Control and Cybernetics

vol. **49** (2020) No. 4

A study of various authentication mechanisms towards the secure Internet of Things networks*

by

Rupali Sachin Vairagade and S. H. Brahmananda

Department of Computer Science and Engineering, GITAM School of Technology, GITAM (Deemed to be University), Bengaluru, India
makde.rupali@gmail.com,
brahmananda.savadatti@gitam.edu

Abstract: Internet of Things (IoT) plays a major function in the public infrastructure, including power grids, control systems, smart cards, smart cities, intelligent transportation, education, and so on. The IoT networks provide ample benefits arising from transmission of the data between the IoT nodes and the servers. However, security constitutes a major concern in the IoT applications, as secret information may get disclosed to the unauthorized third-party in the network. Thus, secure authentication is a major requirement for managing and communicating with respect to the devices in the IoT environment. In this survey, 50 research papers are reviewed, referring to various authentication protocols used for ensuring adequate security in the network. The authentication methods are categorized on the basis of the security mechanisms, namely, the lightweight approach, the identity approach, the mutual authentication approach, and the cryptography-based authentication approaches, with the challenges faced by these existing methods being reported. Moreover, a simple overview is provided based on authentication protocols, toolsets, and evaluation metrics. Conform to this survey, most of the research articles concentrated on the lightweight-based approaches, and the most commonly applied evaluation metrics include packet loss, throughput, and efficiency.

Keywords: Internet of Things, secure authentication, mutual authentication, cryptography-based authentication, lightweight approach, identity approach

1. Introduction

Internet of Things (IoT) is an enabling technology envisioned for public infrastructures, such as health care, power grids, control systems, and smart cities. IoT devices utilize the public networks for transferring huge amounts of information to the target node or nodes. The IoT systems utilize public networks

*Submitted: February 2020; Accepted: January 2021

to transmit huge amounts of data, which makes them a prime target for cyber-attacks. Human safety and IoT security are tied together in the objective of avoiding network disruption (Aman, Chua and Sikdar, 2017). The IoT devices are considered as forming an embedded system, which contains different characteristic features and properties. It is mainly designed to perform the tasks assigned with low processing power and limited storage requirements. IoT is considered to be "headless", since it does not require humans to operate. IoT devices depend on wireless energy transfer or energy-harvesting, but they do not use any battery or power source (Aman, Chua and Sikdar, 2017). In IoT, multicast is one of the powerful and efficient communication modes in the network and data sensing layer (Yao et al., 2013). IoT is used in a wide range of applications, reducing the overall cost of digital devices, including sensors (Wu et al., 2017).

IoT remote users can easily access the network resources over the smart devices by connecting the sensing element or the sensor node into the IoT environment. Once the connection is established, the legitimate user can access the IoT resources through the authentication process. Authentication in IoT has three important aspects, namely something the user is, something the user has, and something the user knows (Dhillon and Kalra, 2017). Security is a particularly important requirement regarding the industrial IoT applications. Certain applications, like automation and process monitoring, require end-to-end authentication for supporting the authenticated and the encrypted data exchange through the sensor networks. The Constrained Application Protocol (CoAP) is used in the application layer of the energy or memory-constrained IoT devices. At the data link layer, cryptographic extensions have been included in the Institute of Electrical and Electronics Engineers (IEEE) 802.15.9 standards (Sciancalepore et al., 2016). The smart city developments usually also contain multiple IoT devices and must rely on an adequate security framework to resist malicious attacks. The device scalability is achieved by employing the hierarchical network structure (Mick, Tourani and Misra, 2017, and Li, Liu and Nepal, 2017).

The most important requirement of IoT security is proper authentication. The initial step to establish a secure session between the IoT devices is to define the authentication mechanism. The authentication process must be performed efficiently and securely without saving confidential information in the device memory. These security issues are being solved by introducing various authentication methods, such as a lightweight approach, mutual authentication, identity-based authentication, and key agreement access control mechanism (Aman, Chua and Sikdar, 2017). In the IoT applications, the entities, such as service providers, sensor nodes, and processing systems have to authenticate the nodes with respect to each other to generate a trusted network. The authentication protocol should not only resist the malicious attacks, but it also should be appropriately "lightweight" to be deployed in poorly perform-

ing edge devices (Porambage et al., 2014a). The security problems are solved using various security schemes, like multi-layered security, signatures, and key agreement-based location privacy model (Wu et al., 2017). Authentication is also one of the most important security features in IoT-enabled industrial applications. Open Authorization (OAuth) is a standard authorization protocol, which allows the user to access the resources securely. The users are authenticated by the security manager using the authentication mechanism for accessing the IoT network. The security manager supervises the local database and maintains the client application of the IoT network (Emerson et al., 2015).

This paper is organized as follows. After the introduction of the present Section 1, Section 2 provides the literature review regarding the IoT authentication methods. Section 3 describes the existing research gaps and issues, and Section 4 provides a simple analysis and discussion. Finally, Section 5 concludes the paper.

2. Related works

This main section of the paper reviews the authentication mechanisms developed in the studies, reported in various research papers. The assumed categorization of the authentication methods is shown in Fig. 1.

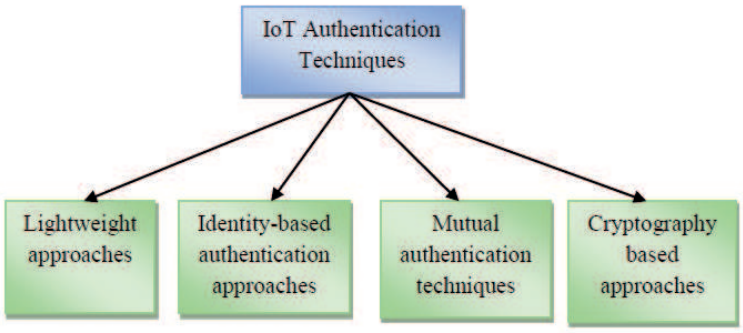

Figure 1: Assumed categorization of IoT authentication techniques

2.1. Lightweight approaches

We consider here the research papers, reporting on studies, based on the lightweight approaches for IoT authentication mechanisms. Thus, Aman, Chua and Sikdar (2017) developed the lightweight-based authentication protocol to achieve efficient processing and storage areas in the IoT applications. It was mainly based on the functions of physical uncloneable features, and the respective lightweight protocol involved two processes, that is – the communication

between the server and the IoT devices, and also the communication among the IoT devices. The mutual authentication protocol developed in this method diminishes the memory requirements, communication overhead and energy. The security feature of this scheme was unique, as it did not save any secret files. In this method, the latency of authentication was high because more messages were exchanged between the entities.

Li, Liu and Nepal (2017) introduced a lightweight protocol for the smart city framework. It concentrated more on the communication cost rather than on effectiveness. It was mainly intended for resource-constrained IoT devices. The battery power utilized by the IoT device was very low. The performance was significantly enhanced using the mutual authentication process. It offered the security features and provided the data authenticity to the user. However, the developed protocol was used in the software emulation and not in the realistic hardware environment.

Yao et al. (2013) developed a lightweight authentication scheme for the secure communication in the IoT environment. It used Nyberg's accumulator for observing the devices in the small-scale applications. The cardinal properties of the scheme were utilized in the resource-constrained devices. The information was easily authenticated through the scheduled receiver and the fragmented data was identified easily. Here, the entropy of the multicast data was not correlated with the signature, hence it authenticated messages with high entropy.

Punithavathi et al. (2019) introduced a lightweight authentication framework to enhance the security of IoT devices. This framework used the cloud-based model to authenticate the IoT devices. The biometric templates were used to identify the privacy issues in the IoT devices. The template protection mechanism was incorporated with the biometric system to enhance the security of the authentication scheme. However, the scalability in relation to the IoT devices was not improved by this framework in the real-world scenario.

Zhou et al. (2019) introduced the lightweight authentication approach to attain better efficiency in the IoT architecture. The crypto modules of the lightweight approach, like exclusive-or (XOR) operation and the hash functions were incorporated together to provide efficient authentication. This approach was more effective in the case of resource-constrained devices, such as IoT devices, and sensors, and also eliminated the computation overhead. This method is mainly suitable for real IoT-cloud circumstances, due to practicality requirements and security.

Yang et al. (2016) introduced a lightweight approach to resolve the bottlenecks in anonymous credentials. The lightweight approach was integrated with the dynamic accumulator of Nguyen's to update the outsourcing paradigm. It used the bilinear map with an asymmetric structure to calculate the pairing operations. However, the performance attained by this method was very low.

Shivraj et al. (2015) developed a lightweight authentication approach to enhance the security of IoT devices. The authentication framework based on the two-factor scheme was utilized to achieve the end-to-end IoT device authentication. The lightweight mechanism integrated Lamport's algorithm with the cryptographic model to attain better security. The performance attained was, however, very low so that the method was not deployed in the real-time scenario.

Tewari and Gupta (2017a) introduced a lightweight protocol to forward the data over the insecure channels. The protocol used the bitwise operation function for the authentication processes, which made the IoT device operations more efficient by utilizing limited computation capabilities and limited resources. Moreover, the communication cost and storage utilization were very low. This protocol was more secure against tango attacks but the cryptanalysis was not effectively performed.

Arafin, Gao and Qu (2017) developed a lightweight authentication mechanism for the IoT devices. The variation dependent error signature mechanism was used for extracting the information about the underlying process variation in the computational unit. The error-based profile was incorporated with the authentication mechanism to generate the two-factor security key model. It especially works well under de-anonymization and identification of the devices and users. The communication cost of this approach was, however, too high.

Porambage et al. (2014a) introduced a pervasive lightweight approach for the distributed IoT environment. Here, the sensor nodes established the secure connection between the end-user and the peer nodes. It also used the pervasive authentication mechanism to offer end-to-end security at the application level. It was more suitable in the resource-constrained environment. However, it could not be applied to the large-scale networks.

Amin et al. (2018) introduced a lightweight authentication protocol for the distributed cloud applications. The registered users securely accessed all the confidential information from the cloud server. It offered appropriate features, like authentication, anonymity, and resisted different kinds of attacks. The informal cryptanalysis ensured that this mechanism was protected under the hardness assumption of hash function. While the password verifier table was held to be very useful in the password update and legal user identification, this method did not use such password verifier table.

Dhillon and Kalra (2017) introduced a lightweight biometric-based authentication scheme to securely access the IoT services. It uses the XOR operation and hash function to ensure the secure working of this approach. The scheme was more robust against various security attacks than the approaches compared with it. It offered the gateway node to the IoT devices for registering the user's information to directly connect the smart device to the sensor node. The scheme was more secure in the presence of an intruder, but it was not actually lightweight in the context of real-time functioning of devices.

Wang et al. (2018) introduced yet another lightweight protocol for the IoT environment. It offered secure communication between the IoT device and the server and among various IoT devices. The computational cost and the storage cost were both low. In this method, however, it was necessary to simulate the protocol with respect to various types of attacks.

Esfahani et al. (2017) developed a lightweight authentication approach to solve the security issues in the IoT industrial environment. It was mainly intended for the machine-to-machine (M2M) communication using the XOR operation and the hash function. It effectively achieved device confidentiality, key agreement, mutual authentication, and resistance against different security attacks. However, it failed to offer authentication between the sensor nodes in the IoT network.

Gope et al. (2018) introduced a lightweight authentication approach for the smart city applications in the distributed IoT services. The assets of the smart city were managed by using IoT communication networks, with information security mechanism. This mechanism was used to solve the data privacy and the security issues of the smart city. Yet, the attacker could easily retrieve the security credentials and perform the forgery attacks.

Mick, Tourani and Misra (2017) introduced a lightweight and hierarchical routing approach for the IoT environment. It used the routing and onboarding framework to solve the privacy and security issues. It achieved reasonable onboarding convergence times and needed minimal network overhead.

Arasteh, Aghil and Mala (2016) developed a lightweight key exchange and secure authentication approach for the IoT networks. This approach was more reliable and secure against Denial of Service (DoS) and replay attacks than other compared approaches. The secure authentication scheme was efficient in terms of storage and computational overhead.

Hammi et al. (2017) introduced a lightweight-based authentication protocol for the IoT industrial environment. The node, wishing to access the network resources, had to be authenticated in the IoT sublayer. This protocol was designed to solve the authentication problems and to offer an energy-efficient and

robust mechanism in the network services. It protected the IoT devices against replay and DoS attacks. Yet, the integrity and confidentiality of the message were not ensured properly.

Janbabaei, Gharaee and Mohammadzadeh (2016) introduced a lightweight and mutual authentication mechanism for the IoT environment. This approach was applicable to the sensors between the mobile node and the stationary node. It offered definite privacy and security features, like untraceability and anonymity. It should be noted that this approach did not consider the trust in the nodes.

2.2. Identity-based authentication approaches

This section elaborates on the identity-based authentication approaches collected from various existing research works.

Salman et al. (2016) developed an identity-based authentication approach for IoT devices. It utilized the authentication and the identification model to translate the specific identities into the shared identity using the gateways, authenticate devices, and virtual addresses. It was secure against replay, man-in-the-middle, and the masquerade attacks. The computational and communication costs were, however, too high.

Witkovski et al. (2015) introduced an Identity Management (IdM) and key-based authentication method for the smart house application related to the IoT devices. IdM allowed the technician for accessing the appliances using a single sign-on in the IoT environment. The attacks originating from the internet were mitigated using the symmetric keys. However, energy consumption was not considered in the design of this mechanism.

Kothmayr et al. (2012) developed a Datagram Transport Layer Security (DTLS)-based end-to-end security mechanism to work under the communication stacks with low power. Here, the authentication was carried out during the DTLS handshake, which was based on X.509 certificates by holding the Rivest, Shamir and Adelman (RSA) keys. It offered authenticity, confidentiality, and message integrity and made the security solution more feasible.

Mishra et al. (2018) developed an efficient authentication mechanism to ensure privacy and security in the IoT services. It offered cloud-assisted services and resisted security attacks, like sensor node and user impersonation attacks.

2.3. Mutual authentication approaches

The research works, which utilized the mutual authentication approaches in the IoT environment are shortly commented upon in this section. Thus, Kalra and

Sood (2015) developed Elliptic Curve Cryptography (ECC)-based authentication approach for the commercial IoT environment. The size of the key in this approach was small. Hence, it was more efficient in terms of computation and offered high-security solutions. It provided secure communication between the cloud server and the embedded devices using the cookies. It provided sufficient security functionality and offered improved authentication. Hence, it was more robust against various security attacks. The coverage capability revealed by the authentication scheme, though, was low.

Saxena, Grijalva and Chaudhari (2016) introduced an authentication and key agreement protocol for the IoT-enabled network services. It made possible efficient and secure communications between the IoT devices, as well as the users. It was more secure against replay, redirection, impersonation, and object theft attacks. This protocol offered forward privacy, anonymity, and untraceability to the IoT devices. The communication overhead was low, but the performance of the key identifier was poor.

Li et al. (2017a) developed an efficient user authentication model to offer surety over the public channels in network communication. It resisted some of the security threats and provided the key security and user anonymity to the IoT device. The authentication mechanism in this approach significantly reduced the redundancy and was provably secure against password and replay attacks. It satisfied the security requirements and attained low computational overhead. The communication cost, though, turned out to be high in the medical care-based IoT system.

Tewari and Gupta (2017a) developed a mutual authentication approach to be used between the server and the IoT device with application of ECC. It was more suitable in the case of the resource-constrained devices in the authentication processes. It offered sufficient security and attained improved performance. However, its communication and computational costs were high.

Li et al. (2017b) introduced an energy-efficient authentication protocol for IoT devices. It offered ideal functionalities, such as untraceability, user anonymity, resistance to stolen mobile device attack, and prevented various other security-related attacks. This protocol was efficient and robust for IoT applications. The privacy problem and security issues were solved. The computational and communicational costs were, however, high.

2.4. Cryptography-based authentication approaches

This section discusses the research papers, which used the cryptographic authentication mechanism. So, Alcaide et al. (2013) introduced an anonymous-based authentication framework to attain privacy preservation in IoT applications by combining threshold cryptography, secret sharing, and recent advances in anony-

mous credentials. The parameters, needed by the system, were not generated centrally, but cooperatively amongst all the nodes in the IoT system. The users were monitored and controlled by the data collectors. The data was collected using the attribute-based access control mechanism. The data collector modified and defined their respective policies without affecting the IoT system.

Zhao et al. (2011) introduced an asymmetry-based mutual authentication approach to serve between the terminal node and the platform of the IoT environment. This scheme was feasible, secure, and required minimum communication cost in the IoT applications. It used a cryptographic model and hash function for securely forwarding the information between the server and the IoT devices.

Alshahrani, Traore and Woungang (2019) introduced a key exchange and authentication approach to enhance privacy protection and security in the smart network. It depended on the symmetric encryption model to achieve adequate authentication in the network by enabling the IoT devices. This encryption model shared the session key with other nodes through the home controller. It attained perfect secrecy by exchanging the secret keys at each communication session. The un-traceability and the un-linkability of the devices were used to ensure the proper functioning of the authentication framework.

Moosavi et al. (2015) introduced a cryptography-based authentication mechanism into the IoT healthcare-related system. The authorization and the authentication of the end-user in the remote device were attained through the medical sensor gateway. It used the key management model between the gateway and the sensor nodes. Hence, it was more secure in the smart IoT environment. It reduced the latency and communication overhead, but the performance attained was very low.

Mahalle et al. (2013) introduced an identity-based access control mechanism for improving the performance of the IoT devices. The concept of an access control model was introduced to protect the IoT devices from the DoS and replay attacks. It is an integrated model based on access control and authentication for the IoT network.

Sciancalepore et al. (2016) introduced a key management approach by integrating the ECC and implicit certificates. This approach significantly enhanced the saving of the airtime due to adoption of the implicit certificates. The approach offered key derivation, peer authentication, fast re-keying, and better protection against various attacks. However, the related energy consumption and computational cost were high.

Kumari et al. (2017) developed a secure authentication mechanism based on the ECC for the cloud server and the IoT devices. It offered more security

against insider and offline password attacks. However, this scheme failed to achieve mutual authentication, key agreement, and device anonymity.

Mahalle, Prasad and Prasad (2014) introduced a threshold cryptography-based authentication mechanism for IoT devices. It established the session key using the threshold cryptography for communication purposes. This approach was more scalable and lightweight under certain criteria, but failed to protect the IoT devices from definite attacks.

Gaikwad, Gabhane and Golait (2015) introduced a three-level authentication scheme for smart IoT devices. This system was eco-friendly and very effective in terms of cost. It was suitable for home automation purposes for easily accessing the cloud server. This system was more secure than those compared to and could be easily controlled and monitored. The working performance of this system was, however, low.

Wallrabenstein (2016) developed a physical unclonable function-based authentication approach for the IoT devices in the network environment. It was suitable for the resource-constrained devices using the cryptographic mechanism. This approach offered end-to-end security with limited storage requirements and low computational overhead. It featured improved security against various attacks and was highly reliable in the network environment. The communication cost of this mechanism, though, was high.

Markmann, Schmidt and Wählisch (2015) developed an end-to-end authentication scheme using ECC. It assigned the federation mechanism to the gateways for the IoT sub-networks. This method was characterized by the improved efficiency and was controlled and monitored in a sensitive manner using the deployment of gateways.

Kothmayr et al. (2013) introduced the DTLS protocol for the IoT-based internet standards. It enabled the security update by reusing the security infrastructure. DTLS was mainly designed to work under communication stacks, which offered IPv6 networks. DTLS handshake was performed using the X.509 certificate, which consisted of RSA keys. DTLS was considered as the most feasible solution for the security problem.

Park, Kim and Bang (2015) elaborated the key agreement and symmetric key-based authentication mechanism for the distributed IoT applications. Here, the distribution center forwarded the key to each sensor node, where the sensor node received and agreed with the key by generating a new session key. Hence, the performance of the system was enhanced. However, the channel was not safe enough to share confidential information.

Ye et al. (2014) introduced an access control and efficient authentication mechanism for the perception layer of the IoT devices. Here, the session key was established using ECC and the mutual authentication was enhanced between the intermediate process, sensor nodes, and the user. This approach effectively solved the problems concerning the resource-constrained devices. It achieved flexible access control and attribute certificates while accessing the data. However, the security problem was not addressed in the perception layer.

Tamboli and Dambawade (2016) developed an efficient and secure authentication mechanism to provide access control for the resource-constrained IoT devices. It enhanced the privacy and the security of the system by offering service level authentication. It reduced the communication overhead, but featured low performance.

2.5. Other IoT authentication techniques

This section addresses the authentication approaches using various methods not mentioned before. Thus, Porambage et al. (2014b) developed and presented an authentication protocol for maintaining the accessibility and the trustworthiness of the IoT devices. For proper authentication a secure connection had to be established between the IoT devices. It also used the certificate-based framework in the IoT applications. The authentication protocol initiated the authentication process and the secure connections between the end-user and the sensor nodes. The approach enhanced the scalability, and heterogeneity of the IoT network. However, it failed to properly address the node-capturing attacks.

Emerson et al. (2015) introduced an OAuth-based authentication approach in order to offer a secure authentication scheme for the IoT network. It was meant for different resource-constrained IoT devices, where each IoT device used the security manager. The proposed approach protected the IoT network against several attacks and unauthenticated users. It offered improved flexibility in managing IoT devices. Yet, even though the cost overhead was low, the database query and the database update were not considered in the framework of this approach.

Wu et al. (2017) developed a key agreement and authentication mechanism for the IoT devices. The users were easily tracked by the session keys and the pseudo-identity, which could have been computed by the attacker. Note that, in general terms, there exist schemes, in which the sensors are injected with a common secret string at the very beginning and such string may be leaked due to the wrong arrangement in the scheme. After the leakage from one sensor, other sensors are threatened by the attackers who master the string. This particular proposal provided enhanced security with respect to various attacks and was meant to be deployed in the resource-constrained devices. It attained improved throughput and efficiency, but the packet delivery ratio was very low.

Hou and Yeh (2015) developed an authentication mechanism for the health-related system. It contained different categories, associated with sensors, like sensor tags, tagged items, and thin sensors. The mechanism offered more robust data communication and secure authentication for the IoT services. It utilized the proof protocol for verifying the tagged objects.

Hammi et al. (2018) introduced a blockchain-based authentication mechanism for the authentication and identification of IoT devices. Moreover, it effectively provided security with respect to data availability and integrity. It created the virtual zones called bubbles for identifying malicious users in the network. The mechanism met the security requirements and resisted different security attacks. Yet, it failed to achieve effective communication between the set of bubbles.

Caparra et al. (2016) introduced an energy-based node selection model to offer authentication between the anchor nodes and the source nodes using the characteristics of the network channel. Here, the anchor nodes estimate the channel to source nodes in an initially externally authenticated fashion, while forthcoming messages are authenticated by comparing the current channel estimate with the initial estimate.

Ning, Liu and Yang (2014) developed an aggregated proof-based authentication method for the distributed layered networks. In this method, the aggregated-proofs were established for multiple targets to achieve backward and forward anonymous data transmission. The Chebyshev maps, homomorphism functions, and the path descriptors were utilized in the mutual authentication scheme. The session freshness was effectively achieved by applying the hash values.

The here mentioned references, making up the content of the survey, are classified on the basis of methods utilized, classification techniques, performance metrics, and software tools, as this is shown in Table 1.

3. Research gaps and issues

This section elaborates on the research gaps and issues, associated with various existing authentication methods. The research issues faced by the lightweight-based authentication mechanism are discussed first. The lightweight approach in Aman, Chua and Sikdar (2017), failed to reduce the latency of the authentication, while in Li, Liu and Nepal (2017), the hardware environment was not supported in industrial-based applications. In Yao et al. (2013), the entropy of the data was not correlated with the signature to perform the secure authentication. The lightweight mechanism proposed in Zhou et al. (2019) was not suitable for the cloud-based IoT environment, and the performance of the

Table 1: Literature survey summary

Authors	**Methods**	**Classification**	**Performance metrics**	**Software tool**
Aman, Chua & Sikdar (2017)	lightweight mutual authentication protocol	lightweight approach	computation burden, memory, energy, and communication load	security protocol verification tool ProVerif (PV)
Li, Liu & Nepal (2017)	lightweight mutual authentication protocol	lightweight approach	authentication time, efficiency	Sky mote in Cooja simulator
Porambage et al. (2014a)	two-phase authentication protocol	others	efficiency, security, memory consumption	-
Yao et al. (2013)	lightweight multicast authentication mechanism	lightweight approach	computation overhead, packet loss, communication overhead, message entropy	-
Kalra & Sood (2015)	secure ECC based mutual authentication protocol	mutual authentication method	computation cost, communication cost	Automated Validation of Internet Security Protocols and Applications (AVISPA) tool
Alcaide et al. (2013)	fully decentralized anonymous authentication protocol	cryptography based approach	computational cost, communication cost	-
Punithavathi et al. (2019)	lightweight framework	lightweight approach	accuracy, security	Python
Alshahrani, Traore & Woungang (2019)	anonymous authentication scheme	cryptography based approach	efficiency, communication overhead	AVISPA tool
Zhou et al. (2019)	lightweight authentication approach	lightweight approach	efficiency, security	Proverif tool

Table 1, continued (part 2)

Authors	**Methods**	**Classification**	**Performance metrics**	**Software tool**
Yang et al. (2016)	lightweight entity authentication scheme	lightweight approach	computational cost, communication cost	Java
Shivrajet al. (2015)	lightweight approach	lightweight approach	security, computational time	Apache Tomcat tool
Moosavi et al. (2015)	secure and efficient authentication protocol	cryptography based approach	communication overhead, communication latency,	Relic-toolkit
Tewari & Gupta (2017a)	ultra-lightweight mutual authentication protocol	lightweight approach	storage, communication cost	-
Arafin, Gao & Qu (2017)	lightweight authentication approach	lightweight approach	threshold voltage	HSpice platform
Porambage et al. (2014b)	pervasive lightweight authentication mechanism	lightweight approach	time, energy	TelosB sensor nodes
Amin et al. (2018)	lightweight authentication protocol	lightweight approach	storage, communication cost, computation cost	AVISPA tool
Emerson et al. (2015)	OAuth based authentication protocol	others	cost overhead	-
Wu et al. (2017)	multigateway based authentication scheme	others	throughput, packet delivery ratio	Proverif
Mahalle et al. (2013)	identity authentication and capability-based Access Control (IACAC) model	cryptography based approach	computational time	AVISPA tool

Table 1, continued (part 3)

Authors	**Methods**	**Classification**	**Performance metrics**	**Software tool**
Dhillon & Kalra (2017)	lightweight user authentication protocol	lightweight approach	computation cost, communication cost	AVISPA tool
Hou & Yeh (2015)	sensor-based communication protocol	others	efficiency	
Sciancalepore et al. (2016)	key management protocol	cryptography based approach	bandwidth, energy	OpenWSN protocol stack
Wang et al. (2018)	ultra-lightweight authentication protocol	lightweight approach	security, computation cost	
Kumariet al. (2017)	elliptic curve cryptography based authentication approach	cryptography based approach	communication cost	AVISPA tool
Mahalle, Prasad & Prasad (2014)	threshold cryptography-based group authentication (TCGA) scheme	cryptography based approach	communication overhead, computational overhead	-
Esfahani et al. (2017)	lightweight authentication protocol	lightweight approach	communication overhead, computational cost	-
Gaikwad, Gabhane & Golait (2015)	secure Kerberos authentication protocol	cryptography based approach	security	security protocol verification tool
Hammi et al. (2018)	blockchain-based authentication mechanism	others	efficiency, cost	Ethereum tool
Salman et al. (2016)	identity-based authentication scheme	identity-based approach	security	AVISPA tool

Table 1, continued (part 4)

Authors	**Methods**	**Classification**	**Performance metrics**	**Software tool**
Saxena, Grijalva & Chaudhari (2016)	authentication and key agreement protocol	mutual authentication method	bandwidth, security	J2ME Wireless Tool Kit (WTK)
Gope et al. (2018)	lightweight and privacy based authentication scheme	lightweight approach	security, communication cost	AVISPA Tool
Li, C. T. et al. (2017a)	efficient user authentication scheme	mutual authentication method	computational cost	-
Tewari & Gupta (2017b)	mutual authentication mechanism	Mutual authentication method	communication cost, storage cost	-
Li, X. et al. (2017b)	robust and energy efficient authentication protocol	mutual authentication method	communication cost, throughput, end-to-end delay, packet delivery ratio	NS-3
Mick, Tourani & Mishra (2017)	lightweight authentication protocol	lightweight approach	convergence time, transmission burden	-
Wallrabenstein (2016)	PUF-based authentication protocol	cryptography based approach	communication cost,	-
Witkovski et al. (2015)	identity management (IdM) & key-based authentication method	identity-based approach	response time	Java
Markmann, Schmidt &Wählisch (2015)	end-to-end authentication scheme	cryptography based approach	time	-
Caparra et al. (2016)	message authentication scheme	others	network lifespan	-

Table 1, continued (part 5)

Authors	**Methods**	**Classification**	**Performance metrics**	**Software tool**
Kothmayr et al. (2013)	datagram transport layer security (DTLS) protocol	cryptography based approach	energy, memory overhead	TelosB
Arasteh, Aghil & Mala (2016)	lightweight authentication protocol	lightweight approach	security	-
Zhao et al. (2011)	mutual authentication scheme	mutual authentication method	security	-
Park, Kim & Bang (2015)	symmetric key-based authentication mechanism	cryptography based approach	data secrecy	-
Hammi et al. (2017)	lightweight mutual authentication protocol	lightweight approach	storage, computing capability	-
Ye et al. (2014)	elliptic curve cryptography based authentication approach	cryptography based approach	computational cost	-
Kothmayr et al. (2012)	datagram transport layer security (DTLS) protocol	identity-based approach	time, energy	-
Ning, Liu & Yang (2014)	aggregated-proof based hierarchical authentication scheme (APHA)	others		-
Janbabaei, Gharaee & Mohammadzadeh (2016)	lightweight authentication protocol	lightweight approach	computational cost	-
Tamboli & Dambawade (2016)	CoAPbased authentication protocol	cryptography based approach	time, communication overhead	Java
Mishra et al. (2018)	efficient authentication approach	identity-based approach	computation, communication, storage cost	-

lightweight approach was very low in the technique, presented in Yang et al. (2016). The performance, attained by the method from Shivraj et al. (2015), was very low, so that it was not deployed in the real-time scenario. Concerning the approach proposed in Arafin, Gao and Qu (2017), the cryptanalysis was not effectively performed, so that the attacks during the communication were possible. The implicit certificate was not applicable in the large-scale networks to perform the authentication process, as this could be seen in Porambage et al. (2014a). The password verifier table was not effectively utilized for updating the identity of the user to achieve secure cryptographic communication in Amin et al. (2018).

Regarding the approach from Wang et al. (2018), the attacker can easily receive the key from the database server and the method also failed to meet the basic security requirements of the authentication protocol. The lightweight protocol failed to ensure authentication between the sensor nodes in the IoT network in the approach of Esfahani et al. (2017). Regarding the technique from Gope et al. (2018), the attacker may easily retrieve the security credentials and perform the forgery attacks. The computational overhead of the authentication mechanism from Mick, Tourani and Misra (2017) was too high. Hence, it was very difficult to implement this mechanism in real-time scenarios. The efficiency of the authentication process was poor in the approach proposed by Arasteh, Aghil and Mala (2016), while the integrity and the confidentiality of the message were not ensured properly by the approach, presented in Hammi et al. (2017). Then, in Janbabaei, Gharaee and Mohammadzadeh (2016), the trust as to performing secure communication between the nodes in the IoT devices was not considered.

We shall now turn to the gaps and issues faced by the mutual authentication approaches. The identity-based approach from Saxena, Grijalva and Chaudhari (2016) featured poor performance of the key identifier. In Kalra and Sood (2015), the coverage capability revealed by the authentication scheme was low. The communication cost was too high in the medical care-based IoT system, presented in Li, C. T. et al. (2017a). Regarding the method proposed in Tewari and Gupta (2017a) and also the one from Li, X. et al. (2017b), the communication and computational costs incurred by them were high. In the work of Zhao et al. (2011), the hardware nodes were not considered.

The cryptography-based approach, proposed in Moosavi et al. (2015), achieved very low performance in establishing a session key for secure communication. The security and the efficiency of the network were not sufficiently accounted for in Alcaide et al. (2013), while with respect to the proposal of Alshahrani, Traore and Woungang (2019), security breaches can occur, due to the non-restriction of the IoT devices. The exact view of the IoT devices, based on, for instance, the use cases was not considered in Mahalle et al. (2013). The energy consumption and the computational cost implied

by the use of the method from Sciancalepore et al (2016) were high. The cryptography-based scheme from Kumari et al. (2017) failed to achieve mutual authentication, key agreement, and device anonymity. The key agreement scheme failed to protect the IoT devices from different attacks as proposed in Mahalle, Prasad and Prasad (2014). The working performance of the system presented in Gaikwad, Gabhane and Golait (2015) was determined to be slow. The method proposed by Wallrabenstein (2016) incurred high communication cost of the key management mechanism. The channel established according to the approach from Park, Kim and Bang (2015) was not safe enough for sharing confidential information. The security problem was not addressed in the perception layer in the method presented by Ye et al. (2014). The performance of the cryptographic mechanism was not improved in the method, proposed in Tamboli and Dambawade (2016).

The identity-based approach, presented in Kothmayr et al. (2012), failed to use the pre-shared cipher key for the constrained nodes. Energy consumption was not considered in Witkovski et al. (2015). The research issues, associated with the two-phase protocol from Porambage et al. (2014b), are related to the failure to address the node capturing attacks. In the method, proposed by Emerson et al. (2015), the database query and the database update were not considered. The delivery ratio of the packets was very low in the approach by Wu et al. (2017). The efficiency was very low for the sensor-based communication protocol, presented in Hou and Yeh (2015). The blockchain-based authentication scheme from Hammi et al. (2018) failed to achieve the communication between the set of bubbles. The anchor lifespan (i.e. the smallest number of authentication processes, after which at least one anchor node runs out of power) of the network was very low in the method, presented in Caparra et al. (2016).

4. Simple statistics and discussion

In this section we present simple statistics and corresponding discussion, related to the IoT authentication-related papers surveyed, based on the authentication methods, the toolset, and the evaluation metrics used.

4.1. The authentication methods proposed

The authentication techniques developed and used in various research papers are categorized here. We distinguish here mainly the authentication methods categorized as lightweight, identity-based, mutual authentication, and cryptography-based. The lightweight approach was used in 19 research works, the mutual authentication approach in 6 papers, and the cryptography-based approach in 14 research papers. The respective proportions can be seen in Fig. 2.

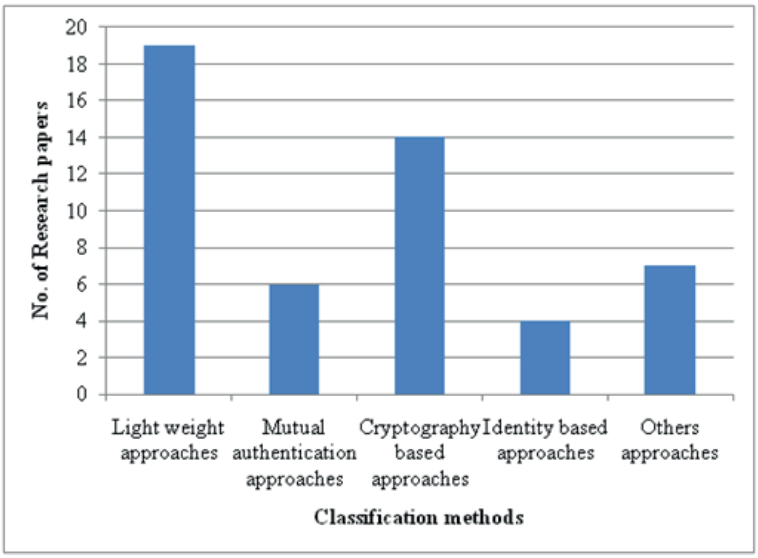

Figure 2: Statistics based on authentication methods

4.2. The toolset-based statistics

We now turn to the toolsets used in various existing authentication methods (note that we do not distinguish here the levels of use of these tools). Thus, for instance, the security verification (ProVerif) tool is used in four research papers of all those surveyed, and the Telos B tool is used in two research works. Further, the Automated Validation of Internet Security Protocols and Applications (AVISPA) tool is used in seven research papers. Then, Java is used in three research works, and the Network Simulator-3 (NS-3) is used in just one report. Finally, such tools as the Apache tomcat, cooja simulator, python, Ethereum tool are used in one research work each. Figure 3 shows clearly that AVISPA is used in the biggest number of the research papers.

4.3. Classification of papers based on evaluation metrics

This section shows and considers the classification of the surveyed papers, based on the evaluation metrics, used in particular studies for purposes of assessing the quality of the methods analyzed in these studies. Table 2 shows the classification of the references in these terms. The evaluation metrics, taken into consideration in the particular studies, are related to memory requirements, communication cost, energy spent, computational cost, efficiency, security, throughput, accuracy, bandwidth, packet loss, and threshold voltage.

Table 2: Classification of references based on evaluation metrics

Evaluation metrics	**References**
Computational cost	Aman et al. (2017); Kalra & Sood (2015); Alcaide et al. (2013); Yang et al. (2016); Amin et al. (2018); Mahalle et al. (2013); Dhillon & Kalra (2017); Wang et al. (2018); Mahalle et al. (2014); Hammi et al. (2017, 2018); Li et al. (2017a); Ye et al. (2014); Janbabaei et al. (2016); Tamboli & Dambawade (2016); Mishra et al. (2018)
Memory	Aman et al. (2017); Porambage et al. (2014a); Tewari & Gupta (2017a); Amin et al. (2018); Kothmayr et al. (2013); Hammi et al. (2017); Mishra et al. (2018)
Communication cost	Aman et al. (2017); Kalra & Sood (2015); Alcaide et al. (2013); Yang et al. (2016); Tewari & Gupta (2017a,b); Amin et al. (2018); Dhillon & Kalra (2017); Kumari et al. (2017); Mahalle et al. (2014); Wallrabenstein (2016); Mishra et al. (2018)
Energy	Aman et al. (2017); Porambage et al. (2014b); Sciancalepore et al. (2016); Gope et al. (2018); Kothmayr et al. (2012, 2013)
Efficiency	Li et al. (2017); Porambage et al. (2014a); Zhou et al. (2019); Hou & Yeh (2015); Hammi et al. (2018)
Security	Porambage et al. (2014a); Punithavathi et al. (2019); Zhou et al. (2019); Shivraj et al. (2015); Wang et al. (2018); Gaikwad et al. (2015); Salman et al. (2016); Gope et al. (2018); Arasteh et al. (2016); Zhao et al. (2016)
Throughput	Moosavi et al. (2015); Wu et al. (2017); Park et al. (2015); Kothmayr et al. (2012); Tamboli & Dambawade (2016)
Bandwidth	Emerson et al. (2015); Sciancalepore et al. (2016)
Packet loss	Yao et al. (2013); Wu et al. (2017); Ning et al. (2014)
Accuracy	Punithavathi et al. (2019); Witkovski et al. (2015)
Threshold voltage	Arafin et al. (2017); Caparra et al. (2016)

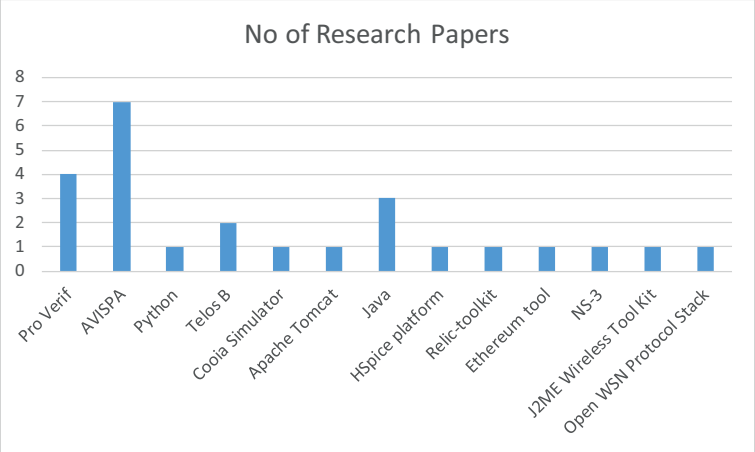

Figure 3: Surveyed publication numbers according to toolsets used

5. Conclusion

The IoT networks provide very substantial benefits in transmitting the data between the IoT nodes and the server. One of the essential aspects of functioning of the IoT networks is authentication. A detailed survey is provided in this paper regarding the IoT authentication methods. The survey encompasses 50 research papers from the recent years. The methods developed and used are classified on the basis of the key management scheme, namely such as the lightweight approach, identity-based approach, mutual authentication approach, and cryptography-based approach. The merits and demerits associated with each of the reviewed works are presented. The research papers that are considered here have been collected through Google scholar, IEEE and other similar services.

The research gaps and issues, related to functionality, are elucidated for the research papers surveyed. Moreover, a simple statistical analysis is performed using the categories of authentication methods, evaluation metrics, and the toolset. From this analysis it definitely appears that the lightweight-based authentication approach seems to be the most widely used IoT authentication method. Then, AVISPA is the toolset used in the biggest number of the research papers considered, and of the metrics used it is communication cost, security, and computation cost that are most widely referred to in assessing the quality of the authentication mechanisms. There are several important challenges, facing IoT technology, which ought to be properly addressed in future works. Once these challenges are successfully addressed, IoT applications can be further developed in such important domains as e-health, intelligent transport, smart cities, and home automation.

References

Alcaide, A., Palomar, E., Montero-Castillo, J. and Ribagorda, A. (2013) Anonymous authentication for privacy-preserving IoT target-driven applications. *Computers & Security*, 37, 111-123.

Alshahrani, M., Traore, I. and Woungang, I. (2019) Anonymous mutual IoT interdevice authentication and key agreement scheme based on the ZigBee technique. *Internet of Things*, 100061.

Aman, M. N., Chua, K. C. and Sikdar, B. (2017) Mutual authentication in IoT systems using physical unclonable functions. *IEEE Internet of Things Journal*, **4**(5): 1327-1340.

Amin, R., Kumar, N., Biswas, G.P., Iqbal, R. and Chang, V. (2018) A light weight authentication protocol for IoT-enabled devices in distributed Cloud Computing environment. *Future Generation Computer Systems*, 78, 1005-1019.

Arafin, M. T., Gao, M. and Qu, G. (2017) VOLtA: Voltage over-scaling based lightweight authentication for IoT applications. In: *IEEE 22nd Asia and South Pacific Design Automation Conference (ASP-DAC)*, 336-341.

Arasteh, S., Aghil, S.F. and Mala, H. (2016) A new lightweight authentication and key agreement protocol for Internet of Things. In: *IEEE 13th International Iranian Society of Cryptology Conference on Information Security and Cryptology (ISCISC)*, 52-59.

Caparra, G., Centenaro, M., Laurenti, N., Tomasin, S. and Vangelista, L. (2016) Energy-based anchor node selection for IoT physical layer authentication. In: *IEEE International Conference on Communications (ICC)*, 1-6.

Dhillon, P. K. and Kalra, S. (2017) A lightweight biometrics based remote user authentication scheme for IoT services. *Journal of Information Security and Applications*, 34, 255-270.

Emerson, S., Choi, Y. K., Hwang, D. Y., Kim, K. S. and Kim, K. H. (2015) An OAuth based authentication mechanism for IoT networks. In: *IEEE International Conference on Information and Communication Technology Convergence (ICTC)*, 1072-1074.

Esfahani, A., Mantas, G., Matischek, R., Saghezchi, F. B., Rodriguez, J., Bicaku, A., Maksuti, S., Taube, M., Schmittner, C. and Bastos, J. (2017) A lightweight authentication mechanism for m2m communications in industrial IoT environment. *IEEE Internet of Things Journal*, **6** (1), 288 – 296.

Gaikwad, P. P., Gabhane, J. P. and Golait, S. S. (2015) 3-level secure Kerberos authentication for Smart Home Systems using IoT. In: *IEEE 1st International Conference on Next Generation Computing Technologies (NGCT)*, 262-268.

Gope, P., Amin, R., Islam, S. H., Kumar, N. and Bhalla, V. K. (2018) Lightweight and privacy-preserving RFID authentication scheme for distributed IoT infrastructure with secure localization services for smart city

environment. *Future Generation Computer Systems*, 83, 629-637.

Hammi, M. T., Livolant, E., Bellot, P., Serhrouchni, A. and Minet, P. (2017) A lightweight mutual authentication protocol for the IoT. In: *International Conference on Mobile and Wireless Technology*, Springer, Singapore, 3-12.

Hammi, M. T., Hammi, B., Bellot, P. and Serhrouchni, A. (2018) Bubbles of Trust: A decentralized blockchain-based authentication system for IoT. *Computers & Security*, 78, 126-142.

Hou, J. L. and Yeh, K. H. (2015) Novel authentication schemes for IoT based healthcare systems. *International Journal of Distributed Sensor Networks*, **11**(11): 183659.

Janbabaei, S., Gharaee, H. and Mohammadzadeh, N. (2016) Lightweight, anonymous and mutual authentication in IoT infrastructure. In: *IEEE 8th International Symposium on Telecommunications (IST)*, 162-166.

Kalra, S. and Sood, S. K. (2015) Secure authentication scheme for IoT and cloud servers. *Pervasive and Mobile Computing*, 24, 210-223.

Kothmayr, T., Schmitt, C., Hu, W., Brünig, M. and Carle, G. (2012) A DTLS based end-to-end security architecture for the Internet of Things with two-way authentication. In: *IEEE Conference on Local Computer Networks-Workshops*, 956-963.

Kothmayr, T., Schmitt, C., Hu, W., Brünig, M. and Carle, G. (2013) DTLS based security and two-way authentication for the Internet of Things. *Ad Hoc Networks*, **11**(8): 2710-2723.

Kumari, S., Karuppiah, M., Das, A. K., Li, X., Wu, F. and Kumar, N. (2017) A secure authentication scheme based on elliptic curve cryptography for IoT and cloud servers. *The Journal of Supercomputing*, **74**,1-26.

Li, N., Liu, D. and Nepal, S. (2017) Lightweight mutual authentication for IoT and its applications. *IEEE Transactions on Sustainable Computing*, **2**(4): 359-370.

Li, C. T., Wu, T. Y., Chen, C. L., Lee, C. C. and Chen, C. M. (2017a) An efficient user authentication and user anonymity scheme with provably security for IoT-based medical care system. *Sensors*, **17**(7): 1482.

Li, X., Peng, J., Niu, J., Wu, F., Liao, J. and Choo, K. K. R. (2017b) A robust and energy efficient authentication protocol for industrial internet of things. *IEEE Internet of Things Journal*, **5**(3): 1606-1615.

Mahalle, P. N., Anggorojati, B., Prasad, N. R. and Prasad, R. (2013) Identity authentication and capability based access control (iacac) for the internet of things. *Journal of Cyber Security and Mobility*, **1**(4): 309-348.

Mahalle, P. N., Prasad, N. R. and Prasad, R. (2014) Threshold cryptography-based group authentication (TCGA) scheme for the internet of things (IoT). In: *IEEE 4th International Conference on Wireless Communications, Vehicular Technology, Information Theory and Aerospace & Electronic Systems (VITAE)*, 1-5.

Markmann, T., Schmidt, T.C. and Wählisch, M. (2015) Federated end-

to-end authentication for the constrained internet of things using ibc and ecc. *ACM SIGCOMM Computer Communication Review*, **45**(4): 603-604.

Mick, T., Tourani, R. and Misra, S. (2017) Laser: Lightweight authentication and secured routing for IoT in smart cities. *IEEE Internet of Things Journal*, **5**(2): 755-764.

Mishra, D., Vijayakumar, P., Sureshkumar, V., Amin, R., Islam, S. H. and Gope, P. (2018) Efficient authentication protocol for secure multimedia communications in IoT-enabled wireless sensor networks. *Multimedia Tools and Applications*, **77**(14): 18295-18325.

Moosavi, S. R., Gia, T. N., Rahmani, A. M., Nigussie, E., Virtanen, S., Isoaho, J. and Tenhunen, H. (2015) SEA: a secure and efficient authentication and authorization architecture for IoT-based healthcare using smart gateways. *Procedia Computer Science*, 52, 452-459.

Ning, H., Liu, H. and Yang, L.T. (2014) Aggregated-proof based hierarchical authentication scheme for the internet of things. *IEEE Transactions on Parallel and Distributed Systems*, **26**(3): 657-667.

Park, N., Kim, M. and Bang, H. C. (2015) Symmetric key-based authentication and the session key agreement scheme in IoT environment. In: *Computer Science and its Applications*. Springer, Berlin, Heidelberg, **330**, 379-384.

Porambage, P., Schmitt, C., Kumar, P., Gurtov, A. and Ylianttila, M. (2014a) Two-phase authentication protocol for wireless sensor networks in distributed IoT applications. *IEEE Wireless Communications and Networking Conference (WCNC)*, 2728-2733.

Porambage, P., Schmitt, C., Kumar, P., Gurtov, A. and Ylianttila, M. (2014b) PAuthKey: A pervasive authentication protocol and key establishment scheme for wireless sensor networks in distributed IoT applications. *International Journal of Distributed Sensor Networks*, **10**(7): 357-430.

Punithavathi, P., Geetha, S., Karuppiah, M., Islam, S. H., Hassan, M. M. and Choo, K. K. R. (2019) A lightweight machine learning-based authentication framework for smart IoT devices. *Information Sciences*, 484, 255-268.

Salman, O., Abdallah, S., Elhajj, I. H., Chehab, A. and Kayssi, A. (2016) Identity-based authentication scheme for the Internet of Things. *IEEE Symposium on Computers and Communication (ISCC)*, 1109-1111.

Saxena, N., Grijalva, S. and Chaudhari, N.S. (2016) Authentication protocol for an IoT-enabled LTE network. *ACM Transactions on Internet Technology (TOIT)*, **16**(4): 25.

Sciancalepore, S., Piro, G., Boggia, G. and Bianchi, G. (2016) Public key authentication and key agreement in IoT devices with minimal airtime consumption. *IEEE Embedded Systems Letters*, **9**(1): 1-4.

Shivraj, V. L., Rajan, M. A., Singh, M. and Balamuralidhar, P. (2015) One time password authentication scheme based on elliptic curves for Internet of Things (IoT). In: *IEEE 5th National Symposium on Infor-*

mation Technology: Towards New Smart World (NSITNSW), 1-6.

Tamboli, M. B. and Dambawade, D. (2016) Secure and efficient CoAP based authentication and access control for Internet of Things (IoT). In: *IEEE International Conference on Recent Trends in Electronics, Information & Communication Technology (RTEICT)*, 1245-1250.

Tewari, A. and Gupta, B. B. (2017a) A lightweight mutual authentication protocol based on elliptic curve cryptography for IoT devices. *International Journal of Advanced Intelligence Paradigms*, **9**(2-3): 111-121.

Tewari, A. and Gupta, B. B. (2017b) Cryptanalysis of a novel ultra-lightweight mutual authentication protocol for IoT devices using RFID tags. *The Journal of Supercomputing*, **73**(3): 1085-1102.

Wallrabenstein, J. R. (2016) Practical and secure IoT device authentication using physical unclonable functions. In: *IEEE 4th International Conference on Future Internet of Things and Cloud (FiCloud)*, 99-106.

Wang, K. H., Chen, C. M., Fang, W. and Wu, T. Y. (2018) On the security of a new ultra-lightweight authentication protocol in IoT environment for RFID tags. *The Journal of Supercomputing*, **74**(1): 65-70.

Witkovski, A., Santin, A., Abreu, V. and Marynowski, J. (2015) An IdM and key-based authentication method for providing single sign-on in IoT. In: *IEEE Global Communications Conference (GLOBECOM)*, 1-6.

Wu, F., Xu, L., Kumari, S., Li, X., Shen, J., Choo K. K. R., Wazid M. and Das A. K. (2017) An efficient authentication and key agreement scheme for multi-gateway wireless sensor networks in IoT deployment. *Journal of Network and Computer Applications*, 89, 72-85.

Yang, Y., Cai, H., Wei, Z., Lu, H. and Choo, K. K. R. (2016) Towards lightweight anonymous entity authentication for IoT applications. In: *Proceedings of Australasian Conference on Information Security and Privacy*. Springer, Cham 265-280.

Yao, X., Han X., Du X. and Zhou X. (2013) A lightweight multicast authentication mechanism for small scale IoT applications. *IEEE Sensors Journal*, **13**(10): 3693-3701.

Ye, N., Zhu, Y., Wang, R. C., Malekian, R. and Qiao-min, L. (2014) An efficient authentication and access control scheme for perception layer of internet of things. *Applied Mathematics & Information Sciences*, **8**(4): 1617.

Zhao, G., Si, X., Wang, J., Long, X. and Hu, T. (2011) A novel mutual authentication scheme for Internet of Things. In: *IEEE International Conference on Modelling, Identification and Control*, 563-566.

Zhou, L., Li, X., Yeh, K. H., Su, C. and Chiu, W. (2019) Lightweight IoT-based authentication scheme in cloud computing circumstance. *Future Generation Computer Systems*, 91, 244-251.