Review of Computer Engineering Research
2019 Vol.6, No.1, pp.35-44
ISSN(e): 2410-9142
ISSN(p): 2412-4281
DOI: 10.18488/journal.76.2019.61.35.44

IDENTIFICATION OF PRIVACY AND SECURITY RISKS OF INTERNET OF THINGS: AN EMPIRICAL INVESTIGATION

Muhammad Hamza[1+]
Muhammad Azeem Akbar[2]
Muhammad Shafiq[3]
Tahir Kamal[4]
Ali Mahmoud Baddour[5]

[1,2,5]*School of Big Data and Software Engineering, Chongqing University, China.*
[1]*Email: hamzajee541@gmail.com*
[2]*Email: azeem.akbar@ymail.com*
[5]*Email: baddour.ali85@gmail.com*
[3,4]*School of Computer Science & Technology, Chongqing University of Posts and Telecommunications, China.*
[3]*Email: shafiqk786@hotmail.com*
[4]*Email: tahirkamal2@hotmail.com*

(+ Corresponding author)

Article History
Received: 20 December 2018
Revised: 30 January 2019
Accepted: 4 March 2019
Published: 8 May 2019

Keywords
Internet of things
Privacy
Data security
Data integrity
Confidentiality
Empirical investigation.

ABSTRACT

The internet of things (IOT) is a phenomenon of connected devices over the internet to ease human life. It is a system where a separate computing device embedded with sensors is connected to other devices or to the cloud through the different infrastructures of the Internet. The implication of the IOT is still challenging in a geographically distributed environment. Particularly, the main challenges are associated with data privacy and security. In this study, we investigate in the report the risks/issue related to IoT data privacy and security from the existing literature for the last two years and provide a review. We identify a total of seven issues related to IoT data privacy and security. The findings revolved that Privacy, Security, confidentiality, and integrity are the most significant issues for IoT in the current era. The findings of this study provide the researchers with a body of knowledge about the critical issues faced by the users and practitioners of IOT across the globe.

Contribution/Originality: In this paper, we conducted the literature review to find out the main challenges that are being faced by challenges related to privacy and security mainly, authentication and access control, confidentiality and integrity IOT devices users and as well as for IOT manufacturer. We highlighted seven, privacy, trust on the device and conducted a questionnaire survey from different organizations and from different research experts and ranked it accordingly.

1. INTRODUCTION

The Internet of Things is a term used for describing interconnected devices through the Internet. The connection allows data transfer and advanced capabilities as compared to a single device working alone. A connection to a central server or to a cloud service is most of the time added to the system especially when storage or processing power beyond the capacity of the single device is required or data gathering is needed to enable further analysis. It is being controlled and monitored by the organization remotely. The IoT gadgets are embedded with sensors and handling power that empower them to be conveyed in numerous situations. It will contribute to the huge change to the world's future society, it can contribute to the living style and in business models. The IOT application includes smart home [1] smart cities [2] smart grids [3] vehicular Ad-Hoc Network (VANETs) [4] medical and healthcare instruments [5] etc. It is envisioned that a number of IoT devices will reach up to 41 Billion

by 2020 with an estimated cost of $8.9 trillion [6] according to international data corporation (IDC). These devices will be able to get information about a person's behaviors, analyze and can take action [7]. In simple it will ease human life incredibly.

Apart from the advantages of IoT devices or network, there are various issues particularly related to security and privacy. Because the IoT devices manufacturing industries are failed to implement robust security and privacy related mechanisms in their devices, cybersecurity experts and researchers have unveiled the risks using a large number of unsecured IOT devices. The devices may come under different attacks and privacy of the user may be unveiled by attackers.

However, by considering the state of the art literature, we noted that very limited research has been conducted to address the problems related to IoT security and privacy. As security and privacy is the fundamental activity of IOT, though we are motivated to explore the barriers and risks of IOT faced by the user across the globe. To this, we have conducted an informal literature review and explore the critical risk of IOT security and privacy. We further conduct a questionnaire survey with real-world practitioners to validate the findings of the literature review and to explore the additional critical risk of IOT security and privacy. The findings of this study assist researchers and practitioners to develop the tools and strategies to overcome these barriers and to enhance the confidant of IOT users in real life. To adders the objective of this study, we propose the following research questions (RQ):

RQ1: What are the risks for IOT security and privacy, as investigated from the literature?

RQ2: What are the limitations of IoT devices?

RQ3: What techniques are used to address the risks of IOT?

RQ4: What practitioners think about the risks of IOT security and privacy?

2. RESEARCH OBJECTIVE

Various studies were conducted to address the problem faced by the IOT users. Maple [8] highlighted that the privacy of data in IOT phenomena is very significant. Thus our key objective of this review the Literature from 2017-2019 and to highlight the most critical risks of IOT and the suggested approaches to address these risks. The ultimate objective of this study is to develop a comprehensive technique to mitigate the risk of IoT data security and privacy. The current study is an initial step towards the development of proposed tools, in which the critical risks and the used approaches are explored.

3. RESEARCH METHODOLOGY

To conduct this study, we applied two different research approaches i.e. literature review and empirical investigating (questionnaire survey).

3.1. Literature Review

To conduct the literature review, we extracted the latest published studies in the field of IOT security and privacy. The literature review approach is an effective way to determine the state-of-the-art work related to a research topic. Various other researcher adopts this method to explore the existing literature in different other software engineering domains [9-13].

3.2. Empirical Study

To validate the findings of the literature review, we conduct an empirical study with IOT practitioner by using questionnaire survey. Though, the following steps are involved to conduct a questionnaire survey:

3.2.1. Data Collection via Questionnaire Survey

The method used to assess the findings of the literature questioner survey technique was adopted, the questionnaire survey is used to ask industry practitioners about the main factors that influence on IoT devices. The questionnaire (Appendix A) was designed on the Risk of IOT devices. The main objective of designing a questionnaire is to get an opinion from the industry practitioners about the importance of factors targeted by us [13]. The importance of factors was marked upon a criterion of "strongly agree"," agree", "disagree", "strongly disagree". The questionnaire was also designed to note the project management structure adopted by industry. The survey participants were asked to mark their organization. Furthermore, the participants have an open choice to write down any other factor which they consider to be important. More suggestions to improve questionnaire were also asked in the form of comments. The questionnaire was assessed by a pilot study by involving five software field experts from industry having more than good experience in related field. Based on this study the final version of the questionnaire was used for data collection. It consists of three parts: section one collects demographic data of the respondent, in section, the identified factors for literature were enlisted, and ask respondents, and section three collect comments and other new factors identified by participants. The participants were informed that their raw data is confidential and would not be shared in such a form with any other company that could reveal the company's or identity.

3.2.2. Data Source

In this study, the targeted population was the software practitioners that have more than five years of experience in the related field in managing IOT projects. Searching a suitable sample for the survey is not an easy task for which no exhaustive register for target population exists [9]. Hence the participants were evaluated by using the snowball technique [10] that is typically used in questionnaire study where members are difficult to locate [11].

Like the other studies regarding survey based [12] an initial invitation to the participants of this research work were sent to participate via LinkedIn group, mailing list, industry contacts of the research team. The main focus is on software practitioners in industry who participated in this research. The contact points were requested to email the link of an online survey to other industry software practitioners in their contact in order to provide help in the characterization of unknown populations [10]. The contact persons were asked to inform about the total number of participants in order to keep a check on the total number of surveys completed.

Since as we have used email, LinkedIn, industry contacts and snowball technique, so it is acknowledged that the sample data is not truly random. However, it is difficult to search for the experts dealing with IOT based techniques in the industry as indicated by Akbar, et al. [13] if a truly representative sample is difficult to arrange then, the research should try to omit as much bias as possible. Similarly, in order to make the sample representative in the industry of IOT manufacturer, practitioners, different participants were invited from a different industry group to participate in this research. These participants were from ten different countries which include Australia, India, Malaysia, Ireland, Saudi Arabia, UK, and US. The participants involved work in organizations which are familiar with IOT based on working security and privacy. Furthermore, some of the participant roles in their organization ranges from team leaders to software projects managers. Therefore, we are confident enough about the results we gather from these experts regarding security and privacy risk of IOT devices.

A total of 81 responses were collected from the practitioners. All the responses were reviewed manually in order to verify the completeness of questionnaires. Though, four questionnaires were rejected because of incomplete entries. Finally, we include 77 accepted questionnaires in our study for further analysis. A sample of the questionnaire survey is presented in Appendix-A.

3.2.3. Data Analysis Method

To organize the data gathered from the questionnaires were use the frequency analysis scheme to group data scores as it is helpful in analyzing the descriptive information. The percentage of each data variables were reported using the frequency tables. The frequencies defined can be used to compare variable within or across the groups and can also be suitable in nominal, ordinal and numerical data [11, 14-16]. In order to identify the factors, the occurrence of each factor was measured in the questionnaire. Finally, the ranking of each factor can be marked by comparing it with the other factors.

4. FINDINGS

4.1. Findings of the Literature Review

While conducting the literature review, we investigate the IOT security and privacy risks and the limitations of the IoT devices to apply the data security and privacy algorithms, as discussed in the following sections:

4.1.1. Extracted IOT Risks by using Literature Review

R1 (Authentication and Access control) is a serious issue for users in IoT devices, so to overcome this risk/ challenges researcher provided Datagram Transport layer protocol (DTLP) and username/Password pair authentication for users of IoT devices, Kothmayr, et al. [17] and Maple [8] highlighted the impact of authentication and access controls risks in IOT. They further reported that it is important to address the authentication risk to develop the trust of IOT technology.

R2 (**Access control**): different schemes are used namely Discretionary Access Control (DAC) & role-based access control (RABC) and Attribute-based access control (ABAC). Access control is an important aspect of IOT. It is significant that the access control of the IoT devices is authentic to secure the data and maintain the privacy of the users, data stored and shared among users' components.

R3 (Confidentiality and Integrity) being secret is one's right that is a critical challenge in IOT, to address these challenges different schemes such as Key Management scheme (KMS) and Public key Infrastructure algorithm is being used. Roman, et al. [18] highlighted that confidentiality of IOT user is an important attributed. Maple [8] conducted a recent study and mention that the IOT users still facing the problems of confidentiality and integrity [18] also mention the confidentiality and integrity as a risk for IOT.

Table-1. Investigated factors.

S.No.	IoT risks	References	Existing techniques to address the risks
R1	Authentication	[17]; [8]	(1) Datagram Transport Layer protocol (DTLP) (2) Username/ Password pair
R2	Access control	[8]	(1) Discretionary Access Control (DAC) (2) Role-based access control (RABC) (3) Attribute-based access control (ABAC)
R3	Confidentiality and Integrity	[18]; [8]	(1) Key Management scheme (KMS) (2) Public key Infrastructure algorithm
R4	Privacy	[8]; [21]; [22]	(1) Attribute-Based Encryption (ABE), (2) Key policy attribute Encryption (KP-ABE) (3) Virtual private Network (VPN), Transport Layer Security (TLS),
R5	Secure Middleware	[23]; [24]; [25]; [26]	(1) eXtensible Messaging and Presence Protocol (XMPP). (2) AES and DHKE (3) UBOOT (Universal Boot loader)
R6	Policy Enforcement	[27]	(1) Security policy engine (SPE)
R7	Trust on Device	[8]	(1) Fulfill the end user requirement

R4 (Privacy) is considered a major concern in IOT. To address this challenge Researchers provided different schemes such as Attribute-Based Encryption (ABE), Key policy attribute Encryption (KP-ABE), Virtual Private Network (VPN), Transport Layer Security (TLS) that still need to improve [19, 20]. To maintain the privacy of the IoT devices from the different harmful attacks, there is a lack of automatics mechanisms to handle the risk of data privacy in IOT. Rest of the investigated risks are enlisted in Table 1.

4.1.2. Investigated Limitation of the IOT Devices

Battery capacity IOT devices are small and have low battery power, it is not possible to implement advanced Cryptographic Algorithm because of high power consumption that can drain the devices' resources. Researchers need to consider this limitation.

Computing Power because of a current cryptographic algorithm that drains the battery significantly some other algorithms and techniques have been developed namely Encrypted Query Processing Algorithms, applying Physical Layer authentication and analog characteristics transmitter. But these schemes still need more intention to overcome these limitations. All the other limitations are provided in Table 2.

Table-2. Limitation of IOT devices.

S.No.	IOT Limitations	References	Existing techniques to address the risks
L1	Battery Capacity	[28]	Minimize the security requirement. Increase the battery capacity Energy from natural resources
L2	Computing Power	[29]; [30]	Physical Layer authentication. The encrypted query processing algorithm Identity-based Encryption (IBE)

4.2. Results of Empirical Study

To validate the findings of the literature review, we conducted a questionnaire survey study. The results of the empirical study are presented in Table 3. Table 3 is classified into three broad categories: Positive, Negative and Neutral. The positive category represents the opinions of the practitioners who agree with the findings of literature review, Negative category presents the response of the participants who don't think the investigated factor have a negative impact of IoT paradigm. The neutral category presents the opinions of the respondents who are not sure about the identification of literature review.

The empirical findings show that most of the respondents agree with the investigated factors as they could negatively affect the IoT devices.

According to the frequency analysis R5 (Privacy, 95%) is declared as the most important risk factor that has a negative impact in a geographically distributed environment [31-33]. It is not surprising as this risk is also highlighted in the literature as a critical challenge for IOT devices. Medaglia and Serbanati [34] indicated that to secure the data in the context of IOT, comprehensive and efficient algorithms are still needed. Hwang [35] and Frustaci, et al. [36] also highlighted the importance of data security in IoT devices and networks.

Table-3. Analyzed results of survey respondents.

S. No.	Investigated Risk factors	No. of complete responses=77							
		Positive			Negative			Neutral	
		SA	A	%	SD	D	%	N	%
R1	Authentication	28	44	91	1	2	4	2	14
R2	Trust building	21	41	92	3	7	18	5	18
R3	Access control	24	29	87	6	8	13	13	12
R4	Confidentiality and Integrity	19	39	92	5	6	16	8	10
R5	Privacy	17	32	95	5	7	12	16	8
R6	Secure Middleware	21	39	89	3	9	12	5	6
R7	Policy Enforcement	23	36	77	4	7	11	7	9

The second and third most important risk factors are R4 (Confidentiality and integrity, 92%) was declared as the second most critical risk for IOT phenomena. Shukla and Tripathi [37] emphasized that confidentiality and integrity of data is a fundamental requirement of every user. They further underlined that IoT devices still not capable to secure the data to a confident extent.

According to the survey results, R1 (Authentication, 91%) was cited as the third most significant risk for IOT context. The authentication is still a problem in IOT networks and devices as the number of users are involved in daily usage devices (e.g. Smart doors, microwave Owen, house usage devices, etc.). Zheng, et al. [38] also highlighted that authentication is one of the critical risks for IoT phenomena in common usage devices. They further highlighted that the lack of comprehensive and compact algorithm causes the lack of data security.

In a negative category, we noted that (Trust Building, 18%) was declared as the most significant reported influencing factor. According to the 18% of respondents, R2 doesn't have any negative impact on identified risk on IoT devices.

R6 (Secure Middleware, 12%) and R7 (Policy Enforcement, 11%) was declared as the second and third highest reported factors in GSD.

R2 (Trust Building, 18%) was cited as the most important factor in the neutral category. This indicated that 18% of participants don't sure as the R2 has a positive impact on task allocation process. R1 (Authentication, 17%) was declared as the second most cited factor in the neutral category.

Table-4. Summary of the research questions.

Research questions	Findings
RQ1: What are the risks for IOT security and privacy, as investigated from the literature?	Authentication (R1), Access control (R2), Confidentiality and Integrity (R3) Privacy (R4), Secure Middleware (R5), Policy Enforcement (R6), Trust on Device (R7)
RQ2: What are the limitations of IoT devices?	Battery Capacity (L1) Computing Power (L2
RQ3: what techniques are used to address the risks of IOT?	Datagram Transport Layer protocol (DTLP), Username/ Password pair, Discretionary Access Control (DAC), Role-based access control (RABC), Attribute-based access control (ABAC), Key Management scheme (KMS), Public key Infrastructure algorithm, Attribute-Based Encryption (ABE), Key policy attribute Encryption (KP-ABE), Virtual Private Network (VPN), Transport Layer, Security (TLS), eXtensible Messaging and Presence Protocol (XMPP), AES and DHKE, UBOOT (Universal Boot loader), Security policy engine (SPE), Fulfill the end user requirement
RQ4: What practitioners think about the risks of IOT security and privacy?	According to the practitioners, all the investigated risks are important to address to the success of IOT phenomena. The most important risks are:

5. SUMMARY OF FINDINGS

The objective of this study is to investigate the risks of IOT faced by users and practitioners. We have applied for both the literature review and empirical study (questionnaire survey) approaches to investigate the risks and the limitation of the IoT devices. The detail summary of the research question is presented in Table 4.

6. CONCLUSION AND FUTURE WORK

This research work is based on a literature review and questionnaire survey that were conducted to explore the factors that can negatively impact the IOT paradigm. The findings of this study provide the body of knowledge to researcher and practitioner, to successfully implement the IOT application in the real-world environment.

During the literature review, we have identified a total of 7 Risk factors that can negatively impact on the IoT devices. To validate the findings of the literature review study, an empirical study (questionnaire survey) was conducted with real-world practitioners. According to the results of the empirical study, the majority of the

practitioners are agreed that the investigated factor have a negative impact on IoT devices. In addition, we identified the existing tools and techniques used to address the risks of IOT. The results of empirical study revolved that Privacy, Trust building, and Authentication are the most critical risk factors for IOT phenomena. The ultimate aim of this study is to develop a comprehensive algorithm which could assist to address the risks of IOT devices. This study contributes to the development of the proposed model. We believe the current study provides the body of knowledge to researcher and practitioners to IOT. In the future, we will develop a comprehensive algorithm to address the highlighted risk of IOT.

Funding: This study received no specific financial support.
Competing Interests: The authors declare that they have no competing interests.
Contributors/Acknowledgement: All authors contributed equally to the conception and design of the study.

REFERENCES

[1] M. Wahidur, M. H. Rashid, and R. Islam, "Embodiment of IOT based smart home security system," vol. 6, pp. 2321-9653, 2018.

[2] B. Hammi, R. Khatoun, S. Zeadally, A. Fayad, and L. Khoukhi, "IoT technologies for smart cities," *IET Networks*, vol. 7, pp. 1-13, 2017.

[3] Z. M. Fadlullah, A. K. Pathan, and K. Singh, "Smart Grid Internet of Things," *Mobile Networks and Applications*, vol. 23, pp. 879–880, 2018. Available at: https://doi.org/10.1007/s11036-017-0954-2.

[4] Z. Abdulkader, A. Abdullah, M. T. Abdullah, and Z. A. Zukarnain, "A survey on sybil attack detection in vehicular ad hoc networks (VANET)," *Journal of Computers*, vol. 29, pp. 1-6, 2018.

[5] A. Sharma, T. Choudhury, and P. Kumar, "Health monitoring & management using IoT devices in a cloud based framework," presented at the International Conference on Advances in Computing and Communication Engineering (ICACCE). IEEE, 2018.

[6] K. L. Lueth, "Why the internet of things is called internet of things: Definition, history, disambiguation," *IoT Analytics*, vol. 19, 2014.

[7] I. Saif, S. Peasley, and A. Perinkolam, "Safeguarding the internet of things: Being secure, vigilant, and resilient in the connected age," *Deloitte Review*, vol. 17, 2015.

[8] C. Maple, "Security and privacy in the internet of things," *Journal of Cyber Policy*, vol. 2, pp. 155-184, 2017.

[9] M. A. Akbar, J. Sang, A. A. Khan, M. Shafiq, S. Hussain, H. Hu, M. Elahi, and H. Xiang, "Improving the quality of software development process by introducing a new methodology–AZ-model," *IEEE Access*, vol. 6, pp. 4811-4823, 2018. Available at: https://doi.org/10.1109/access.2017.2787981.

[10] M. Shafiq, Q. Zhang, M. A. Akbar, A. A. Khan, S. Hussain, F.-E. Amin, A. Khan, and A. A. Soofi, "Effect of project management in requirements engineering and requirements change management processes for global software development," *IEEE Access*, vol. 6, pp. 25747-25763, 2018. Available at: https://doi.org/10.1109/access.2018.2834473.

[11] M. A. Akbar, J. Sang, A. A. Khan, F.-E. Amin, S. Hussain, M. K. Sohail, H. Xiang, and B. Cai, "Statistical analysis of the effects of heavyweight and lightweight methodologies on the six-pointed star model," *IEEE Access*, vol. 6, pp. 8066-8079, 2018. Available at: https://doi.org/10.1109/access.2018.2805702.

[12] M. A. Akbar, M. Shameem, J. Ahmad, A. Maqbool, and K. Abbas, "Investigation of project administration related challenging factors of requirements change management in global software development: A systematic literature review," presented at the International Conference on Computing, Electronic and Electrical Engineering (ICE Cube). IEEE, 2018.

[13] M. A. Akbar, M. Shafiq, J. Ahmad, M. Mateen, and M. T. Riaz, "AZ-model of software requirements change management in global software development," presented at the International Conference on Computing, Electronic and Electrical Engineering (ICE Cube). IEEE., 2018.

[14] A. Mateen, M. Sehar, K. Abbas, and M. A. Akbar, "Comparative analysis of wireless sensor networks with wireless multimedia sensor networks," presented at the IEEE International Conference on Power, Control, Signals and Instrumentation Engineering (ICPCSI). IEEE, 2017.

[15] M. Mateen, J. Wen, Nasrullah, and M. A. Akbar, "The role of hyperspectral imaging: A literature review," *International Journal of Advanced Computer Science and Applications*, vol. 9, pp. 51-62, 2018. Available at: https://doi.org/10.14569/ijacsa.2018.090808.

[16] N. Nasrullah, J. Sang, M. Mateen, M. A. Akbar, H. Xiang, and X. Xia, "Reversible data hiding in compressed and encrypted images by using Kd-tree," *Multimedia Tools and Applications*, pp. 1-20, 2019. Available at: https://doi.org/10.1007/s11042-018-7130-y.

[17] T. Kothmayr, C. Schmitt, W. Hu, M. Brünig, and G. Carle, "DTLS based security and two-way authentication for the internet of things," *Ad Hoc Networks*, vol. 11, pp. 2710-2723, 2013. Available at: https://doi.org/10.1016/j.adhoc.2013.05.003.

[18] R. Roman, C. Alcaraz, J. Lopez, and N. Sklavos, "Key management systems for sensor networks in the context of the internet of things," *Computers & Electrical Engineering*, vol. 37, pp. 147-159, 2011. Available at: https://doi.org/10.1016/j.compeleceng.2011.01.009.

[19] A. Mateen, K. Abbas, and M. A. Akbar, "Robust approaches, techniques and tools for requirement engineering in agile development," presented at the IEEE International Conference on Power, Control, Signals and Instrumentation Engineering (ICPCSI). IEEE, 2017.

[20] A. Mateen, M. Azeem, and M. Shafiq, "AZ model for software development," *arXiv preprint arXiv:1612.08811*, 2016.

[21] X. Wang, J. Zhang, E. M. Schooler, and M. Ion, "Performance evaluation of attribute-based encryption: Toward data privacy in the IoT," presented at the In Communications (ICC), 2014 IEEE International Conference on. IEEE, 2014.

[22] J. Su, D. Cao, B. Zhao, X. Wang, and I. You, "ePASS: An expressive attribute-based signature scheme with privacy and an unforgeability guarantee for the internet of things," *Future Generation Computer Systems*, vol. 33, pp. 11-18, 2014. Available at: https://doi.org/10.1016/j.future.2013.10.016.

[23] L. Peng, W. Ru-Chuan, S. Xiao-Yu, and C. Long, "Privacy protection based on key-changed mutual authentication protocol in internet of things," presented at the In China Conference Wireless Sensor Networks. Springer, Berlin, Heidelberg, 2013.

[24] D. Conzon, T. Bolognesi, P. Brizzi, A. Lotito, R. Tomasi, and M. Spirito, "The virtus middleware: An xmpp based architecture for secure IoT communications, in: 2012," presented at the 21st International Conference on Computer Communications and Networks, ICCCN 2012, Munich, Germany, 2012.

[25] M. Isa, N. Mohamed, H. H. S. Adnan, J. Manan, and R. Mahmod, "A lightweight and secure TFTP protocol for smart environment, in: ISCAIE 2012 – 2012," presented at the IEEE Symposium on Computer Applications and Industrial Electronics 2012, Kota Kinabalu, Malaysia, 2012.

[26] S. Sicari, A. Rizzardi, L. A. Grieco, and A. Coen-Porisini, "Security, privacy and trust in Internet of Things: The road ahead," *Computer Networks*, vol. 76, pp. 146-164, 2015. Available at: https://doi.org/10.1016/j.comnet.2014.11.008.

[27] F. Siddiqui, M. Hagan, and S. Sezer, "Embedded policing and policy enforcement approach for future secure IoT technologies," in *In Living in the Internet of Things: Cybersecurity of the IoT - 2018: Proceedings*, 2018, p. 10.

[28] Y. Yang, L. Wu, G. Yin, L. Li, and H. Zhao, "A survey on security and privacy issues in internet-of-things," *IEEE Internet of Things Journal*, vol. 4, pp. 1250-1258, 2017. Available at: https://doi.org/10.1109/jiot.2017.2694844.

[29] W. Trappe, R. Howard, and R. S. Moore, "Low-energy security: Limits and opportunities in the internet of things," *IEEE Security & Privacy*, vol. 13, pp. 14-21, 2015. Available at: https://doi.org/10.1109/msp.2015.7.

[30] H. Shafagh, A. Hithnawi, A. Droescher, S. Duquennoy, and W. Hu, "Poster: Towards encrypted query processing for the internet of things," in *Proceedings of the 21st Annual International Conference on Mobile Computing and Networking, ser. MobiCom '15. New York, NY, USA: ACM*, 2015, pp. 251–253.

[31] J. Ahmad, A. M. Butt, M. Hussain, M. A. Akbar, and W. U. Rehman, "The deep neural network based classification of fingers pattern using electromyography," presented at the 2nd IEEE Advanced Information Management, Communicates, Electronic and Automation Control Conference (IMCEC). IEEE, 2018.

[32] S. Akram, M. Shafiq, and M. A. Akbar, "Automated risk analysis model for software development enhancement," *International Journal of Multidisciplinary Sciences and Engineering*, vol. 7, pp. 23-27, 2016.

[33] A. Mateen and M. A. Akbar, "Estimating software reliability in maintenance phase through ann and statistics," 2016.

[34] C. M. Medaglia and A. Serbanati, *An overview of privacy and security issues in the internet of things. In the internet of things.* New York: Springer, 2010.

[35] Y. H. Hwang, "Lot security & privacy: Threats and challenges," in *Proceedings of the 1st ACM Workshop on IoT Privacy, Trust, and Security. ACM*, 2015.

[36] M. Frustaci, P. Pace, G. Aloi, and G. Fortino, "Evaluating critical security issues of the IoT world: Present and future challenges," *IEEE Internet of Things Journal*, vol. 5, pp. 2483-2495, 2018. Available at: https://doi.org/10.1109/jiot.2017.2767291.

[37] A. Shukla and S. Tripathi, "Security challenges and issues of internet of things: Possible solutions," presented at the 3rd International Conference on Internet of Things and Connected Technologies, (ICIoTCT 2018), 2018.

[38] S. Zheng, N. Apthorpe, M. Chetty, and N. Feamster, "User perceptions of smart home IoT privacy," in *Proceedings of the ACM on Human-Computer Interaction, 2 (CSCW)*, 2018.

Appendix-A: (questionnaire survey)

Section-A1 Respondents personal detail				
Full Name (optional)				
Email address				
Job title industry/academic				
Working Experience (Years)				
Section-A2 Respondents organization detail				
Name of organization (optional).				
Primary business of your organization	Research	Conslteny	Development	
Please specify the nature of your organization?	National	Multinational	Not sure	Others
Please specify the types of your organization?	Developer		Saler	
How long the IOT paradigm is in operation in your organization? (Years)				

Section B-Internet of things (IOT), risks.
The aim of this section is to specify the risks that could negatively impact the IOT implementation Please rank each risk according to your understanding and experience.

S.D= Strongly Disagree, D= Disagree, N= Neutral, A=Agree, S.A= Strongly Agree

Sr.NO	Identified Risks	S.D	D	N	A	S.A
R1	Authentication					
R2	Access control					
R3	Confidentiality and Integrity					
R4	Privacy					
R5	Secure Middleware					
R6	Policy Enforcement					
R7	Trust on Device					
Please add additional risk if any.						