International Journal of Recent Technology and Engineering (IJRTE)
ISSN: 2277-3878, Volume-8 Issue-4, November 2019

Vulnerabilities to Internet of Things and Current State of the Art of Security Architecture

Md. Forhad Rabbi, Ashique Jubayer, Syed Montasir Hossain

Abstract*: *Internet of Thing (IoT) is one of the most popular systems these days. This ensures internet connectivity of physical devices and everyday objects. This technology is getting popular day by day due advanced technology and cheap price. However, IoT has some vulnerability issues to deal with. The main hindrance of popularity exploitation of IoT is security. In this paper, the study reflects about the most modern technology, IoT and its security and vulnerabilities where the factors of intrusions in IoT and different types of protocols are explored by studying different papers. In this paper, we have followed the structure of Kitchenham [28] to conduct a systematic literature review. We have performed the SLR by collecting some relevant papers from the well-known databases like IEEE xplore, ACM, Springer, Elsevier, etc. Our main purpose is to analyze the recent research works according to the security issue and come up with a result in order to intend to have future research on security of IoT.

Keyword: Cyber Security, Internet of Things, Cyber Physical System, Vulnerability, Systematic Literature Review.

I. INTRODUCTION

Internet is the ubiquitous component of our daily life. It is the system of connecting interconnected devices with the TCP, the protocol suit of internet globally. It is the network of networks. It doesn't only broaden our communication sector it also has great influence in the area of business, academic, trading, health, entertainment and many more. This generates massive data by the users and usually people share their data via internet. By using the same concept of internet, the Internet of Things (IoT) enters into the modern technology in the year of 1982 with a coke vending machine at Carnegie Mellon University (CMU). By the report of statista the connected devices around the world in 2025 will be 75.44 billion, 2 devices per human at average [26] and International Data Corporation (IDC) announced that with a rate of 17% of compound growth it will reach up to 1.3 trillion U.S dollar [24] which proves the popularity of IoT. IoT comes with a huge prominent feature in human life but it has some constraints.

Manuscript published on November 30, 2019.
* Correspondence Author
Md Forhad Rabbi*, Department of CSE, Shahjalal University of Science and technology, Sylhet, Bangladesh. Email: frabbi-cse@sust.edu
Ashique Jubayer, Department of CSE, Sylhet Engineering College, Sylhet, Bangladesh. Email: ashiquejubayer357@gmail.com
Syed Montasir Hossain, Department of CSE, Sylhet Engineering College, Sylhet, Bangladesh. Email: jami.sec15@gmail.com

These constraints made IoT vulnerable. The manufacture of IoT was planned without thinking these constraints [27]. As this technology performed in wireless mode this cause more vulnerable. In a study it shows that 70% of power consumption is done due to usage of wireless communication [25] which depicts the energy capacity constraints of IoT dollar [26] which proves the popularity of IoT.

IoT comes with a huge prominent feature in human life but it has some constraints. These constraints made IoT vulnerable. The manufacture of IoT was planned without thinking these constraints [24]. As this technology performed in wireless mode this cause more vulnerable. In a study it shows that 70% of power consumption is done due to usage of wireless communication [27] which depicts the energy capacity constraints of IoT device. Besides storage management, identity management there is a big deal with privacy and security concerns.

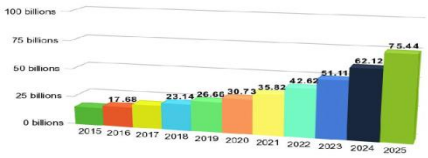

Fig1: Rapid growth of connected IoT devices

In this paper we are going to discuss the security facts of IoT devices including different types of attacks, different communication and security protocol and architectures along with remedy of vulnerabilities of IoT.

II. SYSTEMATIC REVIEW

Systematic literature review means to identify, evaluate and explain all available research studies according to the relevant questions or topic area or interested sectors of research. A SLR method concludes in common phenomena by studying the individual research paper. We have followed the Kitchenham's methodology to build up the SR method by formulating questions, reviewing protocols, data sourcing, searching strategy, data extraction and data synthesis. After that we have performed a result on systematic review and conclude with a scope of further research on this topic.

	Search String
1	Cyber security OR privacy OR Safety OR reliability OR dependability
2	IoT OR Internet of Things OR cyber physical system OR Internet of Everything, Wireless sensor network OR Radio Frequency Identification Device, Machine to machine.

A. Research Question:

Security is the greatest hindrance in the development of IoT where the data are not safe because of the intruder. Heterogeneity causes a problem in terms of developing security as different IoT device have different types of architecture. Several studies have been conducted on the security purpose of the IoT and we have formulated our questions on the basis of architectural overview and different types of cyber attacks. We mention the following questions as to develop the SLR:

Q1. What are the key factors of intrusion of IoT devices?
Q2. What are the most popular attacks in terms of IoT?
Q3. What are the different types of attacks in different layers of IoT?
Q4. What are the security features of the recent technologies?
Q5. What are the proposed security architectures of IoT?

B. Review Protocol:

According to Kitchenham reviewing protocol means how the systematic literature review is going to be conducted, how to extract data and analyze them and how to search and select the relevant studies. The review protocol includes data source, search techniques, study selection strategy, data extraction and data synthesis. All the portions are elaborately described below:

Digital Libraries	Publishers	Website link
IEEE Explore	IEEE	Ieeexplore.iee.org
SpringerLink	Springer	Link.springer.com
Academia	Academia	Academia.edu
Researchgate	---------	researchgate.net
ScienceDirect	Elsevier	Sciencedirect.com
ACM Digital Library	acm	dl.acm.org

C. Data Sources:

The sources include research paper from 2013 to 2019, March in the following electronic libraries. These electronic libraries are selected for data sources for the purpose of study and analyze. The following table shows the electronic digital libraries selected for the systematic review:

D. Research Strategy:

The strategy of searching is followed by two main terms. They are cyber-security and IoT. Lists of following terms are constructed for each of the terms. They are formed as the synonyms of the two terms. “And” is used to connect the two words and “OR” is used to mention the synonym of the word. They are shown below:

E. Data Extraction:

The sorted data are extracted from the selected papers for the discussion of the topic. The data are included within the systematic review paper.

F. Data Synthesis:

The papers are selected by studying abstract, introduction and conclusion. Most of them are read in topics/points that are relevant to the systematic review topic.

Stage	Selection criteria	Number of Papers
1	Extracting all papers based on search string	47
2	Exclusion based on titles	5
3	Exclusion based on abstract and conclusion	3
4	Exclusion based on full paper	5

G. Result of Systematic Review:

In this section, we have populated the result of the systematic review. The results concentrate on the basis of the questions that have been formulated in the “question formulation” section. The questions are given answer by analyzing the papers from top to bottom manner as per the aim of this paper. This section is included with some charts and tables along with some statistical data and information.

***Q1.** What are the key factors of intrusion of IoT devices?*

Internet of Things has the most complex architecture in nature in terms of its manufactured process, diversity of devices in architecture [1, 2, 3]. We have got some major key factors that are responsible for intrusion and will be answered by this question.

Heterogeneity: A huge amount of devices are connected to each other and they are different in architecture as the manufacturing and in using environment. The diversity of IoT depends on the interoperability of the hardware, terms and conditions of use, sensors, platforms and different types of protocols which increases the probability to lessen the rate of exchange of the data between different devices[4].

A common standard must have to follow to reduce the risk of attack vectors whereas ISO/IEC JTC 1 type organization are following some standard in manufacturing the devices[5].

A middleware or protocols or a framework can be the solution of diverse interoperability of IoT devices.

Resource constraints: Most of the IoT devices are limited in storage and fixed battery consumption. This limited resources attracts the vector attacker to attack these devices. They can manipulate and change the behavior of the devices by seizing the device capacity.

So for that reason, a lightweight and straight forward framework can be implemented as the security mechanism of the IoT device and AES(Advanced Encryption Standard) and TLS(Transport Layer Security) is not possible[6] [7].

Unauthenticated and Unauthorized: Authentication and authorization is one of the most important features that can help IoT device to get attacked from the intruder. Lack of proper authentication mechanism, chances of unauthorized access get high to change the real data [8].

IETF (Internet Engineering Task Force) has identified this issue is one of the major problems in terms of vulnerability of IoT devices [9].Authorization mechanism can be developed by Role Based Access Control (RBAC) or Attribute Based Access Control (ABAC)[10].Moreover Zigbee is also providing this feature to the IoT device though. Besides Bootstrapping is another solution for this issue. Bootstrapping is the process when the devices are getting connected in a particular location and time which provides security and privacy parameters by measuring authentication and authorization [11]

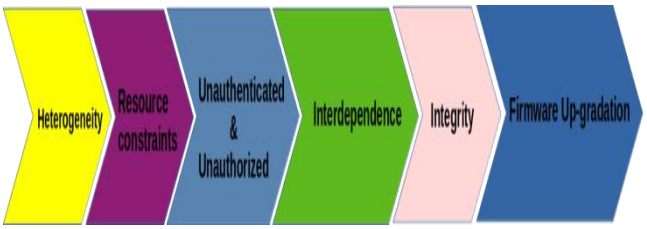

Fig2: Factors of intrusion in IoT devices

Interdependence: Interdependency means how the different devices are independently functioning the services in the IoT also depend on each other. IoT services are unified, interdependent systems. As the IoT becomes more popular, interdependency has a great effect on the availability and flexibility [10]. It is hard to manage the IoT device as for the interdependency of the devices. It does not only communicate with each other but also it can be controlled by different multiple devices for its interdependence feature [14].

Integrity: Data integrity is the vital feature for embedded system. The sending data and receiving data should be accurate and exact for data interoperability. But in presence of intruder it can be harmed and the data format or data can be manipulated. Non-physical attack like spoofing, sniffing, buffer overflow may happen and encryption based data transfer can solve this problem [15].In the application layer the integrity of data can be confirmed by end to end security [11].

Firmware upgradation: Firmware is the software that is installed in the device hardware with set of instruction, how the hardware will interact with each other. It is to be updated after a certain period of time when the update from the manufacturing company is on live. But live update of firmware is not possible in all cases and sometimes users have to install it manually [17]. However, the vulnerable devices can be identified by analyzing the firmware by side channel attack[18].A mobile security company named Ali have reported 90% of IoT device firmware has security issues [19]. Still there is possibility to attack device in the time of firmware update from the remote server [20].

Q2. What are the most popular attacks in terms of IoT?

Buffer Overflow: Excessive amount of data in the buffer causes this type of vulnerability. It is one of the non-physical threats [21]. It causes vulnerability in the application layer in case of privacy leak [22].

Man in the middle attack: A cyber-physical eavesdropping type attack where an intruder is entered into two parties at the time of their sharing data and gets access over the information and can manipulate the data. It is a non-physical threat [23].

DDOS (Distributed Denial Of Service): A non physical threat which overloads a service or database by sending packets to the target devices through the application layer is known as DDOS attack and sometimes a group of devices worked as botnet to pursue a large server which was attacked in 21st October 2016 by the Domain Name System provider DYN known as Mirai Botnet which affects Github, Twitter [24][25]. The Mirai malware posses over 500000 devices all over 164 countries [12]

Brute Force Attack: An easy method to get access over the device which is password protected and an intruder can access the device by thoroughly inputting the password until it matched the actual password. Because of lack of storage capacity and less ability of sensors to compute the environment can cause this type of attack [13].

Cross Site Scripting: A client-side scripting where an attacker can change the targeted device by changing the content of the graphical interface by injecting java script code [14]. Side Channel Attack: This type of attack is originated because of limitation of device and encryption-decryption mechanism [15].

Eavesdropping: An unlawful access over the devices between the communication of two devices and manipulate it and takes privilege of the unsecured transmission of the data [3]. A poor IoT configured network lightweight encryption and decryption mechanism of the devices can lead to this threat [2].

Q3. What are the different types of attacks in different layers of IoT?

Investigating every one of the papers we have amassed every one of the layers that exist in the IoT device. By addressing this inquiry, we will examine the layers and the digital physical dangers that happen in each layer.

i) Application Layer: It gives the UI to perform explicit applications and perform testing and monitoring [15]. In this layer the qualities of youth gadget that is integrity, authentication and privacy is confirmed [16].

ii) Application Support & management Layer: This layer manages business procedure model and execution, authorization, Key trade and management [17].

iii) Service Layer: Virtual element work VE Resolution, VE service, VE and IoT monitoring, It likewise gives secure information control between the IoT devices, connectivity setup, buffering [18].
iv) Transport/Network Layer: Hostile to DDOS, encryption mechanism, identity authentication, network management, network interfaces, communication channels, security of correspondence is the primary prerequisite of this layer [20]. For ensuring the correspondence security TLS/SSL or IPsec is utilized in encryption [19]. This layer is eluded as the cutting edge network [23].
v) Perceptual Layer: The principle goal of this layer is to gather or perceptual information from the earth with sensors and actuators. In fundamental IoT engineering it transmits information to the system layer.
In short and neighborhood runs it gives hub collaboration [19]. The risk in this layer is most extreme on account of the nature of this layer is mind boggling than other layers [14].
vi) Processing/middleware Layer: This layer fills in as the interface between the components of the IoT devices. It associates those segments which are intended to be associated at the season of production.
vii) Threats: As middleware is the most significant layer to connect the correspondence between the components of the IoT devices, so it turns out to be all the more compromising when it turns out to be more open [8]. Non-authorization attack, data attacks, storage attacks, session assaults are the significant assaults in this layer

Q4. *What are the protocols and threats including them?*

Bluetooth: Bluetooth is the most mainstream short separation correspondence protocol. It gives security among the sender and recipient by requesting that consent be combined with gadgets to share data. The information is sent by scrambled as figure message and decode at the collector end so no capture attempt will be helpful.
Threats: Bluesnarfing, Bluebugging, Bluejacking, Interception as in passive eavesdropping, DoS, Spoofing.
Zigbee: Zigbee is a short range information transmits correspondence, convention with low power utilization where life of battery is for a long time and the information move rate is from 50 kilobits/Sec to 250 kilobits [20] [14].
This convention gives a system key which gets confirmed and approved yet this get powerless on the grounds that the key isn't encrypted [14] [21]. Zigbee has four layers. They are application, network, the MAC (media access control) and physical layer.
Threats: Sniffing attack causes due to not having encryption system [14].The most common attack in Zigbee is man in the middle attack [21].As it has constrained like fixed key at the time of registration which makes this communication protocol as vulnerable. Reply attack can cause major issue in this protocol.
RFID: In lot devices the vast majority of them has RFID (Radio Frequency Identification) tags [7] which are a 128 piece microchip and makes the gadget exceptionally identifiable [50] which is known as Electronic Product Code [22]. It moves information through recurrence wave. According to Burhan et al it has three sections that is tagged, reader and database. It gives encryption strategy, however does not have any security as far as perusing the information from tags. It utilizes Automatic Identification and Data Capture (AIDC) technology [21] to move data. RFID can be characterized into two types. Active and uninvolved where dynamic has a battery and latent uses vitality with the assistance of the labels.
Threats: Spoofing is mainly initialized for lack of proper authentication in RFID system, RF interface on RFID, Social engineering, Tracking, Unauthorized access, Virus, Eaves dropping, Man in the Middle, Killing Tags.
6Lowpan: It expends low vitality over IEEE 802.15.4 by empowering transmission of IPv6 packets [25] and gives fragmentation, header compression, encapsulation and reassembling its very own usefulness.
Threats: Fragmentation Attack, Authentication Attack, Confidentiality Attack.
5G: For lot gadgets 5G is the best creation of foundation with more stockpiling limit and gigantic availability more than the 4G which lead zero dormancy between the gadget and the user [14]. This will give a multi-space and multi-correspondence between various gadgets in various networks. It is the fifth era cell innovation with better coverage, data move rate, it will be accessible inside 2025 [7]

Threats: DDoS

NFC: Near Field Communication is the most brief range correspondence innovation utilized in it which is remote and transmit information with a constrained data transfer capacity in installment exchanges system [20] [29].
Threats: Relay attack, Man in the Middle, eavesdropping, Data corruption and insertion, Wormhole.
Wireless Sensor Network: A remote correspondence between gadgets where information is transmitted through recurrence wave inside a restricted bandwidth. WSN is coordinated with five sections naming as sensors, battery, microcontroller memory and radio Transceiver [53] which functions as the information transmission medium. It moves information from source to base hub.
Threats: Jammers, Sink hole, Injection, Side channel attacks, Relay Attacks, Buffer overflows, Unfairness, Replay Attacks, Traffic Analysis, Sybil, Selective Forwarding, Synchronization Attack, False Routing, Crypto Attacks, Hello and Session, Flooding, Eavesdropping.

Table1: Different types of attacks in communication protocols

Technology	Mechanism	Security	Threats
Bluetooth	Wireless	Encryption, Authentication	Bluesnarfing, Bluebugging, Bluejacking, Interception as in passive eavesdropping, DoS, Spoofing

RFID	Frequency wave	Encryption	Spoofing, RFID system, RF interface on RFID, Social engineering, Tracking, Unauthorized access, Virus, Eavesdropping, Man in the Middle, Killing Tags.
Zigbee	Wireless	Encryption, Integrity	Sniffing, Man in the middle, Replay Attack
6lowpan	Compliant radio, Ethernet interface	Key, Encryption, Authentication	Fragmentation Attack, Authentication Attack, Confidentiality Attack.
WSN	Wireless	Key, Encryption, Authentication	Jammers ,Sinkhole, Injection, Side channel attacks,RelayAttacks,Bufferoverflows,Unfairness,ReplayAttacks,TrafficAnalysis,Sybil,SelectiveForwarding,Synchronization Attack, False Routing, Crypto Attacks, Hello and Session, Flooding, Eavesdropping.
5G	Wireless	Authentication, Authorization	DDoS
NFC	Radio Frequency wave	Key, Authentication	Relay attack, Man in the Middle, eavesdropping, Data corruption and insertion, Wormhole

Q5. What are the proposed security architecture of IoT?

Different papers have proposed different architectural view along with intrusion detection system.In this section we are going to discuss about the proposed architecture and different mechanism to prevent and reduce the cyber-physical attacks of IoT.

Fitted Solution: In Tamanna Siddique et al [17] this arrangement has been proposed to verify its components in three levels. They are device, communication and server level security. First level security is underscored in server level by interfacing with the cloud server with cloud calculation which has appropriate verification and approval methodology. The stockpiling framework in the server ought to be in the cryptographic framework so no information can be perused by the intruder. In the second layer, the corresponding layer the correspondence among gadget and server or clients and server is to be encouraged by security calculation with legitimate guidelines and guidelines which can shield the assault all things considered and the information transmitted by TLS and DTLS encryption is exceptionally recommended. Third layer assurance is created in the equipment layer. The gadget level is a layer installed with microcontroller and programming and predefined antivirus.

Besides, regular updates must be advanced from the assembling organization.

IPM: Huansheng Ning et al (2012) [15] proposed their engineering plan for the security of U2IoT gadgets which incorporates industrial, local, national and worldwide IoT devices; integration of different Unit IoT. Unit IoT highlights are systems and sensors, distributed control hubs alongside the board and brought together server farm.

IPM contains with Information Security, Physical Security and Management, Security. Information security manages security layer and security necessities which involves algorithms, protocols, and capacities that are incorporated for canny activities.

Physical security characterizes the natural items that are identified with the IoT gadget for example movement detection, localization are the fundamental perspective. And in conclusion the board security incorporates arrangements for industrial, local and national principles and guidelines.

SDN: Software Defined Networking is the new open research alternative so as to give safety efforts for the IoT gadgets which expands the usefulness of the system and decreases the expense and equipment complexity [23]. In the FLAUZAC Olivier et al 2015, they have proposed an SDN based building solution. The engineering has three layers: physical layer, SDN-perfect virtual switch and an SDN controller and the Operating System layer.

They prescribed to utilize a numerous SDN controller so that in the event that an SDN controller neglects to carry out its responsibility, at that point different controllers will most likely do their favored job. In the instance of a solitary controller SDN will be fizzled if that controller is by one way or another stall out for any reason. For this they use Open Daylight Controller which gives the help of Cluster-based High Availability model.

Cryptography based: As a result of heterogeneity of gadgets and low power utilization it is difficult to give appropriate security to the installed devices. R. Nandini et al proposes cryptography based answer for the security motivation behind the IoT devices. In that paper, they propose to utilize ECC, mCrypton and AES cryptography to have secure transmission information to the cloud server.

ECC (Elliptical Curve cryptography) calculation depends on the elliptic bind hypothesis which has 164 piece key to what might be compared to 1024 piece key of different algorithms. This calculation has little in key size and capacity. MCrypton is 64, 96 and 128 piece key based algorithm, is utilized for minor gadgets like RFID. The calculation depends on Crypton and it has high power utilization ability.

Propelled Encryption Standard gives 128/192/256 bits key with incredibly solid high security. This utilized as an open or private key. This calculation is utilized in electronic scrambled information.

Mobility First network: Xiruo Liu et al characterize another convention for the IoT gadgets that is middleware which interfaces the equipment in the nearby framework to the worldwide Mobility First Network. They included Name Resolution Service to the middleware which gives naming and key management. Besides two key trade conventions Choo's 3PKD [14] convention and Needham-Schroeder convention can make the IoT reliable and give lightweight arrangements.

IP based solution: As TCP/IP isn't tied down enough to give adequate security to the system layer of the IoT devices [2] for its constrained plan technique.

III. CONCLUSION

Security is the major point in terms of IoT devices. Because of its complex architecture and some definite feature like heterogeneity, limitations it differs from device to device. IoT device as it is the revolutionary technology for modern science but because of the lack of security it should be taken into concern to secure IoT devices.

In this paper we have already discussed about the characteristics of the devices, different types cyber-physical attacks, OSI layer based threats and different proposed architecture from different papers. This paper will help researchers to know about the different types of intrusions and their behavior and which threats attack different layers of IoT devices. This will lead an important countermeasure for the threats for improving and inventing new architecture of IoT to provide proper security.

REFERENCES

1. M. A. Burhanuddin , Ali Abdul-Jabbar Mohammed , Ronizam Ismail and Halizah Basiron (2017) - Internet of Things Architecture: Current Challenges and Future Direction of Research. International Journal of Applied Engineering Research, 12(21):11055-11061.
2. Se-Ra Oh and Young-Gab Kim (2017). Security Requirements Analysis for the IoT. International Conference on Platform Technology. DOI:10.1109/PlatCon.2017.7883727.
3. Wei Zhou, Yuqing Zhang, and PengLiu (2018)-The Effect of IoT New Features on Security and Privacy: New Threats, Existing Solutions, and Challenges Yet to Be Solved. IEEE Internet of Things Journal (Volume: 6 , Issue: 2 , April 2019)
4. Se-Ra Oh and Young-Gab Kim (2017). Security Requirements Analysis for the IoT. International Conference on Platform Technology and Service (PlatCon).
5. M. A. Burhanuddin , Ali Abdul-Jabbar Mohammed , Ronizam Ismail and HalizahBasiron (2017) - Internet of Things Architecture: Current Challenges and Future Direction of Research.International Journal of Applied Engineering Research,12(21):11055-11061.
6. M.U. Farooq, Anjum Khairi and Sadia Mazhar (2015).A Critical Analysis on the Security Concerns of Internet of Things (IoT).International Journal of Computer Applications 111(7):1-6
7. Kazi Masum Sadique, Rahim Rahmani, and Paul Johannesson (2018). Towards Security on Internet of Things: Applications and Challenges in Technology. Journal of Procedia Computer Science,141, 199-206.
8. Tobias Heer , Oscar Garcia-Morchon, René Hummen ,SyeLoongKeoh, Sandeep S. Kumar, and Klaus Wehrle-(2011).Security Challenges in the IP-based Internet of Things. Journal ofWireless Personal Communications 61(3):527-542 .
9. Sachin Upadhyay. (2018). On Going Challenges and Research Opportunities: In Internet Of Thing (IoT) International Journal of Engineering Technologies and Management Research, 5(2:SE), 216-222. DOI: 10.5281/zenodo.1195065.
10. Tyson Macaulay-(2017). Threats and Impacts of the IoT. RIoT Control, pp.221-278.DOI: 10.1016/B978-0-12-419971-2.00012-1.
11. Rwan Mahmoud, TasneemYousuf, Fadi Aloul, Imran Zualkernan, 2015.Internet of Things (IoT) Security: Current Status, Challenges and Prospective Measures.10th International Conference for Internet, DOI:10.1109/ICITST.2015.7412116.
12. Hallman, Roger A.; Bryan, J.; Palavicini, G.; Divita, J. and Romero-Mariona, J. (2017). IoDDoS — The Internet of Distributed Denial of Service Attacks - A Case Study of the Mirai Malware and IoT-Based Botnets.In Proceedings of the 2nd International Conference on Internet of Things, Big Data and Security - Volume 1: IoT BDS,ISBN 978-989-758-245-5, pages 47-58. DOI: 10.5220/0006246600470058.
13. Weizhe Zhang, Baosheng Qu, 2013.Security Architecture of the Internet of Things Oriented to Perceptual Layer. International Journal on Computer, Consumer and Control (IJ3C), Vol. 2, No.2,page:37.
14. Burhan, M.; Rehman, R.A.; Khan, B.; Kim, B.-S. IoT Elements, Layered Architectures and Security Issues: A Comprehensive Survey. Sensors 2018, 18, 2796.
15. Huansheng Ning, Hong Liu ,2013. Cyber-Physical-Social Based Security Architecture for Future Internet of Things.IEEE Computer Society Press Los Alamitos, CA, USA,Volume 46 Issue 4, pages 46-53.
16. Rwan Mahmoud, TasneemYousuf, FadiAloul, Imran Zualkernan,2015.Internet of Things (IoT) Security: Current Status, Challenges and Prospective Measures.10th International Conference for Internet,DOI:10.1109/ICITST.2015.7412116.
17. Dina Gamal Darwish,2015.Improved Layered Architecture for Internet of Things.International Journal of Computing Academic Research (IJCAR) ISSN 2305-9184, Volume 4, Number 4 (August 2015), pp.214-223.

18. Standards for M2M and the Internet of Things.TR-0057 Service Layer. Retrieved from http://www.onem2m.org/getting-started/onem2m-overview.
19. R.Nandhini ,Aparna R , P.Srilakshmi, 2018.Study on Security issues in Internet of Things. International Journal of Research and Analytical Reviews (IJRAR) ,Volume 5, Issue 3,pages 165-168.
20. Mohammed Tawfik, Ali M. Almadni ,Alhasan A. Alharbi ,2015..A Review: the Risks And weakness Security on the IoT.IOSR Journal of Computer Engineering (IOSR-JCE)e-ISSN: 2278-0661,p-ISSN: 2278-8727,PP 12-17.
21. Hezam Akram Abdul-Ghani, Dimitri Konstantas Mohammed Mahyoub,2018. A Comprehensive IoT Attacks Survey based on a Building-blocked Reference Model. The International Journal of Advanced Computer Science and Applications(IJACSA), Volume 9 Issue 3, 2018..
22. El Mouaatamid, O., Lahmer, M., &Belkasmi, M. (2016). Internet of Things Security: Layered classification of attacks and possible Countermeasures. Electronic Journal of Information Technology, 0(9). Retrieved from http://www.revue-eti.net/index.php/eti/article/view/98.
23. FLAUZAC Olivier, GONZALEZ Carlos, NOLOT Florent,2015.New Security Architecture for IoT Network. Journal of Procedia Computer Science 52(1):1028-1033 ·
24. R.Nandhini ,Aparna R , P.Srilakshmi,2018.Study on Security issues in Internet of Things. International Journal of Research and Analytical Reviews (IJRAR) ,Volume 5, Issue 3,pages 165-168.
25. Jorge Granjal, Edmundo Monteiro, and Jorge Sá Silva, 2015. Security for the Internet of Things: A Survey of Existing Protocols and Open Research issues. Published in IEEE Communications Surveys & Tutorials, v: 17, issue:3 , DOI:10.1109/COMST.2015.2388550.
26. Jacob Wurm , Khoa Hoang , Orlando Arias, Ahmad-Reza Sadeghi and Yier Jin,2016.Security Analysis on Consumer and Industrial IoT Devices.21st Asia and South Pacific Design Automation, DOI:10.1109/ASPDAC.2016.7428064.
27. Maruf Pasha,Syed Myhammad Waqas Shah, 2016. Security Framework for IoT Systems. international Journal of Computer Science and Information Security (IJCSIS), Vol. 14, No. 11.
28. Barbara Kitchenham, O. Pearl Brereton, David Budgen, Mark Turner, John Bailey, and Stephen Linkman. 2009. Systematic literature reviews in software engineering - A systematic literature review. Inf. Softw. Technol. 51, 1 (January 2009), 7-15.
29. HezamAkram Abdul-Ghani, Dimitri Konstantas Mohammed Mahyoub,2018.A Comprehensive IoT Attacks Survey based on a Building-blocked Reference Model. The International Journal of Advanced Computer Science and Applications(IJACSA), Volume 9 Issue 3, 2018.

AUTHORS PROFILE

Dr. Md Forhad Rabbi is working as an Associate Professor of Department of Compute5r Science and Engineering, Shahjalal University of Technology, Bangladesh. He has completed hes PhD in Computing from Australia and current research focus is HCI, IoT, Social Computing, E Governance.

Ashique Jubayer is a final year student of B,Sc. In CSE program at Sylhet Engineering College. He has research interest on IoT and it Security.