Journal of Sustainability Science and Management
Volume 17 Number 9, September 2022: 162-178
eISSN: 2672-7226

SYSTEMATIC LITERATURE REVIEW FOR LIGHTWEIGHT AUTHENTICATION ALGORITHM IN THE IoT

SAKIINAH ALTAF HUSSAIN*, AZNI HASLIZAN AB HALIM* AND NAJWA HAYAATI MOHD ALWI

Faculty of Science and Technology, Universiti Sains Islam Malaysia (USIM), Bandar Baru Nilai, 71800 Nilai, Negeri Sembilan, Malaysia.

**Corresponding author: sakiinahaltaf.fst@gmail.com, ahazni@usim.edu.my*
Submitted final draft: 17 June 2022 *Accepted: 8 July 2022* http://doi.org/10.46754/jssm.2022.09.011

Abstract: The Internet of Things (IoT) being a promising technology of the future is expected to generate a tremendous amount of data that may be exposed to security flaws. Hence, to protect IoT applications from hackers, lightweight cryptography has been identified as one of the suitable mechanisms since it is designed to fulfil security demands in resource-constrained hardware and software. This paper aims to analyse the current security requirements in designing lightweight cryptography for IoT applications, specifically for integrity and authentication algorithms. There are three objectives to focus on: Determine the current state of integrity and authentication research, investigate the integrity and authentication requirements, and analyse the lightweight authentication algorithm currently used. The Kitchenham systematic review method was adopted using a four-step process. The selected articles in this study were retrieved from four reputable databases and 57 of them were deemed suitable for analysis after meeting the selection criteria. From this systematic literature review, it was discovered that there were three active research focuses on the IoT. The research focuses were mostly on cyberattacks against IoT applications, system security requirements and algorithms for lightweight authentication. Furthermore, the analysis also revealed the convergence of lightweight authentication algorithms to ensure the future sustainability of applications. This study may provide researchers with a reference in designing lightweight authentication algorithms to achieve the desired security requirements for sustainable security management in IoT.

Keywords: Lightweight cryptography, authentication, integrity, IoT application.

Introduction

The Internet of Things (IoT) is a modern concept in which everyday objects such as office and home appliances are linked through the Internet with the ability to interact with each another. It enables the direct integration of smart devices with virtual world sensors, RFID tags, smartphones and wearable devices (Li *et al.*, 2017). The application domains available via IoT networks such as environmental surveillance, healthcare, smart cities, military relations and intelligent transportation systems have been advancing at a rapid pace (Almulhim *et al.*, 2019). It was expected that more than a billion sensors, actuators, GPS devices, mobile devices and other smart items have been linked to the Internet in 2020 (Columbus, 2017).

The number of IoT devices in public networks has increased tremendously and such systems are always communicating to collect data from the real world. The data is gleaned from authorised users and sent to terminal nodes via a wireless network (Bosch *et al.*, 2008). The terminal nodes will store and relay the information to the main platform. These many layers of communication process will become vulnerable to cyberattacks if no security system is implemented (Blackburn & Robshaw, 2016). Thus, mutual authentication is necessary during the communication process to ensure data security.

Mutual authentication is extremely important in IoT security. In an unprotected perimeter, a remote user may gain unauthorised

access into nodes by using hacking applications (Delvaux *et al.*, 2016). Once paired, unique information can be extracted from specific nodes. As a result, remote-user authentication is critical, since deploying resourceful gateway nodes in IoT networks will speed up data transmission and increase system efficiency in terms of processing capacity, battery backup, memory, speed and other factors (Wendt & Potkonjak, 2014). The IoT devices differ from traditional wired networks in terms of architecture, characteristics and applications. Using conventional encryption is not practical for low-resource devices. Therefore, to encrypt data in such devices, the lightweight algorithm has emerged as one of the best implementations without consuming a lot of energy (Shen *et al.*, 2019).

Thus, it is really important to secure the data that execute functionalities of IoT by incorporating cryptograph technology in smart devices. This is to ensure that the data transmitted through wireless transmission is secured and shared among intended devices only. The data may be secured with an encryption algorithm, where a secret key is used to code and decode it (Delvaux *et al.*, 2016).

Cryptography may be used to ensure the authenticity and integrity of data but traditional cryptography approaches require a significant amount of resource allocation. Therefore, different approaches in securing the network must be considered because IoT devices have limited processing power, memory and battery life (Sharma *et al.,* 2017). Due to these limiting factors, lightweight cryptography has been established to manage the security of low resource devices. Lightweight cryptography is not only aimed at securing data but it also ensures that the energy consumption and memory usage in IoT devices are as low as possible (Shen *et al.*, 2019).

One example of a highly researched lightweight cryptography method is Smart Health which is also known as e-health and is used in hospitals. One of the functions of e-health is to consistently monitor a patient's condition. Hence, it is crucial to secure the patient's data transmitted between e-health devices (Cherdantseva & Hilton, 2013). Outside the hospital, doctors may be interested in reviewing the medical history of their patients. If a hospital's IOT system is not secure, hackers may gain access to devices, take over their functions and change the data they collect. Altered and compromised data may also cause a delay or mistake in administering treatment that could harm patients.

Applying lightweight cryptography in IoT applications can reduce the risk of compromising data privacy. The first process in IoT is the exchange of data over the Internet. This part of the system is most vulnerable which is frequently targeted by hackers. On its own, the data transmitted by a given endpoint may not raise any privacy concerns. However, fragmented data from various endpoints may produce sensitive information when gathered, collated and evaluated.

In this paper, the lightweight authentication algorithm is reviewed following a systematic literature review (SLR) described by Kitchenham *et al.* (2004) which defines systematic review as "a means of identifying, evaluating and interpreting all available research relevant to a particular research question or topic area or phenomenon of interest". A systematic review is well-known in the fields of software engineering and medical research and it is also used in other fields because it is evidence-based and the results are more accurate than mere observations or viewpoints (Taylor *et al.*, 2020). The Internet of Things will become the new norm in the near future, and a good security system is needed to build people's confidence in using its devices. As a result, each IoT device needs a distinct identity that can be verified when it tries to connect to a gateway or central server. It is important for IT system managers to track each device that logs into a system. Therefore, the objectives in this study are to: (1) Analyse the current state of integrity and authentication research for lightweight algorithms in IoT applications, (2) Study the integrity and authentication requirements of

the algorithms and (3) Analyse the algorithms currently in use. The knowledge gained from this study may contribute to the:

(a) Development of better lightweight algorithms

(b) Provision of suitable security requirements for lightweight algorithms and

(c) Discovery of strengths and weaknesses in previous studies on lightweight algorithms

Research Method

The review process is shown in Figure 1. The first process entailed the formulation of research questions. The search for publications which included source of selection and keywords was then carried out based on inclusion-exclusion criteria. In the last step, information from selected publications were extracted, stored and arranged in a list.

Formulation of Research Questions

The research questions (RQ) are stated in Table 1. With respect to RQ1, the question tried to answer the general view of the research trend in the integrity of IoT applications based on a lightweight authentication algorithm. To address RQ1, the number of published journals and conferences dated from 2011 until 2021 were identified. RQ2 investigates the integrity and authentication requirements of lightweight algorithms and RQ3 examined the lightweight algorithms currently used in IoT applications.

Search Process

The most crucial aspect of a SLR is the search process. The search for articles in the English language was conducted in seven phases as illustrated in Figure 2 from the following databases:

- IEEE Digital Library
- Springer/Elsevier
- Scopus
- Google Scholar

Figure 2 explains the outline of the search process. Phase 1 was a general literature search using keywords like "*authentication*" and "*integrity*" and "*IoT application*" and "*lightweight cryptography*". In Phase 2, all articles with their titles and abstracts containing the keywords were downloaded. In Phase 3, once all the downloaded articles had been read, the articles were arranged according to topic such as the security, architecture and algorithms. A total of 52 articles were selected in Phase 3, and in Phase 4 and Phase 5, a refined search was carried out on the 52 articles using synonyms of Phase 1 keywords (e.g., "*authentication*" was changed to "*verification*"). After these phases, five articles were found to match the synonyms that focused on topics in the SLR.

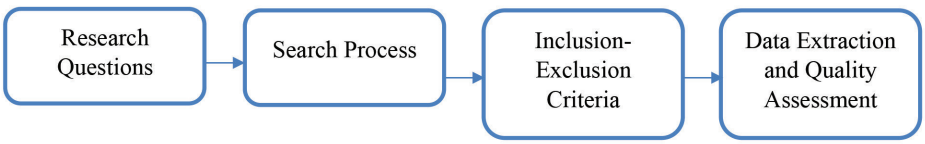

Figure 1: The steps of the SLR described by Kitchenham *et al.* (2004)

Table 1: Three research questions to address in this study

No.	Details
RQ1	1. What is the current research trend in integrity and authentication algorithms of IoT applications? 1.1 What are the attacks that can jeopardise the integrity of IoT applications?
RQ2	2. What are the security requirements and mechanisms needed to resolve integrity and authentication attacks?
RQ3	3. Which lightweight algorithm is suitable to achieve integrity requirements in IoT?

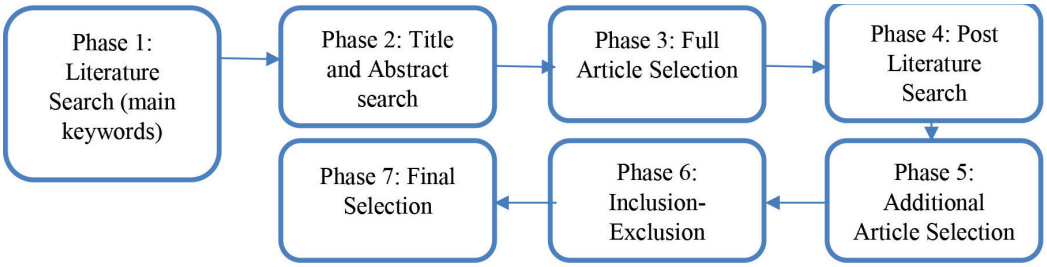

Figure 2: Search process of SLR

Inclusion and Exclusion Criteria

Before the articles were accepted as primary articles, they were screened against the inclusion and exclusion criteria in Phase 6. The inclusion criteria in Table 2 were used to pick the primary articles. After that, articles that fell into the exclusion criteria in Table 3 were excluded.

Data Extraction and Quality Assessment

The objective of data extraction after final article selection in Phase 7 was to consistently obtain outcomes to answer the review questions. A data extraction form must be completed to precisely and impartially capture the information received from selected articles. Table 4 outlines five criteria used to evaluate the quality of selected

Table 2: Criteria used in accepting searched articles

INC#	Inclusion Criteria
INC1	The integrity of IoT applications must be a major topic of the publication
INC2	The article should explain the methods of authentication algorithms in IoT applications

Table 3: Criteria used in excluding searched articles

EXC#	Exclusion Criteria
EXC1	The article did not focus on integrity and authentication in IoT applications
EXC2	The article does not explain the authentication algorithm in IoT applications
EXC3	Short articles, proposals, Technical Papers, Doctoral workshops and tutorials that were not peer-reviewed

Table 4: Data extraction and quality assessment

Item	Answer
QA1: Was the article peer-reviewed?	Yes/No
QA2: Was there a clear statement of the objectives?	Yes/No/Partially
QA3: Was there adequate description of the context in which the research was carried out? For example, did it clearly state the problems that led to the research, descriptions of research methodology used, etc.	Yes/No/Partially
QA4: Was the data collection performed thoroughly? For example, did the evaluation of the proposed approach answer the research questions? did the article provide a thorough discussion of results?	Yes/No/Partially
QA5: Was the simulation results rigorously analysed?	Yes/No/Partially

articles, which was according to the quality assessment criteria used by Dybå (2008) and Salleh (2011). The following ratio scales were used: Yes = 1 point, No = 0 point and Partially = 0.5 point.

Results and Discussion

The outcome of the SLR is presented in this section. Each subsection contained information that answered the research questions in Table 1.

RQ1: What is the current research trend in integrity and authentication algorithms of IoT applications?

The number of articles presented from 2011 to 2020 before the quality assessment is shown in Figure 3. The chart shows that lightweight authentication in IoT applications was not a priority in the early years of 2011 to 2014. Starting from 2015 onwards, the number of articles increased exponentially as smart devices became affordable and gained widespread usage (Pal *et al.*, 2018). From 2011 until 2014, research on lightweight algorithms was also at an early stage. The topics discussed in the articles were mostly on attacks that could occur in IoT applications, the security requirements to protect the applications and proposals of suitable algorithms. Figure 3 shows the number of articles that had been found based on the keywords used (*lightweight cryptography, authentication, integrity and IoT applications*). There were 109 papers that corresponded with the keywords. A total of 57 articles were retrieved after thorough selection based on inclusion-exclusion criteria and quality assessments in Tables 2, 3 and 4, of which 52 were found from the primary search and the other five were selected from the second search using the keyword "*verification*".

Figure 4 shows the pie chart of the number of articles classified according to the topics in IoT security, namely attacks, security mechanisms and algorithms. There were 18 articles on attacks, 26 on security requirements and mechanisms, and 13 on the algorithms of lightweight cryptography. To understand how lightweight cryptography worked in securing an IoT system, the articles on IoT attacks that were related to authentication and integrity were analysed and reviewed. The attacks could detect vulnerabilities in IoT applications and determine the security requirements needed to prevent them. Security requirements also highlighted the importance of enforcing security policies in IoT applications. Once security requirements had been established, the suitable algorithms could be designed.

RQ1.1: What are the attacks that can jeopardise the integrity of IoT applications?

Numerous attacks had been carried out against IoT applications. This paper would be focusing on attacks that jeopardised the authenticity and integrity of the applications. Analysis of the 52 primary articles found that most incidents

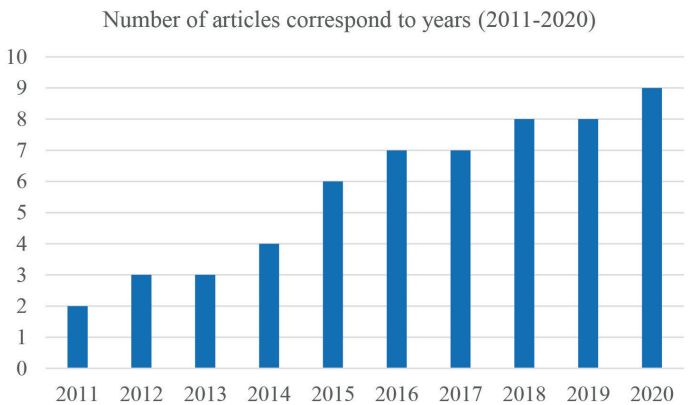

Figure 3: Numbers of articles after inclusion and exclusion criteria (2011-2020)

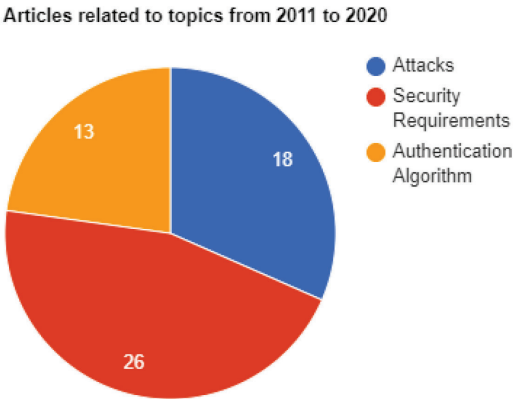

Figure 4: Classification of articles (2011 to 2020)

comprised man-in-the-middle (MIM) attacks, linkage attacks, data manipulation, side-channel attacks, unauthorised access, hash collision and spoofing. From the primary articles, 18 discussed the attacks that threatened the integrity of IoT applications. Table 5 lists the articles that discussed specific attacks and their mechanism.

MIM attacks seemed to be the most common which occur when hackers hijack the data traffic between devices and cloud-based applications. A hacker could break into the communication between two systems to delay or spoof them (Brinkmann *et al.*, 2013; Liu *et al.*, 2015). MIM presented a credible threat to IoT applications since the damage caused might vary from small to huge, depending on the hackers' goal. This type of attack could cause disruptions in IoT applications, especially if the

Table 5: Articles that discuss attacks on the integrity of IoT applications

Authors	Attacks	Mechanism
1. Liu *et al.* (2015) 2. Brinkmann *et al.* (2013) 3. Grobauer *et al.* (2011) 4. Kaaniche and Laurent (2017) 5. Cherdantseva and Hilton (2013) 6. Aleisa and Renaud (2017) 7. Ahmed *et al.* (2018) 8. Abdulghani *et al.* (2019) 9. Claycomb and Nicoll (2012) 10. Grobauer *et al.* (2011)	Man-in-the-middle attack	The hacker intercepts a communication between two systems and tricks the recipient into thinking they are still getting a legitimate message
1. Kumar *et al.* (2018) 2. Miorandi *et al.* (2016) 3. Cherdantseva and Hilton (2013)	Linkage attack	The hacker manipulates the intercepted data without interfering with the actual IoT applications, stealing critical information in the process
1. Roman *et al.* (2013) 2. Williams *et al.* (2016) 3. Yu and Guo (2016) 4. Abdulghani *et al.* (2019) 5. Grobauer *et al.* (2011) 6. Miorandi *et al.* (2016)	Data manipulation	Using SQL injection and cross-site scripting, the hacker attacks IoT apps directly

1. Harnik *et al.* (2017) 2. Abdulghani *et al.* (2019) 3. Grobauer *et al.* (2011) 4. Cherdantseva and Hilton (2013) 5. Aleisa and Renaud (2017)	Side-channel attack	Due to the lack of security mechanisms in storing IoT data, the hacker indirectly leaks private data that has already been generated and processed by the IoT applications
1. Kaaniche and Laurent (2017) 2. Kothmayr and Thomas (2013) 3. Abdulghani *et al.* (2019) 4. Williams *et al.* (2016) 5. Claycomb and Nicoll (2012)	Unauthorised access	Due to the lack of effective encryption measures, hackers can gain access to poorly encrypted data
1. Rashid *et al.* (2012) 2. Aleisa and Renaud (2017)	Hash collision	Because the hash function has varied input lengths and short fixed-length output, the hacker may indirectly reveal private data previously collected and processed by the IoT application. As a result, there is a chance that two different inputs may yield the same output
1. Hasan and Mohan (2019) 2. Kumar *et al.* (2018)	Spoofing	Attack impersonates a legitimate user of a device to gain access to IoT applications

authentication security was weak. Furthermore, MIM could cause the attacker to harvest personal information and login credentials. The lack of security in IoT applications would encourage MIM attacks since the hacker could send command-and-control instructions of the IoT applications to execute false outputs.

To solve MIM attacks, Kaaniche and Laurent (2011) used a robust encryption mechanism between the client and server. Connection was established only after the server authenticated a client's request by presenting and validating a digital certificate. The risk of unauthorised access and sensitive data leaks would increase as the interconnected links between data sources and IoT applications grow, with each additional link increasing the risk exponentially (Kumar *et al.*, 2018). This type of attack occurred when numerous data sources were intercepted and cross-referenced, resulting in partial data identification (Cherdantseva & Hilton, 2013). The hackers could tamper with the intercepted data without interfering in the IoT applications themselves. Unauthorised access could disclose information and sensitive data. The hackers could also modify, erase and copy data to jeopardise the integrity of IoT applications.

Physical security measures would be among the best methods to prevent unauthorised access to data stored on the cloud or physical server (Williams *et al.*, 2016). Some examples included deploying security guards, physical barriers, CCTV monitoring and locks on servers and terminals. Due to the utilisation of connected sensors and actuators, it would also be good to integrate physical security measures with IoT technology (Claycomb & Nicoll, 2012).

Data manipulations occur when the hacking results in modification of records (Williams *et al*., 2016). The hackers would modify the information after intercepting or accessing data to benefit themselves (Grobauer *et al.*, 2011). Exploiting multiple vulnerabilities in IoT applications (such as SQL injection and cross-site scripting) and taking advantage of inadequate security mechanisms (such as small or weak passwords) were two examples of data modification (Miorandi *et al.*, 2016).

IoT data breaches could be avoided by using secured storage techniques that incorporated cryptographic schemes (Yu & Guo, 2016). An example cryptographic-based storage strategy was the Shamir Secret Sharing method, in which aggregated IoT data could be securely stored in

an object (Williams *et al.*, 2016). POTSHARDS is an example of a non-cryptographic-based approach that provided long-term security for IoT data without the need for encryption (Roman *et al.*, 2013). The security aspect of this approach was based on the division of data into many segments, each with its own pointer and then scattered over separate storage servers. If an attacker wanted to retrieve data from a single segment, he must first obtain all of the segment's pointers, which was difficult as they were spread across many storage points (Abdulghani *et al.*, 2019).

A side-channel attack is predicated on the finding of information by analysing the algorithmic implementation's accessible side features such as process timing, power consumption and even accompanying sounds (Harnik *et al*., 2016). This type of attack could occur owing to a lack of secure IoT data processing and storage mechanisms such as storing unencrypted data in the cloud or on IoT applications. Data leakage attacks on Cascading Style Sheets (CSS) such as file confirmation and understanding the content of files had been discussed in Aleisa and Renaud, (2017). A hacker who knew the plain text content of a file could use file confirmation to see if a duplicate had been saved elsewhere in the CSS (Abdulghani *et al.*, 2018). When learning the contents of a file, the hacker could obtain highly sensitive information because he already recognised the majority of the file and had tried to guess or identify the unknown portions by comparing the encryption output with the observed ciphertext (Cherdantseva & Hilton, 2013).

The ways to mitigate side-channel attacks involved the use of transient data storage. Transient data storage refers to the ability to keep or discard data after a system had completed its tasks. Nonetheless, a small number of studies had focused on how to manage ephemeral IoT data created during system execution (Harnik *et al.*, 2017). The significance of transient data would arise from the processing of data during system execution to generate new versions of data that could be stored or deleted according to the users' requirements (Cherdantseva & Hilton, 2013).

Spoofing happens when a hacker impersonates an authorised user to access a system or vice versa. The hacker sends fake data to IoT devices, causing them to mistakenly believe it was from the original source. As a result, the attacker would have complete access to the devices, rendering them vulnerable (Hasan & Mohan, 2019).

Replaying is a type of attack in which a service that had been authorised was forged by a second "duplicate call" to repeat authorised commands (Kumar *et al.*, 2018). When a hacker eavesdropped a secure network communication used by IoT devices, then intercepted the data and fraudulently delayed or resent it, the recipient could be misled into doing what the hacker wanted. The added risk of replay attacks was that after obtaining a message from IoT devices and networks, a hacker would not even need specialised skills to decode it (Hasan & Mohan, 2019).

RQ2: What are the security requirements and mechanisms needed to resolve integrity and authentication attacks?

This section discusses security requirements and mechanisms to resolve attacks relating to integrity of IoT applications. There are 21 articles discussing the topic of security requirements and mechanisms. Table 6 below shows the articles that discussed security requirements for IoT applications. From the articles, there are five security requirements related to authentication and integrity. These requirements explained their functionality to uphold security policies and the need to establish authentication protocols.

Lightweight solutions should consider the constrained nature of devices. Computational limitation would affect the implementation of cryptographic techniques and protocols supported by the applications (Aswale *et al.*, 2015). By optimising energy consumption, lightweight security systems must strike a balance between power requirements and battery capacity

Table 6: Studies on security requirements for IoT applications

Authors	Security Requirements	Description
1. Aswale *et al.* (2019) 2. Al-Fuqaha *et al.* (2015) 3. Gubbi *et al.* (2013) 4. Davoli *et al.* (2019) 5. Hameed *et al*. (2019)	Lightweight mechanism	Light-weight security mechanism must be designed with device limitations in mind such as energy consumption, limited memory and computational processing
1. Ahanger and Aljumah (2019) 2. Dhumane *et al.* (2016) 3. Liu *et al.* (2017) 4. Cai *et al.* (2016)	End-to-end security	Provisioning for security must cover secure storage, communication, content, authentication and integrity
1. Bansal and Kumar (2020) 2. Yaqoob *et al.* (2019) 3. Das *et al.* (2018) 4. Hammi *et al.* (2017) 5. Grobauer *et al.* (2011)	Privacy	Users want to keep their personal information private while getting the services they need
1. Alam *et al.* (2020) 2. Li *et al.* (2020) 3. Grobauer *et al.* (2011) 4. Sharma *et al.* (2018)	Identity management	Authentication helps to identify users which can be performed through the login of username, biometrics, etc.
1. Sicari *et al.* (2015) 2. Deep *et al.* (2019) 3. Mohsen and Jha (2016)	Mobility	Mobility requires the ability to accelerate tendencies for the device to provide transparent services while ensuring that the user will not experience interruptions or disconnections of network

of devices. IoT applications needed a security algorithm that uses less memory, consumes less power and could quickly execute a command.

Another practical would be end-to-end security. Communication between IOT devices would go through numerous administrative domains. Thus, provisioning for security must cover the complete span of a connection including secure storage, communication, content, authentication and system integrity (Dhumane *et al.*, 2016). Privacy is when the magnitude and nature of the IoT necessitates a special focus on issues of privacy to protect the data and information of users from exposure in the IoT environment (Cai *et al.*, 2016).

IoT application requires performing identification and anonymity verifications whether at the individual device or larger grouping level. The security must include dependable ways for managing device and user identities as well as the ability to handle links between these identities in a flexible manner (Alam *et al.*, 2020). This included the seamless integration of diverse services across several domains to link different devices and users as well as flexible support for identity management and mutual authentication for users, devices, apps and associated services. Security solutions must recognise that foreknowledge of the participants in an interaction was not always possible and would give means to deal with the size of the number of identities in the system (Sharma *et al.*, 2018). Because of the scalability issue, identity would not always be managed finely and frequently had to be managed in a more scalable fashion like employing one identity to refer to several entities (Grobauer *et al.*, 2011). While identification might be thought of as a generic security requirement, the size of the IoT would necessitate novel ways of identifying management. This requirement had

helped in terms of authentication, whereby different users of IoT applications could be authenticated via logging in to the applications, biometric identification and radio frequency identification (RFID) tags.

The IoT could be tremendously operating on a large scale, with individual components being highly mobile. Thus, mobility requirements were needed. Such systems must be extremely dynamic (Sicari *et al.*, 2015). Mobility could be divided into three categories namely dynamic infrastructure, location privacy and multiple jurisdictions. Because of the dynamic topology and resource-constrained nature of IoT devices, data transmission routing would become critical. In most cases, nodes in the IoT did not need to connect to the Internet, instead they could connect through any network such as Wireless Sensor Network (WSN), Wireless Local Area Network (WLAN) or Personal Area Network (PAN) (Deep *et al.*, 2019). In a real-time environment, the security approach must take into accounts the extent of the variances in structure, location and architecture. Security solutions that allowed smooth transition of jurisdictions and information exchange between connected devices, users and things were required to facilitate the mobility of connected devices, people and things (Mohsen & Jha, 2016). Mobility ensures that the data stored in the database could be synchronized with mobile devices to execute the accurate outcome in any place (Deep *et al.*, 2019).

IoT architecture required a security mechanism to be implemented at every layer. This is to safeguard each layer with security protection so that any attacks that occurred within the layer would not be possible. Table 7 shows the security mechanism for every IoT layer.

Based on Table 7, a MIM attack could occur in the perception and network layer. Besides MIM, unauthorised access could also occur in these two layers plus the application layer. Thus, privacy protection by end-to-end authorisation must be applied in these two layers to combat this attack. Data manipulation and spoofing could occur in three layers which were perception, network and application layer, thus, it was important to establish authentication key management. From Table 7, it was important to

Table 7: IoT layers concerning security mechanism

Authors	IoT Layer	Authentication Algorithm	Attacks	Security Mechanism
Singh and Chatterjee (2015)	Application	Multiple authentications using physical context	Data manipulation, spoofing	Authentication
Lai *et al.* (2013)	Perceptual, network and application	Privacy-preserving using ECC	Unauthorised access	Privacy protection
Nicanfar *et al.* (2014)	Network and perceptual	Authentication and key management using entity ID and serial number	A man-in-the-middle attack, unauthorised access	Intrusion detection system Privacy protection
Schmitt *et al.* (2016)	Perceptual, network and application	Two-way authentication using RSA and ECC	Data manipulation	Authentication key management
Ye *et al.* (2014)	Network and perceptual	Access control using ECC	Spoofing	Access control mechanisms

launch a strong authentication method to protect the IoT applications from attacks, as well as to protect the integrity of IoT system.

RQ3: Which lightweight algorithm is suitable to achieve integrity requirements in IoT?

There were various lightweight algorithms proposed by authors that focused on the authentication and integrity of IoT applications. These algorithms were reviewed to determine the strength and weaknesses of IoT.

Yangling (2013) defined the intelligent service security in terms of application protocol. It combined cross-platform communication with encryption, signature and authentication to boost the capabilities of IoT applications. On the other hand, Kothmayr and Thomas (2013) introduced a two-way authentication protection scheme known as the Datagram Transport Layer Security (DTLS) protocol which was based on RSA and optimised for IPv6 over Low Power Wireless Personal Area Networks (6LoWPANs) and is located between the transport and application layers. Furthermore, Hammi *et al.* (2017) suggested a robust shared authentication protocol for WSNs which focused on Optimization of Communication for Ad hoc Reliable Industrial Networks (OCARI). OCARI proposed that at the MAC sub-layer of OCARI, all nodes wishing to access the network should be authenticated.

Turkanovi (2014) introduced a polynomial schema with two suitable key management systems using hash protocols. The algorithm could handle authentication and prevent MIM attacks. Later, Wu (2017) proposed a transmission model with signature-encryption schemes, which addressed IoT protection requirements through Object Naming Service (ONS) inquiries. It ensured the identity verification, network trustworthiness and data integrity of users and the system. Lee (2017) provided an authentication protocol for IoT devices with limited memory and processors, which used lightweight encryption based entirely on XOR manipulation for anti-faking and privacy protection. Lastly, Ye *et al.* (2014) proposed authentication encryption using Elliptic Curve Cryptography (ECC) to control user access.

Lara-Nino *et al.* (2018) proposed the Elliptic Curve Lightweight Cryptography (ECLC) to provide key agreements to secure IoT data. In a WSN, the ECLC allowed nodes to connect with each other under low processing and storage requirements. Khammash *et al.* (2021) proposed using ECLC for Mobile Ad-hoc Network (MANET) due to the benefits of its key size and cost. The key size in MANET cost far less than other cryptosystems like RSA, implying easier data administration, fewer memory needs and less bandwidth usage during key exchange over the communication channel. The cost of ECC computations was lower than that of other public key cryptography techniques. As a result, such algorithm was projected to extend the network's lifetime, whereas alternative exponentiation-based algorithms might result in the early consumption of all nodes' power budget throughout the network layers (Khammash *et al.,* 2021).

Based on Table 8, the authentication schemes proposed in previous works used hybrid solution algorithms to protect integrity and authentication in IoT applications. These algorithms had their own strength to meet the objectives and disadvantages that could jeopardise the integrity of IoT applications.

Conclusion

This paper aimed to achieve three objectives. The first objective was to analyse the current state of integrity and authentication research for the lightweight algorithm. Based on the articles reviewed, there were still IoT applications that had issues with authentication and integrity. One of the issues involved e-health devices that contained sensitive and private data such as bank accounts, user IDs and user health condition (Davoli *et al.*, 2019). In order to analyse the integrity of IoT, attacks that disrupted the integrity of applications had been identified and discussed such as MIM attacks, data manipulation and spoofing. The

Table 8: Authentication schemes for IoT

Author	IoT Layer	Algorithm	Strength	Weakness
Yanling (2013)	Application	Context/multiple credentials using physical context	Packet encapsulation to reduce the overhead of data resources	DoS attack is not considered
Khammash *et al.* (2021)	Network and perception	Assymmetric encryption using ECC	The cost of ECC computation is lower than that of other public key cryptography techniques	Vulnerable to side-channel attacks
Kothmayr and Thomas (2013)	Application and network	Encryption/ asymmetric using RSA	Low overhead and high interoperability	Using UDP over DTLS leads to unreliable authentication
Hammi *et al.* (2017)	Perception	Encryption/ symmetric asynchronous One Time Password (OTP)	Resistant to replay and some DoS attacks	No performance measurement done in comparison with other schemes
Wu (2017)	Application, network and perception	Encryption using AES symmetric	Resilient to attacks, data confidentiality, access control and client privacy	Location privacy is not considered
Lee (2017)	Network and perception	Encryption/ symmetric using XOR	Authentication of RFID tags with readers	Location privacy is not considered
Lara-Nino *et al.* (2018)	Network and perception	Encryption using ECC known as ECLC	Achieve greater efficiency and flexibility than the aforementioned alternatives. They have been adopted in a wide range of applications and in some cases, under critical constraints	ECLC must observe the lengthy latencies and the hardware/processing overhead compared with symmetric lightweight cryptography
Turkanovi (2014)	Network and perception	Encryption/ symmetric + hash	Resistant to replay attacks, man-in-the-middle attacks, impersonation attacks, privileged insider attacks, stolen smart card attacks and smart card breach attacks	Communication cost is higher than other schemes
Ye *et al.* (2014)	Network and perception	Encryption/ asymmetric using ECC	Resistant to DoS, replay attack, eavesdropping, node capture and man-in-the-middle attacks	Brief discussion related to attribute-based access control

second objective was to study the integrity and authentication requirements of IoT applications. The main security requirements in this article were focused on authentication and integrity. They included lightweight solutions, end-to-end security, privacy, identity management and mobility. The protocols of IoT application architecture and security mechanism related to authentications and integrity in IoT applications were also discussed. Lastly, discussion regarding lightweight algorithms and schemes were analysed to achieve the desired design requirement for authentication in IoT applications. A lot of research needed to be done

on the adoption of ECC as proposed by Ye *et al*. (2014). This method might not be fully efficient but was easy to manage and could meet the security requirements for authentication.

In conclusion, as wireless technology keeps growing, more challenges need to be addressed. It is hoped that this SLR could contribute as a reference for IoT developers and system designers to address authentication and integrity requirements.

Acknowledgements

The authors like to thank Universiti Sains Islam Malaysia (USIM) and the Higher Education Ministry for funding this research through the Fundamental Research Grant Scheme (FRGS/1/2019/ICT03/USIM/02/1).

References

Abdulghani, H. A., Nijdam, N. A., Collen, A., & Konstantas, D. (2019). A study on security and privacy guidelines, countermeasures, threats: IoT Data at rest perspective. *Symmetry, 11*(6), 774. DOI: 10.3390/sym11060774

Ahanger, T. A., & Aljumah, A. (2019). Internet of Things: A comprehensive study of security issues and defense mechanisms. *IEEE Access, 7*, 11020-11028. DOI: 10.1109/access.2018.2876939

Ahmed, A., Latif, R., Latif, S., Abbas, H., & Khan, F. A. (2018). Malicious insiders attack in IoT based Multi-Cloud e-Healthcare environment: A systematic literature review. *Multimedia Tools and Applications, 77*(17), 21947-21965. DOI: 10.1007/s11042-017-5540-x

Al-Fuqaha, A., Guizani, M., Mohammadi, M., Aledhari, M., & Ayyash, M. (2015). Internet of Things: A survey on enabling technologies, protocols, and applications. *IEEE Communications Surveys & Tutorials, 17*(4), 2347-2376. DOI: 10.1109/comst.2015.2444095

Alam, S., Siddiqui, S. T., Ahmad, A., Ahmad., R., & Shuaib, M. (2020). Internet of Things (IoT) enabling technologies, requirements, and security challenges. In *Advances in data and information sciences* (pp. 119-126). Berlin/Heidelberg, Germany: Springer.

Aleisa, N., & Renaud, K. (2017). Privacy of the Internet of Things: A systematic literature review. *Proceedings of the 50th Hawaii International Conference on System Sciences* (2017). DOI: 10.24251/hicss.2017.717

Almulhim, M., Islam, N., & Zaman, N. (2019). A lightweight and secure authentication scheme for IoT based e-health applications. *International Journal of Computer Science and Network Security*, *19*(1), 107-120.

Aswale, P., Shukla, A., Bharati, P., Bharambe, S., & Palve, S. (2019). An overview of Internet of Things: Architecture, protocols and challenges. In *Information and communication technology for Intelligent Systems* (pp. 299-308). Berlin/Heidelberg, Germany: Springer.

Azni, A. H., Ahmad, R., & Noh, Z. (2013). Survivability modeling and analysis of mobile ad hoc network with correlated node behavior. *Procedia Engineering*, *53*, 435-440.

Azni, A. H., Ahmad, R., Noh, Z. A. M., Hazwani, F., & Hayaati, N. (2015). Systematic review for network survivability analysis in MANETS. *Procedia-Social and Behavioral Sciences*, *195*, 1872-1881.

Bansal, S., & Kumar, D. (2020). IoT Ecosystem: A survey on devices, gateways, operating systems. *Middleware and Communication. International Journal of Wireless Information Networks*, *27*, 1-25.

Blackburn, S. R., & Robshaw, M. J. (2016). On the security of the Algebraic Eraser Tag Authentication Protocol. *Applied Cryptography and Network Security Lecture Notes in Computer Science,* 3-17. DOI: 10.1007/978-3-319-39555-5_1

Bösch, C., Guajardo, J., Sadeghi, A., Shokrollahi, J., & Tuyls, P. (2008). Efficient Helper Data Key Extractor on FPGAs. *Cryptographic Hardware and Embedded Systems–CHES 2008 Lecture Notes in Computer Science,* 181-197. DOI: 10.1007/978-3-540-85053-3_12

Brinkmann, A., Fiehe, C., Litvina, A., Luck, I., Nagel, L., Narayanan, K., Ostermair, F., & Thronicke, W. (2013). Scalable Monitoring System for Clouds. In *Proceedings of the 2013 IEEE/ACM 6th International Conference on Utility and Cloud Computing, Dresden, Germany*. 9-12.

Cai, H., Xu, B., Jiang, L., & Vasilakos, A. V. (2016). IoT-based Big Data Storage Systems in Cloud Computing: Perspectives and challenges. *IEEE Internet Things Journal*, *4*, 75-87.

Cherdantseva, Y., & Hilton, J. (2013). A reference model of information assurance and security. *2013 International Conference on Availability, Reliability and Security*. DOI: 10.1109/ares.2013.72

Claycomb, W. R., & Nicoll, A. (2012). Insider threats to Cloud Computing: Directions for new research challenges. *2012 IEEE 36th Annual Computer Software and Applications Conference*. DOI: 10.1109/compsac.2012.113

Columbus, L. (2017, December 11). 2017 Roundup of Internet of Things Forecasts. *Forbes*. https://www.forbes.com/sites/louiscolumbus/2017/12/10/2017-roundup-of-internet-of-things-forecasts/?sh=3d933e2f1480. Access on 15 May 2021.

Das, A. K., Zeadally, S., & He, D. (2018). Taxonomy and analysis of security protocols for Internet of Things. *Future Generation Computer System, 89*, 110-125.

Davoli, L., Veltri, L., Ferrari, G., & Amadei, U. (2019). Internet of Things on Power Line Communications: An experimental performance analysis. In Kabalci, E., Kabalci, Y., (Eds.), *Smart grids and their communication systems* (pp. 465-498). Singapore: Springer.

Deep, S., Zheng, X., & Hamey, L. (2019). A survey of security and privacy issues in the Internet of Things from the layered context. *arXiv 2019*. arXiv: 1903.00846

Delvaux, J., Gu, D., Verbauwhede, I., Hiller, M., & Yu, M. D. (2016). Efficient fuzzy extraction of PUF-Induced Secrets: Theory and applications. *Lecture Notes in Computer Science Cryptographic Hardware and Embedded Systems – CHES 2016,* 412-431. DOI: 10.1007/978-3-662-53140-2_20

Dhumane, A., Prasad, R., & Prasad, J. (2016). Routing issues in Internet of Things: A survey. In *Proceedings of the International Multiconference of Engineers and Computer Scientists, Hong Kong* (Volume 1, pp. 13-20).

Dybå, T., & Dingsøyr, T. (2008). Empirical studies of Agile Software Development: A systematic review. *Information and Software Technology*, *50*(9-10), 833-859.

Grobauer, B., Walloschek, T., & Stöcker, E. (2011). Understanding Cloud Computing Vulnerabilities. *IEEE Security and Privacy*, *9*, 50-57. DOI: 10.1109/MSP.2010.115.

Grobauer, B., Walloschek, T., & Stöcker, E. (2011) Understanding Cloud Computing Vulnerabilities. *IEEE Security and Privacy*. 9, 50-57. DOI: 10.1109/MSP.2010.115.

Gubbi, J., Buyya, R., Marusic, S., & Palaniswami, M. (2013). Internet of Things (IoT): A vision, architectural elements, and future directions. *Future Generation Computer System*, *29*, 1645-1660.

Hameed, S., Khan, F. I., & Hameed, B. (2019). Understanding security requirements and challenges in Internet of Things (IoT): A review. *Journal Computer Network Communication*, 9629381.

Hammi, M. T., Livolant, E., Bellot, P., Serhrouchni, A., & Minet, P. (2017). A Lightweight Mutual Authentication Protocol for the IoT. In *International*

Conference on Mobile and Wireless Technology (pp. 3-12). Singapore: Springer.

Harnik, D., Pinkas, B., & Shulman-Peleg, A., (2017). Side channels in Cloud Services: Deduplication in Cloud Storage. *IEEE Security and Privacy, 8*, 40-47. DOI: 10.1109/MSP.2010.187

Hasan, M., & Mohan, S. (2019). Protecting actuators in Safety-Critical IoT Systems from control spoofing attacks. In *Proceedings of the 2nd International ACM Workshop on Security and Privacy for the Internet-of-Things* (pp. 8-14).

Herder, C., Yu, M. D., Koushanfar, F., & Devadas, S. (2014). Physical unclonable functions and applications: A tutorial. In *Proceedings of the IEEE* (Vol. 102, no. 8, pp. 1126-1141, Aug).

He, D., & Zeadallyn, S. (2015). An analysis of RFID Authentication Schemes for Internet of Things in healthcare environment using Elliptic Curve Cryptography. *IEEE Internet of Things Journal*, *2*(1), 72-83.

Kaaniche, N., & Laurent, M. (2017). Data security and privacy preservation in Cloud Storage environments based on cryptographic mechanisms. *Computer Communications*, *111*, 120-141. DOI: 10.1016/j.comcom.2017.07.006.

Khammash, M., Tammam, R., Masri, A., & Awad, A. (2021). Elliptic Curve Parameters Optimization for Lightweight Cryptography in Mobile-Ad-Hoc Networks. In *2021 18th International Multi-Conference on Systems, Signals & Devices (SSD)* (pp. 63-69). IEEE.

Kitchenham, B. (2004). Procedures for Performing Systematic Reviews, *33*(2004), 1-26. Keele, UK: Keele University.

Køien, G. M. (2011). Reflections on trust in devices: An informal survey of human trust in an Internet of Things context. *Wireless Personal Communications*, *61*(3), 495-510.

Kothmayr, Thomas. (2013). DTLS based security and two-way authentication for The Internet of Things. *Ad Hoc Networks*, *11*(8), 2710-2723.

Kumar, P. R., Raj, P. H., & Jelciana, P. (2018). Exploring data security issues and solutions in Cloud Computing. *Procedia Computer Science*, *125*, 691-697. DOI: 10.1016/j.procs.2017.12.089

Lai, C., Li, H., Lu, R., & Shen, X. S. (2013). A secure and efficient Group Authentication and Key Agreement Protocol for LTE Networks. *Computer Network*, *57,* 3492-3510.

Lara-Nino, C. A., Diaz-Perez, A., & Morales-Sandoval, M. (2018). Elliptic curve lightweight cryptography: A survey. *IEEE Access*, *6*, 72514-72550.

Lee, J. Y. (2017). A lightweight authentication protocol for Internet of Things. In *International Symposium on Next-Generation Electronics, Kwei-Shan*.

Li, F., Lai, A., & Ddl, D. (2011). Evidence of Advanced Persistent Threat: A case study of malware for Political Espionage. *Malicious and Unwanted Software (MALWARE)*. 2011 6th International Conference on IEEE, 2011, pp. 102-109.

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

Li, Y., Gao, M., Yang, L., Zhang, C., Zhang, B., & Zhao, X. (2020). Design of and research on Industrial Measuring Devices based on Internet of Things technology. *Ad Hoc Networks*, *102*, 102072.

Liu, C., Ranjan, R., Yang, C., Zhang, X., Wang, L., & Chen, J. (2015). Top-down levelled multi-replica Merkle Hash Tree based secure public auditing for dynamic big data storage on Cloud. *IEEE Transanctions on Computers*, *64*, 2609-2622. DOI: 10.1109/TC.2014.2375190

Liu, X., Zhao, M., Li, S., Zhang, F., & Trappe. (2017). W. A security framework for the

Internet of Things in the future Internet architecture. *Future Internet*, *9*, 1-27.

Miorandi, D., Sicari, S., De Pellegrini, F., & Chlamtac, I. (2016) Internet of Things: Vision, applications and research challenges. *Ad Hoc Networks*, *10*(7), 1497-1516.

Mohsen, N. A., & Jha, N. K. (2016). A comprehensive study of security of Internet-of-Things. *IEEE Transanctions on Emerging Topics in Computing*, *5*, 586-602.

Nicanfar, H., Jokar, P., Beznosov, K., & Leung, V. C. M. (2014). Efficient authentication and key management mechanisms for smart grid communications. *IEEE System Journal*, *8*, 629-640.

Pal, S., Hitchens, M., & Varadharajan, V. (2018). Modeling identity for the Internet of Things: Survey, classification and trends. In *Proceedings of the 2018 12th International Conference on Sensing Technology (ICST), Limerick, Ireland*. 3-6 December 2018, pp. 45-51.

Rashid, F., Miri, A., & Woungang, I. (2012). A secure data deduplication framework for Cloud environments. In *Proceedings of the 2012 Tenth Annual International Conference on Privacy, Security and Trust, Paris, France* (pp. 81-87). DOI: 10.1109/PST.2012.6297923

Roman, R., Zhou, J., & Lopez, J. (2013). On the features and challenges of security and privacy in distributed Internet of Things. *Computer Networks*, *57*(10), 2266-2279.

Salleh, N., Mendes, E., & Grundy, J. (2011). The effects of openness to experience on pair programming in a Higher Education context. In *2011 24th IEEE-CS Conference on Software Engineering Education and Training (CSEE&T)* (pp. 149-158). IEEE.

Schmitt, C., Noack, M., Stiller, B., & Tiny, T. O. (2016). Two-way authentication for constrained devices in the Internet of Things. In *Internet of Things* (pp. 239-258). Amsterdam, The Netherlands: Elsevier.

Shahbodin, F., Azni, A. H., Ali, T., & Mohd, C. K. N. C. K. (2019, January). Lightweight cryptography techniques for MHealth cybersecurity. In *Proceedings of the 2019 Asia Pacific Information Technology Conference* (pp. 44-50).

Sharma, V., Kim, J., Kwon, S., You, I., Lee, K., & Yim. K. (2018). A framework for Mitigating Zero-Day Attacks in IoT. *arXiv 2018*. arXiv: 1804.05549

Shen, J., Yang, H., Wang, A., Zhou, T., & Wang, C. (2019). Lightweight Authentication and Matrix-Based Key Agreement Scheme for Healthcare in Fog Computing. *Peer-to-Peer Network Application, 12*(4), 924-933.

Sicari, S., Rizzardi, A., & Grieco, L. A. (2015). A security, privacy and trust in Internet of Things: The road ahead. *Computer Network*, *76*, 146-164.

Singh, A., & Chatterjee, K. (2015). A Secure Multi-Tier Authentication Scheme in Cloud Computing Environment. In *Proceedings of the 2015 International Conference on Circuits, Power and Computing Technologies [ICCPCT-2015], Nagercoil, India.*

Singh, S., Sharma, P. K., Moon, S. Y., & Park, J. H. (2017). Advanced lightweight encryption algorithms for IoT devices: Survey, challenges and solutions. *Journal of Ambient Intelligence and Humanized Computing*, 1-18.

Taylor, P. J., Dargahi, T., Dehghantanha, A., Parizi, R. M., & Choo, K. K. R. (2020). A systematic literature review of Blockchain Cyber Security. *Digital Communications and Networks*, *6*(2), 147-156.

Turkanovi, M. (2014). A Novel User Authentication and Key Agreement Scheme for Heterogeneous Ad Hoc Wireless Sensor Networks, based on the Internet of Things Notion. *Ad Hoc Networks*, *20*, 96-112.

Wendt, J. B., & Potkonjak, M. (2014). Hardware Obfuscation Using PUF-Based Logic. In *2014 IEEE/ACM International Conference*

on Computer-Aided Design (ICCAD) (pp. 270-271). IEEE.

Williams, Patricia, A. H., & Vincent. M. (2016). Always connected: The security challenges of the healthcare IoT. *IEEE 3rd World Forum on IoT (WF-IoT)*. 2016. DOI: 10.1109/wf-iot.2016.7845455 2

Wu, Z. Q. (2017). A Security Transmission Model for Internet of Things. *Chinese Journal of Computers*, *34*(8), 1351-1364.

Yanling, Z. (2013). Research on Data Security Technology in Internet of Things. *Applied Mechanics and Materials*, *433-435*, 1752-155.

Yaqoob, I., Hashem, I. A. T., Ahmed, A., & Kazmi, S. A. (2019). Internet of Things Forensics: Recent advances, taxonomy, requirements, and open challenges. *Future Generations Computer System*, *92*, 265-275.

Ye, N., Zhu, Y., Wang, R. C., Malekian, R., & Qiao-min, L. (2014). An efficient authentication and access control scheme for perception layer of Internet of Things. *Applied Mathematics & Information Sciences, 8*, 1617-1624.

Yu, S., & Guo, S. (2016). *Big data concepts, theories, and applications*. Cham, Switzerland: Springer International Publishing. (pp. 1-437). DOI: 10.1007/978-3-319-27763-9