Communications in Mathematics and Applications
Vol. 13, No. 1, pp. 401–415, 2022
ISSN 0975-8607 (online); 0976-5905 (print)
Published by RGN Publications
DOI: 10.26713/cma.v13i1.1980

http://www.rgnpublications.com

Review Article

Data Security Challenges with its Defence Strategies of Internet of Things: Critical Review Study

Shuruq Zayed Al-Otaibi

Information Science Department, Arts Faculty, King Saud University, Prince Turkey St., Riyadh, Saudi Arabia
szalotaibi@ksu.edu.sa

Received: November 17, 2021 **Accepted:** February 21, 2022

Abstract. Due to the sensitivity of the data security issue and the lack of studies focused on data security in the Internet of Things (IoT) environment; this paper-through the methodology of critical review of relevant previous and recent studies-aimed to extract the most important challenges or problems and technical and defence strategies and solutions related to securing data in IoT. That is all In order to serve as a practical guide to benefit the concerned ones. As for the results of the studies, there were several things, including: that the most common security issues and challenges within the previous studies were: confidentiality, privacy and encryption effectiveness, and authentication methods are the best methods for securing data by nearly 60%, and the most important of these methods is lightweight authentication, multi-factor authentication, then mutual authentication. In addition, it is necessary to pay attention to securing all layers of the IoT. Especially the perception layer; as it is the main interface for the attack for easy physical access to the end nodes and web interfaces. Moreover, there are several modern technologies and methods that contribute to securing data such as: lightweight systems, digital twins, Software-Defined Network (SDN), edge computing and engineering, fog computing, trust computing, Context aware of accessibility. As for the recommendations, the study recommended all the following. IoT service providers should adopt several security methods, techniques and protocols in order to raise the level of security during data transfer and storage. The concerned organizations and bodies should issue unified laws and frameworks in order to standardize the work in IoT environment and In order to protect the confidentiality and privacy of data.

Keywords. Internet of Things, Data security, Confidentiality, Privacy, Authentication, Access control, IoT

Mathematics Subject Classification (2020). 68W10, 97P10, 97P20, 60-11

1. Introduction

The *Internet of Things* (IoT) is a group or network of many interconnected devices that work together, to conduct communications and data processing over the Internet without human intervention [5]. With the growing rate of adoption of IoT technologies, more devices are connecting to the Internet every day [7]. The IoT environment allows the physical devices connected to it such as vehicles, home appliances, etc. to communicate and even interact with each other [16], which in turn has led to IoT becoming a part of our daily life, and this applies to all aspects of human life from smartphones to smart devices that used in industry [4]. As we can see, IoT technologies are widely used in industrial production, industrial automation, and IoT-based analytics to enhance the productivity and efficiency of industrial infrastructures. It also seems clear to us the importance of IoT technologies in the business success of stakeholders such as companies and vendors, as it helps them understand business requirements and desired outcomes. We also see the importance of IoT in social applications such as smart homes, healthcare, shopping malls, schools etc. [12, 15, 16].

Despite the many advantages of IoT, there are growing security risks that must be taken into account and addressed [4]. While IoT has brought benefits such as convenience, accessibility, and unparalleled efficiency, IoT has created serious threats to security and privacy in recent years [16]. The information used and transmitted via IoT contains important information about people's daily and personal lives, banking information, location, geographic information, environmental and medical information as well as many other sensitive data [4].

In addition, the infrastructure of the Internet of Things has security holes and vulnerabilities that enable it to receive risks and distribute them on a much larger scale than the Internet. This is because the four layers of IoT that play a major role in the security issue of the Internet of Things environment. So, to make the Internet of Things reliable and secure; we need to adequately secure these four basic layers [7]. In the following figure, we will see the names of the four layers and their most important uses:

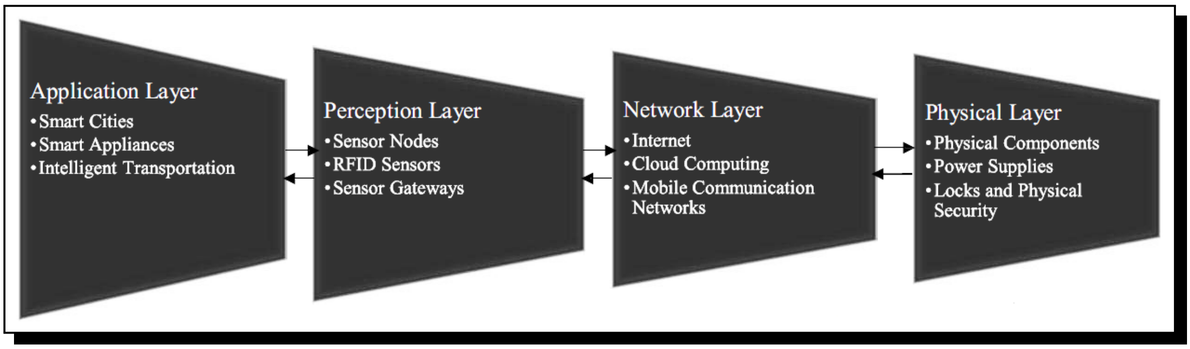

Figure 1. IoT layers, ref. [7]

The consequences of IoT security failures can be dire, especially if those failures are related to professional sectors or areas of sensitive or personal information. Therefore, conducting studies and research related to security issues in IoT is of the utmost importance and urgency [10]. The idea of conducting the current paper has come based on that most of the studies deal with the security of the IoT environment in general and the lack of studies that focus on IoT data security in particular. So, this paper-through a critical review of the latest scientific studies - aimed to extract the latest challenges, defence strategies solutions and technologies for securing data in IoT environment in order to serve as a practical guide to benefit the concerned ones, especially researchers and IoT service providers.

Therefore, it is possible to formulate the problem of the current paper in the following question:

❑ **What are the most important and latest challenges, defence strategies and technologies associated with securing data in the Internet of Things environment?**

Knowing that this paper consists of five parts: introduction, Reviews' details, results, discussion and conclusion.

2. Reviews' Details

The researcher considered that the appropriate methodology for the problem of the current study is the critical review in order to weigh the most important and best technical and strategic solutions to secure data in the Internet of Things environment. A critical review is a critical evaluation of several documents (or books, chapters or articles). It is not just a summary of the content, but rather a careful reading of the document and then issuing judgments about it with justification for these provisions [8].

The following is a review of the latest studies that correspond to the problem of the current paper-which published between 2016-2021 AD - and is arranged chronologically from newest to oldest:

❑ **A study [1] in (2021) entitled: 'Emerging IoT Applications in Sustainable Smart Cities for COVID-19: Network Security and Data Preservation Challenges with Future Directions'**

This study aimed by a critical review of the literature -published between 2019-2021 - and a comparative analysis between previous studies and the current study; to display the most important IoT applications that were used during the Covid-19 pandemic, such as Tawakkalna, Aarogya, and Setu. Then identifying the most important gaps, challenges and security requirements for those applications. The study found that one of the most important problems facing these applications is maintaining the confidentiality and privacy of patient data from any spying or attack. The most important solutions were development a collaborative authentication plan of Ellipse Curve Cryptography (ECC), and development a mutual authentication plan of a lightweight secret key. The study was also distinguished by presenting technical research directions to address these problems such as edge engineering techniques like edge-layered technology, edge and fog computing techniques, block-chain, machine learning, digital twins, and context aware accessibility.

❑ **A study [2] in (2021) entitled: 'A double-blockchain architecture for secure storage and transaction on the Internet of Things networks'**

This paper aimed to propose a system based on double block-chain; to improve communication integrity, and to enhance the way information is compressed for stored data. As this study sees that IoT environments face three challenges: detection of intrusions and attacks, secure communication, and storage of information compression. Therefore, a system will be proposed to improve information security using cryptography (ECC); which is a cryptography based on elliptic mathematics for generating public keys. The data compression within the system will be ensured by the compressed sensing (CS) method. The experimental results proved the effectiveness of the proposed system in terms of the following characteristics: storage capacity, and encryption speed. Moreover, the system has an accuracy of 96%, which is better than systems based on asymmetric encryption algorithms such as RSA and DSA.

- **Study [5] in (2021) entitled: 'Survey on Data Security Techniques in Internet of Things'**

This study aimed - through the method of literary review and theoretical survey - to define the most important security challenges and threats facing data security in the Internet of Things environment, such as data privacy, identity verification and access control, due to weak encryption techniques and weak programs and interfaces protection. The study was also characterized by proposing multiple techniques to address data security problems within IoT such as using of Automata Cellular technology, which is an automation for simulating natural processes through a complex behavioural pattern for cells. The study also recommended a new type of asymmetric RSA encryption algorithm called Memory Efficient Multiple Key Generation Scheme (MEMK) when dealing with sensitive data, using a machine learning algorithm such as a support vector machine or SVM for classification or regression, and Paillier cryptography -which based on asymmetric public key algorithm- for data privacy and integrity.

- **A study [6] in (2021) entitled: 'Mutual authentication and data security in IOT using hybrid mac id and elliptical curve cryptography'**

This paper aimed to suggest an approach or system for achieving mutual authentication in order to provide stronger authentication by using hybrid MAC-ID. The proposed approach achieved by using Mac-ID devices and Mac-ID gateways and implemented by using Java platform. The approach used and ECC cryptography for authentication and data communication between user and server, while it used a hybrid MAC-ID for the mutual authentication between IoT devices and the server. The results proved that the proposed approach is faster than other methods based on the asymmetric cryptography algorithm 'RSA' and the advanced cryptography algorithm 'AES'. This approach does not allow the unauthorized user to access the hardware and server and then change some data in the database.

- **Study [13] in (2021) entitled: 'Secure Data of Industrial Internet of Things in a Cement Factory Based on a Blockchain Technology'**

This study aimed to propose a model based on block-chain technology to secure data in industrial environments that use IoT. Where the study considers IoT is a central environment threatened by several threats such as: electronic attacks that targeting data confidentiality, devices failure and data jams. Therefore, this study targeting overcoming these mentioned problems through the proposed model by exploiting block-chain technology's ability to provide a high level of security through P2P networks, it is also characterized by low computing complexity. The proposed model is scalable and has a Lightweight security system. The proposed model has proven its effectiveness in smart industrial environments.

- **Study [15] in (2021) entitled: 'Security Threats and Artificial Intelligence Based Countermeasures for Internet of Things Networks: A Comprehensive Survey'**

This study aimed-through using literature review and in-depth survey methodologies of a number of a based on artificial intelligence techniques studies-to provide a comprehensive perception regarding the security threats in IoT and the practical solutions related to artificial intelligence (AI) and *machine learning* (ML); to deal with these threats. This study was characterized by the multiple classification explanations that supported by detailed tables such as: the IoT's layers threats table, the appropriate layers protection protocols, the security problems addresses by machine learning techniques types(main and sub, and finally the security problems that addresses by machine learning algorithms. Examples of the suggested techniques by the study are: deep learning techniques such as CNN and DNN neural networks for data manipulation and poisoning problems, shallow learning techniques such as decision tree DT and SVM for malicious code injection and inversion problems, and Rule-based machine learning techniques such as SNN and FNN neural networks for evasive problems.

- **A study [11] in (2020) entitled: 'A Survey on Privacy and Security of the Internet of Things'?**

This theoretical survey aimed to provide reader with a comprehensive survey about the latest IoT technologies, with a special focus on what has been achieved in the areas of privacy and security threats, malicious attacks and vulnerabilities in IoT, and then explaining the countermeasures. The study also has identified several security concerns and threats such as the integrity, confidentiality, privacy and availability of data, as well as linking these threats to the relevant Internet of Things layers. In addition, the study determined several security requirements such as network security, identity management, and trust management have also been defined. This study is characterized by its important proposed taxonomy that contains the most important threats to both privacy and confidentiality of IoT and the countermeasures for these threats as follows. The confidentiality has threats like Spear-Phishing, Spoofing, and Sybil. The privacy has threats like identification, location tracking and tracing, and profiling. The countermeasures has user-based solutions like confidentiality protocols, access control, authentication, security awareness and privacy by design.

- **A study [12] in (2020) entitled: 'IoT Privacy and Security: Challenges and Solutions'**

This study aimed to propose a business model for IoT consisting of two layers: generic and stretched, with identification of privacy and security elements in each layer, in order to overcome several security gaps associated with IoT such as confidentiality, privacy, and interoperability. The proposed model has been implemented by cloud/edge technologies as follows: The bottom layer consists of IoT nodes, which are generated by Amazon Web Service (AWS) as virtual machines. The middle layer (edge) is implemented by using Raspberry Pi 4 hardware and by Green-grass Edge Environment in AWS. As for the upper layer (the cloud), cloud services for IoT environment in AWS were used. Moreover, security protocols and certificates of authenticity were used between the layers of the model. The model has proven its effectiveness after experiments.

- **A study [14] in (2020) entitled: 'Edge-based auditing method for data security in resource-constrained Internet of things'**

This study aimed to suggest an approach or a business model in order to deal with data security problems, especially during outsourcing such as cloud computing. Therefore, the study proposed a lightweight and reliable audit model that based on data representation by binary tree method, and in order to improve audit efficiency, the binary tree had designed to be self-balancing. The model also based on edge computing technology; so data pre-processing job is offloaded to the edge, which processes the hidden files uploaded by users to ensure file privacy, which reduces computing burden and improves task processing efficiency as well as data protection. The model also suggested an improved association mechanism between data blocks and nodes on the binary tree, so that all nodes on the binary tree could be fully exploited — instead of using the current traditional leaf nodes — in order to reduce the number of binary trees. The study also compared the proposed model with the traditional methods, and the experimental results showed its effectiveness in auditing, managing big data, and providing safer IoT.

- **A study [10] in (2019) entitled: 'Current research on Internet of Things (IoT) security: A survey'**

This paper aimed - through using literature review and survey methodologies of a number of recent research that published between 2016 and 2018- to identify the most important research issues related to security of IoT environment, research trends and open issues. The study also touched on important related tools and techniques. This study is distinguished by pointing to the security problems of IoT, and by the deep technical solutions to these problems. This study also indicated to important mechanisms for securing data (such as encryption, authentication and secure routing) in a very detailed manner, as the study considered them the most important data protection techniques in IoT. Also, the study referred to emerging technologies for supporting data protection in IoT such as Software-Defined Network (SDN) and block-chain technologies.

- **A study [16] in (2018) entitled: 'The Effect of IoT New Features on Security and Privacy: New Threats, Existing Solutions, and Challenges Yet to Be Solved'**

The current study aimed - through a literary review and content analysis of studies that published between 2013 to 2017 – to make a survey of the most important characteristics of IoT environment, which is summarized in eight characteristics as follows: ubiquitous, diversity, interdependence, constrained, myriad, intimacy, mobileand unattended. Then, the study discussed the security and privacy effects of these features in detailed manner, including threats, solutions and opportunities that are caused by these features. Then, the study summarized and linked those characteristics, challenges and solutions through an important table presented in the study. The study found that the IoT applications most danger threats are insecure communication protocols, privacy leaks, and unprotected mobile applications.

- **A study [4] in (2017) entitled: 'Security challenges in the Internet of Things: survey'**

The study aimed through the literature review methodology; to identify the challenges facing the Internet of Things environment, and to list the most important requirements and solutions related to those challenges. This study is characterized by its detailed and expanded subdivisions for the security challenges of IoT such as: challenges during implementation, privacy challenges, infrastructure challenges, service quality challenges, protocols and encryption challenges. The study is also distinguished by summarizing the most important security requirements to be provided in IoT, and by addressing some important solutions such as using of lightweight systems and techniques, raising the level of security in communication networks by improving the level of communication protocols, and developing legal frameworks for security and privacy of IoT.

❑ **A study [3] in (2016) entitled: 'Data Security and Privacy in the IoT'**

This paper aimed - through the literature review method - to identify the main challenges of data security and privacy in IoT (such as heterogeneity of Internet of things devices, dynamics of the Internet of things environment, limited computing resources etc). The paper stated that the IoT vulnerabilities often arise due to not adopting well-known security technologies, such as encryption, authentication, and access control. This paper also summarized the IoT research trends that address some security issues, such as encryption ineffectiveness and data loss issues.The study also suggested some solutions related to these issues such as using white box encryption techniques, and using a system of a sensors network that capable of taking response actions automatically in data loss status (such as Kinesis devices).

❑ **A study [7] in (2016) entitled: 'Security in Internet of Things: Challenges, Solutions and Future Directions'**

This study aimed - through a literary review and content analysis of previous studies - to reach the most important problems and security challenges for each of the four layers of the Internet of Things environment in a detailed and extensive manner. Examples of application layer problems are applications based on nodes tampering and the inability to receive patches. Examples of perception layer problems are eavesdropping and data noise. Examples of network layer problems are attacking storage units and unauthorized access. Examples of physical layer are hardware failures and natural disasters. Then, the study presented a table of the most important appropriate approaches and methods; in order to secure the layers of IoT. In addition, the table mentioned the restrictions for each method. The study also suggested methods and to overcome these limitations in order to verify their effectiveness in future studies, such as proposing an application of sensors to capture data from physical entities to calculate the threat index and then implementing the event response in the real time. The study also suggested an important framework for raising the level of security on Internet networks; however, the framework still needs to be tested.

❑ **A study [9] in (2016) entitled: 'Security in Internet of Things Systems'**

This paper aims- through the methodology of theoretical survey and literary review- to introduce IoT technology initially, and then define the most important trends and future emerging opportunities for the uses of IoT in several sectors (such as the agricultural, environmental, and industrial sectors etc). The study, also, presented two independent parts. The first part dealt with the most important security and privacy challenges facing IoT, such as the lack of global laws regarding security and privacy in IoT. The second part was about the most important future work related to issues and solutions linked to the subject of security in IoT, such as security protocols and effective encryption issues. The study concluded that countries and organizations must consider policies related to IoT technologies and the other related technologies, then collecting and circulating them. The study emphasized that policies should be based on four main pillars: infrastructure, human capital, incentives, and good governance.

3. Results

By using the study methodology-which is a critical review of previous studies- the researcher reached the following results:

- Most of the studies were similar in using literature review, theoretical survey and content analysis methodologies, and the studies [2, 4, 6, 12, 13] were distinguished by proposing practical systems or models and then testing them, the study [7] was characterized by proposing a framework, but without testing it. As for the study [1], it was characterized by the use of critical review and comparative analysis.
- The two studies [1, 13] were distinguished in that they talked about IoT that related to specific professional fields, such as the Industrial Internet of Things (IIoT) in [13] and the Internet of Things for healthcare (HIoT) in [1].
- Several studies were distinguished by mentioning the issues and challenges related to data security in the Internet of Things environment, which can be summarized in the following table:

Ref.	Security challenges
[1, 4, 6, 9–13]	Confidentially
[1, 4–6, 9, 11, 12, 16]	Privacy
[1, 5, 9, 11]	Integrity
[1, 4, 5, 9, 11]	Authorization
[3, 5, 6, 10, 11]	Access control
[1, 4, 6, 10, 11]	Authentication
[1, 3, 4, 12]	Interoperability
[1, 11]	Availability
[3, 7]	Data quality and purity
[1, 2, 4, 11, 16]	Secure connection
[3, 9, 11]	IoT dynamics
[3, 9–11, 14]	Resources restrictions
[1–3, 5, 9, 10]	Encryption efficiency
[10]	Secure routing
[10, 11]	Trust management
[7, 10, 13]	Hardware failure
[5, 7, 10, 16]	Weak software protection
[1, 2, 7]	Data spying and eavesdropping

- The study [10] was distinguished by noting that authentication methods are the most common methods for securing data by 60%, and that the most common authentication methods within previous studies are Lightweight authentication, then multi-factor authentication, then mutual authentication. As shown in the following figure:

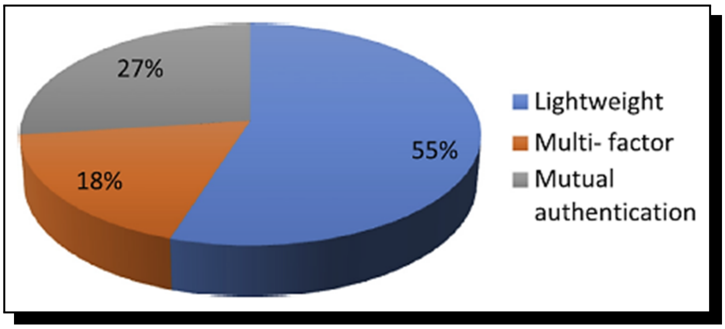

Figure 2. Trends in the use of authentication methods, ref. [10]

- The study [16] was distinguished by indicating the most important challenges facing data security in Internet of Things applications, which are data leakage, and insecure communication protocols. The IoT applications most severely affected by both of these challenges are smart networks, then smart homes and digital healthcare that suffer from data leakage. As well as the smart agricultural and industrial field, which suffers from insecure communication protocols, as we can see in the following figure:

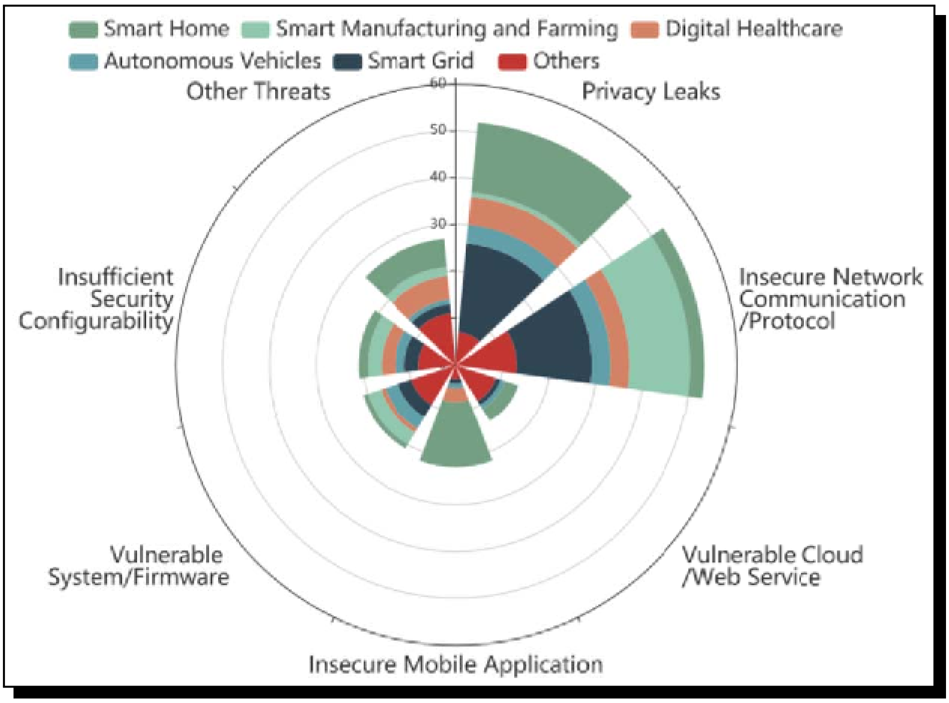

Figure 3. Security challenges in IoT applications, ref. [16]

- Some studies were distinguished by presenting practical techniques and methods as solutions to secure data as follows:

Ref.	Solutions
[10]	Multi-factor authentication using biometric hashing and anonymity, Lightweight technologies and systems, such as lightweight encryption.
[1,2,4,10,13]	IoT systems that have protocols that support authentication, namely MQTT, DDS, Zigbee and Zwave.
[10]	White box encryption techniques.
[3]	Using RFID, Zigbee, or WiFi for short-range communications, and using WSN for long-range communications.
[5]	Networks of sensors capable of automatically taking response actions in data loss status (such as Kinesis devices).
[3]	Block-chain technologies for better efficiency in security, confidentiality and privacy.
[1,2,10,12,13]	Using the Consensus algorithm (PoAh) instead of (PoW) within blockchain technologies; to ensure secure authentication, scalability and speed.
[13]	ECC encryption technologies for better authentication.
[1,2,6]	Cellular Automation, MEMK Algorithm, SVM Algorithm and Paillier Encription for better privacy and integration.
[5]	Edge computing techniques; for better privacy and confidentiality.
[1,12,14]	Digital twins techniques, fog computing, machine learning, and Context aware accessibility.
[1]	Trust computing technologies for access control, and trust-based access control (TBAC) technologies.
[10]	SDN technology to secure data.
[1,10]	Compressed Sensing (CS) technology for data compression.
[2]	Data representation by a self-balanced binary tree - instead of traditional leaf nodes - for the efficiency of the audit process, and using a Merkle hash tree (MHT) for data integrity.

Some studies were distinguished by providing useful practical recommendations for IoT providers in order to secure that environment as follows:

Ref.	Recommendation
[4,9]	Global legal frameworks for data security and privacy related to IoT must be developed and defined; due to the lack of unified laws and local and international standards.
[1,3,4]	Protocols and standards -for heterogeneous equipment and devices- must be reviewed and integrated; in order to achieve the compatibility.
[3]	Cryptographic protocols must be designed to be efficient and scalable for deployment on large-scale IoT systems and devices with limited computational resources.
[14]	Cloud service providers use methods to secure data in the cloud such as "Third Party Audit (TPA)".
[1]	Using business models for hardware protection, such as the Non-Copyable Physical Functions (PUF) model, to ensure network device validation and authentication

Contd. Table

Ref.	Recommendation
[10]	Using IPv6 instead of IPv4 when there is a very large number of devices, as indicated by [5]. And using the Transport Layer Security (TLS) protocols such as TLS-PSK and TLS-DHE-RSA to authenticate and encrypt communications.
[4]	Identification between devices and then exchange some public and private keys by 'knots' in order to avoid data theft.
[7,10]	Securing all IoT layers, especially the perception layer. For the easy physical accessing to the end nodes and web interfaces.
[3]	Good device calibration must be done between network devices; to ensure quality.

- The study [4] was characterized by categorizing security challenges into the following categories:

  Implementation challenges (e.g. methods for protecting confidentiality and privacy of sensitive data), privacy challenges, network infrastructure challenges (e.g. data storage within incompatible devices), service quality challenges (e.g. the ability to collect and transmit large volumes of data from sensors, and then store it in an appropriate cloud computing system), security threats (e.g. unauthorized access) and cryptographic and protocol challenges (e.g. high cost of encryption, complexity of security protocols).
- Studies [7, 10, 11, 15] agreed to present the security challenges and their solutions associated with each layer of IoT.
- The study [1,2,10,12,13] agreed on the importance of using block-chain technologies in order to secure data, and the study differed [2] By pointing to the importance of the double block-chain.
- The study [10] was distinguished by presenting a design model for the confidentiality structure in IoT, and the study [15] was distinguished by presenting a model for the structure of IoT based on AI cloud services for a more secure environment.
- The study [5] was distinguished, as it is the only study that referred to a general and unified framework, which is ACE, for IoT security issues such as authentication and authorization in restricted environments, which was presented by the Internet Engineering Task Force.
- The study [16] is distinguished as it the only study that defined the security threats and the appropriate solutions of IoT, from the perspective of the characteristics of IoT.
- The study [11] was distinguished by identifying of the most important security requirements for IoT environment, namely: network security, data privacy, especially beneficiaries' personal data, identity management through control of authentication, access and trust management, in order to prevent the leakage of sensitive information.
- The studies [10,11,15,16] were distinguished by presenting important lists and tables of IoT security challenges and solutions.

4. Discussion

By viewing and analysing the critical review results of previous studies that published between 2016-2021 and amounted to 15 studies; the researcher reached the following results:

- There are many security issues and challenges facing data security in IoT within the previous studies, which are summarized in table [1], and to know which are most common and threatening of those challenges, they were represented through the following chart:

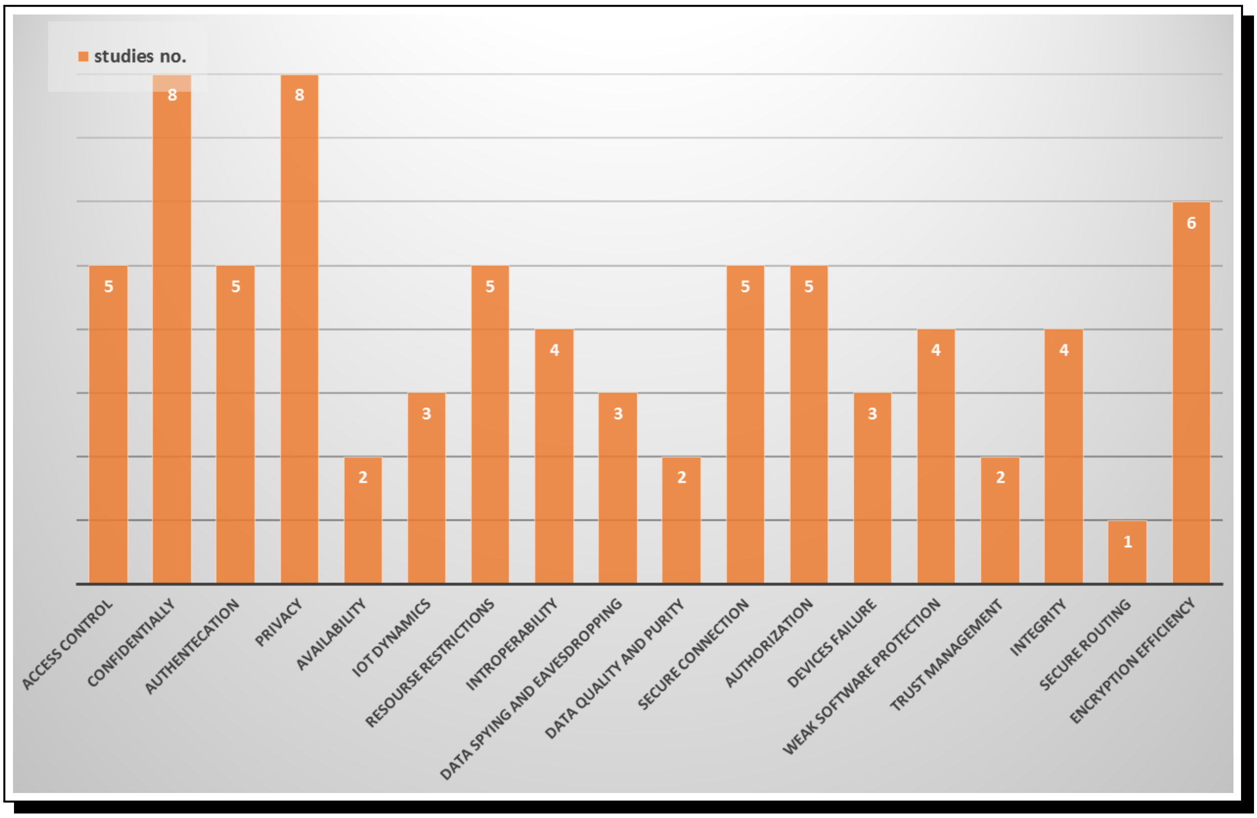

Figure 4. Data security challenges within previous studies

From the Figure 4, we find that the most common security issues and challenges were: confidentiality and privacy, then encryption effectiveness, then each of: authentication, access authorization, access control, secure communication, and resource restrictions.

- Authentication methods are the best methods for securing data by approximately 60%, and the most important of these methods are: Lightweight authentication, then multi-factor authentication, and then mutual authentication.
- The most important data security challenges in IoT applications are data leakage, and insecure communication protocols.
- Attention must be paid to securing all layers of IoT, especially the perception layer; because it is the main attack interface due to the easy physical accessing to end nodes and web interfaces. The security protocols must be used by the transport layer (TLS) like 'TLS-PSK' and 'TLS-DHE-RSA' –that are widely used – for authenticating and encrypting communications.
- It is preferable to use IoT systems that have protocols that support authentication such as MQTT, DDS, Zigbee and Zwave.
- Local and global frameworks, laws, policies and protocols must be developed in order to unify the work of the various devices within IoT, and to ensure the confidentiality

and privacy of data. As none of the previous studies referred to any unified framework or protocol except for one study [5] which referred to a general and unified framework called 'ACE' for security issues such as authentication and authorization in restricted environments and presented by Internet Engineering Task Force.

- There are several technologies, that may contribute to securing data in IoT such as:lightweight systems, edge computing, fog computing, trust computing, digital twins, block-chain, software-defined networking, machine learning, and various cryptographic techniques such as: white box, ECC, Paillier, lightweight cryptography.
- The most common security requirements in the Internet of Things are: network security, data privacy (especially personal data), identity management through authentication and access control, and trust management in order to prevent leakage of sensitive information.
- The current paper is similar to the study [1] in using the critical review methodology, and it is similar to the studies [3–5, 11, 15] in that they all aim to extract the most important challenges, techniques and solutions related to IoT environment, and the current paper is similar to studies [3, 5] in that they all aiming to extract the most common challenges, solutions and technologies related to data security - in particular - in IoT.

5. Conclusion

Through all mentioned in the results and discussion, and the most important ones were: the most common issues within the previous studies are confidentiality, privacy, encryption effectiveness, access control, and access authorization. Also, there is an absence or dearth of laws, protocols, and local and global frameworks that unify the IoT work and protect IoT environment from the common security vulnerabilities and problems; so the researcher recommends the following:

- Researchers should conduct more research that discusses the security of IoT environment and specifically the security of data, and conducting practical researches that based on proposing systems, models and frameworks in particular.
- IoT service providers must adopt several security methods, techniques and protocols in order to raise the level of security during the data transfer and storage.
- Concerned organizations and bodies must issue unified laws, policies and frameworks in order to standardize work in IoT environment and to protect the confidentiality and privacy of data.

Acknowledgements

All thanks to King Saud University, which supported this research until it appeared in this final form.

Competing Interests

The authors declare that they have no competing interests.

Authors' Contributions

All the authors contributed significantly in writing this article. The authors read and approved the final manuscript.

References

[1] M. Adil and M.K. Khan, Emerging IoT applications in sustainable smart cities for COVID-19: Network security and data preservation challenges with future directions, *Sustainable Cities and Society* **75** (2021), 103311, DOI: 10.1016/j.scs.2021.103311.

[2] K. Aldriwish, A double-blockchain architecture for secure storage and transaction on the Internet of Things networks, *International Journal of Computer Science and Network Security* **21**(6) (2021), 119 – 126, DOI: 10.22937/IJCSNS.2021.21.6.16.

[3] E. Bertino, Data security and privacy in the IoT, in: *Proceedings of the 19th International Conference on Extending Database Technology*, March 15-18, 2016, Bordeaux, France, *Open Proceedings*, pp. 1 – 3, (2016), DOI: 10.5441/002/edbt.2016.02.

[4] H.R. Ghorbani and M.H. Ahmadzadegan, Security challenges in internet of things: Survey, *2017 IEEE Conference on Wireless Sensors (ICWiSe)*, pp. 1 – 6, (2017), DOI: 10.1109/ICWISE.2017.8267153.

[5] F.A. Habeeb and Q.M. Hussien, Survey on data security techniques in Internet of Things, *Al-Kunooze Scientific Journal* **2**(2) (2021), 27 – 37.

[6] H. Kumar and G. Deepak, Mutual authentication and data security in IoT using hybrid mac id and elliptical curve cryptography, *Turkish Journal of Computer and Mathematics Education* **12**(11) (2021), 501 – 507, URL: https://turcomat.org/index.php/turkbilmat/article/view/5913.

[7] S.A. Kumar, T. Vealey and H. Srivastava, Security in Internet of Things: Challenges, solutions and future directions, *2016 49th Hawaii International Conference on System Sciences (HICSS)*, 5772 – 5781, (2016), DOI: 10.1109/HICSS.2016.714.

[8] SCU Learning Experience Team (2020), *Writing a critical review*, Learning zone, Southern Cross University, available at: https://www.scu.edu.au/media/scueduau/staff/teaching-and-learning/talking-teaching/writing_a_critical_review.pdf.

[9] M.S. Lingam and A.M. Sudhakara, Security in Internet of Things systems, *International Journal of Engineering Research & Technology* **4**(29) (2016), 1 – 5, URL: https://www.ijert.org/research/security-in-internet-of-things-systems-IJERTCONV4IS29040.pdf.

[10] M.M. Noor and W.H. Hassan, Current research on Internet of Things (IoT) security: A survey, *Computer Networks* **148** (2019), 283 – 294, DOI: 10.1016/j.comnet.2018.11.025.

[11] M.M. Ogonji, G. Okeyo and J.M. Wafula, A survey on privacy and security of Internet of Things, *Computer Science Review* **38** (2020), 100312, DOI: 10.1016/j.cosrev.2020.100312.

[12] L. Tawalbeh, F. Muheidat, M. Tawalbeh and M. Quwaider, IoT privacy and security: Challenges and solutions, *Applied Science* **10** (2020), 4102, DOI: 10.3390/app10124102.

[13] S.M. Umran, S. Lu, Z.A. Abduljabbar, J. Zhu and J. Wu, Secure data of industrial Internet of Things in a cement factory based on a blockchain technology, *Applied Sciences* **11**(14) (2021), 6376, DOI: 10.3390/app11146376.

[14] T. Wang, Y. Mei, X. Liu, J. Wang, H.-N. Dai and Z. Wang, Edge-based auditing method for data security in resource-constrained Internet of Things, *Journal of Systems Architecture* **114** (2021), 101971, DOI: 10.1016/j.sysarc.2020.101971.

[15] S. Zaman, K. Alhazmi, M.A. Aseeri, M.R. Ahmed, R.T. Khan, M.S. Kaiser and M. Mahmud, Security threats and artificial intelligence based countermeasures for Internet of Things networks: A comprehensive survey, *IEEE Access* **9** (2021), 94668 – 94690, DOI: 10.1109/ACCESS.2021.3089681.

[16] W. Zhou, Y. Jia, A. Peng, Y. Zhang and P. Liu, The effect of IoT new features on security and privacy: new threats, existing solutions, and challenges yet to be solved, *Internet of Things Journal* **6**(2) (2018), 1606 – 1616, DOI: 10.1109/JIOT.2018.2847733.