah, Chamoun Maroun, and Ahmed Serhrouchni. 2019. A Survey of Internet of Things (IoT) Authentication Schemes. *Sensors* 19 (03 2019). https://doi.org/10.3390/s19051141

[17] Mahdi Fotouhi, Majid Bayat, Ashok Kumar Das, Hossein Abdi Nasib Far, S. Morteza Pournaghi, and M.A. Doostari. 2020. A lightweight and secure two-factor authentication scheme for wireless body area networks in health-care IoT. *Computer Networks* 177 (2020), 107333. https://doi.org/10.1016/j.comnet.2020.107333

[18] Antoine Gallais, Thin-Hinen Hedli, Valeria Loscrì, and Nathalie Mitton. 2019. Denial-of-Sleep Attacks against IoT Networks. In *CoDIT 2019 - 6th International Conference on Control, Decision and Information Technologies*. Paris, France. https://hal.inria.fr/hal-02060608

[19] Hua Guo, Ya Gao, Tongge Xu, Xiyong Zhang, and Jianfeng Ye. 2019. A secure and efficient three-factor multi-gateway authentication protocol for wireless sensor networks. *Ad Hoc Networks* 95 (2019), 101965. https://doi.org/10.1016/j.adhoc.2019.101965

[20] Badis Hammi, Sherali Zeadally, Rida Khatoun, and Nebhen Jamel. 2022. Survey on Smart Homes: Vulnerabilities, Risks, and Countermeasures. *Computers & Security* (03 2022), 102677. https://doi.org/10.1016/j.cose.2022.102677

[21] Asma Haroon, Munam Ali Shah, Yousra Asim, Wajeeha Naeem, Muhammad Kamran, and Qaisar Javaid. 2016. Constraints in the IoT: The World in 2020 and Beyond. *International Journal of Advanced Computer Science and Applications* 7, 11 (2016). https://doi.org/10.14569/IJACSA.2016.071133

[22] Alex Hern. 2017. Hacking risk leads to recall of 500,000 pacemakers due to patient death fears. https://www.theguardian.com/technology/2017/aug/31/hacking-risk-recall-pacemakers-patient-death-fears-fda-firmware-update

[23] Xiaojing Jia, Debiao He, Neeraj Kumar, and Kim-Kwang R. Choo. 2019. Authenticated key agreement scheme for fog-driven IoT healthcare system. *Wireless Networks* 25 (2019), 4737–4750. https://doi.org/10.1007/s11276-018-1759-3

[24] Qi Jiang, Jianfeng Ma, Fushan Wei, Youliang Tian, Jian Shen, and Yuanyuan Yang. 2016. An untraceable temporal-credential-based two-factor authentication scheme using ECC for wireless sensor networks. *Journal of Network and Computer Applications* 76 (2016), 37–48. https://doi.org/10.1016/j.jnca.2016.10.001

[25] Qi Jiang, Sherali Zeadally, Jianfeng Ma, and Debiao He. 2017. Lightweight three-factor authentication and key agreement protocol for internet-integrated wireless sensor networks. *IEEE Access* 5 (2017), 3376–3392. https://doi.org/10.1109/ACCESS.2017.2673239

[26] Haqi Khalid, Shaiful Jahari Hashim, Sharifah Mumtazah Syed Ahmad, Fazirulhisyam Hashim, and Muhammad Akmal Chaudhary. 2021. SELAMAT: A New Secure and Lightweight Multi-Factor Authentication Scheme for Cross-Platform Industrial IoT Systems. *Sensors* 21, 4 (2021). https://doi.org/10.3390/s21041428

[27] Constantinos Kolias, Georgios Kambourakis, Angelos Stavrou, and Jeffrey Voas. 2017. DDoS in the IoT: Mirai and Other Botnets. *Computer* 50, 7 (2017), 80–84. https://doi.org/10.1109/MC.2017.201

[28] Ritika Raj Krishna, Aanchal Priyadarshini, Amitkumar V. Jha, Bhargav Appasani, Avireni Srinivasulu, and Nicu Bizon. 2021. State-of-the-Art Review on IoT Threats and Attacks: Taxonomy, Challenges and Solutions. *Sustainability* 13, 16 (2021). https://doi.org/10.3390/su13169463

[29] Adesh Kumari, Srinivas Jangirala, M. Yahya Abbasi, Vinod Kumar, and Mansaf Alam. 2020. ESEAP: ECC based secure and efficient mutual authentication protocol using smart card. *Journal of Information Security and Applications* 51 (2020), 102443. https://doi.org/10.1016/j.jisa.2019.102443

[30] Joonyoung Lee, Sungjin Yu, Myeonghyun Kim, Youngho Park, and Ashok Kumar Das. 2020. On the Design of Secure and Efficient Three-Factor Authentication Protocol Using Honey List for Wireless Sensor Networks. *IEEE Access* 8 (2020), 107046–107062. https://doi.org/10.1109/ACCESS.2020.3000790

[31] JoonYoung Lee, SungJin Yu, KiSung Park, YoHan Park, and YoungHo Park. 2019. Secure Three-Factor Authentication Protocol for Multi-Gateway IoT Environments. *Sensors* 19, 10 (2019). https://doi.org/10.3390/s19102358

[32] Shancang Li, Theo Tryfonas, and Honglei Li. 2016. The Internet of Things: a security point of view. *Internet Research* 26 (04 2016), 337–359. https://doi.org/10.1108/IntR-07-2014-0173

[33] Xiong Li, Jianwei Niu, Saru Kumari, Fan Wu, Arun Kumar Sangaiah, and Kim-Kwang Raymond Choo. 2018. A three-factor anonymous authentication scheme for wireless sensor networks in internet of things environments. *Journal of Network and Computer Applications* 103 (2018), 194–204. https://doi.org/10.1016/j.jnca.2017.07.001

[34] Jie Lin, Wei Yu, Nan Zhang, Xinyu Yang, Hanlin Zhang, and Wei Zhao. 2017. A Survey on Internet of Things: Architecture, Enabling Technologies, Security and Privacy, and Applications. *IEEE Internet of Things Journal* 4, 5 (2017), 1125–1142. https://doi.org/10.1109/JIOT.2017.2683200

[35] Ran Liu and Jinfeng Wang. 2017. Internet of Things: Application and Prospect. *MATEC Web of Conferences* 100 (01 2017), 02034. https://doi.org/10.1051/matecconf/201710002034

[36] Khalid Mahmood, Waseem Akram, Akasha Shafiq, Izwa Altaf, Muhammad Ali Lodhi, and SK Hafizul Islam. 2020. An enhanced and provably secure multi-factor authentication scheme for Internet-of-Multimedia-Things environments. *Computers & Electrical Engineering* 88 (2020), 106888. https://doi.org/10.1016/j.compeleceng.2020.106888

[37] Parushi Malhotra, Yashwant Singh, Pooja Anand, Deep Kumar Bangotra, Pradeep Kumar Singh, and Wei-Chiang Hong. 2021. Internet of Things: Evolution, Concerns and Security Challenges. *Sensors* 21, 5 (2021). https://doi.org/10.3390/s21051809

[38] Rafael Martínez-Peláez, Homero Toral-Cruz, Jorge R. Parra-Michel, Vicente García, Luis J. Mena, Vanessa G. Félix, and Alberto Ochoa-Brust. 2019. An Enhanced Lightweight IoT-based Authentication Scheme in Cloud Computing Circumstances. *Sensors* 19, 9 (2019). https://doi.org/10.3390/s19092098

[39] Jiaqing Mo, Zhongwang Hu, and Wei Shen. 2022. A Provably Secure Three-Factor Authentication Protocol Based on Chebyshev Chaotic Mapping for Wireless Sensor Network. *IEEE Access* 10 (2022), 12137–12152. https://doi.org/10.1109/ACCESS.2022.3146393

[40] Hichem Mrabet, Sana Belguith, Adeeb Alhomoud, and Abderrazek Jemai. 2020. A Survey of IoT Security Based on a Layered Architecture of Sensing and Data Analysis. *Sensors* 20 (06 2020), 3625. https://doi.org/10.3390/s20133625

[41] Lavinia Nastase. 2017. Security in the Internet of Things: A Survey on Application Layer Protocols. In *2017 21st International Conference on Control Systems and Computer Science (CSCS)*. 659–666. https://doi.org/10.1109/CSCS.2017.101

[42] Mohammad Nikravan and Akram Reza. 2020. A Multi-factor User Authentication and Key Agreement Protocol Based on Bilinear Pairing for the Internet of Things. *Wireless Personal Communications* 111 (2020), 463–494. https://doi.org/10.1007/s11277-019-06869-y

[43] JiHyeon Oh, SungJin Yu, JoonYoung Lee, SeungHwan Son, MyeongHyun Kim, and YoungHo Park. 2021. A Secure and Lightweight Authentication Protocol for IoT-Based Smart Homes. *Sensors* 21, 4 (2021). https://doi.org/10.3390/s21041488

[44] Arezou Ostad-Sharif, Hamed Arshad, Morteza Nikooghadam, and Dariush Abbasinezhad-Mood. 2019. Three party secure data transmission in IoT networks through design of a lightweight authenticated key agreement scheme. *Future Generation Computer Systems* 100 (2019), 882–892. https://doi.org/10.1016/j.future.2019.04.019

[45] OWASP. 2019. OWASP INTERNET OF THINGS TOP 10 2018. https://owasp.org/www-pdf-archive/OWASP-IoT-Top-10-2018-final.pdf

[46] Shantanu Pal, Michael Hitchens, Tahiry Rabehaja, and Subhas Mukhopadhyay. 2020. Security Requirements for the Internet of Things: A Systematic Approach.

Sensors 20 (10 2020), 5897. https://doi.org/10.3390/s20205897

[47] Mingping Qi and Jianhua Chen. 2021. Secure authenticated key exchange for WSNs in IoT applications. *The Journal of Supercomputing* 77 (2021), 13897–13910. https://doi.org/10.1007/s11227-021-03836-y

[48] Km. Renuka, Saru Kumari, and Xiong Li. 2019. Design of a Secure Three-Factor Authentication Scheme for Smart Healthcare. *Journal of medical systems* 43 (2019), 1–12. https://doi.org/10.1007/s10916-019-1251-3

[49] Jongseok Ryu, Jihyeon Oh, Deokkyu Kwon, Seunghwan Son, Joonyoung Lee, Yohan Park, and Youngho Park. 2022. Secure ECC-Based Three-Factor Mutual Authentication Protocol for Telecare Medical Information System. *IEEE Access* 10 (2022), 11511–11526. https://doi.org/10.1109/ACCESS.2022.3145959

[50] Dipanwita Sadhukhan, Sangram Ray, G. P. Biswas, M. K. Khan, and Mou Dasgupta. 2021. A lightweight remote user authentication scheme for IoT communication using elliptic curve cryptography. *The Journal of Supercomputing* 77 (2021), 1114–1151. https://doi.org/10.1007/s11227-020-03318-7

[51] Mohammad Javad Sadri and Maryam Rajabzadeh Asaar. 2021. An anonymous two-factor authentication protocol for IoT-based applications. *Computer Networks* 199 (2021), 108460. https://doi.org/10.1016/j.comnet.2021.108460

[52] Masoumeh Safkhani, Nasour Bagheri, Saru Kumari, Hamidreza Tavakoli, Sachin Kumar, and Jiahui Chen. 2020. RESEAP: An ECC-Based Authentication and Key Agreement Scheme for IoT Applications. *IEEE Access* 8 (2020), 200851–200862. https://doi.org/10.1109/ACCESS.2020.3034447

[53] Shreeya Swagatika Sahoo, Sujata Mohanty, and Banshidhar Majhi. 2021. A secure three factor based authentication scheme for health care systems using IoT enabled devices. *Journal of Ambient Intelligence and Humanized Computing* 12 (2021), 1419–1434. https://doi.org/10.1007/s12652-020-02213-6

[54] Omar Said and Mehedi Masud. 2013. Towards Internet of Things: Survey and Future Vision. *International Journal of Computer Networks* 5 (02 2013), 1–17.

[55] Elmustafa Sayed Ali Ahmed and Zeinab Kamal. 2017. Internet of Things Applications, Challenges and Related Future Technologies. *world scientific news* (01 2017). https://www.researchgate.net/publication/313651150_Internet_of_Things_Applications_Challenges_and_Related_Future_Technologies

[56] Pallavi Sethi and Smruti R. Sarangi. 2017. Internet of Things: Architectures, Protocols, and Applications. *Journal of Electrical and Computer Engineering* 2017 (2017). https://doi.org/10.1155/2017/9324035

[57] Geeta Sharma and Sheetal Kalra. 2020. Advanced lightweight multi-factor remote user authentication scheme for cloud-IoT applications. *J Ambient Intell Human Comput* 11 (2020), 1771–1794. https://doi.org/10.1007/s12652-019-01225-1

[58] Sooyeon Shin and Taekyoung Kwon. 2019. A Lightweight Three-Factor Authentication and Key Agreement Scheme in Wireless Sensor Networks for Smart Homes. *Sensors (Basel, Switzerland)* 19 (2019).

[59] Hui Suo, Jiafu Wan, Caifeng Zou, and Jianqi Liu. 2012. Security in the Internet of Things: A Review. *Proceedings - 2012 International Conference on Computer Science and Electronics Engineering, ICCSEE 2012* 3 (03 2012). https://doi.org/10.1109/ICCSEE.2012.373

[60] Feifei Wang, Guoai Xu, Chenyu Wang, and Junhao Peng. 2019. A Provably Secure Biometrics-Based Authentication Scheme for Multiserver Environment. *Security and Communication Networks* 2019 (2019). https://doi.org/10.1155/2019/2838615

[61] Fan Wu, Xiong Li, Lili Xu, Pandi Vijayakumar, and Neeraj Kumar. 2021. A Novel Three-Factor Authentication Protocol for Wireless Sensor Networks With IoT Notion. *IEEE Systems Journal* 15, 1 (2021), 1120–1129. https://doi.org/10.1109/JSYST.2020.2981049

[62] Anhao Xiang and Jun Zheng. 2020. A Situation-Aware Scheme for Efficient Device Authentication in Smart Grid-Enabled Home Area Networks. *Electronics* 9, 6 (2020). https://doi.org/10.3390/electronics9060989

[63] Guosheng Xu, Shuming Qiu, Haseeb Ahmad, Guoai Xu, Yanhui Guo, Miao Zhang, and Hong Xu. 2018. A Multi-Server Two-Factor Authentication Scheme with Un-Traceability Using Elliptic Curve Cryptography. *Sensors* 18, 7 (2018). https://doi.org/10.3390/s18072394

[64] Hailong Yao, Qiao Yan, Xingbing Fu, Zhibin Zhang, and Caihui Lan. 2022. ECC-based lightweight authentication and access control scheme for IoT E-healthcare. *Soft Computing* 26 (2022), 4441–4461. https://doi.org/10.1007/s00500-021-06512-8

[65] SungJin Yu, KiSung Park, and YoungHo Park. 2019. A Secure Lightweight Three-Factor Authentication Scheme for IoT in Cloud Computing Environment. *Sensors* 19, 16 (2019). https://doi.org/10.3390/s19163598

[66] SungJin Yu and YoungHo Park. 2020. SLUA-WSN: Secure and Lightweight Three-Factor-Based User Authentication Protocol for Wireless Sensor Networks. *Sensors* 20, 15 (2020). https://doi.org/10.3390/s20154143

Table 2. Overview of MFA IoT schemes and their characteristics

Source	Domain	Factors	Performance	Verification	Strengths & Weaknesses
[15]	Smart healthcare	U&P, SC, B	R: 7T(H) L&A: 1T(EXP) + 7T(H)	AVISPA	+Lightweight -Basic architecture -No PC, SCC
[31]	Multi-gateway	U&P, SC, B	L&A: U: 1T(F) + 14T(H), GW: 5T(H), CS: 9T(H)	BAN, AVISPA	+Relevant architecture +Lightweight -Not extensive SA, no SCC
[57]	Cloud-IoT	U&P, SC	R: 3T(H) L&A: 9T(H) + 3T(E)	BAN, ROM, AVISPA	+Extensive SA & FV +Includes PC & SCC -Basic architecture
[26]	Cross platform industrial IoT	U&P, SC, B	L: 1H(P) + 1H(M) + 5T(H) + 1T(PE) + 4T(SE) + 2T(SD) A: 2T(H) + 1T(AV) + 2T(SE) + 3T(SD)	BAN, AVISPA	+Extensive SA +Relevant architecture -Not extensive comparison -No PC, SCC
[63]	Generic multi-server	U&P, SC	L&A: U: 3T(PM) + 9T(H), S: 3T(PM) + 6T(H)	BAN	+Extensive SA +Relevant architecture -Limited FV, no SCC
[48]	Smart healthcare	U&P, B, USB	L&A: U: 9T(H) + 2T(B) + 3T(M), S: 4T(H) + 4T(M)	ROM	+Improved existing scheme -Not extensive comparison -Limited FV, no SCC
[64]	Smart healthcare	U&P, B, PUF	N/A	BAN, ROR, AVISPA	+Sophisticated architecture +Extensive FV -Unclear performance analysis
[36]	IoMT	U&P, SC, B	10T(H) + 6T(PM)	ROM	+Includes PC & SCC -Basic architecture -Limited FV
[33]	WSN	U&P, SC, B	L&A: U: 2T(PM) + 8T(H), GW: T(PM) + 8T(H), SN: 4T(H)	BAN	+Relevant architecture +Lightweight –Limited FV, no SCC
[6]	Cloud-IoT	U&P, SC, B	L&A: 1T(F) + 30T(H)	BAN, ROR, AVISPA	+Highly sophisticated +Relevant architecture +Extensive FV
[65]	Cloud-IoT	U&P, SC, B	L&A: U: 12T(H), Cloud: 6T(H), CS: 16T(H)	BAN, AVISPA	+Relevant architecture +Lightweight -Limited SA & comparison
[5]	Smart healthcare	U&P, SC, B	L&A: U&SN: 4T(H) + 1T(F), GW: 8T(H)	BAN, TP	+Relevant architecture +Extensive SA -No PC, SCC
[30]	WSN	U&P, SC, B	L&A: U: 1T(F) + 6T(H), SN: 4T(H), GW: 9T(H)	BAN, ROR, AVISPA	+Relevant architecture +Extensive SA & FV -Limited comparison, no SCC
[52]	Single server	U&P, SC, PUF	L&A: U: 1T(PUF) + 3T(PM) + 5T(H), S: 3T(PM) + 5T(H)	ROR	+Extensive SA +Improved existing scheme -Basic architecture -Limited FV & comparison
[2]	Smart healthcare	U&P, SC	A: S: 8T(H) + 4T(PM) + 1T(Exp), PDA: 1T(BP) + 1T(H) + 4T(PM)	BAN, ROR, AVISPA	+Extensive FV +Extensive comparison -No PC, SCC

Source	Domain	Factors	Performance	Verification	Strengths & Weaknesses
[49]	Smart healthcare	U&P, SC, B	L&A: 6T(PM) + 19T(H) + 2T(B)	BAN, ROR, AVISPA	+Extensive SA & FV -No SCC
[42]	Generic IoT	U&P, SD, B	N/A	BAN, AVISPA	+Extensive SA -Unclear performance analysis
[50]	Generic IoT	C, U&P, B	L&A: U: 2T(H) + 1T(PM) + 2T(SE/SD), SN: 1T(H) + 1T(PM) + 2T(SE/SD), GW: 2T(H) + 4T(SE/SD)	AVISPA	+Extensive SA +Extensive comparison -Limited FV -Requires user certificate
[7]	Generic IoT	U&P, SC, B	L&A: 20T(H) + 10T(SE/SD)	ROR	+Includes PC, SCC -Limited FV
[60]	Generic multi-server	U&P, SC, B	L&A: U: 3T(PM) + 1T(SE) + 7T(H), RC: 1T(PM) + 1T(SD) + 1T(SE) + 5T(H), S: 2T(PM) + 1T(SD) + 4T(H)	BAN, ROM	+Improved existing scheme +Extensive SA -No SCC
[23]	Cloud-IoT	U&P, SC	L&A: U: 2T(PM) + 5T(H) + 1T(BP), FN: 2T(PM) + 4T(H) + 1T(BP), Cloud: 3T(PM) + 9T(H) + 1T(BP)	Modified BRP	+Sophisticated scheme +Relevant architecture -No performance comparison -Limited FV
[47]	WSN	U&P, SC	L&A: U: 3T(PM) + T(SE) + 7T(H), GW: 1T(PM) + 2T(SE/SD) + 6T(H), SN: 2T(PM) + 1T(SD) + 3T(H)	N/A	+Relevant architecture -Missing formal verification -No SCC
[39]	WSN	U&P, SC, B	L&A: U: 11T(H) + 3T(C), GW: 9T(H) + 1T(C), SN: 4T(H) + 2T(C)	ROM, ProVerif	+Extensive SA +Extensive comparison -No SCC
[43]	Smart home	U&P, SD	L&A: 42T(H)	BAN, ROR, AVISPA	+Extensive SA & FV -Minimal comparison
[17]	WSN	U&P, SD	L&A: 34T(H)	ROR, ProVerif	+Extensive SA, lightweight -Basic scheme
[51]	WSN	U&P, SC	L&A: U: 6T(H) + 2T/SE/SD), GW: 10T(H) + 2T(SE/SD), SN: 5T(H)	BAN, ROR	+Improved existing scheme +Lightweight -Limited comparison
[13]	WSN	U&P, SC, B	L&A: U: 1T(B) + 9T(H) + 3T(PM), GW: 12T(H) + 1T(PM), SN: 5T(H) + 2T(PM)	BAN, ProVerif	+Relevant architecture +Improved existing scheme -No SCC
[44]	WSN	U&P, SC, B	L&A: U: 11T(H), GW: 17T(H), SN: 5T(H)	AVISPA	+Improved existing scheme +Extensive comparison -Limited FV & SA

Key Terms used in Table 2
Domain: IoMT = Internet-of-Multimedia-Things, WSN = Wireless sensor network
Factors: U&P = Username and password, SC = Smart card, SD = Smart device, B = Biometric (unspecified), PUF = Physically unclonable function, C = Public key certificate
Performance - Actions and roles: R = Registration, L = Login, A = Authentication, U = User, S = Server, GW = Gateway CS = Control server, SN = Sensor node, RC = Registration center, FN = Fog node
Performance - Operations: T(PM) = ECC point multiplication, T(H) = Hash, T(F) = Fuzzy extractor, T(B) = Bio-hash T(PUF) = PUF function, H(P) = Hash related to bilinear pairing, H(M) = Hash related to group of ECC, T(SE) = Symmetric encryption T(SD) = Symmetric decryption, T(PE) = Public-key encryption, T(AV) = Asymmetric signature verification, T(M) = Modular arithmetic T(Exp) = Exponentiation, T(BP) = Bilinear pairing, T(E/D) = Encryption/decryption unspecified, T(C) = Compute Chebyshev polynomial
Verification: ROM = Random oracle model, ROR = Real-or-random model, BAN = Burrows-Abadi-Needham logic AVISPA = Automated Validation of Internet Security Protocols, TP = Tamarin Prover
Strengths & Weaknesses: SA = Security analysis, FV = Formal verification, PC = Password change, SCC = Smart card change