Security Attacks inIoT: A Survey

Jyoti Deogirikar
Dept.of Computer Engineering
R.A.I.T
Navi Mumbai, India
jyotideogirikar1111@gmail.com

Amarsinh Vidhate
Dept.of Computer Engineering organization
R.A.I.T
Navi Mumbai,India
vidhate.amarsinh@gmail.com

Abstract— **Internet of Things (IoT) is one of the most buzzing and discussed topic in research field today. Some of the researchers are also looking future of the world in this technology. Since then significant research and development have taken place on IoT, however various vulnerabilities are observed which shall keep IoT as a technology in danger. As a result, there are so many attacks on IoT have been invented before actual commercial implementation of it. The present study discusses about various IoT attacks happening, classify them, its countermeasures and finding the most prominent attacks in IoT. A state of the art survey about the various attacks have been presented and compared including their efficiency and damage level in IoT.**

Index Terms: - Internet of Things (IoT), Attacks, Physical Attacks, Network Attacks, Software Attacks, Encryption Attacks.

I. Introduction

The human development growth rate has been increasing rapidly by using different technologies since last two centuries. One of the promising technologies is computing power which is increasing exponentially. With the increase, agraph of cost and size decreases whereas performance and number of users keep on increasing. There will be a tremendous increase in number of connections and networks through which almost everyone is connected through different devices like desktop, laptop, smartphones, PDA, etc. The prominent reasons are size, cost as well as IPv6 which allows billions of addresses, which is sufficient to provide IP address to each object instead of each device. The future will be communicating with various entities of an object through internet and it is nothing but Internet of Things (IoT)

Internet of things (IoT) is a group of interconnected devices and people in which devices can communicate with each other without human intervention [1]. Internet of things can be applied in various areas such as transportation, farming, healthcare, etc.The advantages of IoT are almost unlimited and its applications are changing the way we work and live by saving time and resources. It is also opening new opportunities for growth, innovation, and the exchange of knowledge between entities.

The term Internet of Things was first introduced as an idea in 1999 by Kevin Ashton [2], which has now evolved into a reality that interconnects real world sensors, electronic devices, and systems to the Internet. The internet of things has been drawing wide attention in recent years. In the year of 2005, International Telecommunication Union (ITU) has released an annual report on "Internet of Things" [3]. In the report, ITU has pointed that RFID and intelligent computing technology had opened an era that interconnecting global things altogether at macro level.

The Internet is the heart and center supporting for IoT, hence almost all the security threats that lie within the internet propagate to IoT as well. Compared with other traditional networks, the sensitive nodes of the IoT are assigned in positions without manual supervision, with theweak capability and limited resources, making the security issues of the IoT quite troublesome. Furthermore, the fast development and wider adoption of IoT devices in our lives signify the urgency of addressing these security threats before deployment. Due to intrinsic limitation of processing capability and speed, the traditional security counter measures are not applied as it is for IoT based security threats. The paper is an attempt to survey various types of security attacks and its associated depth and impact on the entities.

In this paper, diverse IoT attacks are discussed with their existing solutions. Further these IoT attacks are classified according to vulnerabilities of the attack used to compromise the network. Subsequent to that, few attacks are shortlisted as dangerous attack from each category according to their less possibility of detection and capacity to impact the network. These attacks are explained in detail and are compared with their parameters at the end.

The paper is organized as follows. Section II is the literature survey on IoT and security threats. Section III gives an overview of IoT architecture and attacks on IoT. In Section IV, a state of the art comparison of attacks has been presented. Section V concludes the paper.

II. Literature Survey

IoT is a technology which is still under development and need many improvements in it at adifferent level. The architecture of IoT is explained in detail in [4] [5] [6]. They describe three layers of IoT architecture. While in papers [7][8], itadds one more layer i.e. middleware layer whose functions are service management, stored data received from network layer in thedatabase, etc. Change in the layer does not make much change in IoT technology as well as its flaws.

In [6] [9] [10] [11] [12], different vulnerabilities and possible attacks on IoT are explained. In [6] it classifies attacks in four groups based on the vulnerability used by an adversary in the attack. In [13] [14] describes possible attacks on OSI layer. The references [15] [16] [17] focuses on the security challenges of an IoT system; however, most of these papers address only specific types of threats based on specific security objectives. Thereare no such robust proposed techniques which will solve most of the security issues of IoT. At present, very few papers address the multiple issues with common solutions in IoT.

There is atremendous need to find a common solution on security issues of IoT which will cover most of the issues at one solution. It is difficult to implementa solution for each attack because of computing and battery power constraint. IoT is based on other technologies like RFID and WSN. So, security flaws and issues in base technology will automatically inherit to IoT. In[18] addresses the security threats and attacks on RFID systems whereas survey over RFID attack and its prevention techniques are explained in detail in [19]. One of the dangerous attacks is side channel which uses side channel information. The amount of time required for the attack and analysis depends on the type of attack (Differential Power Analysis, Simple Power Analysis, Timing, etc.) According to [20], SPA attacks on smartcards typically take a few seconds per card, while DPA attacks can take several hours. According to [21], it is also possible to determine which operations are done at intermediate layer in block cipher. In [22] different attacks on cryptography are explained.Solutions for different security attacks on IoT are explained in [23] [24] [25][26].

IoT is seen as the future of theworld. Many applications have been proposed on the basis of IoT like structural health of buildings, waste management, air quality, noise monitoring, traffic congestion, city energy consumption, smart lighting etc. In paper [27], list of IoT applications and its benefit to society have mentioned. These applications will help to use resources efficiently and effectively. There are many issues in IoT. Some of them are mentioned below:

- For each attack there is separate solution. If we implemented all these solutions in IoT it will create lots of overhead on IoT and will reduce its performance.
- Currently used standards and protocols may not handle large amount of traffic from intelligent or mobile devices which connect to the internet at the same time.
- To fulfill current requirement of IoT (low power consumption, optimized algorithms, etc.), we need well defined architecture which will support large number of devices.

III. Different Security Attacks In IoT

In figure 1, a common IoT architecture is given. According to many researchers [4], IoT technology works on three layers perception layer, network layer and application layers as shown in Figure 1. Perception Layer involves various types of data sensors like RFID, Barcodes or any other sensor network. The aim of this layer is to obtain information from the environment by using sensors and then send it to the network layer. The aim of network layer is to transmit the data collected from the perception layer to any specific information processing system through internet, mobile network or any other kind of reliable network. The aim of the IoT of developing smart environment is accomplished at the application layer.The security of IoT is a big challenge because of complexity, heterogeneity and a large number of interconnected resources. The adversary can perform the attack on IoT system by damaging or tampering some node i.e. physical vulnerability, or from within its network by using faults in routing protocol and other network related protocol, or by using malicious program and by breaking encryption strategy i.e. encryption attack. Based on these vulnerabilities we classify the attack in four categories, as physical attack, network attack, software attack and encryption attack as shown in Figure 2. From each category, we considered one attack that is most dangerous from all the attack of that category.

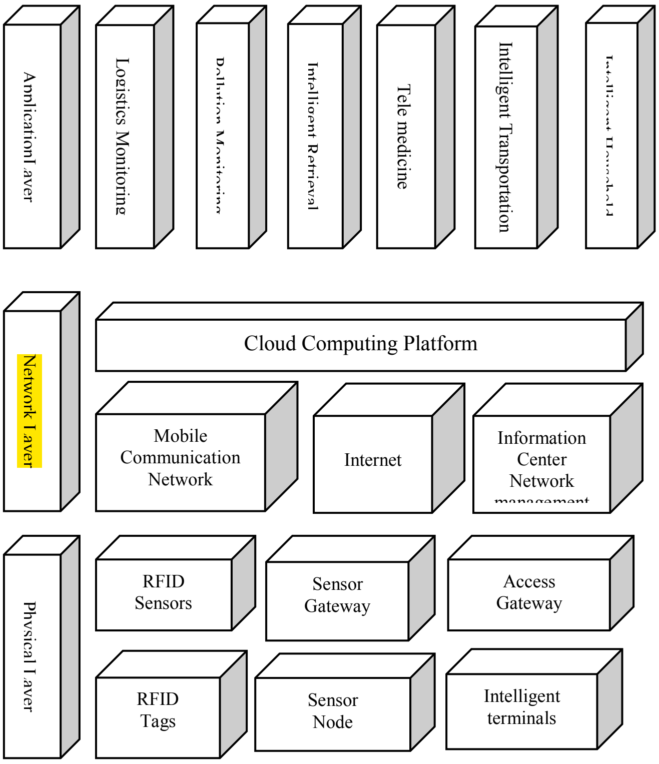

Fig.1: Architecture of Internet of Things [4]

From physical attack, malicious node injection attack has been the dangerous attack. Since it is not only stopping the services but also modify the data. From network attack, sinkhole attack is the most risky attack. It not only attracts all the traffic towards the base station, but also the attacker can initiate other threats such as selective forwarding, altering or dropping the packets. From software attack, we select worm attack as most unsafe. Worms are probably the most destructive and dangerous form of malware on the internet. It is the self-replicating program which harms the computer by using security holes in networking software and hardware. It can delete the files in system, steals the information like passwords, they can also change the passwords without your notice, it causes the computer lockouts, etc.

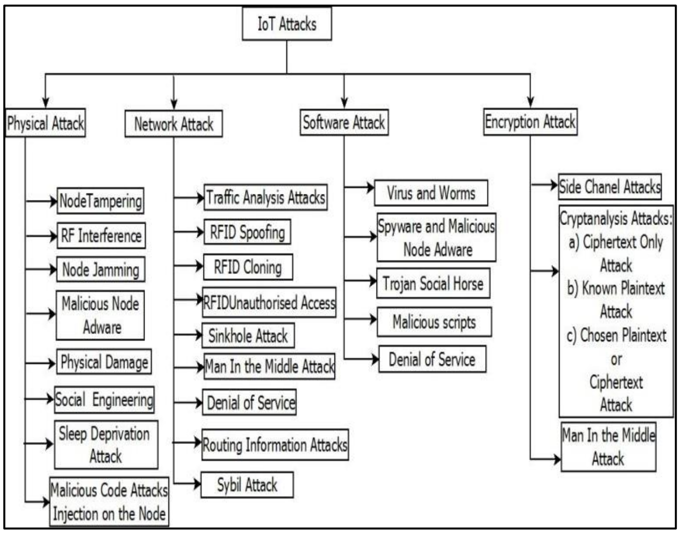

Fig. 2:IoT and its security attacks

From encryption attack, side channel attack is the most difficult to handle. It is very difficult to detect because attacker uses the side channel information to perform the attack.

A. Physical Attacks

Physical attacks are concentrated on hardware devices in the system.

*1) Node Tampering:*In this attack attacker physically alters the compromised node and can obtain sensitive information such as encryption key [10].

*2) RF Interference on RFIDs:*The attacker performs Denial of service attack by sending noise signals over radio frequency signals. These signals are used for RFID's communication [11].

3) *Node Jamming in WSNs:*By using jammer the attacker can disturb the wireless communication. It causes Denial of service attack [10].

4) *Malicious Node Injection:* In this attack, attacker physically injects a new malicious node between two or more nodes. It then modifies the data the passes the wrong information to the other nodes.The attacker uses the multiple nodes to perform malicious node injection attack [24]. The adversary first inserts a replica of the node B. After that, inserts other malicious nodes (node M1). Both these nodes work together to execute the attack. Thus collision is occurring at the victim node. Because of these, the attacked node cannot receive/send any packet. Hence, the conclusion of watchdog nodes might be affected by incorrectly announcing the attacked node (the legitimate node) as acting maliciously. To prevent this attack, we use a monitoring verification (MOVE) scheme. It can check the monitoring node(s)' result and correctly identify any malicious behavior. According to the acknowledgment, the verifier node will decide whether the node is malicious or not.

5) *Physical Damage:* The attacker physically harms components of IoT system and it results in Denial of service attack.

6) *Social Engineering:* The attackerphysicallyinteracts and manipulates users of an IoT system. The attacker obtains sensitive information to achieve his goals.

7) *Sleep Deprivation Attack:* The aim of theattacker is to use more power that results in shutting down of nodes [17].

8) *Malicious Code Injection:* The adversary physically introduces a malicious code into the node of IoT system. The attacker can get full control of IoT system[17].

B. Network Attacks

These attacks are focused on the network of IoT system.

1) *Traffic Analysis Attacks:* The attacker intercepts and examines messages to obtain network information [10].

2) *RFID Spoofing:* An adversary spoofs RFID signals. Then it captures the information which is transmitted from a RFID tag. Spoofing attacks give wrong information which seems to be correct and that the system accepts [11].

3) RFID Cloning: In this attack, adversary copying data from pre-existing RFID tag to another RFID tag. It does not copy original ID of RFID tag. The attacker can insert wrong data or control the data passing via the cloned node [6].

4) *RFID Unauthorized Access:* If the correct authentication is not provided in the RFID systems, then theadversary can observe, alter or remove information on nodes [6].

5) *Sinkhole Attack:* In a sinkhole attack an adversary compromises a node inside the network and performs the attack by using this node. The compromised node sends the fake routing information to its neighboring nodes that it has the minimum distance path to the base station and then attracts the traffic. It can then alter the data and also drop the packets.

In paper [25]gives the simple technique to identify sinkhole nodes. In proposed technique, when a node send a packet to its neighboring node it creates the entry of hop distances and ID in its database. It then computes the average hop-count except minimum hop-count and compares average and minimum value. If this minimum value is too small as compared to the average hop-count, then it is vulnerable to sinkhole attack.

6) *Man in the Middle Attacks:* The attacker over the internet intercepts the communication between the two nodes. They obtain the sensitive information by eavesdropping [6].

7) *Denial of Service:* An attacker floods the network with large traffic so that services are unavailable to its intended users [9].

*8) Routing Information Attacks:*In thisattack, the attacker can make the network complex by spoofing, modifying or sending routing information. It results in allowing or dropping packets, forwarding wrong data or partitioning the network.

9) Sybil Attack: In this attack, malicious node that takes the identities of multiple nodes and acts as them. For e.g. in Wireless Sensor Network, voting system single node can vote many times [17].

C. Software Attacks

The attacker performs the attack by using virus, worm, spyware, adware etc. to steal data, deny the services, etc.

1) *Phishing Attacks:* The attacker obtains the private information like username, passwords by email spoofing and by using fake websites.

2) *Virus, Worms, Trojan horse, Spyware and Aware:* An adversary can damage the system by using malicious code. These codes are spreads through email attachments, downloading files from the Internet.The worm has the ability to replicate itself without any human action.We can use worm detector, anti-virus, firewalls, intrusion detection system to detect the virus. The paper[26]combines anomaly and signature detection with honeypot to protect the system from worms. This hybrid scheme takes the advantage of honeypot and anomaly/signature detection and provides the protection against worms.

3) *Malicious Scripts:* By injecting malicious script the attacker can gain access to the system.

4) Denial of Service: The attacker blocks the users from the application layer by denying services.

D. Encryption Attacks

These attacks depend on destroying encryption technique and obtain the private key.

1) *Side-channel Attacks:* The attacker uses the side channel information that is emitted by encrypting devices. It is neither the plaintext nor the cipher text, it contains information about power, thetime required to perform theoperation, faults frequency, etc. Attacker uses this information to detect the encryption key.

There are different types of side-channel attack such as timing attacks, Simple and Differential Power Analysis, and Differential Fault Analysis Attacks[23]. Here, we consider timing attack.Timing attacks are dependent on the time require for executing operations. It gives the information of the secret keys. By using this information an attacker can find fixed Diffie-Hellman exponents, factor RSA keys, and break other cryptosystems [23]. Cryptosystems process different inputs in different time. Because of branching and conditional statements, RAM cache hits, processor instructions that run in non-fixed time, etc.

Timing computations are providing to a statistical model. It provides the guessed key bit to a certain extent of assurance.

Cryptanalysis of a Simple Modular Exponentiation: Diffie-Hellman and RSA operations involve calculation of R = y mod n, where n is public and y can be obtained by a listener. The adversary wants to search the secret key x. To perform the attack, the victim must calculate yx mod n for many values of y, where y, n, and the estimation time are known to the adversary and x remains the same. The needed data and timing computation might be gained by secretly listening on an interactive protocol. Hence, an adversary could see the messages received by the target and calculate the time required to respond to each y. A common method to stop timing attacks is to perform all operations in such a way that they take absolutely the same amount of time by adding delay. Sometimes this is difficult.

2) *Cryptanalysis Attacks:* In thisattack, the adversary obtains the encryption key by using either plaintext or ciphertext. Based on methodology used, there are different types of cryptanalysis attacks [6].

a) Ciphertext Only Attack: In this the attacker can access the ciphertext and determine the corresponding plaintext [23].

b) Known Plaintext Attack: In this method, the attacker knows the plaintext for some parts of the ciphertext. The aim is to decrypt the remaining part of the ciphertext utilizing this information [23].

c) Chosen Plaintext Attack: The attacker gets to choose what plaintext is encrypted and find the encryption key. [23]

d) Chosen Ciphertext Attack: By using the plaintext of chosen ciphertext the attacker can find the encryption key [23].

3) *Man in the Middle Attacks:* When two users are interchanging the key the attacker intercepts the communication and obtains the key [17].

IV. COMPARISON

We compare these four attacks by considering various parameters such as damage level, existing proposal and detection chances, vulnerability, etc. The comparison of these four attacks is summarized in Table I. Physical layer is targeted for malicious node injection attack as the node is physically injected into the network. While sinkhole attack is done at network layer as in this attack routing information is attracted to the node which has the lowest distance to the base station. The worm attack is performed at the application layer by inserting malicious code and side channel attack is performed at both application layer and physical layer because the attacker uses the side channel information emitted by the encryption device. All these attacks except side channel attack are active attacks, as they can modify the information. In side channel attack, attacker simply finds encryption key by using side channel information hence it is difficult to detect this attack. All these attacks result in severe damage as they modify the data, drop the packets, steal the private information and encryption key, etc. The chances of detecting malicious node injection attack are low because the attacker creates the replica of the victim node. Hence, neighboring node cannot identify the existence of replicated node. While detecting the sinkhole attack is difficult when the compromised node is near to the base station i.e. 1 or 2 hop distance. Worm can be detected by anti-virus thus to prevent we have to update the anti-virus, should not open the spam e-mails, or browse the suspicious sites, etc. The malicious node injection attack can be prevented if we could avoid replication of victim node. While in Sinkhole attack, the attacker cannot compromise the node if the node authentication is provided. The malicious node injection attack uses hidden node vulnerability whereas in sinkhole attack node authentication is not provided. People don't follow security policies such as accessing infected sites or files, spam e-mails, outdated anti-virus, etc.

TABLE I: COMPARISON OF DIFFERENT IOT ATTACKS

Classifications /Parameters	**Classification Types**			
	MaliciousNode Injection Attack	**SinkholeAttack**	**WormAttack**	**Side-Channel Attack**
OSI Layer	Physical [12].	Network [13].	Application [14].	Application, Physical [1].
Attack Type	Active -As the attacker compromise the node [9].	Active -As it provides the wrong information those results in packet dropping [9].	Active -As it modifies the files [6].	Passive -As the attacker can find encryption key by using the side channel information [1].
Attacker Location	External, Internal	External	Both	Internal
Attack Threat	Availability -due to collision at the victim node it cannot transmit the packet [24].	Availability, Confidentiality -As all the data is attracted to the compromised node [6].	Availability, Integrity, Authenticity -As it can delete, modify the data [6].	Confidentiality, Integrity -by using side channel information it can find the encryption key [1].
DamageLevel	High -As it can modify the data and pass the wrong info to other nodes [9].	High -As all data is flowing through compromised node the attacker can do anything with packet [9].	High -As it can delete files, mail documents [6].	High -As the attacker can obtains the secret key without detecting [1].
DetectionChances	Low -As it is replica (clone) of legitimate node [24].	Difficult -To detect when it is near to base station [25].	Anti-virus can identify it [14].	Negligible because adversary uses side channel information [22].
Possibilityof Prevention	Yes - If we could avoid replication attack [24].	Yes -if node authentication is provided [6].	Yes -by avoiding suspicious sites, files [14].	Yes -By using preventive methods[22].
Attacks based on	InsertingMalicious Node [24].	Routing [25].	MaliciousCode [14].	Side Channel Information [22].
Vulnerability	WirelessNatureand HiddenNode Problem [24].	Node Authentication is not provided [6].	Not followingSecurityPolicies [14].	Side-channel information [22].
Existing solutions and their limitations	Not Possible to detect if morethan two nodes aremalicious, Consumes power because ofoverhearing [24]	When Malicious Nodenear to thebasestation (1 or 2 hop distance), Algorithm cannotaccurately detect sinkholenode[24]	New worms are created everyday [14]	Affect the performance ofthe system [23].

Hence are prone to worm attacks. While computation each device emits some side channel information and this information is used by an adversary to crack the encryption key. Many solutions are provided for each attack but they have some limitations. With increase in numbers of malicious node, malicious node injection attack becomes difficult to detect. The internet worms are created everyday so there are some limitations in detection of worms.

V. CONCLUSION

As IoT uses network architecture which is similar to traditional network architecture for communication among different devices, flaws of traditional network architecture is also inherited in it. With the development of IoT, many kinds of attacks also have been invented to breach the security of IoT devices. Researchers have proposed different solutions on these attacks to tackle it. However implementation of all these security measures and techniques together consumes computation as well as battery power of devices which is not acceptable for IoT technology and its devices. There is a need of a security mechanism which handles maximum security problems but it should be light weight and robust for fit for IoT technology. Many of the attacks on IoT have been discussed and classified above. Some of these attacks can be avoided by just keeping some security precaution while the development of any application like checking node identity while communication or using devices which are difficult to tamper. However some attacks which are known, which are difficult to detect or prevent, there has been a need to find asecure and efficient solution.

VI. FUTURE WORK

As IoT uses network architecture based on the traditional network architecture for communication among different devices, lacunas of traditional network architecture has been inherited in it and vulnerabilities also. There shall be a great need of a refinement of the existing network architecture or to create a new network architecture which is lightweight, effective and more secure, possible to solve performance and security related issues till great extent. The authors look forward the issues and a refinement at the security layers at each network layer as a future work.

REFERENCES

[1] T. Yousuf, R. Mahmoud, F. Aloul, I. Zualkernan, "Internet of Things (IoT) Security: Current Status, Challenges and Countermeasures", International Journal for Information Security Research (IJISR), Volume 5, Issue 4, December 2015.

[2] K. Ashton, "That 'internet of things' thing.", RFID Journal 22, no. 7, 2009, pp.97-114.

[3] "The Internet of Things", International Telecommunication Union. ITU Internet Reports 2005.

[4] L. Li, "Study on security architecture in the Internet of Things," International Conference on Measurement, Information and Control (MIC), pp. 374-377,Harbin, China, 2012,.

[5] R. Mahmoud, T. Yousuf, F. Aloul and I. Zualkernan, "Internet of things (IoT) security: Current status, challenges and prospective measures," 2015 10th International Conference for Internet Technology and Secured Transactions (ICITST), pp.336-341,London, 2015,

[6] I. Andrea, C. Chrysostomou and G. Hadjichristofi, "Internet of Things: Security vulnerabilities and challenges," 2015 IEEE Symposium on Computers and Communication (ISCC), pp.180-187,Larnaca, 2015.

[7] L. Patra and U. P. Rao, "Internet of Things — Architecture, applications, security and other major challenges," 2016 3rd International Conference on Computing for Sustainable Global Development (INDIACom), pp.1201-1206, New Delhi, India, 2016,.

[8] M.U. Farooq, M. Waseem, A. Khairi and S. Mazhar "A Critical Analysis on the Security Concerns of Internet of Things (IoT)", International Journal of Computer Applications(0975 8887), Volume 111 - No. 7, February 2015.

[9] Wahid, Abdul, P. Kumar, "A Survey on attacks, Challenges and Security Mechanism In wireless Sensor Network", JIRST- International Journal for Research in Science & Technology, Volume 1, Issue 8, pp. 189-196,January 2015.

[10] S.N Uke, A.R Mahajan, R.C Thool "UML Modeling of Physical and Data Link Layer Security Attacks in WSN", International Journal of Computer Applications, Volume 70– No.11, May 2013.

[11] Li, Hong, Y. Chen, and Z. He. "The Survey of RFID Attacks and Defenses." 8th International Conference on IEEE Wireless Communications, Networking and Mobile Computing (WiCOM), 2012.

[12] Kandah, Farah, Y. Singh, and C. Wang, "Colluding injected attack in mobile ad-hoc networks", IEEE Conference on Computer Communication Workshops (INFOCOM WKSHPS), 2011.

[13] Kaur, Damandeep, and P. Singh, "Various OSI Layer Attacks and Countermeasure to Enhance the Performance of WSNs during Wormhole Attack",International Journal on Network Security 5.1 (2014): 62.

[14] Reed, Damon, "Applying the OSI seven layernetwork model to information security", SANS GIAC GSEC Practical Assignment Version 1.4 b Option One 2003.

[15] D. Singh, G. Tripathi, and A.J. Jara, "A survey of Internet of-things: Future vision, architecture, challenges and services," 2014 IEEE World Forum on Internet of Things (WF-IoT), pp. 287-292, IEEE, 2014.

[16] H. Suo, J. Wan, C. Zou, and J. Liu, "Security in the internet of things: a review," 2012 International Conference on Computer Science and Electronics Engineering (ICCSEE), vol. 3, IEEE, pp. 648-651,2012.

[17] M.U. Farooq, M. Waseem, A. Khairi, S. Mazhar, "A Critical Analysis on the Security Concerns of Internet of Things (IoT)", International Journal of Computer Applications (0975 8887), Volume 111 - No. 7, February 2015.

[18] A. Mitrokotsa, M. R. Rieback, and A. S. Tanenbaum, "Classification of RFID attacks" Gen 15693 (2010).

[19] H. Li, Y. Chen and Z. He, "The Survey of RFID Attacks and Defenses," 8th International Conference on Wireless Communications, Networking and Mobile Computing (WiCOM), Shanghai, 2012,.

[20] Kocher, Paul, et al. "Introduction to differential power analysis." Journal of Cryptographic Engineering 1.1 , pp.5-27 ,(2011).

[21] Kelsey, John, et al. "Side channel cryptanalysis of product ciphers." European Symposium on Research in Computer Security. Springer Berlin Heidelberg, 1998.

[22] Kocher, Paul C. "Timing attacks on implementations of Diffie-Hellman, RSA, DSS, and other systems." Annual International Cryptology Conference. Springer Berlin Heidelberg, 1996.

[23] Zulkifli, M. Zaid W. Mohd, "Attack on Cryptography", (2008).

[24] F. Kandah, Y. Singh, W. Zhang and C. Wang, "Mitigating colluding injected attack using monitoring verification in mobile ad-hoc networks", Security and Communication Networks, pp.1939-0122,2013.

[25] Md. I. Abdullah,M. M. Rahman and M. C. Roy, "Detecting Sinkhole Attacks in Wireless Sensor Network using Hop Count" I. J. Computer Network and Information Security, pp.50-56, 2015.

[26] Jain, Pragya and Sardana, Anjali, "Defending against Internet Worms Using Honeyfarm", Proceedings of the CUBE International Information Technology Conference, pp.795-800,2012.

[27] A. Zanella, N. Bui, A. Castellani, L. Vangelista and M. Zorzi, "Internet of Things for Smart Cities," in IEEE Internet of Things Journal, vol. 1, no. 1, pp.22-32,Feb. 2014,.