Authentication and Access Control in the Internet of Things

Charu Vashisht Singh, Dr. Ashok Verma

Research Scholar, Dept. of CSE, GGITS, India

HoD and Professor, Dept. of CSE, GGITS, India

ABSTRACT: Security has seldom been the focus of device manufacturers who have historically taken their own approach for securing the devices in the IoT. Most devices in enterprise, consumer or industrial IoT continue to be developed and designed to perform specific functions and security is often a neglected theme in the majority of product development lifecycles. The proprietary protocols these devices operate on are primarily characterized by the purpose they are built to serve and offer very limited or no interoperability. With the increasing convergence of IT and OT towards IoT, lack of a common operating framework and security principles pose some serious challenges for device manufacturers and also the consumers.

In an increasingly connected world where we see an explosion of networked and cloud-enabled devices ranging from home appliances to medical devices to consumer electronics, creating and maintaining device and user identities, the relationships between the various entities and ensuring the integrity of devices has remained a constant challenge for consumers as well as for the security leaders. The industry has seen the emergence of several standards from governing bodies and consortiums but we still lack appropriate mechanisms that define how the identity of things (IDoT) should be defined, standardized and deployed across operating networks and entities. Besides the need for verifying identity and establishing trust levels of various entities such as devices, people, applications, cloud services and/or gateways operating in an IoT environment – there's a need to manage 'Identity of Things' or IDoT throughout the lifecycle of things. We also discuss challenges to traditional security solutions such as cryptographic solutions, authentication mechanisms and key management in IoT. Device authentication and access controls is an essential area of IoT security, which is not surveyed so far. We spent our efforts to bring the state of the art device authentication and access control techniques on a single paper.

KEYWORDS: Internet of Things, Authentication, Access Control, Security, Cyber-attacks, Wireless Sensor Networks

I. INTRODUCTION

Internet of things (IoT) is an incipient technology which focus on inter-connection between things or devices to each other and to humans or users to achieve some common goals. IoT is powered by many existing technologies like Wireless sensor and actuator networks (WSAN) and Radio frequency identification (RFID). The idea of Internet of things was first conceived by Kevin Ashton of Auto ID-Center MIT [1]. Due to the wide availability of internet in the form of Wi-Fi, mobile data networks services (3G, 4G LTE), ubiquitous sensing has been already evident. Subsequently, which has opened a door for the things connectivity to each other and to the users, which will ultimately contribute to the smart cities in future. The number of connected devices is expected to increase tremendously, reaching between 50 and 100 billion by 2020 [2]. This large number of connected devices will result in ubiquitous sensing and wide availability of services. In IoT paradigm the information and communication systems will be seamlessly embedded in our environment. Consequently, sensing and processing various physical phenomenon and storing the information on remote clouds [3]. IoT is an integral part of developing smart homes, smart cities and smart healthcare system. IoT will be accepted widely if it gain user's trust by providing durable security and privacy.

IoT security is one of the hot research topic today. Many researchers across the globe are using their efforts to

address various security challenges in IoT. However IoT security is a great challenge because of its heterogeneous nature. Internet of things being the blend of so many technologies, all of these technologies have their own traditional security and privacy flaws, which are to be addressed in IoT context. In this paper we will briefly discuss IoT architecture for security assessment at each layer of IoT. We discuss security threats in each layer and possible attacks that can be launched by the adversaries. We also proposed some counter measures to mitigate the risk of these attacks. IoT infrastructure is very prone to well-known security attacks like Denial of Service (DoS), Replay attacks, Man in the middle, cloning of things, eavesdropping and routing attack are identified in [4]. Atamli et al. [5] classify some IoT specific cyber-attacks such as device tempering, privacy breach, information disclosure, DoS, Spoofing, signal injection and side channel attack. IoT devices are resource constrained and present cryptographic security solutions cannot be applied to these devices which makes it prone to data integrity and confidentiality Problems. Also with exposition to DoS attacks, the three security goals i.e. confidentiality, integrity and availability is hard to achieve. The challenges to traditional security solutions in IoT are discussed in this paper in details. Device authentication and access control mechanism is also a major security issue in IoT. Authentication and access control problems in IoT are due to the large number of devices and machine to machine (M2M) communication nature of IoT. There are some recently proposed techniques for device authentication and access control which are discussed briefly in section 5.

Internet of things have a wide area of applications such as smart home, smart cities, smart healthcare system, intelligent traffic control lights, connected vehicles, smart environment monitoring in industries, smart grids, smart metering, water network monitoring, and smart logistics [3],[5] and many more. The application scope of IoT is not limited to the aforementioned applications. This paper discus generic security problems that can be applied to all application domains of IoT.

1.1 Motivation

The Internet of things must gain user's trust to be broadly accepted by the industry. For achieving trust of user IoT must ensure strong security and privacy of its users. Although it is a very active research topic, there is very little work published, which review the security of IoT [18, 40]. However the work is not up-to-date. As new threats in IoT are identified very often therefore we felt a need of latest and comprehensive review of IoT security to guide researcher about their efforts required in specific security area. Besides this support layer security in IoT is not discussed in available reviews. We fell the gap by identifying and discussing many support layer security issues in our paper. Authentication and access control is a major security challenge in IoT and many work has been done in the area. We provide a study of the latest authentication and access control mechanisms in IoT.

1.2 Paper organization

The rest of the paper is organized as follow: Section 2 discuss IoT Architecture. We present a comprehensive study of security problems in IoT in section 3. In section 4 we present challenges to traditional security solutions in IoT. We discuss state of the art Authentication and Access Control mechanism used in Internet of Things in section 5. Finally we conclude our work in section 6.

II. INTERNET OF THINGS ARCHITECTURE

Internet of things will model the world in near future and will bring comfort to human life. However its security is very important and challenging because of its heterogeneous nature, wide deployment, resource constrained nodes and generation of enormous amount of data every second. IoT network architecture consists of 4 layers [14] as shown in figure 01. This is not a standard architecture for IoT, however most of the proposed architectures have these layers. Therefore we took this architecture as our reference architecture for identifying and classifying different security problems in IoT. Figure 01 shows most widely accepted IoT architecture.

The different layers in IoT are:
2.1 Perceptual layer

This layer consists of devices like sensors and RFID that sense any real world physical phenomenon like RFID tags, weather condition and water level in agriculture field. Wireless Sensor and Actuator Networks and Radio Frequency Identification are the key elements of this layer.

2.2 Network Layer

This layer securely transmit the information collected by perceptual layer sensor devices to fog nodes, main cloud or directly to another IoT node. Different technologies at this layer are mobile networks, Satellite networks, Wireless Ad hoc Network and many secure communication protocols used in these technologies.
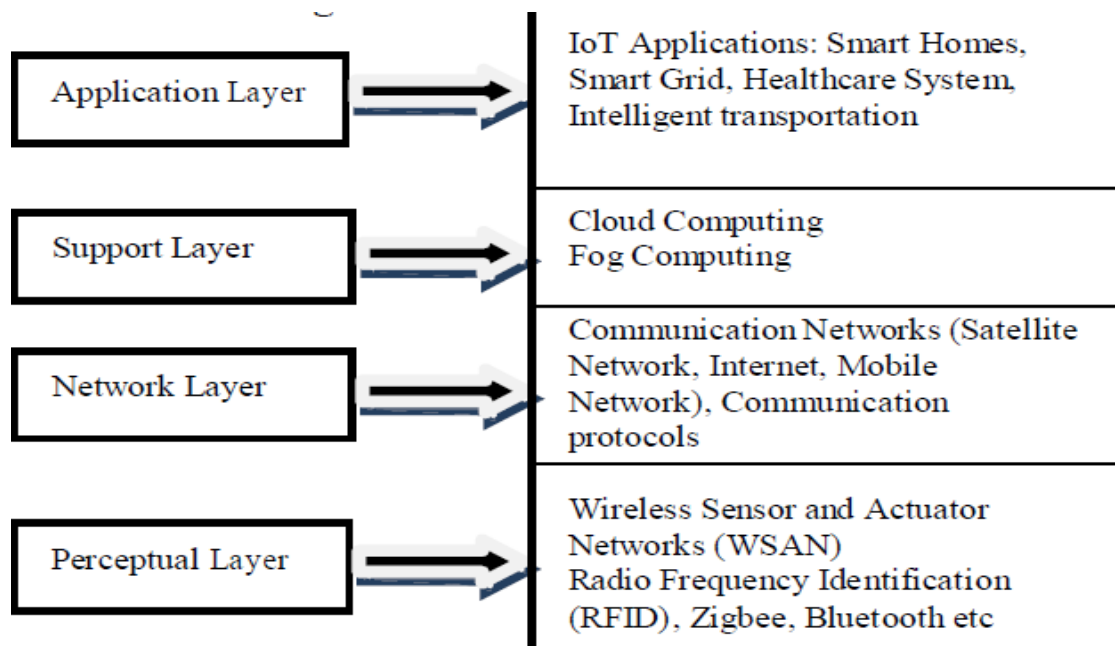

Figure 01. IoT Architecture

2.3 Support Layer

Support layer provide a feasible and effective platform for IoT applications. Different IoT applications can be hosted on fog nodes or main cloud and is accessible via internet by the resource constrained devices. It provides Storage   and computing power to the resource constrained devices.

2.4 Application layer

This layer provides internet of things services to users according to their needs. Users can access to different services using Application layer interface. Different applications are Smart homes, Smart healthcare system, intelligent transportation, Smart agricultures, automated vehicles and many more.

III. SECURITY IN INTERNET OF THINGS (IOT)

Besides gigantic importance and wide applications of IoT, It is not easy to deploy it in mission critical application areas, where security and privacy is of most important concerns. For example a successful security attack on smart healthcare system can cause in loss of many lives of patients, whilst it can also cause in financial loss, and loss of human lives in case of intelligent transportation system. Security of IoT is a challenging area and require further research work to cope with these challenges. We discuss these security challenges
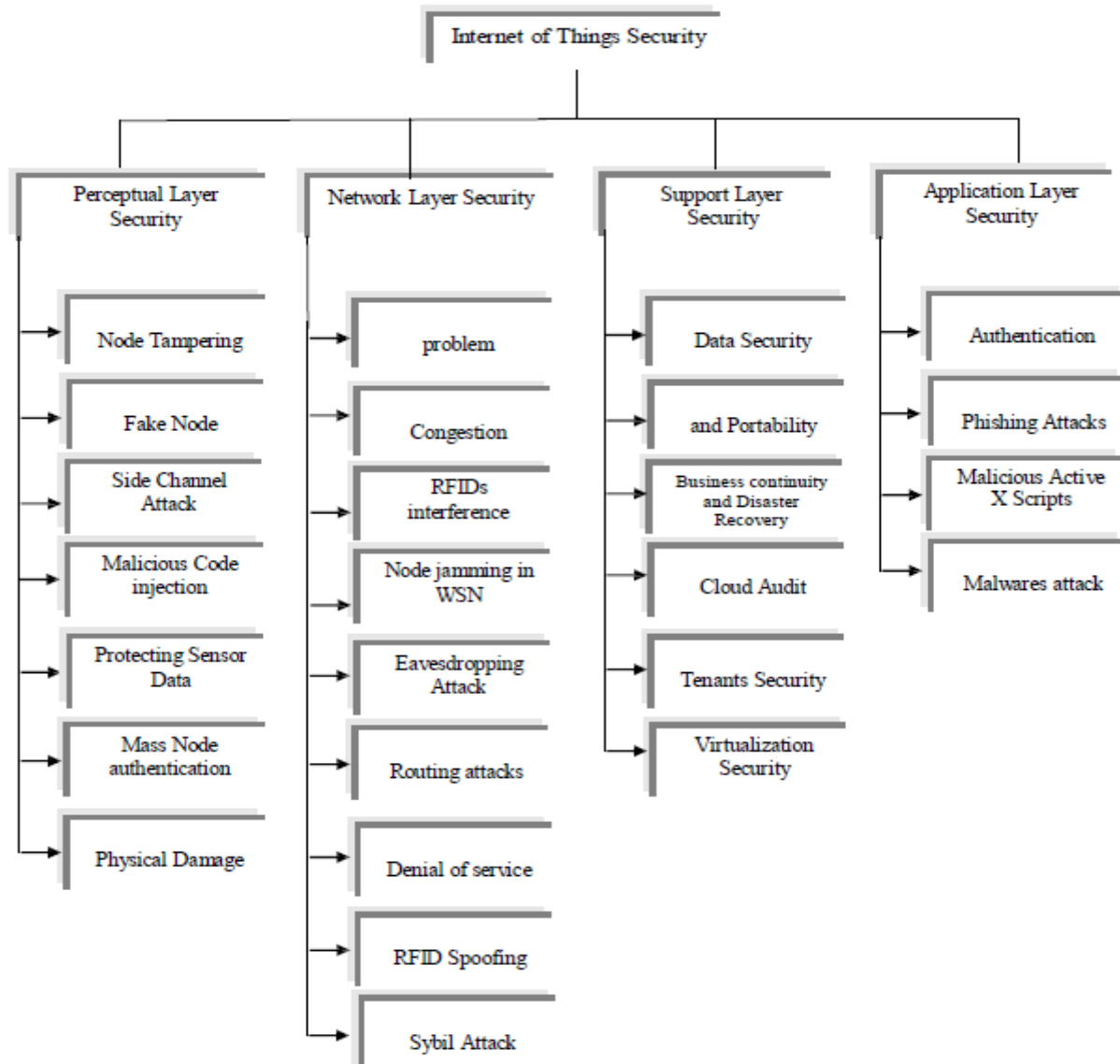
3.1 Perceptual layer Security

Perceptual layer consists of resource constrained IoT devices i.e. Sensors, RFID tags, Bluetooth and Zigbee devices. These devices are more prone to cyber-attacks. As large amount of IoT devices are physically deployed in open fields, it encounter many physical attacks, which are:

3.1.1   Node Tempering

If attacker have physical access to sensor nodes, he or she can replace the full node or part of its hardware or can also connect directly to it to alter some sensitive information and gain access to the node [15]. The sensitive information may be cryptographic keys or routing table's routes.

3.1.2   Fake Node

Attacker can add a fake node to the IoT system and can inject malicious data through this fake node in the network thus making low power devices busy and consuming their energy [18]. It can also act as a man in the middle attack.

3.1.3   Side Channel Attack

Attackers use the information like power consumption, time consumption and electromagnetic radiation from senor nodes to attack encryption mechanisms [18].

3.1.4   Physical damage

The adversary can physically damage the IoT device for Denial of service purpose. IoT devices are deployed in both open and closed vicinities and are more susceptible to physical damage by the attacker.

3.1.5   Malicious Code injection

Adversary physically compromises a node by inserting malicious code to the node that will give him illegal access to the system [41].

3.1.6   Protecting Sensor Data

The confidentiality requirements of the sensor data is low as adversary can place a sensor near to the IoT system sensor and can sense the same value, however its integrity and authenticity is more important and must be secured.

3.1.7   Mass Node authentication

A large number of nodes in an IoT system face authentication problems [18]. Huge amount of network communication require for authentication purpose only thus affecting the performance.

3.1.8   Security Requirements of Perceptual Layer

First of all IoT system must be physically secured from physical access to adversary. Node authentication is also necessary to prevent illegal access to system. The integrity confidentiality of data to be transmitted between nodes

is very important so light weights cryptographic algorithms should be designed to securely transmit data between nodes. Key management is also a problem to be solved in context of IoT.

3.2 Network Layer Security

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

3.2.1   Heterogeneity problem

IoT perceptual layer is the combination of many heterogeneous technologies. The access network have multi access methods, this heterogeneity makes security and interoperability more challenging [18].

3.2.2   Network Congestion problems

A large amount of sensor data along with the communication overhead caused by large number of devices authentication can cause network congestion [18]. This problem should be solved by having a feasible device authentication mechanism and competent transport protocols.

3.2.3   RFIDs interference

This is an attack on network layer in which the radio frequency signals used by RFIDs are corrupted with noise signals hence causing Denial of service [16].

3.2.4   Node jamming in WSN

This is a similar type of attack to radio frequency interference as discussed above for RFIDs. In this attack the attacker interfere the radio frequency of wireless sensor networks and deny the services from WSNs [17]. It is also a type of denial of service.

3.2.5   Eavesdropping Attack

It is the sniffing of traffic in the wireless vicinity of WSNs, RFIDs or Bluetooth [19] due to the wireless nature of device layer in IoT. Every type of attack starts from information gathering via sniffing using some sniffing tools like packet sniffers [20].

3.2.6   Denial of service

The adversary overburden the network with the traffic above its capacity and thus the network is unavailable for useful services to legitimate users.

3.2.7   RFID Spoofing

The attacker spoof RFID signals and read RFID tag, the attacker then send fake data with the original RFID tag and gain full access to the system [21].

3.2.8   Routing attacks

The adversary 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 [22].

3.2.9   Sybil Attack

In Sybil attack a single malicious nodes claim the identity of many nodes and pretend to be these nodes. This node can cause many harms like it can distribute false routing information or it can also rag the WSN election process [23].

3.2.10   Security Requirements of Network Layer

Although the existing core network security is mature enough but still some security concerns exist which are more harmful in the context of IoT, like Denial of service and Distributed denial of service must be prevented at this layer. Communication protocols must be very mature to solve the problem of routing attack, congestion problem and spoofing security problems.

3.3 Support Layer Security

Support layer security is independent from other layers and cloud computing security is a large domain of security. Cloud Security Alliance (CSA) is setting many standard security framework for clouds. And also developing mechanism for continuous cloud audit such as Security Content Automation Protocol (SCAP) [24] and providing trusted results via Trusted computing (TCG) [25]. This layer host IoT user's data and applications so both should be protect from security breaches. Some of the security concern at this layer are:

3.3.1   Data Security

To keep the data confidential and secure in cloud it must be secure from breaches. This can be done by using tools to detect data migration from cloud, data loss prevention tools, file and database activity monitoring. Data dispersion and data fragmentation can also be used for Data security in cloud [26].

3.3.2   Interoperability and Portability

Interoperability and portability among cloud vendors is major problem today. Different   vendors   use   different proprietary standards creating problems for user who want to migrate from one cloud to another. This heterogeneity also create security exposure [26].

3.3.3   Business continuity and Disaster Recovery

Cloud vendors must provide continuation of services in natural disasters like floods, fire and earth quicks disasters. For business continuity clouds physical location should be suitable so that it is affected at the least by such calamities. It should be in the approach of quick response teams. Clouds should also have some data back up plans [26].

3.3.4   Cloud Audit

Cloud security alliance sets many standards for cloud vendors, Continuous audit is required to check the compliance of

these security standards to build user trust.

3.3.5   Tenants Security

Multiple user's data may be located at same physical drive in the cloud or users of Infrastructure as a service (IaaS) may share same physical storage, such users are called tenants. Adversary can steal his/her tenant's data as the data share same physical media.

3.3.6   Virtualization Security

Different cloud vendors used different virtualization techniques. The security of virtualization is important. Virtual machine communication some time bypass network security controls [26]. Secure migration of virtual machine is required as it can be a hurdle in cloud audit.

3.3.7   Security Requirements of Support Layer

Internet of things user's data and application instances resides on cloud and Fog nodes. There security and privacy should not be abused in the cloud. CSA had already set many security standards, laws and regulations for cloud security. The compliance of these security standards should be monitored continuously and IoT systems should only use those clouds which comply with the security standards of CSA. Besides this simple and online cloud audit mechanism is required for the users to audit there cloud vendors for building user's trust.

3.4 Application Layer Security

Different applications at application layer have different security requirements. By now there is no standard for IoT application construction. However data sharing is one of the characteristics of IoT application layer. Data sharing face problems of data privacy and access control [27]. Some of the common security matters of application layer are:

3.4.1   Data Access and Authentication

An application may have many users and different user may have different access privileges. Proper uthentication and access control mechanism is required at application layer [18]. Which is a challenge as describe in the section 5.

3.4.2   Phishing Attacks

The adversary use infected emails or web links to steal legitimate user credentials and gain access using those credentials [28].

TABLE 1
LAYER WISE IoT SECURITY AND ATTACKS

S.#	Attacks	Perceptual Layer	Network Layer	Support Layer	Application Layer	Impact
01	Node Tampering	✓	✗	✗	✗	High
02	Fake Node	✓	✗	✗	✗	High
03	Side Channel Attack	✓	✗	✗	✗	Medium
04	Physical damage	✓	✗	✗	✗	Medium
05	Malicious Code injection	✓	✗	✗	✓	High
06	Protecting Sensor Data	✓	✗	✗	✗	Medium
07	Mass Node authentication	✓	✓	✗	✗	High
08	Internal entity problem	✗	✓	✓	✗	High
09	Network Congestion problems	✗	✓	✗	✗	Medium
10	RFIDs interference	✗	✓	✗	✗	Low
11	Node jamming in WSN	✗	✓	✗	✗	Low
12	Eavesdropping Attack	✗	✓	✗	✗	Low
13	Denial of service	✗	✓	✗	✗	High
14	RFID Spoofing	✗	✓	✗	✗	High
15	Routing attacks	✗	✓	✗	✗	High
16	Sybil Attack	✗	✓	✗	✗	High
17	Data Security	✗	✗	✓	✗	High
18	Interoperability and Portability	✗	✓	✓	✗	Medium
19	Business continuity and Disaster Recovery	✗	✗	✓	✗	Medium
20	Cloud Audit	✗	✗	✓	✗	Medium
21	Tenants Security	✗	✗	✓	✗	High
22	Virtualization Security	✗	✗	✓	✗	Medium
23	Data Access and Authentication	✗	✗	✗	✓	High
24	Phishing Attacks	✗	✗	✗	✓	Medium
25	Malicious Active X Scripts	✗	✗	✗	✓	High
26	Malware attack	✗	✗	✓	✓	High

3.4.3 Malicious Active X Scripts

The adversary can send Active X script to the IoT user through the internet and make the IoT user to run the active x script thus compromising the whole system [29].

3.4.4 Malwares attack

Attacker can attack applications using malwares and can steal data or cause denial of service. Trojan horses, Worms and viruses are some of the dangerous malwares used by adversaries to exploit a system [29].

3.4.5 Security requirements of Application Layer

To cope with the application layer security, strong authentication and access control mechanism is required. Besides these educating the users to use strong password [30] is also important. Strong anti-virus software's are required to protect against malwares.

IV. CHALLENGES TO TRADITIONAL SECURITY SOLUTIONS IN IOT

Security is the basic requirement of any user of digital media. An internet user will not share his confidential and important data on the network unless the network is trusted. With the emergence of cloud computing the security demands of its user also increased as they have to trust on third person owned cloud.   For cloud vendors to attract more users to use their services they need to build user trust through cloud audits and Certification of compliance to CSA security standards or other standards of security. Although legacy network security solutions are mature enough but it is not feasible to apply it in the   context of IoT due to the size of IoT networks heterogeneity in its architecture and resource constrained IoT end nodes.

4.1 Cryptographic techniques

Currently available cryptographic algorithms like symmetric key cryptographic algorithms, Advance encryption standard (AES) is used to insure data confidentiality, which is indeed very secure algorithm. Similarly frequently used asymmetric algorithm for digital signature and key exchange is Rivest Shamir Adelman (RSA) which is also very secure. Secure Hash algorithms (SHA) is used for data integrity and Diffie- hellman (DH) is used for key agreement. Elliptic curve cryptography (ECC) is also an efficient asymmetric cryptographic techniques which is not recently used [35].

All of the aforementioned algorithms are very secure and effective but power hungry and require more CPU power and consume more battery power. These algorithms are therefore not feasible to use for securing IoT. So there is a need to develop new cryptographic algorithms or optimized the existing ones for battery operated IoT devices.

4.2 Key management

Key management is an important and most mentioned research problem in all cryptographic algorithms. Researcher had proposed many solution to this problem [36], [37], [38]. These solutions are somewhat applicable to other networked systems but these are not suited to IoT system because of large scale connected nodes at device layer of IoT architecture. Therefor key management in IoT system is a major research challenge and need more attention to find an ideal solution.

4.3 Denial of Service

Denial of service attack may be more overwhelming in IoT as it can cause in loss of lives if launch successfully on smart cars IoT application [5]. DDoS detection and mitigation solutions for traditional network systems may not   be applicable to IoT system because in IoT we cannot allow even
10 attack messages to sensor nodes before detecting the DoS attack and blocking it because of battery operated resource constrain sensor nodes. Solutions to denial of service detection and mitigation [39] [40] are not effective

and still need attention to design efficient solutions for DDoS detection and mitigation.

4.4 Authentication and Access Control

IoT is focusing on Machine to machine (M2M) mode of communication [18]. For such communication nodes authentications is very important for insuring security and privacy. When two or more nodes are communicating with each other for a common objective they should authenticate each other first in order to block fake node attack. However there is no efficient authentication mechanism for massive number of IoT devices. Which creates a security hole and need to be fill.

V. AUTHENTICATION AND ACCESS CONTROL IN IOT

Internet of things security being a sizzling topic for researcher today, there is a myriad of publication indicating security and privacy issues in IoT. Due to huge number of IoT devices and machine to machine communication feature of IoT, legacy

authentication and authorization techniques are not viable for it. Devices must authenticate each other before exchanging any information between them (M2M communication) which is a challenge for researcher due to massive number of devices. Some of the work related to device authentication and access control in IoT are discussed here.

Chen et al. [6] proposed Capability-based access control model for distributed IoT environment. It supports group access by using single token and guarantee end to end security using IPsec. A requester can use a single token for group access (Group of devices that offer common services) to communicate with any device in the group. Network prefix of unique local identifier (ULA) is used as access group identifier. Each device in the group is identified by a ULA. In a group access token the requester puts its ULA and the network prefix of access group. Hence the devices in the group can verify the token using its ULA and prefix in the token. It can also provide access control based on requester ULA in the token.

The existing standards like TLS and PKI addressed the first three domains of security i.e. confidentiality, integrity and authentication. However access control require attention. As in multi-agents system different agents have different roles, they require different access levels. Rivera et al. [7] proposed the use of User-Managed Access model, which is profile of OAuth 2.0 and provide different access levels to different agents.

OUADDAH et al. [9] proposed Novel access control framework for IoT environment called "SmartOrBAC" which is based on OrBAC model. This model used web services (RESTFUL approach) to enforce the security policies. Organization based Access Control (OrBAC) have some limitations like, it works better in Centralized system, it does not address the collaboration between Organizations and sub organizations and OrBAC does not translate the security policy in to access control mechanism.

Therefore to address these limitation of OrBAC, SmartOrBAC which is an extension of OrBAC is proposed. SmartOrBAC uses web services to ensure secure collaboration between different organizations. They also emphasis on using RESTFULL API for exchanges between organization as it uses a light mechanism.

The interaction between the organizations are defined by agreement between the organizations. The organizations together defined the access rules according to OrBAC format. In SmartOrBAC the contract is not done priori but it can be done on the fly in a spontaneous and dynamic way. SmartOrBAC provides efficient access control for collaborative entities with low power and energy constrained scenarios like such as IoT.

Gaikwad et al. [10] used three level secure Kerberos authentication for smart home system using IoT. It uses secure hash algorithm SHA 1 and advance encryption standard (AES)for security. However neither Kerberos is sustainable solution for authentication nor AES is practical for constrain IoT devices.

Periera et al. [11] proposed Service level access control framework for power constrained devices. The framework allows per service fine grained access control. It merge the idea of Kerberos and RADIUS access control systems for reliable access control framework. It uses the best features of Kerberos, Constrained Application Protocols (CoAP) and RADIUS to create a low power platform for Access control and authentication aspects. The CoAP client get the ticket from the CoAP server, and use this ticket in each future CoAP request. There are Two Steps for Authentication and second for Access control. The user is first authenticated based on credentials like shared key, password or other validator. On successful authentication the CoAP-NAS is informed about the users and its permission, time out of ticket, group etc. CoAP-NAS send a ticket to the user for future requests. In access control step the server will only respond with the correct message if the request message have a valid ticket otherwise it will generate an error message.

A lightweight, secure and scalable Threshold Cryptography based Group Authentication (TCGA) scheme is presented by Mahalle et al. [12], which verify the identity of all nodes in group communication in IoT. Group authentication reduces the overhead of handshake which ensures the less resource usage and help in saving power. This scheme is secure against man in the middle attack.

Panwar et al. [13] proposed security mechanism for IoT using digital certificates with datagram transport layer security (DTLS). For secure communication in IoT, authentication is done by digital certificates provided by certificate authority, which make authentication more robust and replaces the pre- shared key mechanism in DTLS. Client/server authenticated by verifying signature by these steps. 1: client send request to server. 2: Server sends its certificate to client 3: Client verify the certificate by decrypting it with server's public key. 4: after verification, client sends its own certificate to server. 5: server verifies with same procedure and then they can start communication.

Santoso et al. [31] proposed a scheme to ensure strong security for smart home system. The proposed system is based on AllJoyn framework, and uses Elliptic Curve Cryptography for authentication process. System runs on Wi-Fi network and there is Wi-Fi gateway node which is responsible for initial system configuration, authentication of IoT devices and provide mean for user to control the system by mobile device using android application. Authentication process consist of two steps: Mobile device to IoT device (user loads the identity and pre shared key and after mutual authentication home credentials are shared to IoT device) and gateway to IoT device (IoT device connects to gateway and gateway authenticate it by using information send by mobile user device).After this encrypted communication take place.

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: **www.ijircce.com**

Vol. 7, Issue 10, October 2019

TABLE 2
Comparison of Authentication and Access Control Techniques

Ref #	Authentication	Access control	Environment	Security
Chen et al. [6]	Nil	Group Access	Distributed IoT System	IPsec
Rivera et al. [7]	OAuth 2.0	User managed Access Model	Multi Agent IoT system	TLS
Ouaddah et al. [9]	Nil	Organization bases access control	Inter Org anizations	web services
Gaikwad et al. [10]	Kerberos	Nil	Smart Homes (IoT)	AES, SHA1
Beckere et al. [11]	Credentials, shared key, password	Service Level Access control	Nil	DTLS light implementation
Mahalle et al. [12]	Group Authentication	Nil	Wi Fi	Light weigh t cryptographic function
Panwar et al. [13]	Digital certificates	Nil	Nil	DTLS
Santosa et al. [31]	Elliptic Curve Cryptography	Nil	Smart Homes (IoT)	Encryption, Wi Fi
Lee et al. [32]	Light weigh t Cryptography	Nil	Nil	Light weigh t XOR operation
Park et al. [33]	Simple certificates	Nil	Nil	PKI
Zhao et al. [34]	Elliptic Curve Cryptography	Nil	Nil	SHA1

Lee et al. [32] Presents the light weight authentication protocol by enhancing the original RFID system security base on IoT .In the existing RFID protocol authentication is done without encryption which is security flaw. To overcome this problem light weight cryptographic protocol based on XOR method is proposed by which encrypted passwords are used for authentication.

A framework in which permit code structure is created for authentication of IoT devices which simplify the certificate structure and suitable for small IoT devices is proposed by Park et al. [33]. Existing certificate are based on signatures which are hard to apply on resource constrained IoT devices so confirmation code is easy to manage in IoT environment.

Zhao et al. [34] proposed asymmetric mutual authentication scheme for IoT in which authentication is done between terminal node and platform. SHA1 and feature extraction are combine in proposed scheme. By which IoT security is improved as well as reduces the computation and communication cost.

VI. CONCLUSION

Internet of Things security is an active research topic in research industry and academia. It needs further attention and study to explore different security problems in IoT. This paper investigate major security problems in each layer of IoT four layers architecture i.e. perceptual layer, network Layer, support Layer and application layer. The security issues in support layer has not been explored so far in the context of IoT, we present a comprehensive study of support layer security problems in our paper. We also present brief countermeasures to different security challenges to secure IoT systems. We discussed challenges to legacy security solutions in IoT. This paper also present a study of authentication and access control mechanism in IoT. Legacy authentication mechanism is not suitable for IoT devices because these devices are resource constrained and massive in number. Therefore new authentication mechanism is required to authenticate constrained devices in M2M communication. We present a study of the state of the art authentication and access control mechanisms for IoT. This

comprehensive study will guide the researcher as to where efforts should be invested to develop security solutions for IoT.

REFERENCES

[1]. K. Ashton. "That 'Internet of Things' thing." *RFID Journal.* [Online] June 2009. Available: http://www.rfidjournal.com/article/view/4986 (04-04-2014)

[2]. H. Sundmaeker, P. Guillemin, P. Friess, and S. Woelffl´ e. Vision and challenges for realizing the Internet of Things. Cluster of European Research Projects on the Internet of Things, European Commision, 2010.

[3]. J. Gubbi, R. Buyya, S. Marusic, M. Palaniswami "Internet of things (IoT): A vision, architectural elements and future directions." *Future generation Computer Systems [ELSEVIER] Journal* 2013.

[4]. P. Kasinathan, C. Pastrone, M.A. Spirito and M. Vinkovits , "Denial of service detection in 6LoWPAN based internet of things." *9th international conference wireless and mobile computing, Networking and communications.* 2013 Pages 600-607

[5]. A.W. Atamli, A. Martin, "Threat based security analysis for the internet of things." *International workshop on secure internet of things.* 2014 pages 35-43

[6]. B. Chen, Y L. Huang, M G. Unes, "S-CBAC: A secure access control model for supporting group access for internet of things." 2015 IEEE.

[7]. D. Rivera, L. Paris, G. Civera, E. Hoz, I. Maestre, "Applying an unified access control for IoT based Intelligent agent system."*IEEE international conference on service-oriented computing and application.*2015

[8]. S. M. Sajjad, M. Yousaf, "Security analysis of IEEE 802.15.4 MAC in the context of IoT." *Conference on information assurance and cyber security (CIACS).* 2014

[9]. A. OUADDAH, I. PASQUIER, A. ELKALAM, A. OUAHMAN,"Security analysis and proposal of new access control model in the Internet of things." *1st International conference on Electrical and Information Technologies ICEIT*, 2015.

[10]. P. Gaikwad, J. Gabhane, S. Golait, "3 -level secure Kerberos authentication for smart home system using IoT." *International conference on next generation computing technologies* 2015 (NGCT-2015).

[11]. P. Periera, J. Eliasson, J. Delsing, "An authentication and access control framework for CoAP based internet of things." Proceedings , IECON 2014 - 40th *Annual Conference of the IEEE Industrial Electronics Society.*

[12]. P. Mahalle, N. Prasad, R. Prasad, "threshold cryptography-based group authentication (TCGA) scheme for the Internet of things."

[13]. M. Panwar, A. Kumar, "Security for IoT an effective DTLS with public certificates." *International conference on advances in Computer Engineering and application (ICACEA)*, 2015

[14]. 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.*

[15]. A. Perrig, J. Stankovic, and D. Wagner, "Security in wireless sensor networks." Communications of the ACM 47, no. 6 (2004): 53-57.

[16]. L. Li, "Study on security architecture in the Internet of Things." In Measurement, Information and Control (MIC), *2012 International Conference on, vol. 1, pp. 374-377.* IEEE, 2012.

[17]. A. Mpitziopoulos, D. Gavalas, C. Konstantopoulos, and G. Pantziou, "A survey on jamming attacks and countermeasures in WSNs."*Communications Surveys & Tutorials, IEEE 11, no. 4 (2009): 42-56.* [18]. K. Zhao, L. Ge, "A Survey on the Internet of Things Security."Computational Intelligence and Security, *Ninth InternationalConference, IEEE* 2013

[19]. B. Khoo, "RFID as an enabler of the internet of things : issues of security and privacy." In Internet of Things (iT hings/CPSCom), *International Conference on and 4th International Conference on Cyber, Physical and Social Computing, pp. 709-712. IEEE, 2011.*

[20]. 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.*

[21]. A. Mitrokotsa, M. R. Rieback, and A. S. Tanenbaum, "Classification of RFID attacks." Gen 15693 (2010): 14443.

[22]. 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.*

[23]. 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.*

[24]. Open SCAP, http://open-scap.org/page/Main_Page [Online; accessed 25.01.14].

[25]. Open-source TCG Software stack in C. http://trousers sourceforge.net/;2011 [Online; accessed 25.01.14].

[26]. The treacherous 12, Cloud Computing top threats 2016, "Top threats working group, Cloud Security Alliance (CSA)"

[27]. 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.*

[28]. T. N. Jagatic, N. A. Johnson, M. Jakobsson, and F. Menczer, "Social phishing." Communications of the ACM 50, no. 10 (2007): 94-100.

[29]. H. Tobias, et al. "Security Challenges in the IP-based Internet of Things." *Wireless Personal Communications 61, no. 3 (2011): 527-542.*

[30]. C. Ding, L. J. Yang, and M. Wu, "Security architecture and key technologies for IoT/CPS", *ZTE Technology Journal, vol. 17, no. 1, Feb.*

[31]. F. Santoso, N. Vun, "Securing IoT for Smart Home System .", *International Symposium on Consumer Electronics (ISCE) Securing,2015 IEEE*

[32]. J. Lee, W. Lin, Y. Huang, "A Lightweight Authentication Protocol for Internet of Things.", *International Symposium on Next-Generation*

Electronics, ISNE 2014

[33]. A. Park, H. Kim, "A framework of device authentication management in IoT environments*.", *5th International Conference on IT Convergence and Security, ICITCS 2015 – Proceedings*

[34]. G. Zhao, X. Si, J. Wang, X. Long, T.Hu, "A Novel Mutual Authentication Scheme for Internet of Things.", *Proceedings of 2011 International Conference on Modelling, Identification and Control, Shanghai, China, June 26-29, 2011*

[35]. T. Polk, and S. Turner. "Security challenges for the internet of things," http://www.iab.org/wp-content/IAB-uploads/2011/03/Turner.pdf

[36]. S. Shantharajah, K. Duraiswamy, G. Nawaz, "Key Management and distribution for authenticating group communication.*", First international on Industrial and Information System, ISSN: 2164-7011, IEEE*

[37]. W. Abdullah, N. Boudriga, D. Kim, S. An, "An efficient and Scalable key management mechanism for Wireless Sensor Networks.", *16th International Conference on Advanced Communication Technology. ISSN: 1738-9445, IEEE*

[38]. M. Krishna, M. Doja, "Symmetric key management and distributed techniques in Wireless ad hoc Networks.", *Computational Intelligence and Communication Networks (CICN), 2011 International Conference, ISSN: 978-1-4577-2033-8, IEEE*

[39]. P.Kasinathan, C. Pastrone, M. Spririto, M.Vinkovits , "Denial-of-Service detection in 6LoWPAN based Internet of Things.", *9th International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob), IEEE, 2013*

[40]. K.Sonar, H. Upadhyay, "A survey DDoS attack on Internet of Things.", *International journal of Engineering research and Development. Volume 1-, issue 11 (November 2014)*

[41]. A. Francillon, C. Castelluccia, "Code Injection Attacks on Harvard- Architecture Devices." ACM 2008