International Journal of Computing and Network Technology
ISSN (2210-1519)
Int. J. Com. Net. Tech. 7, No. 3 (Sept.-2019)

http://dx-doi.org/10.12785/ijcnt/070302

Internet of Things Security: Issues, Challenges and Counter-Measures

Asifa Nazir[1], Sahil Sholla[2] and Adil Bashir[3]

1.2.3Department of Computer Science & Engineering,Islamic University of Science &Technology, Awantipora, India

Received: 25 May. 2019, Accepted: 13 Augs. 2019, Published: 1 Sept. 2019

Abstract: The Internet of Things (IoT) is one of the most promising technologies that seeks to improve quality of life by providing smart civic amenities. Several smart application domains that are envisaged include agriculture, industry, healthcare, transportation etc. IoT nodes are provided with unique identification numbers having ability to transfer data over the network without requiring human intervention. The ubiquitous communication among IoT devices leads to several security vulnerabilities. This paper presents a survey of security issues, challenges and attacks at different layers of IoT architecture. Moreover, we discuss counter-measures that can be adopted as well as possible future research directions. Security issues along with possible counter-measures are discussed in a layer wise manner with the aim to provide researchers with a bird's eye view of IoT security landscape.

Keywords: Internet of things (IoT), Security, Challenges, Attacks, Counter-measures

1. INTRODUCTION

The term Internet of Things was first introduced by Kevin Ashton in 1999, which actually now grows into reality by interconnecting real world things present in the universe around people to the internet [2]. In recent years IoT has been drawing wide attention of researchers. An annual report on "Internet of Things" was released by International Telecommunication Union (ITU) in 2005 [3].ITU in this report mainly focussed on the RFID and smart computing era that interconnects things at large level globally. IoT applications have been growing rapidly these days due to the presence of technologies like Radio Frequency Identification (RFID) and wireless communicating sensor technology. The RFID technology enables us to uniquely label every single node in network thereby serving as fundamental identification technique in IoT [1].

Internet of Things (IoT) is a system of interconnected computing devices, services and humans provided with unique identification numbers having ability to transmit, share, and communicate data over IoT network without requiring human intervention. IoT has different application domains like healthcare, retail, agriculture, transportation, manufacturing and business. Things in IoT trail an identity method (UID'S) by which each and everything can be identified in an environment of homogenous and heterogeneous devices. Further, every area in IoT is identified by unique IP. With the increased prevalence of IoT there is significant growth in the number of links and networks via which almost everyone connects using devices like desktop, smartphone, PDA, etc. Due to presence of large number of low-cost and small sized sensor devices, technology is putting forward new demands to the Internet technology. Also, IPV6 has made IoT services available more efficiently by accommodating large amount of addresses so as to provide IP address to each thing in IoT network. It has been anticipated that very soon all the smart things that we have around us are going to be internet worked with the aim to provide better services. Therefore, the main aim is to revolutionize the manner people live today by making smart devices around them performing daily tasks whether simple or complex in much more simpler way like smart homes, smart cities, smart transportation, smart grid, smart building, smart environmental monitoring etc. [1].

Since IoT has become a key element of future internet technology, therefore it becomes important to provide satisfactory security mechanism for IoT devices. In IoT context awareness has its own role to play as it refers to the idea of a smart things being aware of their

E-mail address: malikasifa356@gmail.com, sahilsholla @ gmail.com, adilbashir.445@ gmail.com

surroundings, requirements, rules and policies that might be applicable while interacting with other devices. Context awareness provides specific smart services to people based upon their situational (such as location, time, surrounding people or devices, current activity, battery life etc) requirements. Therefore, context awareness tools/techniques need to be developed to enable IoT based devices to be monitored. Researchers are working on Context-Aware security projects so as to provide context-aware security systems for the IoT,that are able to dynamically modify the behaviour of the devices on the basis of the context available. Context-aware systems, collect and hence model context to adapt behaviour of devices with the changing contextual information [4]. Also, most of the data processing in IoT systems may be personal, so security that supports privacy and secured handling of personal information is needed. Even if people claim that their devices are secured, still they are susceptible to various types of security attacks. Hence, security is the critical issue which certainly needs to be addressed at all the three layers (perception layer, network layer and application layer) of IoT devices [5].

Due to the increased number of IoT devices and their heterogeneous nature, security has become an important issue that needs to be addressed at each layer in IoT.Many standards and useful guidelines have been published by different researchers to highlight the security challenges and issues in IoT. Mahmoud Ammar et al. in his paper carried out a comparative analysis of various frameworks based on their architecture, hardware and software constraints [6]. According to their study, security concern of each framework is important and also the protection against each attack at every IoT architecture layer is most contemporary issue faced by IoT.

In recent years, the security issues in IoT and various challenges regarding the security of IoT systems has drawn tremendous research attention. But, yet it is an important challenge today. Edge computing has resulted in many new edge-based security design architectures for IoT security. KeweiSha, et al. presented a detailed literature review of already existing edge-based IoT security solutions including different areas in IoT security like detailed security framework, authentication mechanisms by introduction of firewalls, detection systems and different privacy preserving strategies [7]. HamzaKhemissa and DjamelTandjaoui proposed a lightweight authentication mechanism for energy constrained environment. This mechanism provides both the sensor and the remote user an authentication mechanism consuming limited or low energy. In order to check the truthfulness of information exchanged, use of nonces, exclusive-or operations and keyed-hash message authentication is introduced. Further, their results concluded that this mechanism saves energy thereby providing shield against various kinds of attacks [8].

A security recommendation tool for IoMT solutions has been presented by Faisal Alsubaei and others [9]. An IoMT scenario is the input for this particular tool that species the type of stakeholder, solution, and architecture. List of security issues are identified based upon the input and then accordingly security measures are recommended to address them. Jonathan De C. Silva et al. proposed and hence deployed a novel IoT management platform with user friendly interface called management for devices and networks in IoT (M4DN.IoT).In this paper they have presented a detailed relative analysis of various studied approaches so as to select the best possible approaches among those thereby introducing a new and better IoT network management platform. The solution presented by them is evaluated, demonstrated and hence validated. This network management platform can be used in any electronic equipment like desktop, tablet or smartphone. Moreover its access is available at any location [10].

Industrial internet of things (IIoT) covers essential features of smart systems enriched with new networking technologies like massive dependence on drone technological facilities to have better IoT services. A novel *N*-layered hierarchical context-aware aspect-oriented Petri net model has been presented by Vishal Sharma et al. that evaluates the behaviour of drone by measuring it for possible vulnerabilities using different security guidelines [11]. Location is one of contextual parameter required to achieve smart context-aware IoT systems. Liang Chen et al. presented a survey in which they discussed different solutions that can help in improving the security, privacy and robustness of location–based services in various IoT systems. In their paper they have provided comprehensive overview of various threats and solutions related to global navigation satellite system (GNSS) and non-GNSS. Moreover cryptographic solutions for privacy and security of positioning and location based services (LBS) in IoT are discussed. Finally, advanced strategies regarding the security of positioning solutions and legitimate tools to location-based privacy are presented in detail. The aim of their research is to give new insights to future researchers so as to provide more secure, robust and privacy preserving location-based service system [12].

SchahramDustdar and Florian Rosenberg presented a detailed survey on context aware systems. In this survey paper, they derived a layered conceptual design architecture having different elements common to most

of the context-aware architectures by presenting common architectural principle of context-aware models. The focus of this survey paper is on the design principles of various existing context-aware systems, context-aware middlewares and frameworks so as to ease the deployment of future context-aware applications [13].Ricardo Neisse et al. presented a Model-based Security Toolkit (SecKit) incorporated in the architecture proposed by the iCore Project that facilitates usage control and security of user data in IoT environment. In a Smart city scenario they have showen the application of the SecKit to evaluate its feasibility and hence performance [14].The rest of this paper is organized as follows: Section 2 describes the three layer architectural framework of IoT. In Section 3 general as well as layer-wise security issues are discussed. Section 4 throws light on various security challenges faced by IoT systems. Section 5 gives description of various counter-measures to address security issues and challenges at all the three layers. In Section 6 future directions to have better and secure IoT system are given. Finally, paper is concluded in Section 7.

2. IOT ARCHITECTURE

In order to understand IoT fully, it becomes important to understand IoT architecture which in turn can be described by defining different layers in IoT. Just like in OSI each layer is defined by its roles and the devices (hub, switch, bridge, repeater, router) that are used in that particular layer, similar is the case with IoT. There are different views regarding the number of layers in IoT by various authors. Some authors consider three layer architecture, others have considered four or five layer architecture as their reference. However, according to many investigators IoT mainly operates on three layers termed as Perception, Network, and Application layers as these cover all the other layers involved in four or five layer architecture [15-16].Furthermore, each layer of IoT system must be secured individually because security issues are associated with each of them [17]. Figure1 shows the basic three layer architecture of IoT with respect to technologies and things in IoT comprising each layer.Figure2 shows how three layer architectural framework covers all the other layers. Brief overview of all the three layers is given as follows:

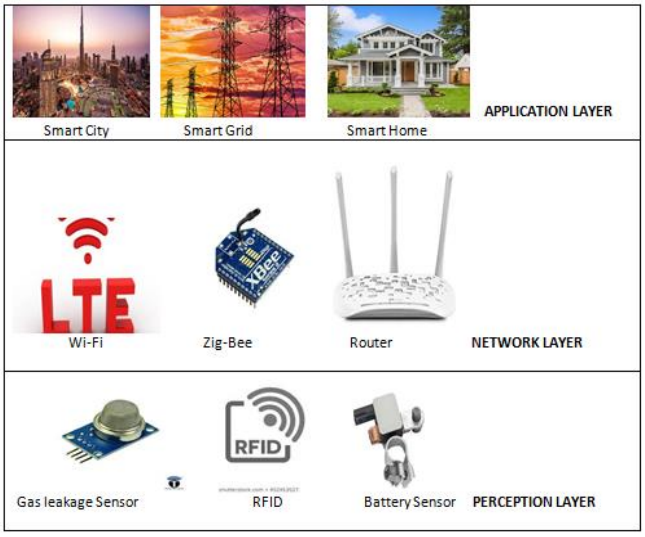

Figure1 Three-layer IoT architecture

A. Perception Layer

This layer is also known as the "Sensors" layer in IoT. The main aim of this layer is to obtain the data from the environment with the help of sensors present in surroundings. In otherwords, IoT node collaboration in local or short range networks is done using this layer. This layer consists of various forms of sensory technologies like temperature sensors, blood pressure sensor, vibration sensors ,heart rate sensor and RFID sensors that helps devices to sense/detect each other. Thus, this layer is responsible for detection, collection, processing of information and then conveying it to the network layer [3].

B. Network Layer

The network layer of IoT is the layer that is responsible for transmission of data over network using different routing protocols. This layer is also responsible for device communication in IoT. Devices like switches, routers, internet gateways or the platforms such as cloud computing etc. are operated at this layer using technologies such as Bluetooth, LTE, Zigbee etc.[18]. These network gateways serve as an intercessor device between various IoT nodes (people, animal, vehicle etc.) responsible for data aggregation, data filtering, and finally transmitting data to and from different sensors to allow communication over the network [19].The processed data is then transmitted over the application layer.

C. Application Layer

The application layer comprises of various applications and amenities that IoT provides. At this layer users interact with the particular smart application like smart city, smart home, smart transportation or smart healthcare application. The application layer must guarantee the confidentiality, authenticity, integrity, and availability of data to the right and legitimate user. Therefore, this layer creates smart environment for application users [20].

3. IOT SECURITY ISSUES

Basic security goals of Confidentiality, Integrity, Availability and Authentication (CIAA) as in any other application also apply to IoT. However, IoT has many constraints such as reduced power and battery resources available which introduce additional concerns. All the layers in IoT discussed above play important role in IoT security. Thus, we need to make sure that all these layers are free from different possible attacks to have secure IoT system. As attacks can be carried out on IoT devices, therefore continuous monitoring of these devices should be done in such a way that integrity of data is maintained. The security issues of IoT can be discussed in two parts: General security issues of IoT and Layer-wise/Layer-specific security issues of IoT as described below:

A. General security issues of IoT

The various security issues that could delay or put difficulties in the rapid deployment and adoption of IoT applications by end-users are discussed below:

1) Confidentiality

Confidentiality is the basic and most important security principle that should be considered to certify that data is secure and hence available to only legitimate users. In IoT user can be human, computer, services, internal objects (devices that are part of the IoT network) or external objects (devices that are not part of the network). Confidentiality deals with various issues that must be addressed such as process of data management, person responsible for manipulation of data, and assurance that the data is secure throughout the process. Also, it should be assured that IoT nodes don't expose the collected confidential information to the neighbouring nodes without proper authorization [18]. For example, in case of patient data or military data related security credentials must be hidden from unauthorized users. To ensure confidentiality on each device all RFID Tags and other identification related information must be encrypted before their transmitted. For example, Blowfish or RSA having lower power consumption with less processing power can be successfully deployed to provide confidentiality on each IoT device [21].Because IoT nodes perform autonomous sensing thereby transferring data to the information processing system over the network, thus it becomes necessary to implement suitable encryption schemes so as to maintain IoT system integrity. Therefore, security mechanisms are must to be devised and implemented to certify secure transmission of data across network [20].

2) Integrity

Since in IoT data is exchanged between different devices, therefore it becomes important to assure the truthfulness of the data; that it is coming from the right sender as well as to certify that the data is not modified while data transmission process. For example, high integrity checks are essential in case of remote patient monitoring system because of the presence of highly sensitive information that must not be modified or lost as that can cause loss of human lives. The integrity feature can be enforced by maintaining end-to-end security, managementof data traffic by the use of firewalls and security protocols. To ensure there is no tampering of sensitive data error detection mechanisms, cyclic redundancy checks, parity checks should be done on each device participating in IoT. Application of WH cryptographic hash functions on each IoT device can help in more secure error detection checks [21].

3) Availability

The users of the IoT should have all the data, devices and services accessible and available whenever required in a timely manner in order to achieve the expectations of IoT system. Also, various components in IoT devices must be strong enough to provide amenities even in adverse situations. For example, a fire monitoring or healthcare monitoring systems would likely have higher availability requirement. Further we need to be ensured that only relevant data is being mined from corresponding databases whether smart healthcare system or any other. The IT people nowadays gather useful information by harnessing the potential of big data that would prove informative to different sectors [20].

4) Authentication

In IoT each object should have capability to clearly identify and hence provide authentication to other objects. Providing authentication between different things in IoT can be very challenging because number of entities (devices, services, service providers etc.) involved is very large especially when devices interact for the first time there should be a proper mechanism of authentication for each and every device [22]. We can achieve authentication between IoT nodes by using various cryptographic algorithms. The interconnected objects in IoT need to authenticate themselves via trustable services which could help in providing secure

communication. Object identification is necessary in IoT and hence each object must be known by its unique ID. This would help to identify fake objects thereby avoiding possible attacks on system. Therefore, in IoT a more secure identity management is needed so as to uniquely recognize the devices.

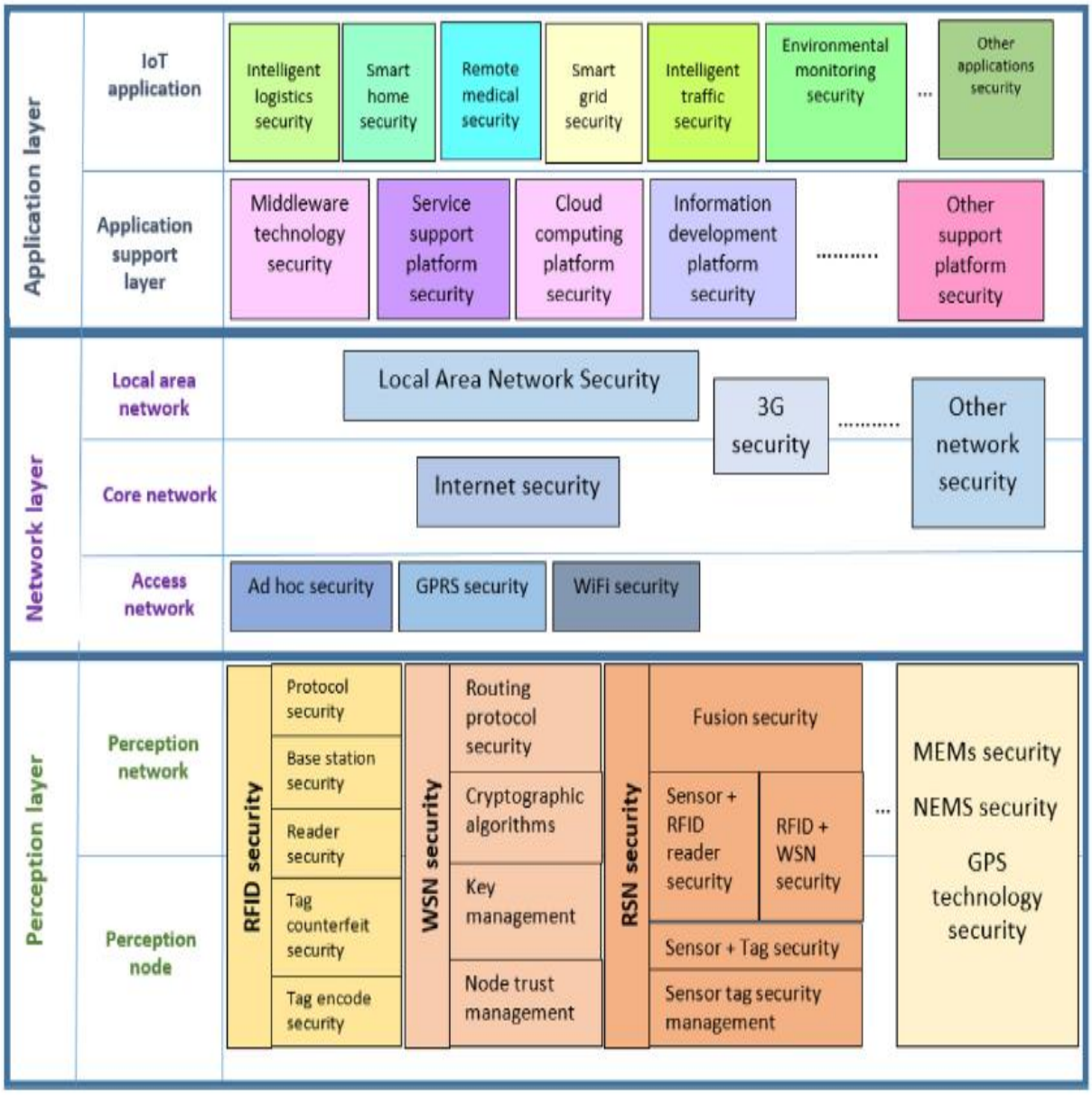

Figure 2: Detailed IoT architecture

5) Security Policies & Key Management System

In IoT it is essential to enforce certain security policies and standards so as to give full assurance that data is managed, secured and transmitted in well-organized manner. Moreover a mechanism to carry out such policies effectively it is must to make sure that every object in IoT is applying the standards, various Service Level Agreements (SLAs) while using various services [23].Sometimes because of the heterogeneous and dynamic nature of devices in IoT policies present may not be applicable. So, enforcement of such policies is necessary to build trust among human users to facilitate scalability of IoT paradigm. As it is known that in IoT to exchange data between different IoT nodes a lightweight key is required, therefore management of key for all architectural frameworks that can ensure trust between devices in IoT is required. Key management is the main issue which needs to be addressed for the security of IoT nodes. Key management includes generation, distribution, storage, updation and destruction of secret key [20].

B. Layer-Specific Security issues of IoT

All the three IoT layers are prone to security vulnerabilities and hence attacks. These can be active, or passive, and can originate from sources outside IoT network or from the sources inside IoT network. An *active* attack actually modifies the data thereby directly stopping the service, while the *passive* kind eavesdrop IoT network information without modifying its service. An in-depth scrutiny of security issues with respect all the three layers in IoT are discussed below:

1) Perception Layer

There are various security issues with respect to perception layer of IoT. Firstly, the efficiency and capability of wireless signals to withstand while being transmitted through different IoT nodes can be compromised by interference signals. Secondly, because of the dynamic nature of IoT devices mainly consisting of energy constrained components like RFID tags, sensors, bluetooth devices or Zigbee devices making them vulnerable to many sets of attacks [1,17]. Thirdly, IoT nodes are mostly active in external environments thereby giving opportunity to different physical attacks discussed in brief below:

a) Node Tempering

The attacker can cause damage to IoT nodes if he or she have physical access to those nodes by directly substituting the entire node or portion of its hardware or can by electronic means interrogate those to gain access to sensitive information .The sensitive information that can be modified are cryptographic keys or routing table [25].

b) RF Interference on RFIDs

A denial of service attack can be applied by creating and sending fluctuating signals used by RFIDs .These signals thus hinder communication in IoT by interfering with RFID signals on RFIDs [26].

c) Node Jamming on WSNs

Just like RF Interference attack, this attack is alike with the difference that this attack is based on WSNs. Interference with radio frequencies of wireless sensor nodes takes place in this attack thereby jamming signals and hence stopping communication between nodes. Further, if an attacker is successful to jam signals over the IoT nodes, he can then effectively stop services of IoT [25].

d) Malicious Node Injection/Fake Node

In this attack , an attacker adds a new fake/malicious node between two or more nodes and can hence control all the data flow operations to and from IoT system so, can even inject malicious data in the network .This is also known as Man in the middle attack [27].

e) Sleep Deprivation Attack

In IoT most of the nodes are powered by replaceable batteries and are programmed in such a way to follow nap routines to avoid reduced battery consumption problem. However, it is because of this attack nodes keep awaking resulting in more power consumption, causing nodes to shutdown [28].

f) Malicious Code Injection

In order to gain illegal entrance to IoT system an adversary compromises IoT nodes by injecting malicious/fake code to the node [29].

g) Social engineering / Physical attack

This attack is actually a kind of physical attack here an attacker physically interacts with IoT system with the aim of influencing the availability of services. The attacker tries to extract private information by manipulating users of system.

h) Side Channel Attack

This kind of attack uses side channel information like power consumed, time consumed and electromagnetic radiations from sensor nodes thereby attacking encryption schemes [30]. By altering the uniqueness information of IoT devices, confidentiality of this layer can beput into threat and hence broken by

replay attack [17]. Details of different physical attacks are discussed in [17,31,32,33,34].After completion of data processing at perception layer, it then has to pass through network layer where various attacks can hinder the communication process in IoT system as discussed next.

2) Network Layer

In this layer it is not necessary for an attacker to remain physically close to the network, various attacks focussed at this layer are sinkhole attack, RFID spoofing, Denial of service attack etc. In addition, of the remote access mechanisms data exchange between devices gives higher opportunity to an adversary for attacks like eavesdropping, traffic analysis, Man-in-the-Middle attack. Further, the key exchange mechanism in IoT must be protected because once keying material is eavesdropped; security of transmitting channel may get fully compromised. Due to heterogeneity and non-restrictive communication nature of IoT (compatibility issues) strong protocols must be used because in IoT everything is connected so an attacker can extract more information about IoT users thereby using it for illegal activities [15].Therefore, protection of network as well as things in the IoT network is equally important. Brief definitions of possible attacks at this layer are given below:

a) Traffic Analysis Attacks

Because of the wireless characteristics of RFID technologies an attacker sniffs out the confidential information or the data flowing and can therefore easily employ his attack. Data sniffing can be done using various applications such as port scanning application, packet sniffer applications etc. [25].

b) RFID Spoofing

In RFID Spoofing, data transmission information is extracted by an adversary via spoofing an RFID signal and mining information from RFID tag [26].

c) RFID Cloning

In RFID cloning data is copied from victim RFID tag to another RFID tag. Both RFID tags have identical information enclosed but does not duplicate ID, by which distinguish is made between an original and effected tag [17].

d) RFID Unauthorised Access

Due to absence of proper validation mechanisms in RFID systems, tags can be accessed by anybody thereby reading, modifying and even deleting data on RFID nodes [17].

e) Sinkhole Attack

A metaphorical sinkhole is created and all the traffic from WSNs is diverted towards it. In this attack privacy of data is attacker thereby sinking all the data packets from being attaining the destination node [35].

f) Man in the Middle Attack

In this type of attack, an attacker in some way over the IoT network copes to enter between the two IoTnodes, accesses authorized data and violates the confidentiality of nodes by passively monitoring thereby restricting data transmission between those two nodes. The main difference from Malicious Node Injection is that the attacker in this class necessarily needs to be physically there but for Man in the middle attack the attacker relies on communication protocols of IoT system [17].

g) Denial of Service

Overburdening the IoT network with more data traffic bombardment exceeding the capacity of network is done by an attacker resulting in network unavailability for useful services to legitimate users [36].

h) Routing Information Attacks

The routing information can be altered by an attacker via spoofing or replaying routing information thereby spreading it in the IoT network resulting in formation of routing loops, distribution of false error messages, division of network, either shortening or extension of source routes, sinking network traffic [37].

i) Sybil Attack

In Sybil attack a single malicious node (Sybil node) claim the ownership of group of IoT nodes and profess to be those nodes. The damages it can cause are distribution of false information in the network, ruining the WSN election process [38].

j) Heterogeneity problem

Due to non-homogeneous nature of various IoT devices, compatibility and hence interoperability are more challenging issues at network layer [39].

k) Network Congestion problem

Since in IoT systems large amount of sensor data is present and hence large number of authentications must be provided, due to which congestion problem comes into existence. Feasible device authentication mechanism can solve this problem [39].After complete processing of data at network layer, it is then being processed at application layer discussed subsequently.

3) Application Layer

The security at application layer is as essential as at any other layer .Many issues are related to application layer as standard and global policy enforcement are yet to be deployed that will help in efficient development of applications in IoT environment. As it is well known that

different applications are having diverse validation approaches due to which integration becomes difficult to certify data privacy, confidentiality and identity authentication. Moreover, data sharing between things in IoT will be creating more overhead on applications to analyse data thereby having large impact on availability of services. While designing a particular IoT application issues that must be taken in consideration are: the way different users will interact, an amount of information that can be shared and the person responsible for managing those applications [20]. Thus, users must have mechanism to control what data they want to reveal and must have awareness of how, by whom and when data will be used. Attacks possible at this layer are given below:

a) Phishing Attacks

The adversary uses infected mails or phishing networking associates to steal credentials of genuine user and hence gains unauthorized access [40].

b) Malicious Active X Scripts

An attacker sends Active X script to the IoT user via internet making user to run executable active x scripts which results either in complete shutdown or data theft [23].

c) Malwares attack

Trojan horses, worms and viruses are some of the dangerous malwares used by an attacker at application layer that steals data or cause denial of service by exploiting IoT system [41].

d) Distributed Denial of Service

In this attack, an attacker executes DOS or distributed denial of service attack on compromised IoT network via application layer thereby exploiting all the users in system. This attack blocks legal users from application layer and provides full application layer access to attacker manipulating databases and sensitive information.

A layer-wise analysis of different attacks at each layer is presented in comprehensive way in the form of table in Table1.

4. IoT SECURITY CHALLENGES

The major challenges while building particular IoTsystem involve:

A. *Heterogeneity*

In IoT numbers of devices are connected with varying capabilities, complexities, vendors, released versions, using diverse technical interconnections with varying bitrates designed for distinct functions. The data in IoT devices can be text, audio, video in any format and size which needs to have number of acquisition devices gathering and analysing data with varying features. Therefore, protocols in consideration to these parameters must be designed to work on all devices in given context [18]. Also it is known that environment in IoT is always changing, hence optimal cryptographic system is needed which would efficiently provide unification of devices [39].

B. Scalability

Another major challenge is the scalability of the IoT, because every new day novel devices get associated with IoT network. It involves issues like addressing/naming conventions, authentication, information management, service management etc. [42].

C. Constrained resources

Energy optimized solution is major constraint of IoT. As many devices are connected via networks, so energy spent for data transmission will be high. The amount of energy used between different devices while transmission process must be optimized to have an efficient utilization of resources. It is thus clear that while developing security solution for particular IoT application intensive care must be taken so as to be confident that minimum resources could be accommodated [43].

D. Localization and tracking capabilities

Various smart things in IoT world must be clearly and uniquely tracked .In smart IoT systems like location aware systems, smart objects must sense the contextual situation autonomously and react to present situations without requiring much human intervention [42].

E. Semantic interoperability and data management

Since in IoT data is exchanged between different devices, thus there should be a standardized format for data exchange to measure interoperability among devices [44].

F. Firmware updates

Every day in IoT world, novel security threats are introduced via internet. So, IoT device users requisite to continuously keep eye on various software updates installed on devices[40,23]. However, all IoT devices may not support live updates. Therefore, IoT device users

may need to unmount some of those devices to install important updates.

G. Implementation of good security algorithms

Due to small size, reduced power and limited memory capabilities (secure IoT requirement) implementation of complex cryptographic algorithms for encryption/decryption process is very challenging. Also, due to these limited capabilities devices may become victim of side channel attacks. It has been researched by various authors that application of lightweight cryptographic encryption ciphers may help in reducing attacks and protecting data in IoT [45].

Table1. Layerwise Attacks on IoT

Name of the Attack	Layer	Solution	Reference
Node tampering	**Perception layer**	To provide physical security in the vicinity of nodes, To have privacy of data at each node, Need for effective authentication and access control mechanisms, Introduction of Light weight encryption protocols for resource constrained devices will help a lot.	[25],[60]
RF interference on RFID's Node			[26]
jamming			[25]
Malicious node injection/Fake node			[27],[39]
Sleep deprivation			[29],[28],[61],[62]
Malicious code injection			[29],[63]
Frequency jamming			[64]-[66]
Side channel attack			[30],[39]
Traffic analysis attack	**Network layer**	To provide secure communication protocol against each attack that can improve performance of IoT system.	[25]
RFID spoofing			[26]
RFID cloning			[17]
RFID unauthorized access			[17]
Routing attacks			[37],[68],[69]
Sinkhole attack			[35],[70],[71]
Man in the middle attack			[17]
Sybil attack			[38],[72]
Denial of service attack			[36]
Congestion and problem of heterogeneity			[39]
Phishing attack	**Application layer**	Introducing secure application code, Using complex passwords, To provide strong access control mechanisms, Continuous monitoring of Databases, Software update checks to protect against malware attacks	[40]
Malicious active-X scripts			[23]
Malwares			[41],[23]

H. Continuous Monitoring and availability

In IoT world devices must always be kept under careful supervision because devices may be compromised, physically damaged or stolen which causes unavailability of services. Further high availability of IoT devices all the time is very essential for real time supervision [42, 43].

I. Trust

Trust is one of the most crucial security challenges to be addressed while building secure IoT system. In order to manage trust various services should be provided like device trust, entity trust and data trust. So, users must be ensured that devices collecting data can be trusted. Also, devices sending data should trust to whom they are sending collected data and the data transmitted must be trustable. One solution to provide trust among participants can be transitive trust mechanism (a user trusting the trusted device of another trusted user) [44, 45].

5. IoT SECURITY COUNTER-MEASURES

It is clear from above discussion that IoT requires security ethics to be imposed at each layer to attain a secure IoT comprehension [24].Security measures at all the three layers; at physical layer for data aggregation, at network layer for routing and transmission purpose, and at application layer to maintain confidentiality, authentication, availability, authenticity and integrity.In this section number of security measures addressing particular security features and privacy goals for IoT is discussed in detail.

A. Authentication control

Zhao et al in 2011 presented an authentication control method between IoT platforms and terminal nodes [46].The basic idea involved in this authentication control scheme is involvement of combination of feature extraction and hashing so as to elude collision attacks.
The property feature extraction has is that of irreversibility which is used to ensure security. Further, it is lightweight which is also good for IoT system because it improves reduced battery problems. The scheme focuses on authentication mechanism when platform attempts to process data towards terminal nodes and not vice versa. Even though this scheme improves security, but the amount of information handled is reduced. Moreover, this method has no practical evidence and works only in theory.

Another method one-time one cipher presented by Wen et al. for authentication purpose at sensor nodes of perception layer based on request reply mechanism. A dynamic variable cipher is enforced using a pre-shared matrix between parties communicating with each other [47].The communicating parties create a random coordinate which serves as the key coordinate. Key coordinate is the one that basically gets conveyed between and not the key itself. The actual key is generated from the random coordinate. With this method information is sent by encoding it with key, key coordinate, object ID and timestamp. The things in IoT communicate with each other by timestamp validation method and can thus deny session in case found invalid. The security of IoT framework can be optimized by changing key coordinates regularly. For large number of IoT architectures the installation of pre-shared matrix must be protected from vulnerabilities.

To address authentication and access control Mahalle et al. presented an authentication mechanism titled Identity Authentication and Capability Access Control (IACAC) between IoT nodes [22]. Their research study attempts to provide both authentication and access control capabilities to attain mutual identity formation. The authentication model proposedby them makes use of public key approach having compatible with movable, distributed and computationally limited nature of IoT devices integrated with existing technologies like Bluetooth, Wi-Fi, Wi-Max etc. Attacks like Man-In-the-Middle attacks can be avoided by enforcement of timestamp authentication messages with each thing in IoT. This approach works in three stages; firstly secret key is generated using concept of Elliptical Curve Cryptography-Diffie-Hellman algorithm(ECCDH), secondly identity formation is done using one-way mutual authentication protocols and finally authentication is applied [48].Using Elliptical Curve Cryptography (ECC), the shared secret key (small size, low computational overhead) is created by combining public key and a private variable. The authentication is granted with access rights, device ID, and a pseudorandom number (result from hashing device ID and access rights) in each IoT device stored. The proposed model not only prevents DoS attacks but also minimizes it as access of resources are granted one ID at a time. Moreover, it is well known fact that devices at perception layer have reduced computational capabilities making it cumbersome to enforce cryptographic security ciphers for security purpose. For this problem, researchers introduced a lightweight authentication protocol to provide security at perception layer [49].If RFID is not secured at the very early stage an adversary can easily enter IoT network by sniffing the Electronic Product Key (EPK) of target tag and program it to another tag. But, the problem can be overpowered by implementation of efficient authentication protocols.

The Capability-based Context-Aware Access Control (CCAAC) is an authorizing model based on a centralized visualization of IoT [50].In this centralized approach a central unit in each activity unit is in responsibility of identity authorization. In this approach a request from delegator is to be decided about granting it to the delegate. However, this approach does not make use of technologies especially designed for context (location, time etc.) dependent environments in IoT. Further, the technical requirements for resource limited contextual environments with various roles involved are missing in this proposed scheme.

An efficient authentication and access control scheme was proposed by Ye et al. for the perception layer of IoT [51]. The main focus of this approach is to provide efficient mutual authentication and secure key establishment between devices in IoT using ECC having small memory and transmission overheads thereby resolving problem of limited resource availability at perception layer of IoT. In this scheme ABAC authorization approach has been

approved as identity access control governance. Information is retrieved based on identity certification attributes using access control policy therby achieving fine-grained access control. However, application of this scheme on resource limited devices is still complex and thus needs further enhancement for better future implementation.

B. Trust Management

Trust is one of the most important security principles that must be established between different IoT devices while they are moving from one owner to other to allow smooth transmission. Individual level access control security mechanisms are established by creating mutual trust between IoT devices from creation to operation and then operation to transmission phase [52].The trust has been established by two methods; first is “key creation method” and second is “token method”. In this method when any novel device enters IoT system it is assigned key creation by privileged system. After this, token is generated by the owner which is then aggregated to RFID identification of particular thing. Because of this mechanism modification of permission by IoT device itself is confirmed when assigned to new owner. Moreover these tokens are modified by owner provided older tokens are provided in advance to replace consent of older tokens.

Another approach discussed in many papers with respect to adaptive or contextual learning is based on situational information. Abie H. et al. presented an Adaptive Security and Trust Management solution (ASTM), the main idea of their solution is to adapt the dynamically changing environmental situations and learn to make changes according to contextual information in hand. However, limitation of this method is that it is more abstract concept rather than certified and implementable for IoT environment [46,53,76].

Glior and Wing proposed a trust model for IoT heterogeneous environment composed of humans, devices involving computable as well as behavioral trust concepts. Their main focus in this research study is to reinforce trust methods by means of behavioral trust so that interest of people in different networks (social networking sites, online games etc.) is boosted. Moreover this model takes into account participation of novel users in networks and trust in this model is accomplished according to the inclination of user towards particular interest. Model takes into consideration users trust by demonstrating how behavioural trust is beneficial to build trust between humans and machines [54].

Atzori et al. presented a new approach for social network of smart IoT objects based on nave model of social associations named Social IoT (SIoT).Authors defined a social network of intelligent objects just like social network for people referring to social relationships between objects. An independent standard model for trust management in SIoT was build by M.Nitti et al. who got inspiration from research studies made in P2P networks. The basic rule for trust value computation of their model is experience of IoT node and context of their neighbours. A feedback system is developed by authors to scrutinize the significance trust value by merging the trustworthiness and centrality of nodes participating [55].

Caminha*et al.* proposed a smart trust evaluation scheme using Machine Learning. This scheme mitigates the on-off attack which threatens the trust value of node [56]. Further trust management might be able to supplement the authentication issues like attacks from corrupted nodes. Zhang et al states that Trust-Based Access Control model (TBAC) to compute trust for access control is relatively new and has been implemented in commercial applications [73].

C. Heterogeneity management

In IoT it is essential to have autonomous centralized /federated architectural system to prevail over the incompatibility issues of various devices, encoded computer instructions and wireless sensor devices. Definition recommended by one of the paper for federated IoT architecture based upon which delegation model is presented [52].This model takes into consideration key IoT features like scalability and suppleness of system. The research conducted by Neisse et al. addressed various issues in IoT by incorporating a security toolkit named SecKit with the MQ Telemetry Transport protocol [57].

A framework called "Secure Mediation GateWay (SMGW)" for perilous architectures have been presented in [58].This model can realize all the pertinent information from distributed nodes. The presented approach is generalized concept of IoT for any kind of distributed architectures and can remove heterogeneity of heterogeneous nodes (electrical, mechanical, telecommunication). Inspiration from the presented approach follow-up of another centralized approach has been proposed by offering the framework for Smart Home based on the SMGW [19].

A standard called IEEE 1905.1 for smart digital home networks with heterogeneous technologies specifying abstraction layer to veil the diversity of media access control topologies [56].By using this protocol an interface is provided to home networking technologies with the aim that integration of data link and physical layer protocols including IEEE 1901over power lines, Wi-Fi/IEEE 802.11 over RF bands and Ethernet over coaxial cables can coexist together.

Various protocols have been presented to address interoperability issue still numerous elucidations of the same standard implemented by diverse parties portrayed a challenge for interoperability [73].In order to avoid such uncertain ambiguities, interoperability analysis between products in ETSI test-bed resulted helpful. PROBE-T_{14} , a research project targets to declare the interoperability of authenticated IoT solutions conducting different interoperability tests like CoAP,6LOWPAN,IoT semantic interoperability.

The general counter-measure for success of IoT technology is the awareness about importance of security of IoT system among people. Various researchers have given explanation regarding the significance of securing IoT and outcomes of not securing IoT. Various IoT devices like SCADA devices, web cameras, traffic control devices and printers were easily accessed by researchers using either default or no- password at all. The results obtained were very fascinating which revealed that many of these IoT things were easily accessible using default or no-password at all. Their analysis proved that if people were not given awareness about using strong passwords and better security protocols then using smart IoT systems will prove critical for them. Table 2 gives a detailed summary of security issues with their corresponding counter-measures.

Table2: Security issues with corresponding Counter-measures

Security issue	Effected layer	Counter-measure	Corresponding Counter-Measures
Trust	Perception Layer	Trust management	[52],[54],[55] ,[56],[73]
Heterogeneity	Network Layer	Heterogeneity management	[74],[19],[57], [56],[73]
Authentication and Access control	Application Layer	Authentication control	[46],[47],[22], [49] ,[50], [51]

6. FUTURE DIRECTIONS

In recent years IoT has been seeing speedy growth in the fields like Smart Pollution Monitoring Systems, Smart Medical Systems, Smart Transportation System and many more. It has been estimated by various analysts that the number of things connected via IoT will grow rapid speed up to 26 million units by 2020 [19].It is thus eminent to address various security challenges in the world of IoT . Future directions for researchers to achieve better and advanced IoT security paradigm are discussed as below:

IoT network involves heterogeneous devices, amenities and protocols to achieve common goal which is connectivity. In order to achieve bigger IoT framework by integrating a network of IoT frameworks (formation of smart town by integrating small smart homes), a need of standard architecture is required that must be ensured to be followed worldwide from large to small level of IoT realization. Therefore, to support wide range of humans, things and services in IoT well defined standard architecture is must. It is known that uniqueness management in IoT is done by exchanging identity information between various communicating IoT devices for the first time. But this process of identification is vulnerable to several passive attacks which can further lead to Man-in-the middle attack and can hence expose the whole system.So, a need of predefined identity management hub is must to supervise the connection process of devices by application of several cryptographic approaches. An accommodation of session layer in IoT architecture for opening, managing and closing connections will help in easing communication between heterogeneous devices. So, development of protocols which can address such matters is must.

For successful implementation of IoT with large number of devices into consideration, IPV4 will certainly not be able to accommodate large number of IP identifiable objects. Because of this reason people now prefer IPV6 which has ability to support 3.4 $x10^{38}$IoT devices. However, such large quantity of devices will generate high amount of traffic resulting in more deferments and increased bandwidth prerequisite. The new generation of communication (5G technology) is expected to provide speed between 10-800Gbps, which when compared with present 4G technology having 2-1000Mbps speed implies that 5G must be capable of handling huge traffic generated by millions of IoT devices. Moreover, 5G technology is expected to accommodate both IPV4 and IPV6 provided with IP translation framework (IPV4/IPV6). The application of 5G technology will be demarcated by numerous technologies currently present and those under development phase like Software Defined Network (SDN), Heterogeneous networks (HetNets) etc. each with their own security challenges [59].

7. CONCLUSION

In this paper we presented a detailed survey on various security attacks possible on IoT system. We have considered the three layer IoT architecture and based on that we examined different attacks possible at each layer with possible counter-measures. Security issues to be addressed in general as well as at each layer have been discussed. Overall this paper presents acomprehensive overview of attacks possible at each layer with possible counter-measures to address corresponding issues. Further, future directions of this research includes standard architectural styles, proper way of managing identity, introduction of session layer in architecture and presence of high speed technology to support huge number of users. This survey paper will help new researchers to get future insights so as to have better future implementation of IoT systems considering different security parameters in advance.

ACKNOWLEDGEMENT

This research work is funded under the seed grant initiative of TEQIP-III project currently being implemented at Islamic university of Science and Technology, Awantipora, Jammu and Kashmir.

REFERENCES

[1] M. Abomharaand G. M. Koien, "Security and privacy in the Internet of Things: Current status and open issues," in Int'l Conference on privacyand Security in Mobile Systems (PRISMS),pp. 1-8 ,2014.

[2] K. Ashton, "That 'internet of things' thing ",RFID Journal 22, Vol 7, pp.97-114,2009.

[3]Srivastava, Lara, and T. Kelly."The Internet of Things",International Telecommunication Union .ITU Internet Reports 2005.

[4] Guanling, Chen and David Kotz, "A Survey of Context-Aware Mobile Computing Research", Dartmouth Computer Science Technical Report ,2000.

[5] Bouij-Pasquier, Imane, AbdellahAitOuahman, AnasAbou El Kalam, and Mina Ouabiba de Montfort. "SmartOrBAC security and privacy in the Internet of Things", In 2015 IEEE/ACS 12th International Conference of Computer Systems and Applications (AICCSA), pp. 1-8., 2015.

[6] Mahmoud Ammar , Giovanni Russello and Bruno Crispo ," Internet of Things: A survey on the security of IoT frameworks", Journal of Information Security and Applications ,Vol. 38, pp. 8–27,2018.

[7]KeweiSha, T. Andrew Yang,Wei Wei, and SadeghDavari," A Survey of Edge Computing Based Designs for IoT Security", Digital Communications and Networks, Vol. 7,pp 18734-18748,2019.

[8]Khemissa, Hamza, and DjamelTandjaoui. "A novel lightweight authentication scheme for heterogeneous wireless sensor networks in the context of internet of things." In 2016 Wireless Telecommunications Symposium (WTS), pp. 1-6.IEEE, 2016.

[9] Faisal Alsubaei, Abdullah Abuhussein, and SajjanShivai,Ontology-Based Security Recommendation for the Internet of Medical Things",IEEE,Vol. 7 ,pp48948-48960, 2019.

[10]Jonathan De C. Silvai, Joel Joe P. C. Rodrigues KashifSaleem , Sergei A. Kozlov , and Ricardo A. L.Rabelo,"M4DN.IoT-A Networks and Devices Management Platform for Internet of Things", IEEE,Vol. 7,2019,pp. 53305-53313.

[11] VishalSharma,GauravChoudary, Yonghoko, and IlsunYou,"Behavior and Vulnerability Assessment of Drones-Enabled Industrial Internet of Things (IIoT)",IEEE,Vol. 6,pp. 43368-43383,2018.

[12] Liang Cheni, SaranThombrei, KimmoJarvinen, Elena SimonaLohan and others, "Robustness,Security and Privacy in Location-Based Services for Future IoT: A Survey",IEEEAccess,Vol. 5,pp. 8956-8977,2017.

[13] SchahramDustdar and Florian Rosenberg," A survey on context-aware systems", Int. J. Ad Hoc and Ubiquitous Computing, Vol. 2, No. 4, pp. 263- 277,2007.

[14] Ricardo Neisse, Gary Steri, Igor NaiFovino, GianmarcoBaldini," SecKit: A Model-based Security Toolkit for the Internet of Things",Computers and security,Vol.54,60-67,2015.

[15] K. Zhao and L. Ge, "A survey on the internet of things security," in Int'l Conf. on Computational Intelligence and Security (CIS), pp.663-667,2013.

[16] L. Atzori, A. Iera, G. Morabito, and M. Nitti, "The social internet of things (siot)–when social networks meet the internet of things: Concept, architecture and network characterization,"Computer Networks, Vol. 56,No. 16, pp. 3594-3608,2012.

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

[18] R. Roman, J. Zhou, and J. Lopez, "On the feature and challenges of security and privacy in distributed internet of things," Computer Networks, Vol. 57,No.10, pp.2266-2279, 2013.

[19]Leo, Marco, Federica Battisti, Marco Carli, and Alessandro Neri."A federated architecture approach for Internet of Things security."In 2014 Euro Med Telco Conference (EMTC), pp. 1-5, 2014.

[20] Matharu, Gurpreet Singh, PriyankaUpadhyay, and LalitaChaudhary. "The internet of things: Challenges & security issues." In 2014 International Conference on Emerging Technologies (ICET), pp. 54-59., 2014.

[21] Andrea, Ioannis, ChrysostomosChrysostomou, and George Hadjichristofi. "Internet of Things: Security vulnerabilities and challenges",In 2015 IEEE Symposium on Computers and Communication (ISCC), pp. 180-187, 2015.

[22] Mahalle, Parikshit N., BayuAnggorojati, Neeli R. Prasad, and Ramjee Prasad. "Identity authentication and capability based access control (iacac) for the internet of things." Journal of Cyber Security and Mobility ,Vol.1, No. 4 ,pp309-348,2013

[23] H. Tobias, et al. "Security Challenges in the IP- based Internet of Things." Wireless Personal Communications 61, Vol. 61,No. 3 , pp.527-542,2011.

[24] 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), London, pp. 336-341,2015.

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

[26] Li, Hong, Y. Chen, and Z. He. "The Survey of RFID Attacks and Defenses ", 8th International Conference on IEEE Wireless Communications, Networking andMobile Computing (WiCOM),pp. 1-4,2012.

[27] 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.

[28] O. Brun , Y. Yin , E. Gelenbe , "Deep learning with dense random neural network for detecting attacks against Iot-connected home environments", ProcediaComput. Sci. 134 , pp.458–463, 2018.

[29] 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, pp. 0975- 8887, Vol. 111 ,No. 7, February 2015.

[30]Zulkifli, M. Z. W. M., and Zaid W. Mohd."Attack on cryptography." Comput.Secur, Vol.12, No.5 ,pp33-45, 2008

[31] 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.

[32] 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), pp. 1-4,2012.

[33] 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.

[34] Liu, Zhe, Patrick Longa, Geovandro Pereira, Oscar Reparaz, and HwajeongSeo. "FourQ on embedded devices with strong countermeasures against side-channel attacks", IEEE Transactions on Dependable and Secure Computing,2018

[35] Md. I. Abdullah, 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.

[36] Wahid, Abdul, P. Kumar, "A Survey on attacks, Challenges and Security Mechanism In wireless Sensor Network", JIRST- International Journal for Research in Science & Technology, Vol. 1, No. 8, pp.189-196, January 2015.

[37] A. Dvir, T. Holczer, L. Buttyan, VeRA - version number and rank authentication in RPL, in: 2011 IEEE Eighth International Conference on Mobile Ad-Hoc and Sensor Systems, pp. 709–714,2011.

[38] K. Zhang , X. Liang , R. Lu and X. Shen , "Sybil attacks and their defenses in the internet of things", IEEE Internet Things J., Vol.1, No. 4, pp. 372– 383,2014.

[39] K. Zhao and L. Ge, "A Survey on the Internet of ThingsSecurity",Computational Intelligence andSecurity-Ninth International IEEEConference,pp. 663-667 , 2013.

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

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

[42] KaziMasumSadique, Rahim Rahmani, and Paul Johannesson," Towards Security on Internet of Things: Applications and Challenges in Technology", The 9th International Conference on Emerging Ubiquitous Systems and Pervasive Networks (EUSPN 2018), Procedia Computer Science, Vol. 141, pp. 199–206, 2018.

[43] NailahSalehAlhassoun, Md Yusuf SarwarUddin, and NaliniVenkatasubramanian,"Context-aware energy Optimization for perpetual IoT-based safe communities", Sustainable Computing: Informatics and Systems,Vol. 22, pp. 96-106,2019.

[44] Harry Chen, Tim Finin and Anupam Joshi, "An ontology for context-aware pervasive computing environments", The Knowledge EngineeringReview, Vol. 18 No.3, pp. 197–207 ,2004.

[45] ArbiaRiahiSfar , Enrico Natalizio , YacineChallal and ZiedChtourou ," A roadmap for security challenges in the Internet of Things", Digital Communications and Networks, Vol. 4 ,No. 2,pp. 118–137,2018.

[46] G. Zhao, X. Si, J. Wang, X. Long, and T. Hu, "A novel mutual authentication scheme for Internet of Things," in Int'l Conference onModelling,Identification and Control (ICMIC), pp.563-566, 2011.

[47] Q. Wen, X. Dong, and R. Zhang, "Application of dynamic variable cipher security certificate in internet of things," in Int'l Conference onCloud Computing and Intelligent Systems(CCIS),Vol. 3,pp.1062- 1066, 2012.

[48] N. Koblitz, "Elliptic curve cryptosystems," Mathematics of computation, vol. 48,No. 177, 203-209, 1987.

[49] J.-Y. Lee, W.-C.Lin, and Y.-H. Huang, "A lightweight authentication protocol for internet of things," Int'l Symposium on Next-GenerationElectronics (ISNE), pp.1-2, 2014.

[50]B. Bayu, P. N. Mahalle, N. R. Prasad, and R. Prasad. "Capability-based access control delegation model on the

federated IoT network", In Proc. of the 15th International Symposium on Wireless Personal Multimedia Communications (WPMC'12), Taipei, China, pp. 604–608. IEEE, September 2012.

[51] Ye N., Zhu Y., Wang R.C., Malekian R., Min L.Q. "An Efficient Authentication and Access Control Scheme for Perception Layer of Internet of Things". Int. J. Appl. Math. Inf. Sci.,Vol. 8,pp.1617–1624,2014.

[52] Y. Xie and D. Wang, "An Item-Level Access Control Framework for Inter-System Security in the Internet of Things," Applied MechanicsandMaterials, Vol. 548,pp. 1430-1432, 2014.

[53] R. Roman, P. Najera, and J. Lopez, "Securing the internet of things," Computer, Vol. 44,No. 9,pp. 51- 58, 2011.

[54] V.D. Gligor, J.M. Wing, Towards a theory of trust in networks of humans and computers, in: B. Christianson, B. Crispo, J.A. Malcolm, F. Stajano (Eds.),Proceedings of the Security Protocols Workshop, Vol. 7114 of Lecture Notes in Computer Science, Springer, pp. 223–242, 2011.

[55] L. Atzori, A. Iera, and G. Morabito, "Siot: giving a social structure to the internet of things", IEEE, Vol. 15, No. 11 ,pp. 1193–1195,2011.

[56] J. Caminha , A. Perkusich , and M. Perkusich ," A Smart trust management method to detect on- offattacks in the internet of things", Secur. Commun.Networks , Vol. 3 pp.1–10 ,2018.

[57] R. Neisse, G. Steri, and G. Baldini, "Enforcement of security policy rules for the internet of things," Int'l Conference on Wireless and MobileComputing, Networking and Communications (WiMob), pp. 165-172, 2014.

[58] M. Castrucci, A. Neri, F. Caldeira, J. Aubert,D. Khadraoui, M. Aubigny, et al., "Design and implementation of a mediation system enabling securecommunication among Critical Infrastructures","Int'l Journal of Critical Infrastructure Protection, Vol. 5,No. 2,pp.86-97, 2012.

[59] X. Duan and X. Wang, "Authentication handover and privacy Protection in 5G hetnets using software-defined networking," CommunicationsMagazine, vol. 53,No. 4, pp. 28-35, 2015.

[60] A. Perrig, J. Stankovic, and D. Wagner, "Security in wireless sensor networks." Communications of the ACM,Vol.47, No.6 ,pp. 53-57,2004.

[61] J. Sherry , C. Lan , R.A. Popa , and S. Ratnasamy , " Blindbox: deep packet inspection over encrypted Traffic", ACM SIGCOMM Comput. Commun.Rev. ,Vol. 45 No. 4 ,pp. 213–226 ,2015.

[62] O. Brun , Y. Yin , J. Augusto-Gonzalez , M. Ramos ,and E. Gelenbe ," Iot Attack Detection with Deep Learning", 2018.

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

[64] Y. Li , L. Shi , P. Cheng , J. Chen , D.E. Quevedo , Jamming attacks on remote state estimation in cyber-physical systems: a game-theoretic approach, IEEE Trans. Automat. Control,Vol.60,No.10 ,2831–2836,2015.

[65] S. Vadlamani , B. Eksioglu , H. Medal , and A. Nandi ,Jamming attacks on wireless networks: a taxonomic survey, Int. J. Prod. Econ,Vol. 172 ,pp76– 94,2016.

[66]Guan, Yanpeng, and XiaohuaGe. "Distributed attack detection and secure estimation of networked cyber-physical systems against false data injection attacks and jamming attacks." IEEE Transactions on Signal and Information Processing over Networks, Vol.4, No. 1,pp.48-59 ,2017.

[67] Jian-hua LI," Cyber security meets artificial intelligence: a survey", Frontiers of Information Technology & Electronic Engineering, Vol.19,No.12,pp.1462-1474,2018.

[68] A. Le , J. Loo , A. Lasebae , A. Vinel , Y. Chen , and M. Chai , "The impact of rank attack on network topology of routing protocol for low-power and lossy networks, IEEE Sens. J. 13 ,Vol.13 ,No. 10,3685–3692,2013.

[69] D. Wu, and G. Hu, "Research and improve on secure routing protocols in wireless sensor networks"networks." In Circuits and Systems for Communications, 2008.ICCSC 2008.4th IEEE International Conference on, pp. 853-856. IEEE, 2008.

[70] S. Sharmila , and G. Umamaheswari , "Detection of sinkhole attack in wireless sensor networks using message digest algorithms", 2011 International Conference on Process Automation, Control and Computing, IEEE, pp. 1–6, 2011.

[71] Cao Q and Yang X. "SybilFence: Improving social- graph-based sybil defenses with user negative feedback",arXiv preprint arXiv,pp.1304-3819 ,Apr 13.

[72] J. Newsome, E. Shi, D. Song, and A. Perrig, "The sybil attack in sensor networks: analysis & defenses." In Proceedings of the 3rd internationalsymposium on Information processing in sensor networks, pp. 259-268.ACM, 2004.

[73] Y. Zhang , X. Wu , "Access Control in Internet of Things: A Survey",Cryptography and Security, Vol. 1 ,pp. 1–15,2016.

[74]B. Anggorojati, P. N. Mahalle, N. R. Prasad, and R. Prasad, "Capability base access control delegation model on the federated IoT network," in Int'l Symposium on Wireless Personal Multimedia Communication (WPMC), pp. 604-608, 2012.

[75] M. Farooq, M. Waseem, A. Khairi, and S.Mazhar, "A Critical Analysis on the Security Concerns of Internet of Things (IoT),"Perception, vol. 111, 2015.

[76] R. Roman, J. Zhou, and J. Lopez, "On the features and challenges of security and privacy in distributed internet of things," ComputerNetworks, Vol. 57,No.10, 2266-2279, 2013.

[77] I. Mashal, O. Alsaryrah, T.-Y. Chung, C.-Z.Yang, W.-H.Kuo, and D. P. Agrawal,"Choices for Interaction with Things on Internet and Underlying Issues," Ad Hoc Networks, Vol.28,pp. 68-90,2015.

[78] Ala Al-Fuqaha, Mohsen Guizani, MehdiMohammadi, Mohammed Aledhari, and MoussaAyyash, " Internet of Things: A Survey on Enabling Technologies, Protocols, and Applications",IEEE , Vol. 17,No. 4,pp.2347-2376,2015.

[79] A. Mitrokotsa, M. R. Rieback, and A. S. Tanenbaum, "Classification of RFID attacks.",Gen,Vol. 15693,No. 14443,2010.

[80] S. Sicari, A. Rizzardi, L. Grieco, and A. CoenPorisini, "Security, privacy and trust in Internet of Things: The road ahead," ComputerNetworks, Vol. 76,pp. 146-164, 2015.

Asifa Nazir She received her bachelor's degree in Computer Science & Engineering from University of Kashmir, Srinagar, J&K in 2015.Next, she received her Master's degree in Information Technology from Central University of Kashmir, Srinagar, J&K in 2018.Currentlly, she is working as a Research Assistant at Islamic University of Science &Technology, Awantipora, J&K in the department of Computer Science & Engineering. Her research interests areIoT, Artificial Intelligence, Network Security, Semantic Web and Wireless Sensor Networks.

Sahil Sholla, is Assistant Professor at department of Computer Science & Engineering, Islamic University of Science and Technology Awantipora, Pulwama ,JK, India .He has received PhD from National Institute of Technology Srinagar, India. His research focuses on technology ethics, security and Internet of Things

Adil Bashir received his Bachelor of Technology (B.Tech) in Computer Science and Engineering from Islamic University of Science and Technology, Jammu & Kashmir, India in year 2011. He has done his Master of Technology (M.Tech) in Communication and Information Technology from National Institute of Technology (NIT) Srinagar, India in 2013. Presently he is Assistant Professor in Computer Science and Engineering department at IUST Awantipora, Jammu and Kashmir, India. His areas of interest are Internet of Things, Wireless Sensor Networks, Embedded Systems and Network Security.