Security Vulnerabilities, Attacks, Threats and the Proposed Countermeasures for the Internet of Things Applications

Article *in* Solid State Technology · September 2020

CITATIONS
10

READS
471

7 authors, including:

Taher M. Ghazal
Skyline University College
44 PUBLICATIONS **166** CITATIONS
SEE PROFILE

Mohammad Kamrul Hasan
Universiti Kebangsaan Malaysia
185 PUBLICATIONS **807** CITATIONS
SEE PROFILE

Rosilah Hassan
Universiti Kebangsaan Malaysia
143 PUBLICATIONS **704** CITATIONS
SEE PROFILE

Shayla Islam
International Islamic University Malaysia
15 PUBLICATIONS **70** CITATIONS
SEE PROFILE

Solid State Technology
Volume: 63 Issue: 1s
Publication Year: 2020

Security Vulnerabilities, Attacks, Threats and the Proposed Countermeasures for the Internet of Things Applications

Taher M. Ghazal[1], Mohammad Kamrul Hasan[2*], Rosilah Hassan[3], Shayla Islam[4], Siti Norul Huda Sheikh Abdullah[5], Mohammed A. M. Afifi[6], Deepak Kalra [7]

[1,6,7] School of Information Technology, Skyline University College, Sharjah, United Arab Emirates.

[1,2,3,5] Network and Communication Technology Lab, Center for Cyber Security, Faculty of Information Science and Technology, Universiti Kebangsaan Malaysia (UKM), 43600 UKM, Bangi, and Selangor, Malaysia.

[4] Institute of Computer Science and Digital Innovation, UCSI University, 56000 Kuala Lumpur, Malaysia.

***Abstract*—** The proposed research is based on the solutions for the Internet of Things (IoT) security threats and vulnerability. It is cleared that IoT is playing a vital role now a day at an organizational level by making it easy while working at enterprises. The level of threats in IoT devices is high to make sure that the integration and evaluation of the different models must be ensured with the orientation of complete security models. Considering that the security of IoT devices is vital; since the assailants have been progressively focusing on various ill-disposed tasks, however fiscal addition and getting too delicate data are the most widely recognized. Being powerless against different sorts of security vulnerabilities. It is advanced that IoT security should be utilized with the complete information security algorithms that is why the research is proposed to set up the solution for IoT security while transmitting the data using IoT devices.

Keywords: We would like to encourage you to list your keywords in this section

I. INTRODUCTION

Internet of Things (IoT) is the latest technology that works with the communication of hardware devices using software and networking systems. It is perceived as a foremost component 4.0 Industrial Revolution (4IR), with a challenging implementation that requires extensive studies to guarantee its correct operation correctly **(Mohd, Hassan, 2019).** It provides the digital unique identifier of the devices based on which the data transmission is possible does not requires and human to human or human to computer interaction for data transmission as device-to-server or device to device data transmission takes place using IoT. The technology is rapidly increasing now a day that is why the machines are becoming more efficient in every field while IoT is giving an interface where the machine-to-machine interaction is possible in terms of appropriate data transmission over the servers.

The major information about IoT technology faces the challenges that should be resolved by proposing different researches contains the cybersecurity issues in which there are different threats which can be the reason of data loss in IoT based system also the evaluation of system become so low because of low-quality information security. Ensuring security for data transmission and storage represents one of the biggest concerns and challenges of IoT **(Ahmed, Hassan, and Othman, 2015)**. Most of the enterprises are using IoT systems but the major complaint is about data security and vulnerabilities which are affecting the quality of service of an IoT system **(Guizani, 2020)**. Ensuring security in IoT represents a challenge in several IoT applications including MANET **(Abdelhaq, Hassan, Alsaqour, 2015)**.

This research is specifically proposed to provide an appropriate solution to IoT threats and vulnerabilities so that the data security over the servers will be improved. It is also cleared that the interactive structure of research is based on two major factors, in which one is threat identification, and the other one is threat mitigation. The approaches of research can vary at the time of actual implementation but this proposal will provide the major context of research and the methods which will be used for threat mitigation. Sometimes, it is not easy to find the domain of threat that is affecting the entire system, which is why there should be a system, which keeps the record of each IoT threat so that the identification will become easy while providing the mitigation techniques for that specific threat. IoT will be the next future of technology most probably as currently many organizations are working on the integration of IoT into their business to ease the working process of an organization **(Marin, 2005)**.

This proposal report contains information about the significance of research in which the discussion about journals that will be used in the research would be discussed. The research question will be defined to develop an understanding of the research topic and to maintain the context of the entire research as required in every research model. A brief literature review is described in which the related work about IoT security is described for better security modeling and execution of IoT services at the enterprise level. Different peer researches are discussed in the research to develop the difference between proposed and existing researches about IoT security vulnerabilities including the challenges in managing information systems security for smart cities **(Zarina, Dian, Maryati, Jamaiah, 2019),** and the use of information-centric approach to solving mobility and security problems for IoT **(Azana, Hassan, 2019)**.

Different solution techniques are also discussed in research methods for completing the entire research. Last but not the least; a conclusion statement is designed for completing the proposal based on IoT security.

II. SIGNIFICANCE OF RESEARCH

This research will be significant at the enterprise level where the level of integration of IoT technology is extremely high shortly. This research will be significant for the different researchers who are currently working on the optimization of data security in IoT based embedded systems. The precautionary measures will also be provided to the IoT developers so that they will be able to utilize the latest information security models and functions that can be used for the optimized deployment of an IoT based system. The interpretation of the research is also described which will make the research model more significant to evaluate the current IoT systems, while the evaluation report will be decision making about the changes in that particular systems. The development approaches of the system must be managed with the different strategies about research analysis to execute a proper and secure system which will also be considered as a complete enterprise solution for SMEs where IoT is currently implemented. This research will also be significant at a specific point where the current IoT systems should be verified and validated, as the proposed solution will be considered as the helping hands' invalidation of an enterprise system in which IoT technology is implemented.

For any administration of a company or an organization, it has to anticipate that the security of information and data should ensure business frameworks and keep the frameworks from being interfered with. The security for the IoT will bolster the company in accomplishing its end goals. To start the improvement of a vital arrangement for safety, it is basic to comprehend the business destinations and the important components of the data security toil. However, the security goals are formerly affected by commercial and natural requirements, and by dangers and vulnerabilities. Measurements are created to permit correlation flanked by current security capacity, as well as the capacity required to meet business prerequisites.

Since the mid of the 21st century, security has become the most significant and energizing profession in ways everywhere throughout the globe. Information on data security showcase the certainty that our information is secured and guaranteed the values and goals of our company has been kept up. Not to under-gauge the effect of security occurrences, which can prompt information misfortune, the breakthrough of individual data, and the spread of computer viruses and misinformation. A company must keep alarmed to the news in regards to security dangers and furnish itself with the most recent knowledge of information security.

The general goal is to execute a scope of activities that largely accomplish the entirety of the security goals of the company. Also, it shall be written and proposed in the English language that is quickly graspable to the

employees. The mentioned significance of the Security Plan portrays shields to ensure information, data, and assets as required under the Gramm–Leach–Bliley Act. The security plan for IoT will incorporate the following:

a) Make sensible endeavors to guarantee the security and privacy of secured information, data, and assets
b) ensure against foreseen dangers or perils to the security or respectability of such data;
c) ensure against unapproved access to or utilization of secured information, data, and assets that could bring about considerable mischief or bother to any client.

This IoT security accommodates components to:

a) Identify and evaluate the dangers that may compromise secured information, data, and assets kept up by the company/organization.
b) Reduction of the Security Events.
c) Oversee and control these dangers.
d) Execute and audit the arrangement.
e) Modify the arrangement to reflect changes in innovation, the affectability of secured information, data and assets, and interior or outside dangers to data security.

IoT Information management would be exploited just once a server has a highly sophisticated connected system arrangement in unreachable or inappropriate for an explicit condition (Hasan et al, 2014; Hasan et al 2019). For the assurance of defense, the majority of the transmission is verified using solid common confirmation and encryption methods that are built inside the endeavor. Considering the obligation of the Networking Board, to assure all Access Points are arranged with legitimate backgrounds as branded by the Issue Specific Security Policy (ISSP). Besides, it isn't just restricted to verification and encryption enterprises, as well as it is the commitment of the end-client to pledge that their computer remains appropriately designed as considered by Enterprise Workstation Standards (EWS). Top Information Security will be answerable for characterizing confirmation and encryption prerequisites just as an advancement of fundamental consistency programs. Summit maintains whatever authority is needed to review all developments related to its network system. It is significant for the information security management to recognize vulnerabilities in conveyed frameworks and get reports of vulnerabilities from outside sources, decide the suitable reaction, and roll out proactive improvements to send frameworks to keep up the security of the conveyed framework. The attention to the area and status of physical resources just as the consciousness of physical security controls and organizes the security data for physical frameworks with the IT security controls.

III. RESEARCH QUESTION

The research question for the proposed research is given below:

i. How IoT threats and vulnerabilities will identify? what would be the best parameters to provide the solution/mitigate that threat or vulnerability?
ii. How IoT threats can be classified to provide the appropriate mitigation technique?
iii. How to improve the framework of IoT security using information security algorithms?

The research in question is describing both of the factors as discussed in the introduction part, that the research is having two major factors in which one is threat identification, and another one is threat mitigation which will be helping in completing the entire research model. The functionalities of research contain the different technical discussions to evaluate the problem with previous researches to develop a proper comparison between existing researches and this proposed research.

The interpretation of core level technology is also described to have a better idea that's what are the actual threats which are considered as the major issues for data centers and enterprises. The designed research question is having core level information about IoT technology whereas the techniques are also asked to fulfill the context of research. For both the hardware and software company, requires Information security, including ideas, strategies, and measures identifying with the insurance of registering frameworks and the data they keep up against purposeful or inadvertent dangers. Therefore, the activities and occasions that compromise information security of IoT devices should be analyzed, and Security models are should be overviewed, as well as explicit specialized and authoritative measures for advancing security. IoT Security

includes the secure frameworks, equipment and working frameworks, recognizable proof of clients, encryption, and access control bundles.

IV. 2. LITERATURE REVIEW

Mentioning that Mobile Phones have become a significant piece of authoritative IT foundations including advantages, for example, expanded efficiency just as security dangers. These dangers are principally identified with unapproved access to corporate information **(Lewis, 2019).** Incorporating cell phones in associations in regards to security includes a succession of choices, extending from the reconciliation approach (cell phones claimed by representatives or by the association) to explicit safety efforts executed on the gadgets. Sometimes the IoT developers make the hardcoded passwords which can be easily changed and accessed by the hackers so that the system would not be secured with a hardcoded password, there should be proper encryption to meet the requirements of information security so that the data of the end-users will be secured in IoT device **(Guizani, 2020).** The password must have a specific criterion that must be managed with the secure interfaces and the proper information security algorithms must be implemented to deploy a secure IoT solution. The interpretation of password setting must also be meeting the context of requirements about IoT functions otherwise the data breaching is possible in which end users will be affected **(Anwar, 2014).**

There are some insecure network services which are also considered as the major threat for an IoT based system because the entire data transmission is based on the network services, and if the network services are weak, the network link may get down from a simple DDoS attack, that is why the network configuration should be extensive and secured. The deployment of a secure network is also necessary for having the managerial security deployment of an IoT system. The IoT systems send the data to the server while the transmission is being done using a network but if the network is weak, the system would not be secured and the situation will be threatening **(Salah, 2019)**

Ecosystems, where the entire IoT system is implemented, can also be weak because, for some devices, the needs of API are necessary otherwise the data transmission would not be possible, that is only certified APIs should be used. In APIs, there must be some errors or malware data which can be the major reason for system failure **(Lopez, 2017).** The system failure should be controlled by using secured API interfaces so that the better controlling and execution must be managed and ensured as per the control level information and analytics to develop the understanding with the IoT devices as the secure interface modeling is required to deploy a secure system (**Meng, 2018)**. Every system requires an update and maintenance because there is a certain limit of every device, after that a device will not be functional and the data of the server will be breached.

Due to lack of countermeasure, the IoT system can face major data loss and the data breach of the system can be the data of any type, that is why it is necessary to maintain the system concerning the specific time while the consideration of system should be validated with different input and output models **(Hassan, 2020) (Obaidat, et al., 2020).** IoT needs a lot of research deploy at the industrial level because there is some extremely complex process, only IoT systems will be the best fit but with high-level information security, otherwise, the data breaching would be the reason of system failure also the organizational failure can be done due to an extensive loss in term of cost (**Loukas, 2018)**

As it has been highlighted that the IoT system is the combination of the hardware, software, and networking interfaces, which means there are several hardware devices. So that it can be used for IoT system but the devices should not be outdated, if the devices are outdated, the system will be failed with the context of requirement because hardware device in an IoT system is the major component, that should be properly evaluated and secured with complete analytics of system management evaluation and approaches (Islam S, et al 2013; Islam S., et al 2017). The integration of outdated devices can also be the reason for different losses not only data loss but also be the reason for physical damage with those devices. A valid device should be used with no expiry otherwise, the system will be considered as the failed system **(Awed, 2018).**

Due to the demand for privacy protection to end-user, it might consider the central system protection for the machine-to-machine interaction based on the privacy level **(Burhan, 2018).** That is why there must be proper privacy policies that can be used as a solution for an IoT based system whereas the technical

interpretation of information can be utilized and managed to develop a major understanding with the system. The methodologies of research can change at the hour of genuine usage however this proposition will give the significant setting of research and the techniques which will be utilized for risk moderation.

Occasionally, it is difficult to track down the space of danger that is influencing the whole framework that is the reason there ought to be a framework, which keeps the record of each IoT risk with the goal that the distinguishing proof will turn out to be simple while giving the relief procedures to that particular threat. IoT will be the following eventual fate of innovation most presumably as at present there are numerous associations which are dealing with the incorporation of IoT into their business to facilitate the working procedure of an association **(Rathore, 2017)**

Data storage and data transfer routes should also be secured with proper encryption of data otherwise the hackers will be able to access the data from the servers, which can also be the reason for system failure. Data transfer should be evaluated with the concatenation of different objects that can be controlled and evaluated as per the requirements of the data storage model. Data security is one of the most important information that should be validated with the concern of analytics about the complete execution and managerial planning that can be validated with the different inputs of data storage management. It is also cleared that the indexing of data should be done to develop the complete instructions about data security considerations and evaluation **(Hussain, 2020).**

Smart Home devices can also become the vulnerability in case if the networking is not secured, in that kind of situation, it is cleared that the combination and evaluation of the device should be checked with different information security parameters to describe the structural view of Smart Home device (Gupta BB., et al, 2020; Sengupta K., 2020). The personal data of users should be secured as the IoT service providers must provide the encrypted data transmission services to their users so that they will be able to execute a proper smart home device for better usability of the IoT system. The crosscheck mode of testing should also be tested with different layouts of the systematic development of a secure IoT environment **(Pereira, 2019).**

.

V. PROPOSED COUNTER MEASURES HANDLING THE THREATS

For the completion of research, the qualitative research method will be used by developing an incident response system that will be having the capability to identify the cyber-attack that can affect the services of IoT systems. The system will be able to perform the following functions:

a) Detect the nature of attack at the time of the attack is coming to the system, the attack type and domain will also be stored into the system
b) The system will also provide the analytical details about the attack so that the mitigation technique can be defined.
c) The system will be implemented at the network side of an enterprise system where the complete execution and concatenation of cyber-attack will be stored into the system
d) The attack will be identified by the unique identifier so that the complete product level information can be developed and shared with the integration of core level information that can be utilized as per the proper orientation of attack data collection
e) The system will instantly report the network department so that they can run the network security commands to secure the entire IoT system.

The mitigation technique to provide the solution to an IoT device whereas the perspective of instructions must be developed and ensured with the proper structural management of an integrated system that can be validated with different species of running a secure IoT system. The devices should be upgraded, as the proposed system will provide updates about the devices so that the status of devices can also be monitored concerning the current situation of that specific device. Data breaching can be controlled as the proper cryptography algorithms will also be provided by the incident response system. Huge numbers of the security highlights, for example, network access control and system examining, accessible for TCP/IP depend on those accessible through the working framework. The accompanying segments diagram TCP/IP security. The following liabilities can be considered as the countermeasure:

4.1 Constraints of Liability:

Expecting no danger for unapproved acts that abuse adjoining the country and the government representation. In such a case of a potential threat, IOT will promptly end its connotation with the policy violator and will give no legitimate indemnification or benefit. It additionally has safety dedicated panels and arrangements build inside Market on Cloud to safeguard the data, for example, the accompanying approaches and controls:

a) Tactics and procedures, which integrate, yet are not constrained to, business lead rules, get to limitation, ensured information gets to logging, and work and occupation job confirmation.
b) Mentioning the Security Dedicated Panels, which incorporate, not just restricted to, information affecting but with the entire encryption of the information in the system, including the powerlessness Monitoring Technical Controls.

4.2 Personality, Access, and Entitlement Management

This part gives administrations identified with jobs and personalities get to rights, and privileges. The correct utilization of these administrations can guarantee that entrance to assets has been given to the correct personalities, at the perfect time, and for the correct reason. These administrations can deliver that entrance to assets is checked and inspected for unapproved or unsuitable use.

4.3 Information Protection Management & IT Maintenance

This part gives benefits that shield unstructured and organized information from unapproved access and information misfortune, as indicated by the nature and business estimation of data. It gives use and access checking and review administrations to follow access to information. the procedure mechanization and work process establishment for security the board. Specifically, Change and Release Management forms assume noteworthy job insecurity on the board.

4.5 Programming, System, and Service Assurance

This part tends to how programming, frameworks, and administrations are structured, created, worked, and kept up all through the product life cycle to make typically verify programming. This segment covers organized plan, danger demonstrating, programming hazard evaluation, structure surveys for security, source code audits and examination, dynamic application investigation, source code control and access observing code/bundle marking and check, quality confirmation testing, and provider and outsider code approval.

VI. CONCLUSION

A complete proposal for IoT security solution is described to ensure that the research will be beneficial and significant in different departments. The reasoning of IoT security threats and vulnerabilities is described with extensive details to make sure that the service level execution of the entire information system based on IoT technology is secured. The major information about IoT technology is discussed highlighting the core IoT security systems by indicating the key challenges and the countermeasures that need to be considered at the system level and the organization level. This study is potential in proposing different countermeasures for the cybersecurity for the different type's threats to protect the data loss in IoT based system to ensure information security. This proposal also suggests that the security management systems in IoT devices empower the IT association to gather, break down, and report security data and security occasions to distinguish, evaluate, survey, and report on IT-related dangers that can add to the association's operational hazard. The IoT system security methods discussed with a high distinction model. Overall, all aspects of the proposal are described to complete the context of the research question which will be solved at the time of the actual implementation of research.

VII. ACKNOWLEDGMENTS

The authors would like to acknowledge the support of Network Communication Technology (NCT) Research Groups, FTSM, UKM in providing facilities for this research. This paper is supported by the National University of Malaysia under the grant GGPM 2020-028.

REFERENCES

11.1. Journal Article

[1] Mohd Z. I., Hassan R. The Implementation of Internet of things using Test Bed in the UKMNET Environment. Asia-Pacific Journal of Information Technology and Multimedia. 2019; 8 (2): 1 – 17.

[2] Ahmed AS, Hassan R, and Othman NE. Improving security for IPv6 neighbor discovery. International Conference on Electrical Engineering and Informatics (ICEEI), Denpasar, 2015: 271-274; doi: 10.1109/ICEEI.2015.7352509.

[3] Abdelhaq M., Hassan R., Alsaqour R. (2011) Using Dendritic Cell Algorithm to Detect the Resource Consumption Attack over MANET. In: Zain J.M., Wan Mohd W.M.., El-Qawasmeh E. (eds) Software Engineering and Computer Systems. ICSECS 2011. Communications in Computer and Information Science, vol 181. Springer, Berlin, Heidelberg

[4] Z. Din, D. I. Jambari, M. M. Yusof and J. Yahaya, "Challenges in Managing Information Systems Security for Internet of Things-enabled Smart Cities," 2019 6th International Conference on Research and Innovation in Information Systems (ICRIIS), Johor Bahru, Malaysia, 2019, pp. 1-6, doi: 10.1109/ICRIIS48246.2019.9073661.

[5] Aman, Azana Hafizah Mohd and Rosilah Hassan. "Internet Protocol Function Enhancement using Information Centric Approach to Solve Mobility and Security Problems for Internets of Things." Proceedings of the 1st International Conference on Informatics, Engineering, Science and Technology, INCITEST 2019, 18 July 2019, Bandung, Indonesia (2019).

[6] C. D. Scott and R. E. Smalley, "Diagnostic Ultrasound: Principles and Instruments", Journal of Nanosci. Nanotechnology., vol. 3, no. 2, (2003), pp. 75-80.

[7] Hussain, F, Hassan, S. (2020). Machine learning in IoT security: current solutions and future challenges. IEEE Communications Surveys & Tutorials.

[8] Lewis, T. G. (2019). Critical infrastructure protection in homeland security: defending a networked nation. John Wiley & Sons.

[9] Ali, B.; Awed, A. (2018) Cyber and physical security vulnerability assessment for IoT-based smart homes. Sensors, 2018, 18, 817. [Cross Ref]

[10] Miorandi, D.; Coen-Porisini. (2018). A risk assessment methodology for the Internet of Things. Compute. Commune. 2018, 129, 67–79.

[11] Rathore, S. (2017). Social network security: Issues, challenges, threats, and solutions.

[12] Burhan, M.; Rehman, R.; Khan, B.; Kim, B.S. (2018) IoT Elements, Layered Architectures and Security Issues: A Comprehensive Survey. Sensors 2018, 18, 2796.

[13] Loukas, G.; Budimir, S.; Bezemskij, A.; Fontaine, J.R (2018). A taxonomy of cyber-physical threats and impact in the smart home. 2018, 78, 398–428.

[14] Manogaran, G., & Lopez, D. (2017). Disease surveillance system for big climate data processing and dengue transmission. International Journal of Ambient Computing and Intelligence, 8(2), 1–25.

[15] Lin, I. C. (2017). A survey of blockchain security issues and challenges. IJ Network Security.

[16] Vitunskaite, M.; Brandstetter, T.; Janicke, (2019). H. Smart Cities and Cyber Security: Are We There Yet? A Comparative Study on the Role of Standards, Third Party Risk Management and Security Ownership. 2019, 83, 313–331.

[17] Butun, I.; Pereira, N.; Gidlund, M. (2019). Security Risk Analysis of LoRaWAN and Future Directions. Future Internet.

[18] Lopez, D., & Manogaran, G. (2016). Data architecture for climate change and disease dynamics. In R. S. Tomar et al. (Eds.), The human element of big data: issues, analytics, and performance. Baca Raton: CRC Press.

[19] Manogaran, G., & Lopez, D. (2017). Spatial cumulative sum algorithm with big data analytics for climate change detection. Computers & Electrical Engineering.

[20] Meng, H.; Thing, V.L.; Cheng, Y.; Dai, Z.; Zhang, L. (2018). A survey of Android exploits in the wild. Comput. Secur. 2018, 76, 71–91

[21] Maiti, A.; Jadliwala, M.; He, J.; Bilogrevic, I. (2019). Side-Channel Inference Attacks on Mobile Keypads using Smartwatches

[22] Al-Garadi, M.A., Mohamed, and Guizani, M., 2020. A survey of machine and deep learning methods for internet of things (IoT) security. IEEE Communications Surveys & Tutorials.

[23] Khan, M. A., & Salah, K. (2018). IoT security: Review, blockchain solutions, and open challenges. Future Generation Computer Systems, 82, 395-411.

[24] Marin. (2005). Network security basics. IEEE security & privacy.

[25] Alladi, T., Chamola, V., Sikdar, B., & Choo, K. K. R. (2020). Consumer iot: Security vulnerability case studies and solutions. IEEE Consumer Electronics Magazine, 9(2), 17-25.

[26] Lewis, T. G. (2019). Critical infrastructure protection in homeland security: defending a networked nation. John Wiley & Sons.

[27] Sengupta, J., Ruj, S., & Bit, S. D. (2020). A Comprehensive survey on attacks, security issues and blockchain solutions for IoT and IIoT. Journal of Network and Computer Applications, 149, 102481.

[28] Reddy, M. P., Reddy, K. S., Reddy, M. I. S., & Srinivas, (2020) G. Host-based information gathering honeypots for network security. In Editor. Board, p. 369

[29] Manogaran, G., & Lopez, D. (2017). A Gaussian process based big data processing framework in a cluster computing environment. Cluster Computing, 1–16.

[30] Lopez, D., Manogaran, G., & Jagan, J. (2017). Modeling H1N1 influenza using mathematical and neural network approaches. Biomedical Research, 28(8), 1–5.

[31] Lopez, D., Gunasekaran, M., Murugan, B. S., Kaur, H., and Abbas, K. M. (2014, October). ‘‘Spatial BigData analytics of influenza epidemic in Vellore, India, In Proceedings 2014 IEEE International Conference on Big Data (pp. 19–24). IEEE.

[32] Mukherjee, B., Heberlein, L. T., & Levitt, K. N. (1994). Network intrusion detection. IEEE Network, 8(3), 26–41.

[33] Manogaran, G., Lopez, D., Thota, C., Abbas, K. M., Pyne, S., & Sundarasekar, R. (2017). Big data analytics in healthcare internet of things. Innovative healthcare systems for the 21st century (pp. 263-284). Springer International Publishing.

[34] Hasan MK, Ismail AF, Islam S, Hashim W, Ahmed MM, Memon I. A novel HGBBDSA-CTI approach for subcarrier allocation in heterogeneous network. Telecommunication Systems. 2019 Feb 15;70(2):245-62.

[35] Hasan MK, Ismail AF, Abdalla AH, Abdullah K, Ramli HM, Islam S, Badron K. Self-organizing joint sensing and power allocation scheme (SJSPA) to coordinate cross-tier interference for LTE-A heterogeneous networks. In2014 IEEE 2nd International Symposium on Telecommunication Technologies (ISTT) 2014 Nov 24 (pp. 11-16). IEEE.

[36] Islam S, Abdalla AH, Habaebi MH, Latif SA, Hasan MK, Saeed RA. Multihoming based mobility management scheme in NEMO: A qualitative and quantitative analysis. In2013 International Conference On Computing, Electrical AND Electronic Engineering (ICCEEE) 2013 Aug 26 (pp. 394-397). IEEE.

[37] Islam S, Hashim AH, Habaebi MH, Hasan MK. Design and implementation of a multihoming-based scheme to support mobility management in NEMO. Wireless Personal Communications. 2017 Jul 1;95(2):457-73.

[38] Obaidat MA, Obeidat S, Holst J, Al Hayajneh A, Brown J. A Comprehensive and Systematic Survey on the Internet of Things: Security and Privacy Challenges, Security Frameworks, Enabling Technologies, Threats, Vulnerabilities and Countermeasures. Computers. 2020 Jun;9(2):44.

[39] Gupta BB, Quamara M. Internet of Things Security: Principles, Applications, Attacks, and Countermeasures. CRC Press; 2020 Feb 24.

[40] Sengupta J, Ruj S, Bit SD. A Comprehensive survey on attacks, security issues and blockchain solutions for IoT and IIoT. Journal of Network and Computer Applications. 2020 Jan 1;149:102481.