Strategies for Internet of Things Data Privacy and Security Using Systematic Review

Sithembiso Khumalo, Amanda Sibiya, Teballo and A. Kekana
University of Johannesburg, South Africa
skhumalo@uj.ac.za
herexcell@gmail.com
tebantonny1@gmail.com

Abstract: The Internet of Things (IoT) now referend to as the Internet of Everything (IoE) has been in existence long before it was identified as a concept. It was introduced with the emergence of the Fourth Industrial Revolution and was aimed at improving people's lives and economies across the globe by connecting physical items to the internet so they can be able to deliver specific services implicitly. The nature of IoT requires that all the systems ensure data privacy and security because much of data that is uploaded into and used by the system is personal and private. Thus, the aim of this research was to identify the tools and strategies that can be used for IoT data privacy and security while also providing a brief but intensive understanding of the concept of IoT and data privacy and security challenges faced by IoT systems. This qualitative research study utilised a pragmatic paradigm and data was collected and analysed using text-based secondary data sources and a PRISMA protocol through systematic review. A PRISMA flow diagram was utilised to assess the eligibility of the sources used for this research. The findings showed that hacking is a major challenge that affects IoT systems and that there are strategies that can be used to protect data such as authentication, encryption technology, and anonymisation amongst many. Additional findings found that the strategies have not yet been found effective, but standards have been set upon the results expected from them. The conclusion is that for the identified strategies to be proven effective, they must be implemented and tested in IoT systems, so further investigation can be conducted if they prove to be ineffective.

Keywords: internet of things (IoT), strategies, tools, data privacy, data security

1. Introduction

The continuous developments in technology have led to several breakthroughs in the field of Information and Communication Technology (ICT) and they include the emergence of the Internet of Things (IoT) – a term discovered by Kevin Ashton in 1999. Rose, Eldridge, and Lyman (2015:5) define IoT as "*scenarios where network connectivity and computing capability extends to objects, sensors, and everyday items not normally considered computers, allowing these devices to generate, exchange, and consume data with minimal human intervention*". IoT does not have one specific definition because people perceive and define it according to how it serves them and according to their own needs (Singh, 2014). Many economies across the world have improved using the IoT, making them more profitable while saving the costs of production and time consumption. Connecting devices and physical items to the internet can assist organisations, decrease data collection limitations by placing data exactly where it is needed, while also providing accurate information which improved reliability.

The concept of IoT has been around for a long time although it is said that it is a concept that came with Kevin Ashton where else he just came up with a more suitable word for the concept (Monther, 2020). Foote (2016) proves that this concept has been around for ages and can be seen in the 1980s where people were able to connect to a Coca Cola machine to check for available drinks before they can purchase. IoT has several advantages including coming with new ways of collecting data, connecting human beings with devices, and connecting devices to the internet, it also has its disadvantages (Weber, 2010). Every system requires some level of privacy and security especially in this type of technology that seems to be more personal and unique for every organisation or person. The many entry points in IoT system and data being shared daily, the system can be prone to cyber-attacks which makes privacy and security a big challenge (Rose *et al* 2015:6). The above mentioned makes it imperative for different IoT security and privacy tools and strategies to be continuously investigated and applied to ensure safety and integrity (Porras, Pänkäläinen, Knutas & Khakurel, 2018). Security in IoT is very important because users entrust the system with personal and sensitive information that when accessed by cyber attackers, they can perform illegal activities that may land users in trouble (Ning, Liu, & Yang, 2013).

This research investigated the tools and strategies of data privacy and security in IoT systems and understanding how these tools and strategies work to ensure the safety of the system. Furthermore, a basic understanding of

what IoT is and the components within IoT were provided, as well as the main challenges that affect privacy and security in IoT (Zhao & Ge, 2013).

2. Research problem, aim and objective

The IoT is a data driven technology used by people and businesses to deliver services that are specific to their needs. This means that personal and private information is uploaded constantly which creates many entry points to the system. For this reason, an IoT system can be prone to cyber-attacks and hacking and people's private information may be used illegally. This makes data privacy and security in IoT a very important aspect to consider because with effective tools and strategies, data can be protected. The main aim of this research was to investigate data privacy and security strategies that can be used to protect data in IoT systems using the systematic review protocol. The main question: *What are the strategies and tools used for data privacy and security on the Internet of Things (IoT).*

3. Literature review

The IoT is an advanced form of technology that has allowed the sharing and trading of data between human being and machines, and/or between two devices without any interference from human beings (Majeed, Bhana, Ha, Kyaruzi, Pervaz, & Williams, 2016). Additionally, the many interconnected devices that are transmitting data and information to both symmetric and non-symmetric systems, an IoT system can be left vulnerable to privacy and security threats. Gulzar and Abbas (2018) argue that the IoT has proven to have more risks than benefits which makes it very challenging and risky for people to rely on it. The idea of introducing IoT was to assist businesses to increase profitability and productivity by having a technology that can interact with people and other devices and improve the value of life for people. However, the fact that data is the main driver of IoT, which means that data is forever being shared and transmitted between devices proves the system to be with many privacy and security faults that need to be addressed (Sfar, 2018). Gillis (2020) defines an IoT *"as a system of interrelated computing devices, mechanical and digital machines, objects, animals or people that are provided with unique identifiers (UIDs) and the ability to transfer data over a network without requiring human-to-computer interaction"*. It consists of four main components including sensors, data processing, connectivity, and user interface that work together seamlessly to provide the required service (Holdowsky, 2015).

The main security and privacy challenge facing IoT systems is hacking where illegal users find ways to get into a system by tracking user footprints through the enormous amounts of data shared and transmitted in the system Stoyanova (2020). Lally and Sgandurra, (2018) add that a lot of IoT system developers put their focus on the cost and usability and only implement measures of privacy and security once the system has been breached and exploited. Some of the strategies that can be used in IoT systems is an authentication system which deals with managing several users for a single device by including things such as biometrics, and digital certificates before access can be granted (Sultana & Gavrilova, 2014:416). Other strategies include encryption technology, anonymisation, routing, and Blockchain based Secure Data Aggregation strategy (BSDA) (Kirichek, Kulik & Koucheryavy, 2016:203). Moreover, none of the tools and strategies investigated have proven to be effective to the system, instead there are standards that have been set and it is hoped that these tools and strategies can meet them (Gionis & Tassa, 2009).

4. Research design and methods

This study used pragmatic paradigm to practically investigate the strategies and tools that are used for data privacy and security on the IoT. This was done by utilising the PRISMA protocol through systematic reviews to collect data on the grey literature and literally go through the data to analyse it to find out what strategies and tools are used in IoT for data privacy and security. To increase the validity of this research, deductive reasoning was used through the study. The study employed a qualitative research method which focused on the quality of textual data collected from databases and grey literatures using the PRISMA protocol. The study utilised a cross-sectional time horizon, where different academic journals are investigated, and results obtained at a single period. Selected journals that were scholarly and peer reviewed in the Information and Knowledge Management discipline and Information Technology were chosen through purposeful sampling. A PRISMA diagram was used for sampling to identify the eligibility criteria of articles that are used. Several articles were found on all the selected databases and grey literature when using the Boolean search string "strategies and IoT and data privacy and data security". The articles provided were screened to eliminate duplicates. The eligibility of the articles was assessed whether the documents are full text articles with the relevant textual information. The study used 37

of the sources found to be eligible to do the research this was completed using a data extraction form which consisted of an eligibility criterion for exclusion and inclusion of data sources (*cf* Appendix A).

Data was gathered from recommended databases (Emerald Insight, EBSCOhost, IEEE Xplore, SAJIM, ACMDL Digital Library and google scholar), these are text based secondary data sources, to help answer the research question. The study searches for academic journals using Boolean search strings: tools and strategies and IoT and data privacy, to gather relevant data and analyse it. The reliability and validity of the study was achieved through deductive reasoning by collecting enough data from different sources that were analysed to draw accurate conclusions. Some sources were excluded from the data analysis as they were irrelevance to the research aim and objective. This process of exclusion and inclusion was completed using a data extraction form which consisted of an eligibility criteria for exclusion and inclusion of data sources (*cf* Appendix A).

5. Results and discussion

This section is based on the articles that matched the eligibility criteria of this research paper. The chart below (figure 1) clearly articulates how the eligibility of the sources used was assessed.

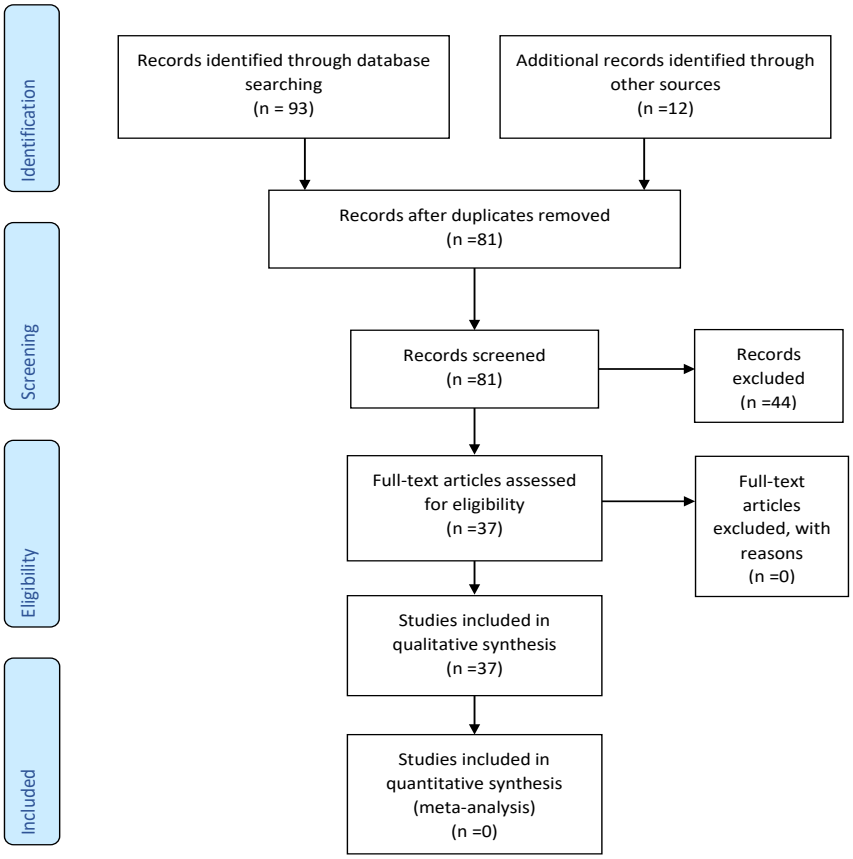

Figure 1: PRISMA flow diagram representation for the sources used for sampling

5.1 Defining the Internet of Things (IoT)

According to the research findings, the concept of IoT was coined by Kevin Ashton in 1999 who defined it as *"interconnected objects that can be uniquely identified with the radio frequency identification system (RFID) technology"*. The IoT is mainly the idea of having electronic systems integrated into physical objects to allow smooth, intelligent, and seamless sharing of information to create a new global infrastructure that can thrive in the fourth industrial revolution (Stankovic, 2014). Furthermore, the main reason why IoT does not have one specific definition is because of the involvement of a lot of research studies, businesses, stakeholders, etc. and all these parties want to define IoT in a manner that best suits their backgrounds, needs, and expectations. From the research findings, it was found that a more interesting idea of IoT, which seems more like a revelation currently, is the idea of Mark Weiser which he came up with in 1991 where he stated that, "The most profound

technologies are those that disappear" which meant that the technologies that will thrive are those that form part of peoples' everyday lives, and this statement was supported by Gartner (2016) where he stated that in 2016, the internet will be connected with more than 60 billion objects which will be 30% more than the objects in 2015. He furthermore stated that the IoT will be one of the trends and key drivers of technology in the 21st century. It is significant to note both the positive and negative sides of IoT and investigate them further.

5.2 Data privacy and security challenges in IoT

According to the research findings, hacking is one of the most prominent privacy and security challenges in IoT systems and there are various forms of threats that can be used to attack (Majeed, Bhana, Ha, Kyaruzi, Pervaz & Williams, 2016). These threats will be discussed further below (Alwarafy, Thelaya, Abdallah, Schneider & Hamdi, 2021).

5.2.1 Hacking

The interconnection of many devices makes the system more prone to cyber-attacks or being hacked more especially if the device connected has poor security or when users leave data streams unprotected (Modi, Patel, Borisaniya, Patel & Rajarajan, 2013). There are several different types of attacks that hackers use to enter IoT Systems (Lu & Xu, 2019).

- *Denial of Service (DoS)* – the hacker may use a bug to attack the system, causing it to fail internally and cause damage to the hardware. The system is then infiltrated by the attacker, and they may use it however they see fit. IoT is most prone to this form of attack. This challenge includes flooding attack or one that simply denies access through a crash.
- *Man-in-the-middle (MITM)* – the hacker gets access and is allowed to listen and peep through a conversation between the sender and the receiver without their permission or knowledge. Once the hacker can eavesdrop, they can be able to replace the data shared between the two parties with fraudulent one (Ngu, Gutierrez, Metsis, Nepal & Sheng, 2017).
- *Node damaging* – this is a form of a physical threat which takes place when the attacker gains physical access to any of the IoT devices. (Tawalbeh, Muheidat, Tawalbeh & Quiwader, 2020).
- *Breakage of cryptographic protocols* – Limited resources can cause the systems; developer to use cryptographic protocols that are weak. Once the attacker hacks the encrypted messages and data, the whole system can be compromised (Roman, Zhou & Lopez, 2013).
- *Shared technology* – in IoT systems, there are many resources that are shared, for example, via virtualization (Rullo, Midi, Serra & Bertino, 2017). The virtual machine monitor of another user can be vulnerable and be penetrated by another user because the monitor can sometimes require the user to allow access (Makhdoom, Abolhasan, Lipman, Liu & Ni, 2019).

5.3 Tools and strategies used for IoT data privacy and security

According to the data that has been collected, the most used tools and strategies for IoT data privacy and security include, Anonymization, Encryption, Authentication, Routing, Blockchain based Secure Data Aggregation strategy (BSDA) and Data privacy frameworks (Ghaffari, Lagzian, Kazemi & Malekzade, 2019). Each of these tools and strategies will be fully explained, as to how they work or how they are used to ensure the security and privacy of data in IoT (Ari, Ngangmo, Titouna, Thiare, Mohamadou, Mohamadou & Gueroui, 2019).

5.3.1 Anonymization

According to the data collected, this is one of the strategies used which generally refers to hiding and modifying data that is related by rearranging some parts or all the original data so that attackers cannot combine and make sense of other information after stealing the anonymized data (Wang, Tong, Shancang, Geyong & Zhiwei, 2021). There is a location privacy protection scheme that has been proposed to utilise k-anonymity and trusted third party policies, where it protects the privacy of the location of the data when a sensing user uploads it and when a requester requests a server that could be untrustworthy (Kirichek, Kulik & Koucheryavy, 2016). In simple terms, k-anonymity hides the identification of the sender of data and upon request, it still does not show the source from which the data comes from. Although the scheme is expensive, it is immune to background attacks.

5.3.2 Encryption technology

According to the findings, encryption technology may be regarded as a process where the sender encrypts the first data using encryption technology, and therefore the receiver decrypts the info using the decryption algorithm.

Cryptographic hashes this is where small messages are read in correspondences to large messages as hashes and main aim of the method is ensure that the hash does not disclose anything related to the original data. Cryptographic hashes can simply be explained as a cryptography technique where data that is new is mixed in ciphertext form by making use of a secret key, transferred in public route and at a later stage decrypted by the receiver with a pre known secret key (Shammar & Zahary, 2019).

IoT encryption this includes encrypting data between IoT devices and back-end systems making use of standard cryptographic algorithms, to keep standard data integrity and to prevent sniffing.

Content encryption the data collected shows that this encryption is only related to data in the storage area, it assists to protect the confidentiality of data one adds into a database in case hackers or unauthorised persons gain access to the content.

5.3.3 IoT authentication

The findings state that IoT devices, begin with an easy static password to authentication mechanisms, through digital certificates and biometrics, nodes that store and/or communicate sensitive data. For instance, healthcare system may become valuable for hackers since they contain valuable information such as patient information and electronic forensic records. Therefore, the healthcare sector should employ means to guard the electronic records from being accessed by unauthorised persons.

A two-factor authentication (2FA) is one among the foremost recommended authentications which needs a user to use a combination of passwords and other authentication forms that do not depend on the knowledge of users, like randomly obtaining a code through Short Message Service (SMS) text. This is followed by a Context-Aware Authentication (CAA), which can be referred as an easily adaptive authentication, where related data and machine-learning algorithms is evaluated on a continuous basis to identify risk of malice without having to bother the end-user in demanding authentication (Jan, Nanda, He, Tan & Liu, 2014). Therefore, the hacker and/or subscriber will be requested to provide a multi-factor token to continue having access if the risk is found to be high. This may create a push or complicated authorisation which can make IoT devices to not have an easy-to-guess password/ authorisation code and keep the info within the devices secured and guarded (Khalid & Majeed, 2016).

5.3.4 Routing

Based on the data collected, routing refers to an unidentified technique used to anonymously sort out the source node to stop the situation information of the source node from leaking. This strategy involves having the power to route users, services and data to servers that are in possession of the user's data. These can use solutions like Amazon's Route service that allows routing based on the geographical location supported by the IP address of network requests done over the web (Tyagi & Goyal, 2020).

5.3.5 Blockchain based Secure Data Aggregation strategy (BSDA) for edge computing empowered IoT

In the data aggregation process, attention focused on the way to aggregate data without privacy disclosure for instance, people that release tasks to be aggregated cannot withstand the leakage of any sensitive information contained within the task (Wang, Garg, Kaddoum & Hossain, 2020). Therefore, they tend to settle on trustworthy workers to finish the task. On the data collected, it shows that the blockchain offers a distribution of ledger that is integrated, peer-to-peer networks, smart contracts and consensus mechanism which allows reliable access control, storage that is secure, and distributed computation, this suggests that applying blockchain to data aggregation will increase the safety and privacy of the information in those tasks (Sciancalepore, & Di Pietro, 2021). For example, purposefully modifying blockchain provide restrictions to workers on tasks that have certain restriction security levels and requirements of completion of requirements (Zanella, Bui, Castellani, Vangelista, & Zorzi, 2014). Furthermore, personal data is then best protected when data from a large group of users or

devices are aggregated, mainly because the information on selected individual is concealed within a more general cohort (Wei, Wu, Long & Lin, 2019).

5.3.6 Data privacy frameworks

Amongst the framework proposed for IoT data security and privacy, Object Security Framework (OSCAR) for IoT is one among the foremost recommended frameworks to use in IoT (Irshad, 2016). This framework is predicated on the concept of object security that introduces security within the appliance payload (Xiong, Rong, Lei, Tian, Liu & Yao, 2020). Although it once considered separate confidentiality and authenticity trust domains, privacy is employed to supply capability-based access control and protection against eavesdropping during the communication. Meaning this security framework protects data from replay attacks by coupling the content encryption key with the duplicate detection (Ferracane, 2019).

6. The effectiveness of IoT tools and strategies in ensuring data privacy and security

Research has been done to find out how are the proposed tools and strategies effective in protecting data within the IoT. Based on the findings that has been collected, it is found that most researchers have not yet tested the tools or the strategies but have set standards as to what these tools and strategies can do in IoT data privacy and security (Cangea, 2019). The proposed standards, amongst others, include improved system performance and secured personalised data (Wang, Zhang, Liu, Bhuiyan & Jin, 2019). These standards or performance can be what is expected after implementing the proposed tools and strategies in securing data and its privacy.

The findings shows that data aggregation schemes ensure data confidentiality, integrity, and real timeliness.

Data confidentiality: data can be able to reach its destination without hackers accessing it or being leaked.

Data integrity: the users can be guaranteed that the data collected by the sensers is real and complete.

Data real timeliness: as soon as data is updated and uploaded by the user, it is received and becomes available in the platform.

7. Conclusions and recommendations

This paper has investigated the tools and strategies that are used in IoT for data privacy and security, while also providing an understanding of the concept of IoT and the security and privacy challenges within it. The use of the PRISMA protocol through systematic review protocol has been of great assistance because it allowed for the identification, evaluation, and summarisation of findings that are relevant to the study of the tools and strategies used in IoT data privacy and security. The findings of this study are not claimed to be universal but have found to be the most popular amongst different resources. The findings of this study have provided information about IoT as a concept and its historical information to shed some light on the technology that is being investigated for strategies that can be used to protects its data. Additionally, the challenges that affect data privacy and security have also been discussed to understand the complexity of the problem that needs the solutions being investigated. It is recommended that another study be conducted, of all the tools and strategies identified in this paper after they have been implemented and tested to find out if they are effective or not. And if they prove to be ineffective, other tools and strategies be investigated that are effective in ensuring data privacy and security in IoT.

In conclusion, the results of this study have been found from investigation the concept of IoT, the challenges facing data privacy and security in IoT, tools and strategies used in IoT data privacy and security, as well as the effectiveness of these tools and strategies using the PRISMA protocol through a systematic review. These findings may be of assistance to other researchers who are looking into IoT strategies and tools for data privacy and security and can be used to expand knowledge. It is however important to note that this study is limited to resources found in in the field of Information and Knowledge Management as well Information Technology. Developments in IoT data privacy and security tools and strategies should be seen as soon as possible considering that people entrust the system with private information. The developers of IoT systems must start considering security and privacy protocols more than they consider the cost, design, and the size. What is important in IoT is to protect the integrity of the data within the system.

Appendix A: Data extraction form and eligibility criteria

DATA EXTRACTION FORM

Topic: **Strategies for Internet of Things data privacy and security using systematic review.**

General Information

Data extractors	Sithembiso Khumalo, Amanda Sibiya and Teballo A. Kekana
Research Question	What are the strategies and tools used for data privacy and security in Internet of Things (IoT)
Setting	N/A
Time	Cross sectional time horizon (9 months)
Protocol and Registration	Systematic Review Protocol
Budget	R1000 for data to conduct the investigation

Eligibility Study

	INCLUDED	EXCLUDED
Publication Type	Article titles, abstracts, and findings on strategies for the Internet of Things data privacy and security.	Non-published material, Sources that are not peer reviewed.
Study Objective	Specific strategies used for data privacy and security on the Internet of Things.	Generic strategies used for data privacy and security.
Language	English	Other languages except English
Methodology	Qualitative	Quantitative, mixed methods
Results	Strategies for IoT data Privacy and security	Generic strategies used for data privacy and security.
Conclusions and Recommendations	Information including further study information related to IoT data privacy and security strategies	Information including further study information related to general data privacy and security strategies
References	Other studies related to IoT data privacy and security strategies	Studies related to general data privacy and security strategies.

References

Alwarafy, A., Al-Thelaya, A.K., Abdallah, M., Schneider, J. and Hamdi, M. 2021. Survey on Security and Privacy Issues in Edge-Computing-Assisted Internet of Things. *IEEE Internet of Things Journal*. 8(6):4004-4022.

Ari, A.A., Ngangmo, O.K., Titouna, C., Thiare, O., Mohamadou, K., Mohamadou, A., and Gueroui. A.M. 2019. *Enabling privacy and security in Cloud of Things: Architecture, applications, security & privacy challenges*. Emerald Publishing limited. Available at https://www.emerald.com/insight/2210-8327.htm.

Cangea, O. 2019. A Comparative Analysis of Internet of Things Security Strategies. *Seria Tehnica*. 71(1):1-10.

Corcoran, P. 2016. The Internet of Things: why now, and what's next? *IEEE Consumer Electronics Magazine*. 5(1):63-68.

Ferracane, M.F. 2019. Data flows and national security: a conceptual framework to assess restrictions on data flows under GATS security exception. *Information Management*. 21(1):44-70.

Foote, K.D. 2016. *A Brief History of the Internet of Things*. DataVarsity. Available form: https://www.dataversity.net/brief-history-internet-things/ Accessed (28 February 2022).

Ghaffari, K., Lagzian, M., Kazemi, M. and Malekzade, G. 2019. A comprehensive framework for Internet of Things development: A grounded theory study of requirements. *Journal of Enterprise Information. 38(1):26-30.*

Gillis, A. 2020. *What is Internet of Things (IoT)?* Tech Agenda. https://internetofthingsagenda.techtarget.com/definition/Internet-of-Things-IoT#:~:text=The%20internet%20of%20things%2C%20or,human%2Dto%2Dcomputer%20interaction.

Gionis, A. and Tassa, T. 2009. k-Anonymization with Minimal Loss of Information. *IEEE Transactions on Knowledge and Data Engineering.* 21(2):206-219.

Gulzar, M. and Abbas, G. 2018. *Internet of Things Security: A Survey and Taxonomy*. 2019 International Conference on Engineering and Emerging Technologies (ICEET). IEEE Xplore.

Holdowsky, J. 2015. *Inside the Internet of Things*. New York: Deloitte University Press.

Irshad, M. 2016. A Systematic Review of Information Security Frameworks on the Internet of Things. *Journal of Internet of Things*. 12(1):1270-1275.

Jan, M.A., Nanda, P., He, X., Tan, Z., and Liu. R. P. 2014. A robust authentication scheme for observing resources on the internet of things environment. *IEEE 13th International Conference on*. Conducted by IEEE.

Khalid, M. and Majeed, S. 2016. A smart visitors' notification system with automatic secure door lock using mobile communication technology. *International Journal of Computer Science and Information Security*. 16(4):97-101.

Kirichek R., Kulik, V. and Koucheryavy, A. 2016. *False Clouds for Internet of Things and Methods of Protection.* St. Petersburg State: St. Petersburg University.

Lally, D. and Sgandurra, G. 2018. Towards a Framework for Testing the Security of IoT Devices Consistently. *1st International Workshop on Emerging Technologies for Authorization and Authentication*. 11263(2018):88-102

Lu, Y., and Xu, L.D., 2019. Internet of Things (IoT) cybersecurity research: A review of current research topics. *IEEE Internet Things Journal*. 6(2):2103–2115.

Majeed, A., Bhana, R., Ha., A., Kyaruzi, I., Pervaz, S. and Williams, M. 2016. Internet of Everything (IoE): Analysing the Individual Concerns Over Privacy Enhancing Technologies (Pets*). International Journal of Advanced Computer Science and Applications (IJACSA*). 7(3):15-22.

Makhdoom, I., Abolhasan, M., Lipman, J., Liu, R. P. and Ni, W. 2019. Anatomy of Threats to the Internet of Things. *IEEE Communications Survey and Tutorial*. 21(2):1636-1675.

Modi, C., Patel, D., Borisaniya, B., Patel, A. and Rajarajan, M. 2013. A survey on security issues and solutions at different layers of Cloud computing. *The Journal of Supercomputing.* 63(2):561-592.

Monther, A.A. 2020. Security Techniques for intelligent spam sensing and anomaly detection in online social platforms. *Journal of Electronic Computer Engineering.* 2(10):143-145.

Ngu, A.H., Gutierrez, M., Metsis, V., Nepal, S. and Q. Z. Sheng. 2017. IoT middleware: A survey on issues and enabling technologies. *IEEE Internet of Things Journal*. 4(1):1-20.

Ning, H., Liu, H., & Yang, L. T. 2013. Cyberentity security on the Internet of Things. *Computer Journal.* 46(4):46-53.

Porras J., Pänkäläinen J., Knutas A. and Khakurel J. 2018. Security on The Internet of Things – A Systematic Mapping Study. *Proceedings of the 51st Hawaii International Conference on System Sciences*.

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

Rose, K., Eldridge, S. and Chapin, L. (2015). *The Internet of Things: an overview Understanding the Issues and Challenges of a More Connected World*. Reston, Virginia: The Internet Society (ISOC).

Rullo, A., Midi, D., Serra, E. and Bertino. E. 2017. Pareto Optimal Security Resource Allocation for Internet of Things. *ACM Trans. Privacy and Security.* 20(4)1-30.

Sciancalepore, S. and Di Pietro, R. 2021. PPRQ: Privacy-Preserving MAX/MIN Range Queries in IoT Networks. *IEEE The Internet of Things Journal*. 8(6)1-19.

Sfar, A.R., Natalizio, E., Challal, Y. and Chtourou, Z. 2018. A roadmap for security challenges on the Internet of Things. *Digital Communications and Networks*. 4(2):118-137.

Shammar, A. E. and Zahary, T. A. 2019. The Internet of Things (IoT): A survey of techniques, operating systems, and trends. *The Internet of Things*. 38(1):6-8.

Singh, J. 2014. Cyber-attacks in cloud computing: a case study. *International Journal of Electronics and Information Engineering*. 1(2):78-85.

Stankovic, A.J. 2014. Research directions for the Internet of Things. *IEEE Internet of Things Journal*. 1(1):7-9.

Stoyanova, M., Nikoloudakis, Y., Panagiotakis, S., Pallis, E. and Markakis, K.E., 2020. A Survey on the Internet of Things (IoT) Forensics: Challenges, Approaches, and Open Issues. *IEEE Communications Survey and Tutorial*. 22(2):1191-1221

Sultana, M. & Gavrilova, M. L. 2014. Face recognition using multiple content-based image features for biometric security applications. *International Journal of Biometrics*. 6(4): 414-434.

Tawalbeh, L., Muheidat, F., Tawalbeh, M. and Quiwader, M. 2020. IoT privacy and security: challenges and solutions. *Journal of Applied Science.* 10 (41): 1-17

Tyagi, A.K and Goyal, D. 2020. *A Survey of Privacy Leakage and Security Vulnerabilities on the Internet of Things. Emerald publishing limited*. Johannesburg: University of Johannesburg.

Wang, R., Tong, X., Shancang, I., Geyong, M. and Zhiwei, Z. 2021. *Privacy Enhancing Techniques on the Internet of Things Using Data Anonymisation*. Beijing: Peking University.

Wang X. Garg S. Kaddoum G. and Hossain H.S. 2020. A Secure Data Aggregation Strategy in Edge Computing and Blockchain empowered Internet of Things. *Journal of the Internet of Things*. 10(2):2327-4662.

Wang, T., Zhang, G., Liu, A., Bhuiyan, M.Z.A. and Jin, Q., 2019. A secure IoT service architecture with an efficient balance dynamic based on cloud and edge computing. *IEEE Internet Things Journal*. 6(3).

Weber, R. H. 2010. Internet of Things–New security and privacy challenges. *Computer law & security review*. 26(1):23-30.

Wei, L., Wu, J., Long, C. and Lin, Y.-B., 2019. The convergence of IoE and blockchain: security challenges. *IT* Professional. 21(5):26-32.

Xiong J., Rong M., Lei C., Tian Y., Liu X., and Yao Z. 2020. A Personalized Privacy Protection Framework for Mobile Crowdsensing in IIoT. *Journal of Industrial Informatics*. 16(6):4231-4241

Zanella, A., Bui, N., Castellani, A., Vangelista, L. and Zorzi, M., 2014. Internet of Things for smart cities. *IEEE Internet of Things Journal*. 1(2):22-128

Zhao, K. and Ge, L., 2013. A survey on the Internet of Things security. *Ninth International Conference on Computational Intelligence and Security*. Conducted by IEEE explore. New York: IEEE Explore.