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

Various types of Security Issues and Challenges for Attacks, according to the Attacking Type, Threat Level and Effects: IoT Security Mechanism

Jayanta Kumar Pahari, Arindam Roy

Abstract: ***IoT (Internet of Things) has been an enormous expansion in the upcoming years Information and Communication Technology. It is anticipated that over near about 5 billion devices will become a component of the IoT in the next upcoming years. Security issues of the IoT network should be the primary priority. In this paper, we analyzed the security challenges in the five layers of the IoT architecture and we proposed their solution. In addition, significant security technologies like encryption are also evaluated with respect to the IoT. Finally, we discuss prevention methods of the security attacks on different layers of IoT and emphasize the future research scope surrounded by the IoT architecture.***

Keywords: ***Internet of Things, Perception Layer, Network Layer, Processing Layer, Secure Device Layer, Application Layer.***

I. INTRODUCTION

The revolution of IoT [1] as a new proceeds in ulterior Internet when the hardware components become the part of the Internet. IoT provides the substance (i.e; unique identity accessible from the network and its status, location) in a unique way. The substances can be tracked down [2]. Many services such as monitoring, tracking and controlling happen to possible with the IoT which evaluate the human communication with the physical substances. RFID (Radio Frequency Identification Devices), infrared sensors, laser scanner, GPS (Global Positioning System) and gas inductors developed are currently used as the IoT. In IoT various parameters of the objects or processes such as sound, light mechanics, chemistry, biology, and position can be monitored and controlled. The great thing about IoT is that all the information is based on real time data. IoT comprises of a network of highly diverse digital objects interacted with each other and with humans too. It provides a sensor network with communication system, store and manage the information, provides access and also handles the privacy protection and data security problems [3]. Comparing the research aspects of security in IoT to security in the Internet, the former is the way complex than the later and therefore needs the significant attention of the researcher and a more precise research methodology and tools should be incorporated.

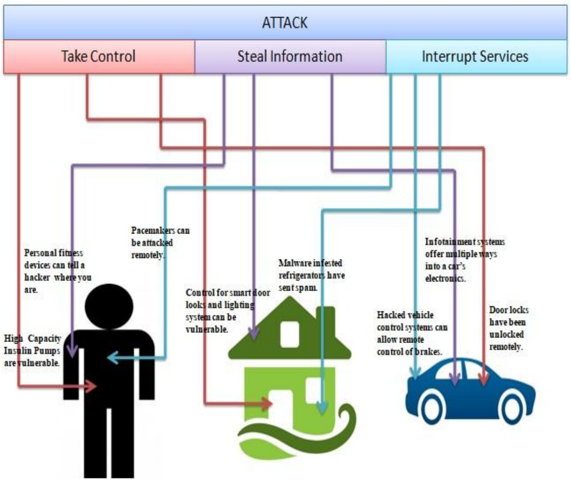
ATTACK
Take Control
Steal Information
Interrupt Services
Personal fitness devices can tell a hacker where you are.
Pacemakers can be attacked remotely.
High Capacity Insulin Pumps are vulnerable.
Control for smart door looks and lighting system can be vulnerable.
Malware infested refrigerators have sent spam.
Infotainment systems offer multiple ways into a car's electronics.
Hacked vehicle control systems can allow remote control of brakes.
Door locks have been unlocked remotely.

Fig. 1: Outline of Internet of Things

IoT devices are increasing sharply day by day to provide the comfort and the smartness of human life. The causes of increasing the number of IoT devices are that they provide full flexibility in human life and achieve the work with enhanced outcomes than humans. It has been noticed that, in 2019, the number of IoT devices will have more than a multiple of 1.73 since 2015. The general idea of simultaneously increasing of number of IoT devices from 2015 to 2025 is shown in the given Fig. 2.

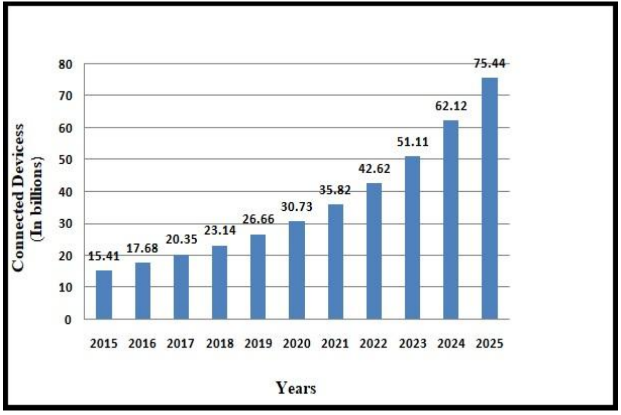

Fig. 2 Number of connected IoT devices from 2015 to 2025

Manuscript published on November 30, 2019.
***** Correspondence Author

Jayanta Kumar Pahari*, Department of Computer Science & Application, Prabhat Kumar College, Contai, Purba Medinipur, West Bengal, India, 721404. Email: jayanta.pahari@gmail.com

Arindam Roy*, Department of Computer Science & Application, Prabhat Kumar College, Contai, Purba Medinipur, West Bengal, India, 721404. Email: arcontai@gmail.com

Retrieval Number: D4434118419/2019©BEIESP
DOI:10.35940/ijrte.D4434.118419
Journal Website: www.ijrte.org

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication

II. RELATED WORK

Ali et al. [4] describes four layer architectures (perceptual layer, network Layer, support Layer and application layer) and proposed a scheme to perform access control and authentication mechanism in IoT.

This proposed system is based on support layer security problems with IoT.

The legacy authentication method is not applicable for IoT devices as these devices are resource constrained and huge number. Therefore a new authentication algorithm is needed for valid constrained devices in the Machine to Machine (MtM) communicate.

Otmane et al. [5] analyzed to introduce new types of attacks against with the OSI layers and the aim of security mechanism and processes to get the security protection against these attacks. The primary attacks on WSN and RFID are recognized, discussed, and obtainable. There needs a solution to stop the vulnerable issues.

In 2017, Ahmed et al. [6] explains a wide-ranging exploration is done depends upon the security event and the solution of IoT. The huge progression of the services of IoT needs the authentic and accurate security method to put off the IoT from different types of security events.

Xiruo Liu et al. [7] introduce an integrated IoT framework depend on the Mobility First future Internet architecture that support as a security solution for the IoT. They also developed a lightweight short-term keying protocol that provides security for communication. But there is no procedure for a long-term membership key with the support of a faithful third party.

In 2016, Pecorella et al. [8] analyze the security issues of IoT, they proposed security mechanism for the device initialization and they also depicted how the security issues of physical layer can effectively amplify the security of IoT systems. But, there is a drawback of the data broadcast rate and the range of communication between the devices is applicable for a short distance.

Mendez et al. [9] challenges from the standpoint of technologies and architecture used. This work highlight also in IoT inherent vulnerabilities as well as the security issues of different layers based on the security mechanism of data privacy, reliability and accessibility. An efficient and effective application of standardized security is required to solve the security threats.

In 2017, Razzaq et al. [10] focus on major security challenges of IoT. Mainly, they are focusing the security attacks and their countermeasures. Due to unavailability of security method in IoT devices, a huge number of IoT devices become accessible by third parties and even this; victims are unknown of being infected. The security requirements are discussed such as confidentiality, integrity, and authentication, etc. The different types of attacks are: low-level, medium-level, high-level, and extremely high-level attacks.

Chen et al. [11] lessons on the summary of IoT security attacks and construct a set of rules and grouping based on the system architecture and application domain. Also explain some key features of IoT. But, there is required to design an all-inclusive security method for the entire IoT architecture.

In 2018, Burhan et al. [12] are focusing on summary about several layered architectures of IoT and classified the attacks regarding security with respect to layers. In addition, a appraisal of mechanisms that provide solutions to these issues is presented with their limitations. Furthermore, several open research challenges associated with the IoT technology.

Sfar et al. [13] major evolution creates its own security and privacy challenges. Most of these challenge outcomes from the intrinsic vulnerabilities of IoT instance and the unyielding coupling of the physical world to the virtual world through intelligent objects. A registration of the big data, ecological unit is required to smooth the progress of the tracking of all objects that may affect the defense of IoT system instance for the period of their life-cycle. IoT communications need to be debated among IoT security issues.

Hezam et al. [14] propose a narrative four-layered IoT architecture depend on building block policy. They have proposed IoT component-based on layer wise attack, which consists of the corresponding components: a) physical objects, b) protocols covering whole IoT stack, c) data, and d) software. But, there is no mechanism to protect the IoT devices from various types of security attacks.

III. RELATIONSHIP TABLE

Table 1: Relationship Table

Name of Attack	Reference No.	Type	Threat level	Effects
Node Tempering	[15]	Physical Damage	High	Change Information
Fake Node Injection	[16]	Cloning	High	Fake Data Manipulation
Malicious code injection	[17]	Privacy	High	Halt Transmission
Sleep denial attack	[18]	Interruption	Medium	Shutdown of nodes
Physical damage	[19]	Active	Medium	Damage the IoT services
WSN node jamming	[20]	Blocking	Low	Communication blockage between nodes

RF interference of RFIDs	[21]	Authentication	Low	Stop Communication by distortion in node
Social Engineering	[22]	Privacy	High	Personal data leakage
Traffic Attack	[23]	Gathering	Medium	Leakage of secret data(about network)
Sinkhole Attack	[24]	Active	Low	Data leakage (Data of the Nodes)
RFID unauthorized access	[25]	Authenticity	Medium	Node information can be temper (Read, Write & Delete)
RFID Spoofing	[26]	Fabrication	High	Intrusion in network Data manipulation
Routing Information Attack	[27]	Eavesdropping	High	Routing loops (Network Destruction)
Man in the Middle Attack	[28]	Modifying Data	High	Data Privacy Violation
Wormhole Attack	[29]	Passive	Medium	Relocation of bits in the network
Hello flood Attack	[30]	Overflow	High	Traffic jamming and channel blockage
Data security	[31]	Privacy	High	Data leakage (User data on cloud)
Virtualization threats	[32]	Active	Medium	Resources destruction
Application security	[33]	Active	High	Privacy Violation
Shared Resources	[34]	Data Hijacking	Medium	Resources Theft
Third-party relationships	[35]	Data Security	High	Data Leakage (User data on cloud)
Underlying Infrastructure security	[36]	Passive	Low	Service Hijacking
Phishing Attacks	[37]	Replication	High	Data Leakage (User credentials data
Malicious Scripts	[38]	Active	High	Hijacking
Virus, Worms, Trojan Horse, Spyware	[39]	Active	High	Resource Destruction & Hijacking
Data Protection and Recovery	[40]	Privacy	Medium	Data loss & Catastrophic Damage
Cryptanalysis Attack	[41]	Data Security	Medium	Breaking the encryption procedure
Denial of Service	[42]	DoS	High	Resource Destruction

IV. Statistical view of IoT

In daily life, any type of smart system does not work properly and cannot process data in a smarter way without IoT. IoT is used in various purposes such as smart home, smart vehicle, healthcare etc. Most of the IoT application is used in smart healthcare or hospitality management system. The percentage of usage of the smart health care system is near about 25%. Second, most use of IoT application, is used in smart industry, and is near about 16%. Then smart city, smart home, smart supply & logistics, business and one after another according to the usage of the IoT. The fig. 3 is described about the percentile usage of IoT.

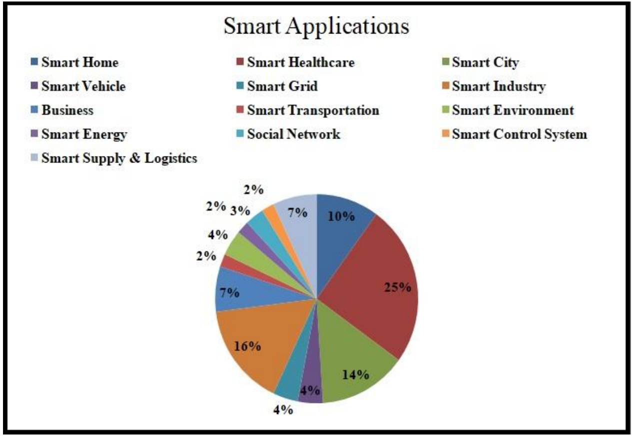

Fig. 3: Percentile Usage of IoT

V. Different Types of ATTACKS in IoT

A. Node Tempering

The node tempering attack may temper the sensor module or reason for damaging by physically transmit complete node or element of existing physical device or although automatically observe the nodes to get authentication permission and replace confidential information [15].

B. Fake Node Injection

The attacker can inject a fake or malicious node between the nodes of the network, hence the attacker achieves access to the network and be able to control all the data flow of the network. It can make the node to stop transmitting the real data and hence destroy the entire network [16].

C. Malicious Code Injection

The nodes of the IoT network can also be compromised by malicious code injecting. DoS attacks in WSN or virus on to the nodes are the most general type of this attack. By this attack, the attacker can gain access to the network, and can make the network to lose resources and hence make the services unavailable [17].

D. Sleep Denial Attack

A node on the remote places in IoT network are mostly powered by replaceable batteries, the nodes are programmed to sleep when they don't in utilize to increase their battery life. In this attack, the attacker keeps the node awake and prevent them falling asleep by feeding wrong input to the node which results in a power consumption hence the node shutdown [18].

E. Physical Damage

The attacker can break the IoT network by attacking on the devices for its personal use. This kind of attack loads with the security that hosts by IoT system. This kind of attack is dissimilar from Node Tempering attack as attacker tries to directly break the IoT services as well as IoT modules in physical damage attack [19].

F. WSN Node Jamming

Wireless sensor network works on the radio frequency. A denial of service can be created by sending the noise signals over the network or by jamming the signals of WSN. This denies the communication between the nodes of the IoT network. The attacker keeps on jamming the signals which result in the denial of services of the IoT [20].

G. RF Interference of RFIDs

RFIDs also work on radio signals as mentioned in WSN network earlier. The difference is that the attacker doesn't need to jam the signals, the attacker can create make the nodes to deny the services just by sending noise signals over the network. This noise interferes with the RFID signal which creates an obstacle in communication of the nodes [21].

H. Social Engineering

In this kind of attack the adversary can abuse the use of IoT system, to obtain valuable and secret information and achieve the task of extracting that kind of confidential information. This kind of attack is classified into physical attack as the attacker directly transmits data with the help of network of IoT to provide job [22].

I. Traffic Attack

The wireless technologies of transmission are sniffed to obtain confidential information. In such cases hacker first obtain information related to the network by using packet sniffers or port scanning application and then attacks on the targeted information [23].

J. Sinkhole Attack

The attack directs all signals from wireless sensor network nodes to a same point. Such attack voids the data safety and drops all the packets as a replacement of delivering to its destination [24].

K. RFID Unauthorized Access

As there is no secured authentication system in RFID systems, the tags are accessible to anyone. It means tags can be manipulated easily [25].

L. RFID Spoofing

In RFID spoofing attacker targets the RFID signal to gain access the information imprinted on the RFID tag. Once the signal spoofed hacker uses it to transmit his own data using the original id. Now hacker obtained the full access to system [26].

M. Routing Information Attack

These are immediate attacks that the enemy by spoofing, replaying or changing routing data can convolute the system and make routing loops, permitting or dropping movement, sending the false error data, shortening or amplifying source courses or in spite of parceling the network[27].

N. Man in the Middle Attack

Web attacker interferes the two sensor nodes to access restricted information and violates the privacy of nodes. Such attack doesn't demand the attacker to be physically appeared on the location of the network. This can be done by using the communication protocol of the IoT [28].

O. Wormhole Attack

Relocation of bits can be done from the original place of bits in the network. The mechanism of relocation is done from that channel of bits, where there is link with low latency [29].

P. Flood Attack

In flood attack, data is overflowed for the reason of sending garbage data's from the attacker's node. As the result, traffic of data is jammed and the network channel is blocked. Only a single despiteful node can execute this and cause jamming of the whole network by making of the large number of traffic [30].

Q. Data Security

Data security is the major concern of a SAAS user. It's the responsibility of the SAAS provider to ensure the security, the data processed and stored on a cloud as plain text. The major security issues occur on the facilitation of data backup provided by the service provider. The data block is offered through a third party in most of the cases which increase the treat of data theft [31].

R. Virtualization Threats

Security of virtual machines is as important as the security of the physical machines and any defect in possibly one may influence the other. Virtualization in processing layer is vulnerable to many types of attacks [32].

S. Application Security

Most of the application of cloud 'Software As A Service (SAAS)' is transmitted through internet i.e. web services. An attacker can easily use the web to get into the network of IoT and can take the data or can perform malicious activities. Security issues in 'Software As A Service (SAAS)' are huge different from usual security challenges of the web. '*Open Web Application Security Project* (*OWASP*) 'had recognized different security vulnerability on SAAS [33].

T. Shared Resources

As virtual machines share same resources, this becomes a security threat to the network. Using concealed channels an attacker can monitor all the shared resources between the virtual machines so the information might be compromised [34].

U. Third-Party Relationships

PaaS not only provides a programming language, it also gives third party network service component i.e. mashups. More than one resource is joint in mashups, which increase security issues like network and data security [35].

V. Underlying Infrastructure Security

With PaaS, lower layers of IoT are not accessible to the developer, underlying layer security is the responsibility of the provider. Even developers can develop a secure application, but its security remains vulnerable due to lower layers of IoT [36].

W. Phishing Attacks

In this kind of attack, the attacker can retrieve useful data and get the authentication permission of private data by using spoofing technique for the user. These attacks used to steal login credentials, information on credit card, etc [37].

X. Malicious Scripts

IoT network is generally associated with the Internet. Entire system closes up and data stealing is caused by running executable active-x scripts take in by the user that reins the access [38].

Y. Virus, Worms, Trojan, Spyware

The attacker affects the IoT system by injecting malignant software in the system which results in changeable outcomes. These types of attacks damage the whole system by refusing its services, altering data and get access to confidential data [39].

Z. Data Protection and Recovery

Privacy of user is involved in the communication with data. By improper procedure and algorithm of data processing the confidential data can be lost or may even cause a catastrophic damage [40].

AA. Cryptanalysis Attack

The purpose of this type of attack is to recover the encryption key which is being used for breaking the mechanism of encryption in IoT system. Cryptanalytic Attacks let the possession of plain text. Chosen plaintext attack, Known plaintext attack, Ciphertext attack are some examples of cryptanalysis attack [41].

BB. Denial of Service (DoS)

The adversary can affect all users in a IoT network system by injecting denial of service attack of the IoT network by the application layer hence not permitted user can get access to system information. This type of attack also blocks the authorized users for communication with application layer. The attacker can get full access to the application layer [42].

VI. PROPOSED ARCHITECTURE

A. Perception Layer

This layer consists with the physical environment and collects all the relevant information from real world with the help of sensor nodes and other physical devices. This layer is also liable for communication between various physical devices. The aim of this layer is to grant services to the network and authentication of devices. This layer utilizes the different sensors such as ZigBee, infrared, RFID and QR code to collect information. Information could be temperature, humidity, vibration, force, pH level pressure, speed, etc. Transmission of information collected is carried out through the network layer to the central information processing unit.

B. Network Layer

The network layer is responsible for communication between different physical devices, management of the network and also for maintenance of information through many communication protocols in an IoT system. There is not yet any fix protocol for IoT, but most common protocol now a day used is MQTT 3.1 and Constrained Application Protocol (CoAP). This layer securely transmits the data retrieved by perceptual layer sensor devices to main cloud or directly to another IoT node. Different technologies in this layer are mobile networks, Satellite networks, Wireless Ad hoc Network and several protected communication protocols used in these technologies. The transmission of information is carried out in this layer. Information transmitted through the different mediums such as RFID, Infrared, satellite and Wi-Fi units depending upon the nature of sensors and sensitivity of data. So, data are sent and received securely from perception layer to all other layers through the network layer.

C. Processing Layer

This layer works to combine the network layer and application layer. All the intelligence and cloud computing is done on this layer. Support layer functionality includes storage of data from lower level layers to the database and service management. On the basis of intelligent computing this layer can compute information and process data automatically.

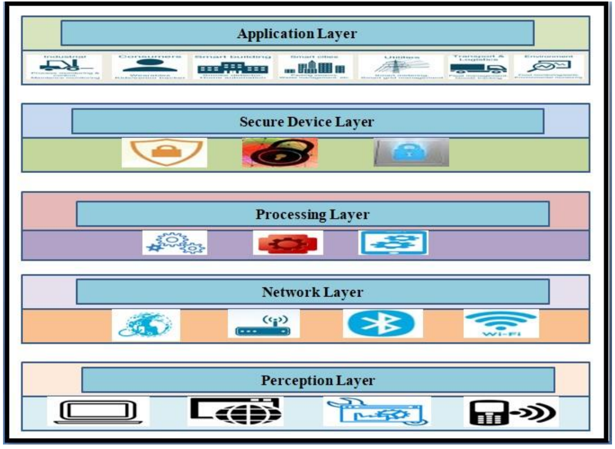

Fig. 4: Proposed Architecture of IoT

Retrieval Number: D4434118419/2019©BEIESP
DOI:10.35940/ijrte.D4434.118419
Journal Website: www.ijrte.org

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication

D. Secure Device Layer

The secure device layer deals with the physical device layer of the IoT solution which are increasingly integrating more security characteristics in together their hardware and software (that is successively on the device) to increase the security level of security device layer.

Characteristics of IoT security architecture:

- Some companies are providing chip level security in the type of 'Trusted Platform Modules (TPMs)' that perform as an origin of confidence by defensive responsive information and credentials (i.e., not releasing encryption keys outside the chip).
- Secure booting guarantee only authenticate software will run and execute on the device.

E. Application Layer

Users can access to different services using the application layer interface. Various types of applications are intelligent vehicle, smart farming, automated car, smart homes, smart health care system, and many more.

Application layer supplied services as per user demand. The processed information about the lower layers is utilized to produce useful services for end users. The information provides a platform for such applications which could benefit the user in many ways such as health, education, personal use, gadgets, household, transportation, communication etc. The information security in IoT should be prepared with feature like confidentiality, identification, etc. As IoT is going be applied in different important fields like health, transportation, industries, smart homes, postal services, etc. thus the security and privacy of IoT should be fool proof. Targeted solution to each security factor should be defined.

VII. Algorithm

We introduce a new encryption technique which can be used in IOT. Cross encryption mechanism is for information reliability, privacy, being non repudiation in data exchange for IOT. This paper analyzes cross encryption algorithm. The proposed algorithm has special features in encryption and decryption with respect to speed even in building keys and it can also enhance internet defense mechanism by several structures during algorithm implementation and using digital signatures. By default, tools and equipments are considered as shown in the following. Steps of a cryptography algorithm are as follows:

Step1: The user or the home neighborhood has a public key that is generated by the symmetric encryption.

Step2: Now data and anything which is needed to be encrypted will be sent to the asymmetric algorithm by the public key.

Step3: Then, the data is encrypted with the asymmetric encryption algorithm and will be sent to the receptor in the internet environment.

Step4: Receptors also have own a private key that even the user or sender is unaware about it.

Step5: The third party cannot guess the passwords of tools and smart appliances because of the private key and it can enhance IOT system security.

Step6: Receptor attempts to decode a data from the sender by the private key and encrypted text. In this paper, we will present a new cross algorithm for increasing speed of building a key and secure access, encryption and decryption and finally less memory requirements in IOT by combining two algorithms of AES and NTRU.

VIII. Conclusion

The advent of Internet of Things has significant contribution towards social development with the other advancements in science and technology. The effort of integrating smart applications under IoT infrastructure will benefit millions of users to access heterogeneous services in a more secured way anywhere anytime and any device which is registered. The proposed security architecture will be an unique to solve the security problems discussed in the paper. The authenticated user is assured of authorized service with more secure data appropriately at the right time. The data communication in the integrated smart services environment will be much more secured from the intruders. By adapting this secure architecture along with the algorithm discussed at different security levels in the IoT smart services environment will facilitate the integrated solutions to all the security issues.

IX. Future Scope

In this paper, we described the security challenges in each layer and its events, with respect to IoT circumstances, which is useful to recognize and to improve the IoT security framework. Advanced IoT security systems, consist of Upgradeable Vulnerability Detection System (UVDS), Intrusion Detection System (IDS), and Predefined Analysis System (PAS) which have necessitate advancing. All the above explained issues will be follow a line of inquiry opportunities in IoT security.

REFERENCES

1. F. Xia, L. T. Yang, L. Wang, and A. Vinel. "Internet of Things", Int. J. Commun. Syst., vol no. 25.9, 2012, pp. 1101–1102.
2. L. Coetzee and J. Eksteen. "The Internet of Things – Promise for the Future? An Introduction", in IST-Africa, 2011, pp. 1–9.
3. I. Andrea, C. Chrysostomou, and G. Hadjichristofi. "Internet of Things: Security Vulnerabilities and Challenges", in International Workshop on Smart City and Ubiquitous Computing Applications, 2015, pp. 180–187.
4. I.Ali, S. Sabir,Z. Ullah. "Internet of things security, device authentication and access control: a review", arXiv preprint arXiv:1901.07309, vol no.14.8, 2019, pp. 456-466.
5. O. El Mouaatamid, M. Lahmer, M. Belkasmi. "Internet of Things Security: Layered classification of attacks and possible Countermeasures", electronic journal of information technology, vol no. 9, 2016, pp. 24-37.
6. A.W. Ahmed,M.M. Ahmed, O.A. Khan, and M.A. Shah "A comprehensive analysis on the security threats and their countermeasures of IoT", International Journal of Advanced Computer Science and Applications, vol no. 8.7, 2017, pp. 489-501.
7. X. Liu, M. Zhao, S. Li, F. Zhang, W. Trappe. "A security framework for the internet of things in the future internet architecture", Future Internet, vol. no. 9.3, 2017, pp. 27- 54.
8. T. Pecorella, L. Brilli, and L. Mucchi. "The role of physical layer security in IoT: A novel perspective", Information,vol no. 7.3, 2016, pp.- 49-65.
9. D.M. Mendez, I. Papapanagiotou, B. Yang. "Internet of things: Survey on security and privacy", arXiv preprint arXiv:1707.01879 , 2017, pp. 1-16.

10. M.A. Razzaq, S.H. Gill, M.A. Qureshi, S. Ullah. "Security issues in the Internet of Things (IoT): A comprehensive study. International Journal of Advanced Computer Science and Applications", vol no. 8.6, 2017, pp. 383-388.
11. H. Chen, S. Zhang, Z. Li, Y. Zhang, Q. Deng, S. Ray & Y. Jin. "Internet-of-things security and vulnerabilities: taxonomy, challenges, and practice. Journal of Hardware and Systems Security", vol. no. 2.2, 2018, pp. 97-110.
12. M. Burhan, R. Rehman, B. Khan, B.S. Kim. "IoT elements, layered architectures and security issues: A comprehensive survey. Sensors", vol. no. 18.9, 2018, pp. 2796-2832.
13. A.R. Sfar, E. Natalizio, Y. Challal, Z. Chtourou. "A roadmap for security challenges in the Internet of Things. Digital Communications and Networks", vol. no. 4.2, 2018, pp. 118-137.
14. H.A. Abdul-Ghani, D. Konstantas, M.A. Mahyoub. "A comprehensive IoT attacks survey based on a building-blocked reference model", International Journal of Advanced Computer Science and Applications, vol. no. 9.3, 2018, pp. 355-373.
15. A. Perrig, J. Stankovic, and D. Wagner. "Security in wireless sensor networks", Communications of the ACM vol. no. 47.6, 2004, pp. 53-57.
16. K. Zhao, L. Ge. "A Survey on the Internet of Things Security", Computational Intelligence and Security, Ninth InternationalConference, IEEE ,2013, pp. 663-667.
17. T. Halim. "A Study on the Security Issues in WSN", Int. J. Comput. Appl., vol. 53.1, 2012, pp. 26-32.
18. T. Bhattasali. "Sleep Deprivation Attack Detection in Wireless Sensor Network", Found. Comput. Sci. New York, USA, 2012, pp.1-7 .
19. M. Jacobson. "Vulnerable Progress: The Internet of Things, the Department of Defense and the Dangers of Networked Warfare", 2015, pp.1-15.
20. M. Li and I. Koutsopoulos. "Optimal Jamming Attack Strategies and Network Defense Policies in Wireless Sensor Networks", IEEE Trans. Mob. Comput., vol. no. 9.8, 2010, pp. 1119-1133.
21. L. Li. "Study on Security Architecture in the Internet of Things", in 1ntemational Conference on Measurement, Information and Control (MIC) Study, no. Mic, 2012, pp. 374–377.
22. I. Ghafir, V. Prenosil, A. Alhejailan, M. Hammoudeh. "Social engineering attack strategies and defence approaches", Future Internet of Things and Cloud (FiCloud), 2016 IEEE 4th International Conference on. IEEE, 2016, pp.145-149.
23. B. S. Thakur and S. Chaudhary. "Content Sniffing Attack Detection in Client and Server Side: A Survey", Int. J. Adv. Comput. Res., vol. no. 3.2, 2013, pp. 7–10.
24. V. Soni, P. Modi, and V. Chaudhri. "Detecting Sinkhole Attack in Wireless Sensor Network", Int. J. Appl. or Innov. Eng. Manag., vol. 2.2, 2013, pp. 29–32.
25. R. Uttarkar and P. R. Kulkarni. "Internet of Things: Architecture and Security", Int. J. Comput. Appl., vol. no. 3.4, 2014, pp. 12–19.
26. S. Issues. "A Survey of RFID Deployment and Security Issues Korea Science A Survey of RFID Deployment and Security Issues A Survey of RFID Deployment and Security Issues Korea Science", J. Inf. Process. Syst., vol. no. 7. 4, 2011, pp. 16–17.
27. W. Chen, R. K. Guha, T. J. Kwon, J. Lee, and Y. Hsu. "A survey and challenges in routing and data dissemination in vehicular ad hoc networks", Wireless Communications and Mobile Computing vol. no. 11.7, 2011, pp. 787–795.
28. R. P. Padhy. "Cloud Computing: Security Issues and Research Challenges", vol. no. 1.2, 2011, pp. 136–146.
29. P. Pongle, G. Chavan. "Real time intrusion and wormhole attack detection in internet of things", International Journal of Computer Applications, vol. no. 121.9, 2015, pp.1-9.
30. M.B. Yassen,S. Aljawaerneh, R. Abdulraziq. "Secure low energy adaptive clustering hierarchal based on internet of things for wireless sensor network (WSN): Survey", Engineering & MIS (ICEMIS), International Conference on. IEEE, 2016, pp. 1-9.
31. D. H. Patil, "Data Security over Cloud", Int. J. Comput. Appl., 2012, pp. 11–14.
32. N. Kilari and C. Applications. "A Survey on Security Threats for Cloud Computing", Int. J. Eng. Res. Technol., vol. no. 1.7, 2012 , pp. 1–10.
33. A. Razzaq, K. Latif, H. F. Ahmad, A. Hur, Z. Anwar, and P. C. Bloodsworth. "Semantic security against web application attacks", Inf. Sci. (Ny)., vol. 254, 2014 , pp. 19–38.
34. K. Dahbur. "A Survey of Risks, Threats and Vulnerabilities in Cloud Computing", in International Conference on Intelligent emantic Web-Services and Applications, 2011, pp. 1-6.
35. K. Hashizume, D. G. Rosado, E. Fernández-medina, and E. B. Fernandez. "An analysis of security issues for cloud computing", vol. no. 4.1, 2013, pp. 1–13.
36. B. R. Chandramouli and P. Mell. "State of Security Readiness", Crossroads, vol. no.16.3, 2010, pp. 23–25.
37. H. Thakur H, S. Kaur. "A Survey Paper On Phishing Detection", International Journal of Advanced Research in Computer Science, vol. no. 7.4, 2016, pp.64-68.
38. J. Wan, N. Cn, and A. No. "Malware detection using pattern classification", 2012, pp. 1-16.
39. M. Akbari Roumani, C.C. Fung, S. Rai, H. Xie. "Value analysis of cyber security based on attack types", ITMSOC: Transactions on Innovation and Business Engineering vol. 1, 2016, pp. 34-39.
40. D.E. Merry Jr, M.J. Hajeck. "Systems and methods for reducing unauthorized data recovery from solid-state storage devices", vol. no. 2.12, 2011,pp.1-14.
41. B. Ndibanje B, H.J. Lee, S.G. Lee. "Security analysis and improvements of authentication and access control in the internet of things", Sensors , vol. no. 14.8, 2014, pp. 14786-14805.
42. Z.K. Zhang, M.C. Cho, C.W. Wang, C.W. Hsu, C.K. Chen, S. Shieh. "IoT security: ongoing challenges and research opportunities", Service-Oriented Computing and Applications (SOCA), IEEE 7th International Conference on. IEEE, 2014, pp. 230-234.

AUTHORS PROFILE

Jayanta Kumar Pahari received MCA degree from Vidyasagar University, WB, India in 2009 and M.Tech in Computer Science and Engineering from MAKAUT, WB, India in 2018. He is currently working as Govt. Approved Part-Time Teacher in Dept. of Computer Science in Prabhat Kumar College, Contai, WB, India. His research interest includes WSN, Network & Cyber Security, IED and IoT.

Arindam Roy received M.Sc. degree in Applied Mathematics, M.Tech in Computer Application and Ph.D in Soft Computing. His research fields include Optimization using Soft Computing, WSN, Precision Agriculture and IoT. He is currently working as Assistant Professor in Dept. of Computer Sc. in Prabhat Kumar College, Contai, WB, India. He has supervised research many projects and guided many research scholars. Dr. Roy published 32 papers in international reputed journals. He is an author of many books and book chapters. Currently, he is an Associate Editor of the journal "Array" in Elsevier group. He delivered many invited lectures in India and Aboard. He visited many countries like China, Japan, South Korea. He was a visiting fellow in Tsinghua University, Beijing, China.