IOT Security Threats and Block chain based solutions

P.Mahalakshmi, G.Geetha

Abstract: ***The Internet of Things (IoT) is one of the important technologies that has taken the attention of researchers. It is the interconnection of things connected with each other and to also with humans, to achieve some goals. In future IoT is expected to be effortlessly integrated into our environment and human will be solely dependent on this technology for comfort and easy life style. Any security concern of the system will directly affect human life. So security and privacy of this technology is primarily important issue to resolve. In this paper, we discuss the threats and vulnerabilities to the security of IoT devices in different domains, different layers, its deployment architecture and provides possible Block chain solution to overcome these issues. The paper also analyzes how the Block chain technology can be used to provide security and privacy in IoT.***

: The Internet of Things (IoT) is one of the important technologies that has taken the attention of researchers. It is the interconnection of things connected with each other and to also with humans, to achieve some goals. In future IoT is expected to be effortlessly integrated into our environment and human will be solely dependent on this technology for comfort and easy life style. Any security concern of the system will directly affect human life. So security and privacy of this technology is primarily important issue to resolve. In this paper, we discuss the threats and vulnerabilities to the security of IoT devices in different domains, different layers, its deployment architecture and provides possible Block chain solution to overcome these issues. The paper also analyzes how the Block chain technology can be used to provide security and privacy in IoT.

Keywords: Block chain, Internet of Things, Security attacks

I INTRODUCTION TO IoT

The IoT is a network environment with intelligently connected devices and systems which comprised of smart machines interacting and communicating with each other. Internet of things (IOT) is a growing wireless technology that connects different things to the internet. As a result, an enormous volume of data are being generated, stored, and that data is being processed into useful actions that can communicate, command and control the things to make our lives much easier and safer. The sensor network technologies play an important role to meet this new challenge. The industrial revolution is creating an environment in which everything will be perceptible, interconnected and intelligent. The growth of IoT drives the digitalization world but at the same time the changing environment brings new threats and A strong provision for security of user's data is much in need. IoT solutions should provide the security and privacy concerns surrounding these devices and the data they collect, generate, and process. Recently, the Block chain technology has gained much attention in providing IoT solutions. Block chain creates a promising applications and can be leveraged to solve security and privacy issues.

II BLOCK CHAIN TECHNOLOGY

Don & Alex Tapscott proposed the concept clearly thatthe block chain data is not stored in any single location, the records are public and easily verifiable. The data is accessible to anyone on the internet and No centralized version of this information exists for a hacker to corrupt. Block chain has the concept of distributed ledger.[25] In traditional way, two persons cannot access the same document at the same time. But in block chain technology both parties can access to the same document at the same time, and the single version of that document is always visible to both of them. It is like a common ledger, but it is a shared document. The distributed part comes into play when sharing involves a number of people.

III SECURITY ATTACKS IN IoT DOMAINS

Before introducing IoT security issues, let us have a description about the three-domain architecture [1] that we consider in our security analysis. The architecture is made up of the following three domains as shown in the fig 3.1

IoT Sensing Domain: The sensing domain has smart objects which has the ability to sense the environment and sends the report to one of the devices in the fog domain. The smart objects change their location very often.

Fog Domain: The fog domain consists of a set of fog devices which are located in areas that are highly populated by many smart objects. Each fog device has a set of smart objects which reports their sensed data to the fog device. The fog device implements operations on the collected data including aggregation, preprocessing, and storage. Fog devices are also interconnected with each other in order to manage the communication and to coordinate them.

Cloud Domain: The cloud domain is composed of a

Revised Manuscript Received on July 22, 2019.

P.Mahalakshmi, Asst prof, *Department of Computer science & Engineering, Jerusalem College of Engineering, Anna University*, Chennai, India

Dr.G.Geetha Prof, *Department of Computer science & Engineering*, Jerusalem *College of Engineering, Anna University*, Chennai, India

large number of servers that are responsible for performing the heavy-computational processing operations on the data reported from the fog devices.

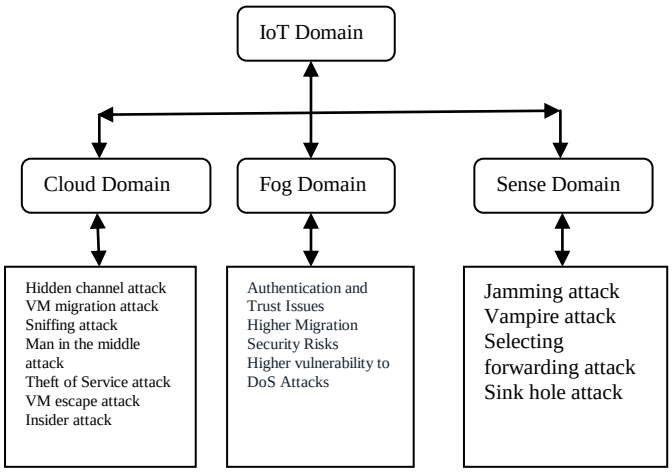

Fig 3.1

A. *Cloud Domain Attacks and Countermeasures*

1. Hidden-Channel Attacks: Although there is a logical separation among the VMs running on the same server, there are still some hardware components that are shared among those VMs such as the cache. This creates opportunities for data leakage across the VMs that reside on the same server.

Averting data from being leaked across VMs that are hosted on the same server can be achieved by one of the following techniques:

• Hard Isolation: The simple idea behind this preventive technique is to maintain high levels of isolation among the VMs

• Cache Flushing: This technique flushes the shared cache every time the allocation of the cache is switched from a VM to another.

• Noisy Data Access Time: This technique incudes random noise to the amount of time needed to fetch data, which makes it hard to tell whether or not the data was fetched from the cache or from the memory.

• Limiting Cache Switching Rate: An easing technique to limit the amount of data that can be leaked across VMs can be achieved by limiting how often the cache is switched from a VM to another VM.

2. VM Migration Attacks: The virtualization technology supports VM migration, which allows moving a VM transparently from a server to another. The term refers to the fact that the application running on the VM is disrupted for a very short duration due to this migration where the disruption is as low as hundreds of milliseconds.

The attacks that exploit VM migration can be divided into two categories based on the target plane:

- Control Plane Attacks: These attacks target the module that is responsible for handling the migration process on a server which is called the migration module that is found in the hypervisor. This gives the attacker the ability to launch malicious activities including the following:
  - ✓ Migration Flooding -where the attacker moves all the VMs that are hosted on the hacked server to a victim server that does not have enough resource capacity to host all the moved VMs.
  - ✓ False Resource Advertising: The hacked server claims that it has a large large amount of free resources.

- Data Plane Attacks: These are the second type of VM migration attacks and these attacks target the network links over which the VM is moved from a server to another. Examples of data plane attacks include:

3. Sniffing Attack:

Sniffing attack is where an attacker sniffs the packets that are exchanged between the source and destination and reads the migrated memory pages.

4. Man-In-The-Middle Attack:

The attacker fabricates a gratuitous ARP Reply packet similar to the one that is usually sent when a VM moves from a server to another. The fabricated ARP packet informs the routing devices that the physical address where the victim VM be present was changed to become the physical address of the attacker's malicious VM. Now the incoming packets that are intended to the victim get routed to the new physical address where the attacker resides.

5. Theft-of-Service Attack

In this attack, a malicious VM misbehaves in a way that makes the hyper-visor assigns to it more resources than the share it is supposed to obtain.

6. VM Escape Attack

Virtual machines are designed in a way that isolate each VM from the other VMs running on the same server, which prevents VMs from accessing data that belongs to other VMs that reside on the same server. However, If a VM escapes the hypervisor layer and reaches the server's hardware, then the malicious VM can gain root access to the whole server where it resides.

7. Insider Attacks

Some sensitive applications may have serious concerns about hosting their collected information on the cloud data center in the first place as the cloud data center administrators will have the ability to access and modify the collected data. This leads to some security attack.

B. *Fog Domain Attacks and Countermeasures*

The fog domain is made up of a set of fog devices where each fog device collects the sensed data that is reported from a set of smart objects.

1. Location: fog devices are placed in areas close to the smart objects. This results in giving the fog devices the ability to respond quickly to changes in the reported data.

2. Mobility: Since the location of the smart object

may change over time, the VMs that are created to manage those objects at the fog domain must be moved from this fog device into another, so as to keep the processing that is performed in the fog device close to the device that is generating data.

3. Lower Computing Capacity: The fog devices that are installed in a particular location are expected to have a lower processing capacity when compared to one offered by cloud data centers as the cloud data centers are made of thousands of servers. These characteristics raise new security threats that are specific to the fog domain and that distinguish it from the cloud domain. The security threats that are specific to the fog domain are as follows:

✓ Authentication and Trust Issues:

An important security concern that needs to be taken into account when assigning a smart object to a fog device is to authenticate first the identity of the fog device. Authentication is not enough, as the smart object also needs to decide whether the owner of the fog device can be trusted. Trust is also an essential as a smart object will be assigned to different fog devices belonging to different entities.

✓ Higher Migration Security Risks:

There is a higher probability that the migrated VMs get exposed to compromised network links or network routers when moving a VM from a fog device into another. This makes it vital to encrypt the migrated VM and to authenticate the VM migration messages that are exchanged among the fog devices.

✓ Higher vulnerability to DoS Attacks:

Since fog devices have lower computing capacities this makes them a low-hanging fruit for denial-of-service (DoS) attacks where attackers can easily overwhelm fog devices.

C. Sensing Domain Attack and Countermeasures

The sensing domain is susceptible to multiple attacks. We summarize some of the most well-known ones:

1. Jamming Attack:

This attack causes a service disruption and takes one of two

- Jamming the Receiver: This attack targets the physical layer in the OSI stack of the receiver (where the receiver is the fog device in the case of a direct connection or another object in the case of a multi-hop connection) where a malicious user (called the jammer) emits a signal (called the jamming signal) that interferes with the authorized signals that are received at the receiver side. The interference degrades the quality of the received signal causing many errors.

- Jamming the Sender: Unlike the previous attack, this type targets the data link layer of the sending object where the jammer in this attack transmits a jamming signal that prevents the neighboring devices from transmitting their packets

Different preventive and detective methods were proposed to eliminate jamming attacks.

- Frequency Hopping: This is a preventive technique where the sender and receiver switch from a frequency to another in order to escape from any possible jamming signal.

- Spread Spectrum: This technique uses a hopping sequence that converts the narrow band signal into a signal with a very wide band, which makes it harder for malicious users to detect or jam the resulting signal.

- Directional Antennas: The use of directional antennas can mitigate jamming attacks from being successful as the sender and receiver antennas will have less sensitivity to the noise coming from the different directions that are different from the direction that connects the sender and the receiver.

- Jamming Detection: The receiver can detect that it is a victim of a jamming attack by collecting features such as the received signal strength (RSS) and the ratio of corrupted received packets.

2. Vampire Attack: This attack exploits the fact that the majority of IoT objects have a limited battery lifetime where a malicious user misbehaves in a way that makes devices abstain extra amounts of power so that they run out of battery earlier which causes a service disruption. Four types of vampire attack are

• Denial of Sleep: Different data link layer protocols were proposed to reduce the power consumption of smart objects by switching them into sleep mode whenever they are not needed.

• Flooding Attack: The adversary can flood the neighboring nodes with dummy packets and request them to deliver those packets to the fog device, where devices waste energy receiving and transmitting those dummy packets.

• Carrousel Attack: This attack targets the network layer in the OSI stack and can be launched if the routing protocol supports source routing, where the object generating the packets can specify the whole routing path of the packets it wishes to send to the fog device.

• Stretch Attack: This attack targets the network layer in the OSI stack. If the routing protocol supports source routing, then a malicious object can transmits the packets that it is supposed to be forwarded to the fog device through very long paths rather than the direct and short ones.

3.Selective-Forwarding Attack: This attack takes place in the case when the nodeis not able to send its generated packets directly to the fog device but must rely on other nodes that lies along the path toward the

fog device to deliver those packets.
4. Sinkhole Attack: A malicious object claims that it has the shortest path to the fog device which attracts all neighboring objects, that do not have the transmission capability to reach the fog device, to forward their packets to that malicious object and count on that object to deliver their packets. Now all the packets that are originating from the neighboring nodes pass by this malicious node. This gives the malicious node the ability to look at the content of all the forwarded packets if data is sent with no encryption. Furthermore, the malicious object can drop some or all of the received packets. Techniques to detect and prevent the malicious objects were proposed and are based on the idea of collecting information from the different objects where each node reports the neighboring node along with the distance to reach those objects.

IV IoT DEPLOYMENT LEVEL ATTACKS

According to IoT deployment architecture [2], the security issues can be classified as low level, high level and intermediate level issues "Fig 4.1"

1. The low level security issues - are at physical and data-link layer. Some of the attacks in this layer are

- Jamming -A kind of Denial of Service attack, which prevents other nodes from using the channel to communicate by occupying the channel.
- Insecure initialization- a procedure of initializing and configuring IoT
- Sybil attack-The Sybil attack in computer security is an attack wherein a reputation system is subverted by forging identities in peer-to-peer networks.
- Spoofing Attack-A spoofing attack is when a malicious party impersonates another device on a network in order to launch attacks against network hosts, steal data, spread malware or bypass access controls.
- Sleep deprivation attack.-the method of making the sensor nodes stay awake.

2. The intermediate level security - deals with routing, communication and session management.

- Replay attack - A replay attack is a form of network attack in which a valid data transmission is maliciously or fraudulently repeated or delayed.
- Buffer reservation attack- The effect of buffer management strategies on 6LoWPAN's leads to *buffer reservation attacks*.
- RPL routing attack- The Routing Protocol for Low-Power and Lossy Networks (RPL) is a novel routing protocol for constrained environments such as 6LoWPAN networks. As the devices are connected to the untrusted Internet, providing security in IPv6/RPL connected 6LoWPANs is challenging.
- Sink hole attack- Sinkhole attack is a type of attack were compromised node tries to attract network traffic by advertise its fake routing update.
- Worm-hole attack- a Denial of Service attack, where attackers create a low-latency link between two points in the network.

3. High level security- deals with the applications that are executed in IoT.

- CoAP security- The constrained application Protocol uses DTLS bindings and provides end to end security.
- Insecure firmware – some attacks are caused by insecure firmware and software.
- Middleware security- The middleware provides the communication among heterogeneous environment.

V IoT LAYER SECURITY ATTACKS

The paper [4] gives an overview of security problems in IoT and possible attacks on each layer of IoT architecture. (Fig 5.1)

1. Perceptual layer Security

Perceptual layer has the IoT devices like Sensors, RFID tags, Bluetooth and Zigbee devices. These devices are more viable to cyber-attacks. As large amount of IoT devices are physically deployed in open fields, it encounters many physical attacks, which are:

- Node Tampering

If attackers have physical access to sensor nodes, he can replace the full node or part of its hardware or can also connect directly to it to modify some sensitive information and gets access to the node. The sensitive information may be a cryptographic key or routing table's routes.

- Fake Node

The attacker introduces a fake node to the IoT system and through this fake node he can inject malicious data into the network which makes the low power devices busy and consumes their energy.

- Side Channel Attack

The attackers use the information like consumption of power, time and electromagnetic radiation from senor nodes to attack the mechanism of encryption.

- Physical damage

IoT devices are deployed in almost all the locality. An individual can physically damage the IoTdevice.

- Malicious Code injection

The individual inserts malicious code to the node so that the node gives him illegal access to the system.

- Protecting Sensor Data

The confidentiality of the sensor data is low as individual can

place a sensor near to the IoT system and can sense the same value, also its integrity and authenticity is important and should be secured.

- Mass Node authentication

All the nodes in an IoT systems face authentication problem. Any individual can intrude and hack the authentication mechanism.

2. Network Layer Security

The network layer has sufficient security measures but some of the security issues still exists. Traditional security issues can affect the integrity and confidentiality of data. Some of the attacks like eavesdropping attack, DoS attack, Man in the Middle attack, and virus invasion are still affecting network layer.

- Heterogeneity problem

IoT perceptual layer has an heterogeneous environment. This heterogeneity leads to security and interoperability issues.

- Network Congestion problems

When a large amount of sensor data is used, it causes communication overhead which in turn leads to network congestion.

- RFIDs interference

Here the radio frequency signals used by RFIDs are interrupted with noise signals which leads to Denial of service.

- Node jamming in WSN

In this attack the attacker interfere the radio frequency of wireless sensor networks and deny the services from WSNs.

- Eavesdropping Attack

This type of attack gathers information using some sniffing tools like packet sniffers.

- RFID Spoofing

Here the attacker spoof RFID signals and read RFID tag and then the attacker sends fake data with the original RFID tag to gain full access to the system [16].

- Routing attacks

Here the attacker can alter the routing information and distribute it in the network to create routing loops, advertising false routes, sending error messages or dropping network traffic [17].

- Sybil Attack

Here a malicious node claims the identity of many nodes and pretends to be these nodes. This initiates false routing information and also disturbs the WSN election process [18].

3. Support Layer Security

The developing mechanism for continuous cloud audit such as Security Content Automation Protocol (SCAP) [19] provides trusted results via Trusted computing (TCG) [20]. This layer implements data and applications so both should be protected from security issues. Some of the security issues at this layer are:

- Data Security

To keep the data confidential and secure in cloud it must be secured from security issues. This can be done by using tools to detect data migration from cloud.To monitor activity Data loss prevention tools can be used. Data dispersion and data fragmentation tools can also be used for Data security in cloud [21].

- Interoperability and Portability

Interoperability and portability among cloud vendors is a vital problem. Different vendors use different proprietary standards which creates problems for user who want to transmigrate from one cloud to another. This heterogeneity also leads to security issues. [21].

- Cloud Audit

Cloud security sets many standards for cloud vendors for which Continuous audit is required to check the agreement of these security standards. This builds user trust.

- Tenants Security

The users data may be located at same physical drive. It may share same physical storage which are called tenants. Individual can steal tenant's data as the data share same physical media.

- Virtualization Security

The security of virtualization is more important. Secure migration of virtual machine can be a hurdle in cloud audit. [21].

4. Application Layer Security

Data sharing face International problems of data privacy and access control [22]. Some of the common security issues of application layer are:

- Data Access and Authentication

An application may have different users and Those user may have different access rights. Proper authentication and access control mechanism must be applied at application layer

- Phishing Attacks

The individual use infected emails or web links to modify legitimate user credentials and gets access by using those credentials

- Malicious Active X Scripts

The individual can send Active X script to IoT users through the internet and makes the IoT user to run the active x script which hacks the whole system and its data.

- Malwares attack

The attacker can attack applications using malwares and can modify data which leads to denial of service. Trojan horses, Worms and viruses are some of the dangerous malwares used by individual to exploit a system [24].

VI BLOCK CHAIN SECURITY SOLUTIONS

The security threats in IoT exploit vulnerabilities of various components such as applications, interfaces, network components, software, firmware, and physical devices, existing at different levels. The users in an IoT paradigm interact with these

components through protocols which may also be dismantled of their security decentralization measures. The countermeasures for security threats address vulnerabilities of this interaction at different layers to get a specific security level. The diverse protocols supporting deployment of components add to the complexity of these counter measures. A comparative analysis of the security threats, and their possible solutions is given for the low-level, intermediate level and high level.

Block chain technology plays a major role in managing, controlling, and most importantly securing IoT devices. This section defines how block chain can provide security solutions challenging IoT security problems. The section first explains which block chain may provide solutions for IoT security problems and then outlines open research challenges.

Background

A block chain is fundamentally a decentralized, distributed, shared, and immutable database ledger that stores registry of assets and transactions across the network. It has chained blocks of data that have been time stamped and validated by miners. The block chain uses elliptic curve cryptography (ECC) and SHA-256 hashing to provide solid cryptographic proof for data authentication and integrity [26].

Also, the block data contains a list of all transactions and a hash to the previous block. The block chain has a full history of all transactions and provides global distributed trust. Trusted Third Parties (TTP) or centralized authorities and services can be interrupted, compromised or hacked.

They can also behave badly and become corrupt in the future, even if they are trustworthy now. In block chain, each transaction in the shared public ledger is verified by a majority consensus of miner nodes which are actively involved in verifying and validating transactions.

Possible block chain solutions

we discuss some of the features of block chain that can be greatly useful for IoT.

Block chain has a 160-bit address space compared to IPv6 which has 128-bit address space[26]. With 160-bit address, block chain can generate and allocate addresses offline for around 1500 IoT devices.

Block chain has been widely used for providing reliable and authorized identity registration, ownership tracking and monitoring of products. Block chain also provides a trust worthy decentralized management, governance, and tracking at every point in the supply chain and life cycle of an IoT device.

- ✓ Data Authentication and Integrity.

By design, data transmitted by IoT devices connected to the block chain network will always be cryptographically proofed and signed by the true sender that holds a unique public key and GUID, and thereby ensuring authentication and integrity of transmitted data. In addition, all transactions made to or by an IoT device are recorded on the block chain distributed ledger and can be tracked securely.

- ✓ Authentication, Authorization, and Privacy.

Block chain smart contracts have the ability to provide a de-centralized authentication rules and single, multiparty authentication to an IoT Device. Also, smart contracts can provides more effective authorization access rules to connected IoT devices.

- ✓ Data privacy

It can be also ensured by using smart contracts which sets the access rules, conditions, and time to allow certain individual or group of users to access data. The smart contracts decides who has the right to update, upgrade, patch the IoT software or hardware, reset the IoT device, initiate a service or repair request, change ownership etc.

- ✓ Secure Communications

IoT communication protocols like HTTP, MQTT, CoAP, XMPP, and routing protocols like RPL and 6LoWPAN, are not secured by design. Such protocols have to be wrapped within other security protocols such as DTLS or TLS for messaging and application protocols to provide secure communication.

With block chain, key management and distribution are totally eliminated, as each IoT device would have his own unique GUID and asymmetric key pair once installed and connected to the block chain network. Therefore, light-weight security protocols that would fit and satisfy the requirements for the computation and memory resources of IoT devices become more feasible.

Some of the Open challenges and future research directions are Interoperability of security protocols, Hardware/firmware vulnerabilities, Resource limitations, Heterogeneous devices, Trusted updates and management, Single points of failure and Block chain vulnerabilities.

VII CONCLUSION

Internet of things security being a innovative topic for researcher today, faces many security and privacy issues. Due to huge number of IoT devices and machine to machine communication feature of IoT, authentication and authorization techniques are hardly possible.

IoT security and privacy are critical factors that meets the high expectations of the technology. This paper specifies block chain based IoT handles most security and privacy threats, while considering the resource-constraints of many IoT devices. In this paper we discussed how the block chain can be used to address and solve some of the most pertaining IoT security problems. The paper also outlines and identifies future and open research issues and challenges that need to be addressed by the research community in order to provide reliable, efficient, and scalable IoT security solutions.

REFERENCES

1. MEHIARDABBAGH AND AMMARRAYES, "INTERNET OF THINGS SECURITY AND PRIVACY" OCT 2017
2. Minhaj Ahmad Khana, KhaledSalah ,"IoT security: Review, blockchain solutions, and openchallenges" Zakariya University Multan, Pakistan Khalifa University of Science, Technology & Research, Sharjah, United Arab Emirates,2018 in IEEE Access.
3. Ali Dorri, Salil S. Kanhere, and Raja Jurdak"Block chain in Internet of Things: Challenges and Solutions "
4. Internet of Things Security, Device Authentication and Access Control: A Review
5. G.Noubir, G.Lin,Low-power DoS attacks in data wireless LANs and countermeasures, SIGMOBILE Mob.Comput. Commun. Rev. 7(3) (2003).
6. S.H.Chae, W.Choi,J.H.Lee, T.Q.S.Quek, Enhanced secrecy in stochastic wireless networks: Artificial noise with secrecy protected zone, Trans.Info for. Sec .9(10)(2014)1617–1628.http://dx.doi.org/10.1109/ TIFS.2014.2341453.
7. W. Xu, T. Wood, W. Trappe, Y. Zhang, Channel surfing and spatial retreats: Defenses against wireless denial of service, in:Proceedings of the 3rd ACM Workshop on Wireless Security, WiSe '04, ACM, New York, NY, USA, 2004, pp.80–89. http://dx. doi.org/ 10.1145/ 1023646. 1023661.
8. L.Xiao, L.J.Greenstein, N.B.Mandayam, W .Trappe, Channel-Based detection of sybil attacks in wireless networks, IEEE Transa. Inf. Forensics Secur. 4 (3) (2009)492–503.
9. Y. Chen, W. Trappe, R.P. Martin, Detecting and localizing wireless spoofing attacks, in: 2007 4th Annual IEEE Communications Society Conference on Sensor, Meshand AdHoc Communications and Networks, 2017,pp.193–202.
10. M. Demirbas, Y. Song, An RSSI-based scheme for sybil attack detection in wireless sensor networks, in : Proceedings of the 2006 International Symposium on World of Wireless, Mobile and Multimedia Networks, IEEE Computer Society, Washington, DC, USA, 2006, pp. 564–570. http: // dx.doi.org /10.1109/ WOWMOM. 2006.27.
11. L.Xiao, L.Greenstein, N.Mandayam, W.Trappe, Using the physical layer for Wireless authentication,in :2007 IEEE International Conference on Communications, 2007, pp. 4646–4651. http://dx.doi.org/10.1109/ICC.2007.767.
12. Y.-W.P.Hong,P.-C.Lan,C.-C.J.Kuo,Enhancing physical-layer Secrecy in multi antenna wireless systems: An overview of Signal processing approaches, IEEE Signal Process. Mag.30(5)(2013)29–40.
13. T. Pecorella, L. Brilli, L. Muchhi, The role of physical layer security in IoT: A novel perspective, Information7(3)(2016).
14. B. Khoo, "RFID as an enabler of the internet of things: issues of security and privacy." In Internet of Things (iThings/CPSCom), International Conference on and 4th International Conference on Cyber, Physical and Social Computing, pp. 709-712. IEEE, 2011.
15. B. S. Thakur, and S. Chaudhary, "Content sniffing attack detection in client and server side: A survey." International Journal of Advanced Computer Research (IJACR) 3, no. 2 (2013): 10.
16. A. Mitrokotsa, M. R. Rieback, and A. S.Tanenbaum, "Classification of RFID attacks." Gen 15693 (2010): 14443.
17. D. Wu, and G. Hu, "Research and improve on secure routing protocols in wireless sensor networks." In Circuits and Systems for Communications, 2008. ICCSC 2008. 4th IEEE International Conference on, pp. 853- 856. IEEE, 2008.
18. J. Newsome, E. Shi, D. Song, and A. Perrig, "The sybil attack in sensor networks: analysis & defenses." In Proceedings of the 3rd International symposium on Information processing in sensor networks, pp. 259-268.ACM, 2004.
19. Open SCAP, http://open- scap. org/ page/ Main_Page [Online; accessed 25.01.14].
20. Open-source TCG Software stack in C.http://trousers sourceforge.net/; 2011 [Online; accessed 25.01.14].
21. The treacherous 12, Cloud Computing top threats 2016, "Top threats working group, Cloud Security Alliance (CSA)"
22. G. Yang, J. Xu, W. Chen, Z. H. Qi, and H. Y. Wang, "Security characteristic and technology in the internet of things," Journal of Nanjing University of Posts and Telecommunications (Natural Science), vol. 30, no. 4, Aug 2010.
23. T. N. Jagatic, N. A. Johnson, M. Jakobsson, and F. Menczer, "Social phishing." Communications of the ACM 50, no. 10 (2007): 94-100.
24. H. Tobias, et al. "Security Challenges in the IP-based Internet of Things."Wireless Personal Communications 61, no. 3 (2011): 527-542.
25. https://blockgeeks.com/guides/what-is- blockchain-technology/
26. A.M.Antonopoulos, Mastering Bitcoin: Unlocking Digital Crypto-Currencies, firsted., O'ReillyMedia,Inc.,2014.

AUTHORS PROFILE

P.Mahalakshmi, Asst prof *Department of Computer science & Engineering Jerusalem College of Engineering, Anna University* Chennai,India

Dr G Geetha received her B.E computer science and engineering from Bharathiar University,Erode in 2000, M.E computer science and Engineering from Sathayabama University,Chennai in 2005 and PhD from Anna University Chennai. Now she is working as professor in the department of Computer Science and Engineering at Jerusalem College of Engineering,Chennai. She has 15 years of teaching experience. Her area of interest includes Network Security, Software Agents and Mobile Agent Security. she is a recognized supervisor for guiding Ph.D Research Scholars of Anna University and Produced 3 Doctorates 2016