Scientific Review
ISSN(e): 2412-2599, ISSN(p): 2413-8835
Vol. 4, Issue. 10, pp: 80-89, 2018
URL: https://arpgweb.com/journal/journal/10
DOI: https://doi.org/10.32861/sr.410.80.89

Academic Research Publishing Group

Original Research **Open Access**

Architectural Layers of Internet of Things: Analysis of Security Threats and Their Countermeasures

Uwazie Emmanuel Chinanu*
Computer Science Department, Nasarawa State University, Keffi, Nigeria

Onoja Emmanuel Oche
Department of Cyber Security, Federal University of Technology, Minna, Nigeria

Joy O. Okah-Edemoh
Computer Science Department, Nasarawa State University, Keffi, Nigeria

Abstract

A pervasive network architecture that interconnect heterogeneous objects, devices, technologies and services called Internet of Things has prompted a drastic change in demand of smart devices which in turn has increased the rate of data exchange. These smart devices are built with numerous sensors which collect information from other interacting devices, process it and send it to remote locations for storage or further processing. Although this mechanism of data processing and sharing has contributed immensely to the information world, it has recently posed high security risk on privacy and data confidentiality. This paper therefore analyses different security threats to data at different architectural layers of Internet of Things, possible countermeasures and other in-depth security measures for Internet of Things. The paper identifies device authentication on IoT network to be of paramount importance in securing IoT systems. This paper also suggests some essential technologies of security such as encryption for securing IoT devices and the data shared over IoT network.

Keywords: Internet of things; Security threats; Privacy; Countermeasures.

1. Introduction

Presently, the number of objects connected to the internet are more than the people in the world. As long as more objects gain the capability to directly connect and communicate with other objects or become physical representations of data accessible via Internet, this gap will continue to grow geometrically. According to Metcalfe's law, "the value of a telecommunication network is exponentially proportional to the number of its connected users". Recent research conducted by Cisco showed that, approximately 50 billion of devices will be connected to the global network by 2020 which implies 6.6 physical devices per person which is quite a large in number of devices [1].

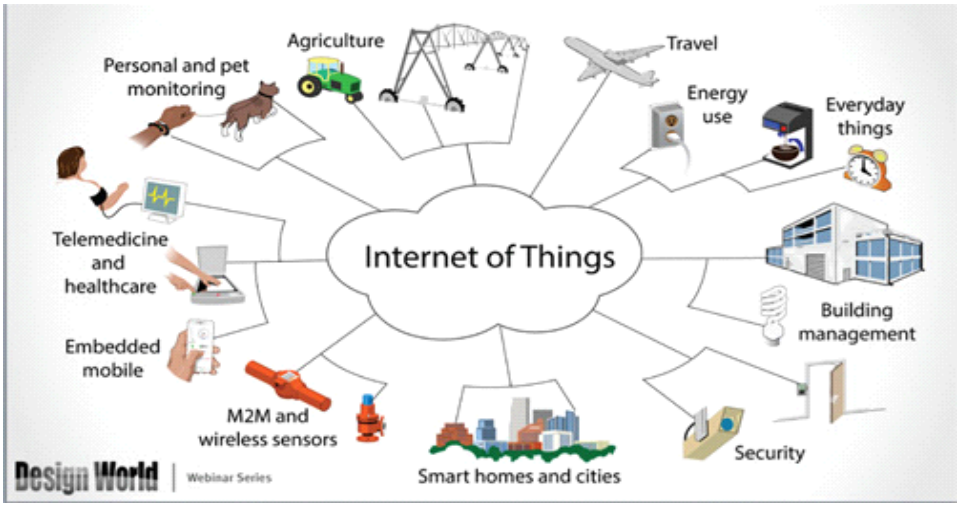
This increase in connected devices and device to device communication has been referred to in many ways: Internet of Things (IoT), Internet of Everything (IoE), Internet of Anything (IoA), Machine-to-Machine (M2M), Industrial Internet of Things (IIoT), to mention but few. The common aspect between all these terms is the connection of new kinds of objects to the Internet in order to build a connected world. In 1999, the term "Internet of Things" was used by Kevin Ashton for the first time in terms of supply chain management [2]. Due to the influence of several and various interpretations of the subject in almost everything from scientific research to electronic marketing, the precise definition of Internet of Things is still a subject of debate. Most often, it is viewed as a paradigm that permits the connection of people to people, people to things, or things to things [3]. In view of device vulnerabilities, attacks and threat analysis, IoT may be considered as the communication between physical objects like mobile phones and some other smart devices that receive and send data and other useful services via public network. The connection to the Internet is possible because of new technologies, such as RFID, wireless networks, Internet Protocol version 6 (IPv6), and fieldbuses [4].

The objective of IoT is to make interconnection between machines. Thus IoT surrounds and connects the real world through these physical devices which are embedded with different types of sensors.

This demands that security of important information on IoT should incorporate different security goals such as identification, data privacy, integrity, availability non-repudiation and confidentiality so that the predicted threats on the development and interconnection of heterogeneous devices will be reduced to the barest minimal as lives function daily with the help of information from smart devices. Most security threat on IoT infrastructures occurred because of no encryption mechanism on data exchange, weak password, insecure data exchange channels and data leakage [5].

Figure 1. Applications of the Internet of Things

*Corresponding Author



2. Security Goals

The security goals of the Internet of things which is the same as information security triad, Data Confidentiality, Integrity and Availability (CIA) suggests that secure connection, and accurate authentication mechanisms should be in place for heterogeneous connections of devices in any network because vulnerabilities, threats and breaches in any of these areas could cause damage to the devices and alter the integrity of information shared via this media [6]. The security goals can be further explained as below.

(i). Data Confidentiality: This entails information is not disclosed to unauthorised users. It results in users' privacy protection. This can be achieved through data encryption which gives room for two way verifications between interconnected devices. Biometric verification can also be implemented at the communicating parties' ends. Confidentiality is also achieved by providing secure connections only to the authorised user. As in the case of IoT, devices ensure that sensor network nodes don't connect to neighbouring nodes and tags don't transmit their data to unrecognized readers [7].

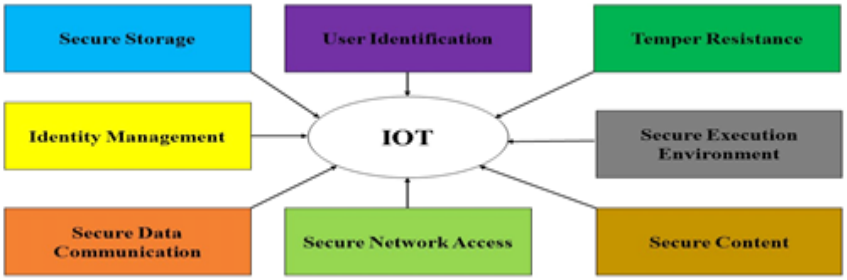
(ii). Data Integrity: This is integrated in information sharing channels in order to protect data from cyber criminals during the communication processes, so that data modification cannot be done by unauthorised users without the system detecting and catching the threat. Data integrity is mostly checked using Hashing, Checksum and cyclic redundancy over the network [7].

(iii) Data Availability: Data availability is one of the major goals of IoT. It therefore means that a mechanism for an uninterruptable access to data from the resources by its user at all conditions should be possible. Data backup operations can ensure Data Availability. Attack such as Denial-of-service (DoS) can be prevented through installation of firewalls on the network in order to ensure data availability to users [8].

Figure-2. Security Goals of the Internet of Things

2.1. Security Requirement for Iot

Figure-3. Security Requirements for IoT [9]



(i). *User Identification*: A security process that ensures proper validation of IoT system user before they use the system [9].

(ii). *Tamper Resistance*: A security requirement that ensures IoT system security even when it is possessed by unauthorised parties. This property can be used to physically or logically probe the unauthorised user [9].

(iii). *Secure Execution Environment*: This focuses on secure environment, code management and runtime environment designed to protect IoT systems against unauthorised software [9].

(iv). *Secure Content*: Also known as Digital Rights Management (DRM), this protects the rights of the digital content used in IoT system [10].

(v). *Secure Network Access*: This provides secure connection to IoT network and services only to authorised devices [10].

(vi). *Secure Data Communication*: This focuses on maintaining security goals of IoT information through authentication of devices, user and entity identity protection, ensuring confidentiality and integrity of shared data and protecting repudiation of communication transactions [9].

(vii). *Identity Management*: This is an administrative security requirement that ensures proper identification of devices on IoT network and controls access to resources based on users' rights and restrictions [9].

(viii). *Secure storage*: This ensures security goals such as confidentiality and integrity of sensitive data stored in IoT systems [10].

3. Iot Architecture

The general architecture of Internet of things is basically made up of four distinct layers based on the scope of this research. These layers are; Perception, Network, Processing and Application layers [11], as shown in the figure below.

Figure 4. IoT Architecture [12]

Each of this architectural layer is specific in it functions and tasks as briefly explained below:

3.1. Perception/Device Layer

This layer is also known as physical or device layer. It collects data obtained from the real world with the support of sensor nodes and other physical devices such as GPS Arduino, Barcodes and RFID [12]. This in turn helps the layer to aid communication between different physical devices. The primary objective of this layer is to provide services to the network and authentication of devices. Devices in this layer possess unique tags which permits strong network connection with most devices using Universally Unique identifiers (UUID) [13]. Information carried from this layer are transmitted and transferred to central processing system.

3.2. B. Network Layer

This layer is in charge of network management, device communication and maintenance of information through different protocols such as MQTT 3.1 and CoAP (Constrained Application Protocol) within the communication in an IoT system. The primary objective of this layer is to collect information gathered by the perception layer and the processing unit and securely transfer them to other layers [13].

3.3 Processing Layer

This layer interconnects (combines) the physical and network layers together. This layer performs intelligent functions such as automatic evaluation of information, processing data based on intelligent computing, and ubiquitous computing function [12].

3.4. Application Layer

This layer supports services (context-aware services) between connected objects in a pervasive way for end users. Information processed at this layer provide a platform to application of IoT which facilitates user needs in different ways such as smart homes and offices [12].

3.4. Attacks at Different Layers

In this section various security threats which threaten the confidentiality of data on each layer will be briefly discussed

3.5. Perception Layer Attacks

Attacks on the perception layer tend to tamper with the physical components of IoT and are relatively difficult to carry out because of the expensive nature of the devices and materials required to carry it out and the attacker needs to have physical contact with the IoT system [12]. Some examples of these attacks are as follows

(i) *Physical Damage*: The attacker interrupts the network of IoT by attacking the devices. This may be due to poor physical security of the infrastructure that hosts IoT system [12].

(ii) *Spoofing*: The target here is the RFID system. The attacker spreads fake information on the RFID system and makes it appear as originating from a reliable and original source thereby capturing information from the network and gaining access to the network completely [14].

(iii) *Malicious Node Injection*: Also known as Man-in-the-Middle Attack tends to take over the communication channel by introducing a new malicious node between the sender and recipient node. The attacker then take charge of data exchange between different nodes in IoT system [15].

(iv) *Node Tampering*: In this attack the adversary tends to cause damages by destroying the sensor node or accessing stored information by physically using intelligent devices to examine nodes on IoT system [14].

(v) *Tag Cloning*: The tags deployed on different devices in IoT systems are mostly visible such that data can be read and easily modified by an attacker that can discover duplicate tag and hence the user cannot differentiate between duplicate and original data.

(vi) *Malicious Code Injection*: This attack is performed mainly by physically injecting a virus code into a node by using plug and play devices in order to gain access and control all IoT system [15].

(vii) *Unauthorized Access to the Tags*: This occurs as a result of poor authentication processes in RFID system thereby leading to modification and complete deletion of data by an attacker.

(viii) Replay Attack: This attack tends to exploit the privacy of the device or perception layer where the attacker modifies or replay node by spoofing the identity and location of the nodes in an IoT system [16].

(ix) *Timing Attack*: This attack targets the confidentiality of an IoT system whereby the attacker gets access of encryption key by monitoring and evaluating the time taken to perform encryption process. Sometimes this might be termed as Side Channel attack when the attacker utilises leaked information on device processing duration to attack the IoT system [17].

(x) *Eavesdropping*: An attacker utilises the RFID wireless characteristic of IoT system to get access to confidential information such as password [18].

(xi) *Social Engineering*: In this attack, an attacker physically communicates with and tricks IoT users in order to gather and gain access to secret information.

3.6. Network Layer Attacks

In this type of attack the attacker's target is the network of the IoT system. Some common examples are:

(i) *Wormhole attack*: In this attack, the attacker receives packets at one network node and tunnels them to another point in the network thereby replaying them into the network from that point [19].

(ii) *Flooding*: The most common flooding attack is DDoS flooding attack. The network is congested with unnecessary tasks and processes thereby flooding the IoT system network with unnecessary packets.

(iii) *Node Replication*: The attacker creates a virtual node by copying the identity of a node and, then sending false messages through random route to slow down and disrupt the network [20].

(iv) *Man-In-the-Middle Attack*: In this attack, the attacker breaches privacy between nodes, access confidential data and sometimes take control over communication by monitoring and interfering with the sensor nodes of IoT system. This attack might be in the form of eavesdropping, routing and replay attack [8].

(ii) *Denial of Service*: This attack involves flooding the network of IoT with much traffic data thereby denying IoT devices of access to network service [21].

(iii) *Traffic Analysis Attack*: This attack can be launched on IoT network using any web browser. Confidential information is accessed from RFID technology due to its wireless characteristics when information about the network is captured. The attacker uses sniffing operation to accomplish the attack [22].

(iv) *Hello Flood Attack*: Is a form of network jamming attack whereby the attacker sends useless messages with the intention of blocking the network channel through large number of traffic.

(v) Sybil Attack: In this attack, neighbouring node in wireless IoT system accepts false messages. The attack tends to claim to hold the identification of many nodes [22].

(vi) *Wormhole Attack*: This involves the relocation of bits and dropping of packets from one node to another or from channel of bits where there is link with low latency.

(vii) *RFID Cloning*: In this type of attack the attacker accesses useful information through mimicking of RFID and copying data from valid RFID to another RFID tag [22].

(viii) *RFID Spoofing*: In this attack, the attacker spoofs the signals of RFID in order to capture the transmission of data and make it to be original thereby transmitting his own data which have original ID of RFID tag hence by showing to be the actual source the attacker can access the IoT system [22].

(ix) *Unauthorized Access of RFID*: The attacker exploits the poor authentication procedure in RFID systems to get access of tags thereby modifying, reading and deleting important data on IoT network [22].

(x) *RF interface on RFID*: This is a form of DoS attack targeted at the RFID, implemented by sending noisy signal across the radio signal thereby stopping all communication in an IoT system [22].

(xi) *Sleep Deprivation Attack*: Most IoT sensor nodes use replaceable batteries as means of power which makes them to operate in sleep routine in order to enhance their battery life span [23]. Whenever sleep deprivation attack is lunched on IoT system, the sensor nodes are unnecessarily kept busy in order to increase the rate of battery consumption.

(xii) *Sinkhole Attack*: The attacker creates a tempting sinkhole for traffic from different nodes of IoT wireless sensor network. The attack targets the confidentiality and privacy of information by obstructing the transmission of packets to their right destination [23].

(xiii) *Routing Information Attack*: This attack tends to change the routing information of IoT network thereby resulting in drop of traffic signal and other network transmission error which in turn causes data not to reach their intended destination.

(xiv) *Selective forwarding*: The attacker restricts some nodes from transmitting or forwarding data packets to required destination for malicious purpose [24].

(xv) *Routing* Threats: This attack occurs when an attacker generates routing loops by altering and falsifying routing information. The network transmission is blocked and the network path is enlarged thereby leading to increase in point-to-point delay [12].

(xvi) *Jamming of node in Wireless Sensor Network*: This is very common in wireless sensor networks. The adversary stops communication by blocking the communication signal after he must have gained access of radio frequencies of wireless sensor nodes of IoT system [16].

3.7. Processing Layer Attacks

This layer is made up of different technologies such as data storage and data processing. One major attack in this layer is cloud attack. Other attacks in this layer are:

(i) *Platform Lower Layer Attack*: The attacker exploits the vulnerability of lower layer IoT data before they are being secured by Platform as a Service (PaaS),

(ii) *Unauthorized Service Access*: The attacker gains unauthorized access to services of IoT systems during data storage and processing thereby deleting and modifying confidential information.

(iii) *Insider Attack*: This takes place mostly within organisations using IoT devices whereby a malicious insider alters and extracts confidential data.

(iv) *Virtualization threats*: The attacker exploits the vulnerability of the virtual machine environment to attack IoT system [24].

(v) *Shared Resources*: Resources sharing platform such as cloud are vulnerable due to resource sharing. Attackers exploit such vulnerability to attack IoT networks.

3.8. Application Layer Attacks

These attacks are used to destroy IoT system using malicious codes such as spyware, virus and worms. Some common examples of software attacks are;

(i) *Application layer software vulnerabilities Attack*: In this attack, Hackers exploit vulnerability in application layer that occur as a result of poor standard code from programmers, one of such is buffer overflow.

(iii) *Phishing Attack*: The attacker uses special software -which are activated or installed by the users unknowingly- to capture login credentials and other important authentication details to gain authorized access to IoT network and system [10].

(iv) *Sniffing Attack*: Here, the attacker introduces a special software called sniffer into the IoT network and system in order to eavesdrop communication and corrupt IoT system.

(v) *Malicious Code Attack*: In this type of attack, the attacker injects malicious codes such as Spyware, Worms, Virus and Trojan Horse into IoT system and network in order to modify data, deny end users of legitimate services and equally hold the device user to ransom.

(vi) *Malicious Scripts Attack*: This is mostly used on web application. Here the attack tends to cut communicating IoT devices via web by shutting down access to necessary applications and services [10].

(vii) *Denial of Service Attack*: The attacker tries to launch attack on all users in a network of IoT system at the same time by injecting denial of service attack on IoT network hence authorized users cannot access network resources effectively.

(viii) *Cryptanalysis Attack*: The attacker aimed at cryptanalyzing the mechanism of encryption in IoT system in order to get the security key combination or get the plaintext from the cipher text without legitimate access [25].

(ix) *Side channel Attack*: Here, the attacker focuses on obtaining the encryption technique in order to hack data by some special technique such as Electromagnetic analysis and power.

(x) *Man In the Middle Attack*: In this type of attack, the attacker intercepts communication channels and signals of IoT system in order to collect useful information and access key exchange process [26].

4. Countermeasures of Iot Achitectural Layers Threats

4.1. Countermeasure of Perception Layer Threats

The Perception provides different security to the physical components of IoT. Some of the Security measures to put in place at this layer are as discussed below.

(i) *Safeguard Physical Infrastructures*: Physical infrastructures that houses IoT system network such as building, cables, masks and antenna should be protected from unauthorised access.

(ii) *Device authentication*: Malicious devices can be kept out of connection to IoT network by authenticating new IoT devices whenever they enter the market [27].

(iii) *Software Verification*: Software authenticity and originality can be verified through the application of cryptographic process such as hash algorithm with the help of device digital signature. This can only be implemented on devices with high processing capabilities [27].

(iv) *Encryption*: Encrypting IoT data using encryption algorithms such as RSA, Blowfish and AES can protect IoT devices against attacks as this turns the data into cipher text so that its content cannot be read by an attacker [28].

(v) *Error Detection Technique*: To avoid altering the content of sensitive information, there is an availability of error detection mechanism on each physical device using cryptographic technique such as hash algorithm which has the ability to utilize low power [29].

(vi) *Data Access Protection*: Encryption schemes such as DSA, RSA, BLOWFISH and DES can provide high data security by preventing the attacker from unauthorized access to data in transit and at rest [14].

(vii) *Risk Assessment*: High data confidentiality and security against breaches in IoT network can be achieved through Dynamic Risk Assessment technique as it provides means of discovering different types of threats to the network. In most cases, RFID runs an auto-kill command of RFID tags whenever an error is discovered with using dynamic risk assessment mechanism. This in turn stops unauthorized access to data [22].

(viii) *Protection of sensitive information*: Privacy of sensitive data is one of the major concern of all security measures in system and information security. A common technique that provides mechanism to hide sensitive information through anonymity of identity is the K-anonymity technique. It provides security for information by hiding its properties such as location and identity

(ix) *Anonymity*: An important requirement for maintaining high data confidentiality as it travels through the network is hiding of private information like data address and location. To achieve this in IoT network, Zero-Knowledge and K-anonymity techniques are normally implemented but K-anonymity technique seems to be the best technique for IoT devices due to its low power consumption rate [29].

(x) *IPSec Security channel*: Encryption and authentication are the two major secure functionalities of IPSec Security channel. These provide security by avoiding Node tampering and eavesdropping through encryption which ensures confidentiality of data and permits a receiver to identify that the sender of the data with a given IP address is fake or real [30].

4.2. Countermeasure of Network Layer Threats

Although the IoT network layer is threatened by different types of attacks, proper counter measures can keep it checked. Some of the counter measures include:

(i) *Active Firewalls*: For filtering the traffic, passive monitoring (probing) to raise alarms, traffic admission control through authentication, and bi-directional link authentication. IoT sensors are very often simple, low-power end devices. Due to the limited functionality of IoT sensors, security processing, such as encryption get handled in hardware [31].

(ii) *GPS location system*: Implementation of GPS system can identify spoofing attack from network layer of the IoT system.

(iii) *Encryption*: Using strong encryption scheme on IoT network nodes and payload of a protocol layer can lower the rate of attack on this layer [31].

(iv) *Data privacy*: Data privacy can be ensured by implementing strong authentication mechanism on sensor nodes to avoid illegal access and data integrity.

(v) *Security aware Ad-hoc Routing (SAR) Protocol*: This protects network of IoT from insider attacks where some security measures are implemented on network packets in order to give an eavesdropper a different result after analysis of received packets.

(iii) *Authentication*: Illegal access of IoT network nodes can be prevented through strong authentication mechanism and implementation of secure encryption schemes. This will also reduce Denial of Service (DoS) which is one of the most common network layer attack to a great extent [32].

(iv) *Routing* security: There is need for secure routing in virtually all applications in sensor networks. In order to secure confidentiality in most routing protocols, different routing algorithms are applied on sensor network on data exchange on different nodes in IoT systems. For routing purpose source routing technique in which transmitted data is stored in packets after analysis, before been sent for processing is applied.

(v) *Hello flood Detection Technique*: Hello message attack in IoT can be prevented by sending a hello message from a node to determine signal strength. If strength is the same as in radio range then routing message and information about a route is received by the receiver.

(vi) *Data Integrity*: Data integrity can be achieved through cryptographic hash mechanism by checking the transmission of data onto the other node. When tampering of data is proved, error correction process can also be applied [33].

4.3. Countermeasure of Processing Layer Threats

Some important concepts of security measures in processing layer are:

(i) *Web application scanners*: Different IoT front end threats can be identified using web application scanner. Other web firewall applications can also be implemented on IoT network to detect potential attacks.

(ii) *Data Fragmentation Redundancy Scattering (DFRS):* DFRS is a simple and fast method of securing essential data on cloud by splitting them into fragments and storing them in different servers. Risk of data theft is at the minimal as data fragment has no useful information about the data.

(iii) *Homomorphic encryption*: In this method of data security, cipher text is re-encrypted before decryption although high computational power is required [33].

(iv) *Encryption*: It helps to overcome side channel attack by firstly encrypting data before sending it to the cloud [25].

(v) *Hyper Safe*: This technique protects memory pages from being altered and also allows restriction of pointing index that monitored data onto the pointer indexes [34].

4.4. Countermeasure of Application Layer Threats

Countermeasures of application layer threats are discussed below:

(i) *Data security*: To avoid unauthorized access to data, encryption and secure authentication mechanism need to be implemented. High confidentiality of data and privacy of entire IoT system will also be achieved via this technique [14].

(ii) *Access Control Lists (ACLs):* Implementing rules that govern access privilege to requests for data will help in monitoring the IoT network thereby ensuring confidentiality of the system and data privacy. ACL can operate by stopping or allowing incoming or outgoing traffic and monitors access requests from many users in the IoT system [33].

(iii) *Intrusion Detection Method*: This security mechanism provides security solutions by producing an alarm whenever there is an intrusion of threat or uncertain activity is performed on the network [35]. The detection process can be achieved through different methods such a data mining technique.

(iv) *Risk Assessment*: An effective security approach can be achieved through implementation of consistent risk assessment procedures. This may in turn enhance the existing network architecture and security plan.

(v) *Firewalls*: This protection mechanism tends to be the most effective especially when authentication, threat analysis, access control list and encryption process fail to stop unauthorized users. Authentication and encryption techniques might fail in a situation where weak password is used but firewall can block threat exploiting such vulnerability. Firewall tends to filter packets through its filtration process hence unwanted packets can be easily blocked [35].

(vi) *Anti-Malware*: Security software such as anti-virus, anti-spyware and anti-adware is essential for the confidentiality, reliability and integrity of the IoT network [36].

IoT Layer	Attack	Method/Target	Countermeasure/Explanation
Perception	Physical Infrastructural Damage	Attacking IoT infrastructure and causing damage to network	Securing physical infrastructures with locks, fire and water resistance, access control and using high quality devices that would not require regular replacement. Providing means of data confidentiality and regular risk assessment
	Spoofing	Spread fake information on RFID	Node to node authentication strong firewall implementation
	Tag Cloning	Tag duplication	Data encryption and device authentication
	Malicious Code Injection	Injecting virus and malware	Installation of anti-spyware and anti-virus on IoT devices.
	Timing Attack	To reverse encryption process and attack data confidentiality	Implementation of secure encryption scheme and complex encryption scheme such as AES and RSA
	Sleep Deprivation	IoT nodes	Device authentication, secure connection with other nodes in IoT system.
	Unauthorized Access to the Tags	To alter and delete information	Secure device authentication with key exchange mechanism. Only authorised device receives and sends data over the IoT network
	Social Engineering	Sensitive information leakage	Maintaining high data privacy and privilege level. Creating awareness and training staff on different forms of espionage.
	RF interface on RFID	Signal distortion	Device authentication. New devices should first be authenticated before communicating over the IoT network
	Malicious Node	Obstructing transmission	Secure booting, using cryptographic

	Injection	process	hash algorithm to validate device software via digital signature on device
	Node Tampering	Damaging Sensor through information alteration	Physical secure design of IoT devices
Network	Wormhole	Bits relocation in IoT network	Implementation of secure routing protocol to provide multiple path between the sender and receiver and checking route presence
	Hello flood	Channel obstruction and traffic congestion/jamming	Hello flood detection cum prevention by sending hello message from a node to verify signal strength and compare its radio range, if similar then accept
	Sinkhole	Node data leakage	Avoid insider attack through security awareness and adhoc routing
	Traffic Analysis	Leakage of network packets and other information	Routing security, secure storage and processing of network packets before data exchange over IoT network.
	RFID cloning	Mimicking RFID to access secret data	Secure authentication of RFID
	RFID Spoofing	Data alteration and transmission control	Implementing GPS system technique to counter the spoof attack.
	Routing Information attack	Destruction of network through routing loops	Encryption routing table
	Jamming Nodes	Obstructing communication between nodes	IPSec-Security channel, node encryption and authentication will ensure data confidentiality
	Routing Threat	Altering routing information	Device authentication and strong firewall implementation
Processing	Data Security Threat	Data modification	Data fragmentation, redundancy and splitting on cloud server
	Application Threat	Data theft	Scanning IoT network using web scanner to discover threat present
	Shared Resources Threat	Control of IoT resources by unauthorised user	Implementing homomorphic encryption mechanism on shared resources
	Virtualization Threat	Damaging IoT resources such as memory	Implementing Hyper Safe technique to protect IoT memory from been altered.
	Man in the Middle Attack	Data interception and theft	Secure data encryption
	Underlying Infrastructure Threat	Lower layer remains unprotected	Store data fragments in different lower layer infrastructures
Application	Software Vulnerability	Exploit software vulnerability and codes	Proper patching and update of software, code debugging and firewall implementation
	Sniffing Attack	Using sniffer to corrupt IoT system	Anti-Malware and system update.
	Script Attack	Shut down access to web applications	Implementing Access Control Lists and Intrusion Detection System
	Cryptanalysis Attack	Hack data by obtaining encryption key	Implementation of strong encryption scheme such as AES and RSA

5. Perforance Evaluation

This paper evaluates and discusses security threats and possible countermeasures to each architectural layer of IoT system. The mechanism, effect and purpose of each attack was elaborately discussed as presented in table 1. In the long run, device authentication on IoT network seems to be of paramount importance if an IoT system must be secure over the internet.

6. Conclusion

IoT surrounds and connects the real world through physical devices which are embedded with different types of sensors that can be attacked. This paper gives an elaborate overview of IoT system in view of its security goals, security requirements, architectural layers & working principle, vulnerabilities, threats and attacks on each

architectural layer and possible countermeasures. In the future, the research will focus on attacks peculiar to IoT on 5G network.

References

[1] Misra, G., 2016. "Internet of things (iot)–a technological analysis and survey on vision, concepts, challenges, innovation directions, technologies, and applications, an upcoming or future generation computer communication system technology." *American Journal of Electrical and Electronic Engineering*, vol. 4.1, pp. 23-32.

[2] Daniele, M., Sabrina, S., and Francesco De, P., 2012. "Internet of things: Vision, applications and research challenges." pp. 1497–1516.

[3] Michael, J. C. and Rush, C., 2013. "Threat Implications of the Internet of Things." In *5th International Conference on Cyber Conflict.* pp. 1-7.

[4] McGibney, A., Rodriguez, A., E., and Rea, S., 2015. "Managing wireless sensor networks within iot ecosystems." *IEEE 2nd World Forum on Internet of Things (WF-IoT)*, pp. 339–344.

[5] Irshad, M., 2016. "A Systematic Review of Information Security Frameworks in the Internet of Things2016 IEEE 18th International Conference on High Performance Computing and Communications." In *IEEE 14th International Conference on Smart City*. pp. 1271-1275.

[6] Malisa, V., Bernard, T. c., Franck, R., Andrzej, D., and Laurent, D., 2014. "OSCAR, object security architecture for the internet of things." In *IEEE 15thInternational Symposium on, Jun 2014.*

[7] Mohsen, N. A. and Jha, N. K., 2016. "A comprehensive study of security of internet-of-things." *IEEE Transactions on Emerging Topics in Computing*, vol. pp, pp. 1-1.

[8] Gang, Z., 2012. "Holistic framework of security management for cloud service providers." *Industrial Informatics (INDIN)*,

[9] Sachin, B., Antonietta, S., Neeli, P., Jaydip, S., and Ramjee, P., 2011. "Proposed Embedded Security Framework for Internet of Things(IoT)." pp. 1-5.

[10] Ma, M., Wang, P., and Chu, C.-H., 2013. "Data management for an internet of things, challenges." In *IEEE International Conference on and IEEE Cyber, IEEE.*

[11] Geng, Y. and Jian, X., 2010. "Security characteristic and technology in the internet of things." *Journal of Nanjing University of Posts and Telecommunications (Natural Science)*, vol. 30,

[12] Andrea, Chrysostomos, C., and George, H., 2015. "Internet of things: Security vulnerabilities and challenges." *Computers and Communication (ISCC), 2015 IEEE Symposium on IEEE, 2015*,

[13] Conzon, D., Bolognesi, T., Brizzi, P., Lotito, A., Tomasi, R., and Spirito, M., 2012. "The VIRTUS middleware, An XMPP based architecture for secure IoT communications." In *21st Inter. Conf.on Computer Communications and Networks, Munich, Germany.* pp. 1-6.

[14] Jin, J., Gubbi, J., Marusic, S., and Palaniswami, M., 2014. "An information framework for creating a smart city through the internet of things." *IEEE Internet of Things Journal*, vol. 1, pp. 112–121.

[15] Leo, M., Battisti, F., Carli, M., and Neri, A., 2014. "A federated architecture approach for internet of things security." In *Euro Med Telco Conference (EMTC), Naples.* pp. 1-5.

[16] Zegzhda, D. and Stepanova, T., 2015. "Achieving internet of things security via providing topological sustainability." In *Science and Information Conference (SAI), London.* pp. 269-276.

[17] Manadhata, P. K. and Jeannette, M. W., 2014. "An attack surface metric Software Engineering." *IEEE Transactions*, vol. 37.3, pp. 371-386.

[18] Soumya, K. D. and Christian, B., 2014. "Securing datatweet IoT architecture elements." pp. 1-3.

[19] Gaitan, N. C., Gaitan, V. G., and Ungurean, I., 2015. "Gradual development of an IoT architecture for real-world things." *2015 IEEE European Modelling Symposium*, pp. 344-349.

[20] Andrea and Lorenzo, V., 2014. "Internet of things for smart cities." *IEEE Internet Things*, vol. 1, pp. 22-32.

[21] Raza, S., Dequenne, S., Chung, T., Voigt, T., and Roedig, U., 2011. "Securing Communication in with compressed IPsec." *DCOSS. IEEE*, pp. 1-8.

[22] Juels, A., 2006. "RFID security and privacy, a research survey." *IEEE Journal on Selected Areas in Communications*, vol. 24, pp. 381- 394.

[23] Lessa, d. S. G., Guimarães, V. T., da, C. R. G., Granville, L. Z., and Tarouco, L. M. R., 2015. "A DTLS-based security architecture for the Internet of Things." *IEEE Symposium on Computers and Communication (ISCC), Larnaca*, pp. 809-815.

[24] Singh, D., Tripathi, G., and Jara, A. J., 2014. "A survey of internet-of-things, future vision, architecture, challenges and services." *Proc. IEEE World Forum on Internet of Things*, pp. 287–292.

[25] Raza, S., Seitz, L., Sitenkov, D., and Selander, G., 2016. "S3K, Scalable security with symmetric keys—DTLS key establishment for the internet of things." *IEEE Transactions on Automation Science and Engineering*, vol. 13, pp. 1270-1280.

[26] Shi, W., 2016. "Edge computing, Vision and challenges." *IEEE Internet of Things*, vol. 3, pp. 637-646.

[27] Sicari, S., Rizzardi, A., Miorandi, D., Cappiello, C., and Coen-Porisini, A., 2016. "A secure and quality-aware prototypical architecture for the internet of things." *Inf. Sys*, vol. 58, pp. 43-55.

[28] Zhang, X., Chang, K., Xiong, H., Wen, Y., Shi, G., and Wang, G., 2011. "Towards name-based trust and security for content-centric network." In *9th IEEE Inter. Conf. on Network Protocols.* pp. 1-6.

[29] Sicari, S., Rizzardi, A., Miorandi, D., Cappiello, C., and Coen-Porisini, A., 2016. "Security policy enforcement for networked smart objects." *Com. Net.*, vol. 108, pp. 133–147.

[30] Neisse, R., Steri, G., and Baldini, G., 2014. "Enforcement of security policy rules for the internet of things." In *IEEE 10th Inter. Conf. on Wireless and Mobile Computing, Networking and Communications.* pp. 165–172.

[31] Aiash, M. and Loo, J., 2015. "An integrated authentication and authorization approach for the network of information architecture." *Journ. of Net. and Comp. Appl.*, vol. 50, pp. 73–79.

[32] Zanella, A., Bui, N., Castellani, A., Vangelista, A., and Zorzi, L., 2014. "Internet of things for smart cities." *IEEE Internet of Things Journal*,

[33] Verma, S., 2017. "A survey on network methodologies for realtime analytics of massive iot data and open research issues." *IEEE Commun. Surveys Tutorials*,

[34] Tahir, R., Tahir, H., McDonald-Maier, K., and Fernando, A., 2016. "A novel icmetric based framework for securing the internet of things." In *IEEE International Conference on Consumer Electronics (ICCE), Las Vegas, NV.* pp. 469-470.

[35] Kothmayr, T., Schmitt, C., Hu, W., Br¨unig, M., and Carle, G., 2013. "DTLS based security and two-way authentication for the internet of things." *Ad Hoc Networks*, vol. 11, pp. 2710 – 2723.

[36] Xin, M., 2015. "A mixed encryption algorithm used in internet of things security transmission system." In *International Conference on Cyber-Enabled Distributed Computing and Knowledge Discovery, Xi'an.* pp. 62-65.