Indonesian Journal of Electrical Engineering and Computer Science
Vol. 18, No. 3, June 2020, pp. 1520~1530
ISSN: 2502-4752, DOI: 10.11591/ijeecs.v18.i3.pp1520-1530

Internet of things (IoT); security requirements, attacks and counter measures

Maria Imdad[1], Deden Witarsyah Jacob[2], Hairulnizam Mahdin[3], Zirawani Baharum[4], Shazlyn Milleana Shaharudin[5], Mohd Sanusi Azmi[6]
[1,3]Faculty of Computer Science and Information Technology, Universiti Tun Hussein Onn Malaysia, Malaysia
[2]Department of Industrial Engineering, Telkom University, Indonesia
[4]Malaysian Institute of Industrial Technology, Universiti Kuala Lumpur, Malaysia
[5]Department of Mathematics, Faculty of Science and Mathematics, Universiti Pendidikan Sultan Idris, Malaysia
[6]Fakulti Teknologi Maklumat dan Komunikasi, Universiti Teknikal Malaysia Melaka, Malaysia

Article Info

Article history:

Received Oct 29, 2019
Revised Dec 31, 2019
Accepted Jan 14, 2020

Keywords:

Attacks
IoT
Security
Sensors
Wireless Sensor Networks

ABSTRACT

Internet of Things (IoT) is a network of connected and communicating nodes. Recent developments in IoT have led to advancements like smart home, industrial IoT and smart healthcare etc. This smart life did bring security challenges along with numerous benefits. Monitoring and control in IoT is done using smart phone and web browsers easily. There are different attacks being launched on IoT layers on daily basis and to ensure system security there are seven basic security requirements which must be met. Here we have used these requirements for classification and subdivided them on the basis of attacks, followed by degree of their severity, affected system components and respective countermeasures. This work will not only give guidelines regarding detection and removal of attacks but will also highlight the impact of these attacks on system, which will be a decision point to safeguard system from high impact attacks on priority basis.

Corresponding Author:

Zirawani Baharum,
Malaysian Institute of Industrial Technology,
Universiti Kuala Lumpur, Persiaran Sinaran Ilmu,
Bandar Seri Alam, 81750 Johor Bahru, Malaysia.
Email: zirawani@unikl.edu.my

1. INTRODUCTION

Internet of things (IoT) is a term referred to network of connected nodes comprising of sensors, software and actuators establishing a smarter life. IoT is a network [1] where devices communicate with each other with no or minimal human participation, here data is continuously gathered and sent to cloud for futuristic analysis and decisions towards better utilization of devices in a smart manner. In the recent years, IoT is under consideration due to its numerous benefits ranging from low power operations, quick response by nodes and applicability to almost every field of life. As stated by Gartner [2], by year 2020 approximately 25 billion distinctively identifiable devices will be part of IoT. Recent developments in IoT have led to smart home, smart health, Industrial IoT and smart transportation for smarter life. In a smart home environment [3] all human belongings are connected to internet, some of them operate on voice commands, monitor and adjust temperature of home and light timings; all in a controlled fashion via IoT. Smart health is an IoT's advancement in healthcare domain; medical records of the patients are kept on one location. As the doctor examines the patient he may append some vital sign monitoring devices to the person and the data from these devices is being gathered and processed in IoT. IoT has become a part of industries as well and the smart industries are monitoring and keeping record of manufactured products their demand and supply. In smart transportation a recent advancement [4] is where passengers can self-check-in using their smartphones.

All these advancements in IoT will lead to a massive network of continuously communicating devices. This will lead to new security threats; opening doors for hackers to get into a system and exploit it for personal benefits. One of the basic reason of device exploitation can be its easy access. Companies are trying to secure their products to the maximum possible extent but there are number of issues being reported on daily basis. Most if not all of these security issues are unaddressed and can lead to detrimental effects. Smart plugs [5] are only a subpart of smart homes, still they are vulnerable to device scanning, brute force, spoofing, and firmware attacks. Poor understanding of the issue is also one of the leading factors towards average security in IoT [1-8] and we believe that good understanding of underlying architecture, security issues, and solutions will lead to improved security in IoT.

In our work we have classified security challenges/issues on the basis of security requirements. These security requirements cover whole system and provide security in seven basic areas. Attacks are further subdivided against each security requirement. Where each attack has a certain impact on system varying from low, medium to high, leading for decisions to guard system on priority basis from high impact attacks.

The rest of the paper is organized as, in section 2 we explained an IoT architecture; for better understanding of the layers and their functionalities. A comprehensive literature review of the security threats/challenges in IoT is present in section 3. This will be followed by conclusion and future work in section 4.

2. IOT ARCHITECTURE

IoT is mainly comprised of number of sensors, actuators and a network which serves as a mode of communication between these devices. Depending upon the different application domains of IoT, the heterogeneity of the devices and the ubiquitous communication (wireless and automatic), necessitates a thorough understanding of the IoT architecture. IoT architecture comprises of four main layers [2, 9]; Perception, Network, Middle-ware and Application layer. These layers are specific to what they do and the devices associated. Architecture here is explained as a structure for physical devices, practical organization, and the mode of communication between devices. IoT Architecture as shown in Figure 1.

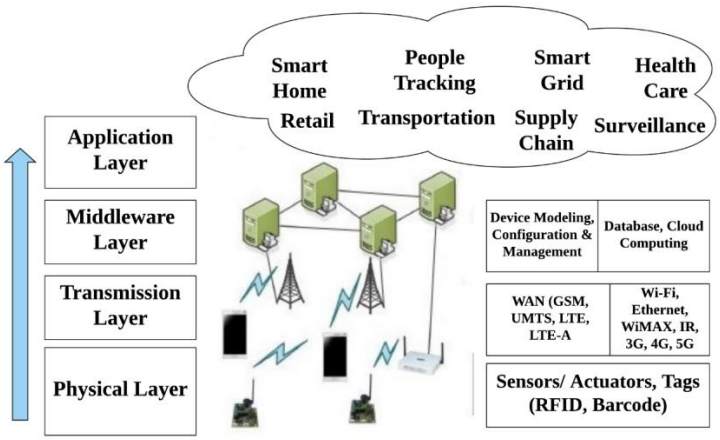

Figure 1. IoT architecture

2.1. Perception Layer

Perception layer is the first layer in IoT architecture and is similar to physical layer of Open System Interconnection (OSI) model. This layer mainly comprises of nodes [2] particularly sensors and actuators which collect data from environment (temperature, humidity, wind speed, location and acceleration). The layer is generally considered as management layer where nodes identification and information collection takes place. Mainly the layer is designed [9] to perceive, gather and process the information and its transmission to network layer.

2.2. Network Layer

This is the layer which serves as a ubiquitous communication channel between different devices. Communication networks comprising of 3G, 4G, Wi-Fi, infrared and WiMAX as the backbone of this layer

and operate cloud computing, internet gateways, switching and routing devices. Network gateways are the points which serve as a basic filter for data transmission between different nodes [2, 7]. This layer mainly transmits the data collected from perception layer to subsequent layers.

2.3. Middle-ware Layer

Heterogeneity of the devices in IoT architecture results into generation of multiple streams of data. This is the point where middle-ware layer works, primarily to serve two basic purposes; service administration and storing the information steams of different underlying layers into database [9]. This layer is also termed as service oriented layer where it decides and monitors different type of services between devices, because this layer has the ability to retrieve, process, compute data and finally an automated decision based on these computations.

2.4. Application Layer

Application layer is the uppermost layer and serves as the point of interaction for user. Generally application layer varies depending upon the services it will offer from smart grid, smart health, smart home, smart transportation to smart industries. Data management done at middle-ware layer facilitates this layer for application management [2, 6].

3. IOT SECURITY ISSUES

All of these above mentioned layers stand pivotal while talking about security because the ultimate purpose of hacker can be shutting down the service or getting unauthorized access to a particular information by attacking a specific layer only [1, 2, 6, 7] The security of IoT network can be broadly classified into two main categories; Technological challenges and security challenges [6]. Technology challenges are the challenges that arise due to heterogeneity and omnipresence of devices whereas the security challenges are those which are primarily due to basic functionalities for system. Technology challenges mainly comprise of scalability, energy, computation, wireless technologies, and distributed paradigm, while security challenges include ensuring confidentiality, integrity, end to end security and all time availability of the services [7]. All these security issues must be understood and fixed for better utilization of IoT.

A system is considered secure when all the security requirements are met successfully [1, 8]. These essential requirements range from confidentiality, integrity, authentication, availability, authorization, non-repudiation to privacy, for each one of them we need to ensure security at a different layer from different threat. Each of the security requirement is meet if the said attacks are understood, their severity and in case of attack any recovery technique are properly listed and available. In the sections given below each of the security requirement is briefly explained along with the summary of attack and countermeasures. Security impact of each attack has been explicitly mentioned, which will help in order to prioritize the attacks and their countermeasures, where the attacks with high impact must be dealt before attacks with low impact. Finally Table 1 has a list of all these security requirements, along with attacks, affected layer, security impact, affected system component, proposed solution and references; as a complete summary of this security survey.

3.1. Confidentiality

Confidentiality prevents any unauthorized access to sensor data in transmission while making it available for those who have authorized access simultaneously [1]. The data reaches to the intended nodes without being accessed by some third party. In order to ensure confidentiality in IoT, cryptographic techniques such as encryption and hashing need to be implemented, keeping in mind that each attack is specific in nature, the IoT layer and its security impact on overall system, so we need different security mechanisms against each attack [8, 10]. Here we discuss each attack in detail and its impact followed by the security measure specific to that attack.

3.1.1. Replay Attack

The identity of one or more nodes are spoofed in this attack. Where one or more devices/ nodes are using same identity in one system. This attack is launched on the perception layer in IoT. This attack mainly harms systems confidentiality as the device is being spoofed and unauthorized access can be achieved. The Impact of the attack is intermediate but it intends to compromise system confidentiality which cannot be taken lightly [6].

The proposed solution states two possible ways; either by a timestamp or by prevention using nonce option, where the values generated will be used for once only, and hence the identity cannot be spoofed [7]. IoT Trust [11] is a platform which is based on software defined network and uses two layer architecture;

object and node layer. Here cross layer authorization ensues node reputation evaluation particularly nodes current state. This approach is good to detect spoofed nodes in IoT.

Table 1. Summary of Classification

Classification	Attack/ Challenges	Affected Layer	Security Impact	Affected System Component	Proposed Solution	Reference
Confidentiality [1], [8], [10]	Replay Attack [6]	Perception Layer	Medium	Device & Data	Introduction of timestamp and nonce options for protecting against replay attacks	[7], [12]
	Man-in-the-Middle Attack [2], [12]	Network Layer	Medium	Data	Hashing algorithms, authentication mechanisms based on signatures, and surveillance of the node behavior	[7]
	Timing Attack [6]	Perception Layer	Low to Medium	Data	Bit checking to remove branches in additive modulus operator	[1], [13]
	Node Capture attack/ Node tempering attack [6]	Perception Layer	Low to medium	Device & Data	Key distribution protocol for node addition and revocation	[1], [14]
	Unauthorized Access to the Tags [2], [12]	Perception Layer	Medium to High	Data	A SVA algorithm is implemented at three layers to ensure secure tag generation and authentication.	[1], [15]
	Unauthorized Access to the Tags [2], [12]	Perception Layer	Medium to High	Data	A SVA algorithm is implemented at three layers to ensure secure tag generation and authentication.	[1], [15]
Integrity [1], [8], [10]	Malicious Data[6]	Perceptio, Application Layer	Low to Medium	Data	Randomized Watermarking Filtering Scheme (RWFS) for IoT	[1], [16]
	Tag Cloning [2]	Perception Layer	Medium to High	Data	Challenge response based authentication protocols	[17]
	Malicious Insider [2]	Middle-ware Layer	Medium to High	Data	RBAC based authorization model	[18]
Authentication [1], [8], [10]	IP Spoofing [7]	Network layer	Medium	Data & Network	Assignment of Active IP address in IoT device and spoofing of IP for IPv4 and IPv6	[7], [19]
	Session establishment and resumption [1], [7]	Transport layer	Medium	Data & Network	BF-IoT based continuous authentication of session	[20], [21], [22]
	Sleep deprivation Attack [2]	Network Layer	Low	Device	Multiple layers as a base for intrusion detection	[7], [23]
Availability [1], [8], [10]	DOS & DDOS attack [2], [24] , [25]	Network, Middle-ware, Application Layer	Medium to High	Device & Network	CEPIDS for attack detection	[19], [27], [28]
	Malicious code injection/ virus,worms, Trojan horse, spyware [2], [29]	Network, Application layer	Medium to High	Data & Network	Signature oriented detection	[29], [30]
Authorization [8]	Identity Spoofing [2]	Perception layer	Medium to High	Data & Device	Localization or channel based detection	[10], [31]
	Spear-Phishing Attack[2]	Application Layer	Medium to High	Data	Guarding system by allowing to use passwords or username for once	[10], [31]
Non-repudiation [1], [8], [10]	Sybil Attack[2]	Network, Perception layer	Low	Device & Network	Sybil attack detection using one time localization	[2], [32], [33]
	Sinkhole Attack[2], [34]	Network Layer	Low & Medium	Network, Data & Device	PRDSA to detect, bypass and identify sinkhole	[34]
Privacy [1], [8]	Insecure software/firmware[7]	Applicatio, transport, network layer	Low, Medium & High	Data & Network	Software updates on regular intervals fixing software /firmware	[35]
	Insecure interfaces[7]	Application layer	High	Data	Constrained Application Protocol (CoAP) implementation	[35], [36]
	End-to-end security[7]	Network layer	Medium	Data	End-to-End Security using session resumption	[37], [38]

3.1.2. Man in the Middle (MIM) Attack

Man in the middle is one of the widely launched attack in wireless sensor networks, here the attacker eavesdrops into the network and tries to get access to confidential data. Initially the attacker is only sniffing the network but at a point when he gets enough knowledge about the system he may impersonate an authorized party. The attack is launched on network layer of the system where data packets are being sent and received. The impact of the attack on system is medium but it effects data confidentiality [2, 12].

The proposed solution states that system can be guarded against MIM by adding proper authentication mechanism which signature based authentication. This mechanism will use digital signatures to authorize all nodes in a system. An external continuous monitoring of the nodes which will help us immune our system from these attacks [7].

3.1.3. Timing Attack

This is another type of eavesdropping where attacker intends to get specific information from the system. The information about the encryption algorithm or full encryption key by carefully monitoring the time of encryption. As this attack is launched on perception layer and the attacker intends to harm data within a system [1, 6].

In proposed solution Ring-LWE (learning with error) is improved to bit checking to remove branches in the additive modulus. By removing branches now there are minimal chances that the key will be compromised as this technique is even secure against chosen plain text attack [13].

3.1.4. Node Capture Attack/ Node Tempering Attack

A perception layer attack where the whole node is captured and tempered to gather information from the system. This is easy to launch because in other attacks the attacker has to get access to system to gather information but here the attacker changes the whole node; as a result the malicious node becomes part of the network which can gather information all the time. The impact can be low to medium which entirely depends upon the application domain of the IoT and the information being sent and received by node [1, 6].

A key distribution protocol for node addition, revocation and fast rekeying is proposed as a solution. Key distribution requires only single message exchange. The proposed technique in addition to security against node capturing attack is also good for devices with low power and low energy [14].

3.1.5. Unauthorized Access to the Tags

RFID tags are an integral part of IoT network. Authorized access to these tags ensures integrity of the system. While if an unauthorized person gets access to the system he may change or delete the tag resulting in loss of confidentiality and integrity of the system [1].

A smart verification Algorithm (SVA) [15] is applied in IoT environment. Here a verification procedure is introduced for authorization of users to access RFID tags in a Quick Response (QR). Encrypted QR codes are compared with original codes in a three layer structure where on first layer a comparison is performed, on second layer values are stored and third layer produces authorized QR codes. Besides protection from un-authorized access, the proposed solution is secure against brute force attack as well.

3.2. Integrity

Integrity is termed as the veracity and reliability in an IoT environment. With the increasing number of devices in IoT, network integrity becomes an important part of system security. Devices in IoT are identified individually and so is the data being transmitted by them, so that when another node receives the data it is found to be reliable. Integrity of the data can be compromised if the received data is not the same as sent or the data gets deleted while traveling on network. So the security must ensure tempering as well as deletion of data. [1, 8, 10] Integrity must be ensured at multiple levels in a system either by proper encryption or access control but specific integrity attacks need special solutions. Here we will discuss attacks that intend to effect system integrity in detail.

3.2.1. Malicious Data

Perception and application layer are vulnerable to malicious data attacks where an attacker injects malicious data into the system, the intention is either to get access to system by doing so or to replace normal data with malicious data. In both of the events the attacker is directly compromising integrity of system data. This attacks is only possible when the attacker can successfully change a node first. This attack effects system's data and its effect can vary from low to medium depending upon the application domain of IoT [1, 6, 8].

Randomized Watermarking Filtering Scheme (RWFS) for IoT is a technique to overcome malicious data injection. At early stages of communication this technique uses en-route filtering to identify and

eliminate malicious data. Homomorphic encryption technique is used to reduce the packet size so that good security can be achieved using less power [16].

a) Tag Cloning

In IoT each RFID tag being generated is uniquely identifiable and these tags are visible and readable by everyone. In tag cloning attack, the same tag is cloned and is made available to authorized users. When the users try to access the original tag they may end up seeing this cloned tag and cannot distinguish between real and cloned tag. This attack is launched at perception layer and its effect may vary from medium to high on overall system [1, 2, 6].

In theory it is quite impossible that a tag is cloned but in practice with minimal this can be achieved. So one of the possible solutions is challenge response authentication protocol. This is a protocol where authentication is performed by a challenge and if the challenge is completed successfully the permission is granted to access the tag else permission is declined. This is effective in case of low power devices because other authentication mechanisms cannot be used for small power [17].

b) Malicious Insider

People inside the organization are considered as the weakest links of the chain when it comes to security. They have access to data depending upon multiple access control levels. Therefore the insiders may end up deleting or tempering original data for personal or any third party's benefits. This security issue can be overcome by implementing good access control mechanisms where not all data will be available to all insiders but only the limited access as per the role of a person in organization. Malicious insiders generally launch attack on middle ware layer and the impact may vary from medium to high [1, 2, 6].

RBAC (Role based access control) is an access control model which will allow access to system based on the role of a specific person. Roles and permission are integral part of this scheme where roles are assigned to users and permissions are assigned to roles. Hence no insider will be able to access confidential information which is not intended to him on the basis of defined role, and when to information is not accessible malicious insiders cannot exploit it [18].

3.3. Authentication

Authentication is a process where different users and devices communicate to validate the originality of device on the basis of predefined credentials. Authentication for small networks is not a problem but as the number of associated devices is increasing in IoT paradigm, manual authentication becomes a problem which ultimately leads to multiple security threats. Authentication must be done using a proper mechanism which is explicit to IoT paradigm [1]. Password based authentication is most common type of authentication but it is merely impractical because of ever increasing number of devices in IoT network. So we need some lightweight authentication mechanism which can be ensure similar security but is designed to keep low power of IoT devices [8, 10]. In this section we will discuss multiple security challenges/ attacks which occur due to poor or no authentication mechanism.

3.3.1. IP Spoofing

In any wireless sensor network, there is a process of node and route discovery prior to transmission which helps data travel over the network. Here only authenticated nodes can participate and the authentication is made possible by end to end communication between devices and each device must acknowledge the neighboring device. Here if any device cannot participate in authentication process it may not be considered part of network and this can lead to non-existence of a device [7]. This attack is launched at network layer where its impact is considered medium.

A dynamic IP address [19] attachment in IoT nodes which can be extended from IPV4 to IPV6 because IPV4 addresses are not enough to meet the future requirements. Simple amendments like IP stack is updated so that it can support exchange messages and avoid using complex cryptographic schemes for authentication.

3.3.2. Session Establishment and Resumption

In IoT network, all devices communicate with each other and the communication takes place once the session is established between corresponding nodes. Sometimes an attacker may hijack this session and start communicating with victim node without being caught. In this way the attacker gets the whole information of a particular node in communication with [20, 21].

BLE (Bluetooth low energy) devices are part of IoT. A frame work proposed on BLE for IoT that is BF-IoT is secure against device spoofing via monitoring continuous work flow. It defends the system by continuously authenticating the identity of a device at the time of session establishment as well as during the session [22].

3.4. Availability

IoT is network of always communicating devices. These devices not only communicate with each other but also transmit bits of data continuously. With increasing amount of data it becomes difficult to ensure device and data availability round the clock [1, 8, 10]. This is where attackers exploit IoT; they damage system availability by launching different attacks. Following are some of the attacks which hurt system availability.

3.4.1. Sleep Deprivation Attack

In IoT most of the sensors are battery operated and hence have limited power supply. In order to extend the life time of such devices, they must follow a sleep routine. In sleep deprivation attack, the nodes are forced to stay up leading to their power drain and finally the node shuts down. When the node shuts down it becomes unavailable where it cannot send and receive data. The best way to keep system safe from this attack is to use multi-layer oriented intrusion detection system [7].

A methodology based on deep learning approach and dense random neural networks is used for online detection of network attacks. This is a predictive technique which gives probability of the network attack by capturing different packets. This technique is equally applicable to all network attacks [23].

3.4.2. Denial of service (DOS) attack and Distributed denial of service (DDOS) Attack

This is one of the most primitive and still widely practiced attack in IoT. DOS is operation oriented attack, where the device is available and active still it cannot respond to network nodes. In this attack the attacker transmits data streams to the attacked node and keeps on transmitting until it exhausts. This also keeps network traffic high and ultimately the authorized nodes cannot communicate with each other. While in DDOS, the attack is launched by continuous flooding of data streams from multiple malicious nodes [2, 24]. All these nodes keep the network traffic high by sending multiple data streams and keep the node busy by responding. Here some legitimate nodes also try to communicate with the node under attack but due to heavy traffic load, their requests are never entertained. This attack can be launched at all layers but the attack at perception layer causes highest damage to the system [25, 26].

Proposed technique is capable of detection and can distinguish between attack and real time traffic. JPCAP is used to capture packets. CEPID (complex event processing intrusion detection) is a system with three layers and each layer is dedicated to perform distinctive tasks; traffic monitoring, packet analysis, event handling and blocking access to the suspected service [27, 28].

3.4.3. Malicious code injection/Virus, Worms, Trojan horse, Spyware

Malicious codes is the generic term for different types of virus, worms and Trojan horses. They intend to harm the system by any mean. Sometimes the attacker injects a malicious code into the system to shut down the whole network which will compromise availability while in other cases this malicious code may get him access to the entire network. Now the attacker can monitor network traffic, nodes and the data being sent and received. Worms can duplicate themselves without human effort and can spread across entire network [13, 29].

One of the most common way to detect a malware or virus in the system is a signature based detection [30]. A malware database has an updated list of all malwares and the system just embeds a malware to perform its comparison with the database. If the results are verified the malware can be detected.

3.5. Authorization

The process of making the information available to authorized users is called authorization. This process is impossible if we do not have proper security measures for devices to let them access required information as per their credentials and limiting them to access information simultaneously [1, 8].

3.5.1. Identity Spoofing

Spoofing is an active attack where the attacker has already got access to the system. The attacker initially stays inactive and only observes network traffic. Upon successfully gathering all the network data, the attacker waits for an anomaly [2, 31]. When a legitimate node stops communication this identity spoofed node takes its place and starts sending signals to neighboring nodes. In this way, the neighboring nodes consider it a legitimate node and start communication which can be detrimental for the whole system.

Two most widely implemented techniques to detect a spoofing attack are localization and channel based detection [10]. Multiple techniques of detection include RSS (received signal strength), AOA (angle of arrival) and TDoA (time difference of arrival), where attack is determined on the basis of transmitted signal location. Meanwhile in any channel based detection we use fingerprints of link signatures to protect and detect attack.

3.5.2. Spear-Phishing Attack

Where most of the attacks in IoT are intended to gather information; they may attack a device or a network to do so. In contrast, Spear-Phishing is the only attack where attack is targeted to a person [31]. Here an email is sent to such a person, who has most, if not all security privileges to the devices and network. This person is tricked to open this email and input his credentials which will be used by the attacker later on. Hence the attacker can get access to the complete system.

One of the best way to guard system from spear-phishing is to familiarize users against such attacks. On technical side security of the system can be ensured to generate a username password combination that can only be used once and can be changed by providing credentials. Using this method will limit the access to the system which is once gained by attacker [10].

3.6. Non Repudiation

Every node in an IoT environment holds a unique identity and one of the purpose of this identity is to trace back the information to the origin. A node cannot deny about a particular information that it was sent by it and this is only possible by assuring non-repudiation or origin. But in IoT environment some nodes might duplicate or use another identity and transmit data, which can lead to serious security concerns [1, 8, 10]. Here we will discuss such issues.

3.6.1. Sybil Attack

This attack is launched by using Sybil nodes and these are the nodes which duplicate and use the identity of other nodes to transmit data. The node is physically present at one location but virtually at more than one locations. Sybil can also be considered as masquerade when it may look like a normal user but it is not. In a normal network each node has to vote for once but during Sybil attack one node may vote for multiple times [2, 32].

Generally the impact of this attack on system is low but its detection is quite difficult. Proposed scheme [33] detects Sybil attack in an environment where we have less probability of detection using one time localization and incurring minimal overhead in terms of storage, communication and computation.

3.6.2. Sinkhole Attack

This is a compromised node attack, here the node makes itself attractive and available to nearby nodes. The fake node broadcasts a fake routing information to the nearby routes and by doing this the traffic of all nearby nodes travels to it. It receives and discards all data while the sender believes that data has been successfully sent. This may result in great energy consumption and heavy network traffic but in reality no data reaches destination [2].

Probe Route based Defense Sinkhole Attack (PRDSA) is designed to sense, locate and sidestep from a sinkhole attack simultaneously. Using multiple routing mechanisms PRDSA effectively identifies a sink and this can be even done once the attack has been launched. This scheme is good in terms of network security and improves lifetime of a network [34].

3.7. Privacy

IoT is a network of heterogeneous devices and the generated data needs to be kept secure from un-authorized access as well as from leakage of any personal information of a human, machine or network. Privacy is a high priority area when talk about the medical application domain of IoT. Where exposure of one's medical record can pose multiple threats. Similarly if an attacker can access a smart homes data, he may be able to predict the daily routine of a person. Here the user must have the right to share the quantity of information to external world [1, 8]. In this way it is important to have better privacy measures and here we will discuss some of the threats to privacy of system.

3.7.1. Insecure Software and Firmware

IoT devices are connected through web and multiple software systems which are part of system [7].These background software are the core point for attacks. In order to ensure system security these software must be updated and upgraded at regular time intervals. The coding languages e.g. XML, XSS, JSON needs to be tested prior to deployment because these issues may penetrate deep down into layers and compromise whole system and make the data available to attackers. Hence proper software testing of all open source software must be done prior to their release and security patches must be introduced post release [35].

3.7.2. Insecure Interfaces

IoT services and their accessibility vary depending upon the application domains. These services may be accessed via smartphone or web portal. These interfaces not being an integral part of IoT network

have poor security mechanisms and are vulnerable to many attacks. One of the drastic effect can be compromised privacy [7, 35].

Testing all software interfaces & complete IoT testing must be done. A proposed solution [36] Constrained Application Protocol (CoAP) which is a specialized web transfer protocol, uses two layers message and receive. COAP is designed for small devices having low power supply and ensures secure communication by adding an extra cover of security to system.

3.7.3. End-to-end security

In IoT, all communication is node-to-node where data is transmitted from one node and received at another node. While data in transition is susceptible to many attacks, a proper mechanism is required to ensure security of data from its starting point to its destination, called end to end security. Here data privacy ensures that data being sent is received in original and reliable form [37].

An end-to-end session resumption is ensured using session resumption scheme. This scheme transfers encrypted session states of datagram transport layer security (DTSL) to end user who has infinite supply of resources as compare to the system with limited resources. This technique is an extension of ancient DTSL handshake where client and server keep communication live by resuming the session and without credential exchange again and again. This technique is better in terms of security along with its applicability to resource constrained sensor environment [38].

4. CONCLUSION & FUTURE WORK

IoT is in limelight since last decade as it brought ease to almost every field of life; smart home, industry, medicine and transportation. These advancements have made life easy as IoT can be accessed via smart phone or web from anywhere in world. These progressions did get attention of attackers and there are multiple attacks being launched every day. There are seven basic requirements in an IoT paradigm for complete system security ranging from confidentiality, integrity, availability, authentication, authorization, non-repudiation to privacy. Here we have made these security requirements a base and listed possible attacks which can harm these security requirements. Furthermore we explained these attacks along with their impact on system, affected layer of IoT architecture, affected system component and proposed solution. This work will give directions for IoT system security requirements, their impact as a priority measure to handle these issues and countermeasures to protect and detect attack. In future we can work on the limitations of proposed solutions and can extend this work with respect to IoT domains. As the impact of security will be different in each IoT domain and so will be the priority of issue to be resolved.

ACKNOWLEDGEMENTS

This research work is sponsored by Telkom University, Bandung Indonesia under its publication scheme and by Ministry of Education Malaysia under FRGS grant vote no 1611.

REFERENCES

[1] Gurkan Tuna, *et al.*, "A survey on information security threats and solutions for Machine to Machine (M2M) communications," *J.Parallel distrib. Compu* 2017.

[2] M.U. Farooq *et al.*, "A Critical Analysis on the Security Concerns of Internet of Things (IoT)," *International Journal of Computer Applications* (0975 8887) Volume 111-No. 7, February 2015.

[3] Afshana Khanum, *et al.*, "An enhanced security alert system for smart home using IOT," *Indonesian Journal of Electrical Engineering and Computer Science (IJEECS),* Vol. 13, No. 1, pp. 27-34 ISSN: 2502-4752, DOI: 10.11591/ijeecs.v13.i1.pp27-34, January 2019.

[4] S.Singh, *et al.*, "*Internet of Things (IoT): Security Challenges, Business Opportunities & Reference Architecture for E-Commerce*," Green Computing and Internet of Things (GCIoT), 2015 International Conference on. IEEE, 2015, pp. 1577-1581.

[5] Zhen Ling, *et al.*, "Security Vulnerabilities of Internet of Things: A Case Study of the Smart Plug System," *IEEE Internet of Things Journal,* 2017.

[6] Rwan Mahmoud, *et al.*, "*Internet of Things (IoT) Security: Current Status, Challenges and Prospective Measures*," 2015 10th International Conference for Internet Technology and Secured Transactions (ICITST), 2015.

[7] Minhaj Ahmad Khan, *et al.*, "IoT security: Review, Blockchain solutions, and open challenges" *Future Generation Computer Systems* 2018.

[8] Noel Toy, *et al.*, "Light weight authentication protocol for WSN using ECC and hexagonal numbers," *Indonesian Journal of Electrical Engineering and Computer Science (IJEECS),* Vol. 15, No. 1, pp. 443-450 ISSN: 2502-4752, DOI: 10.11591/ijeecs.v15.i1.pp443-450, July 2019.

[9] Shivangi Vashi Jyotsnamayee Ram Janit Modi, *et al.*, "*Internet of Things (IoT) A Vision, Architectural Elements, and Security Issues*," International conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud) 2017.
[10] M. Harun Yilmaz *et al.*, "*A Survey : Spoofing Attacks in Physical Layer Security*," 40th Annual IEEE Conference on Local Comp. Networks, IEEE, pp. 812-817, 2015.
[11] Chen, J. *et al.*, J Ambient Intell Human Comput (2018). "https://doi.org/10.1007/s12652-018-0887"
[12] Andrea, *et al.*, "*Internet of Things: Security vulnerabilities and challenges*," 2015 IEEE Symposium on Computers and Communication (ISCC), pp. 180-187,Larnaca,2015.
[13] Jaegeun Moona, et al., "IoT application protection against power analysis attack," Computer & Electrical Engineering, Volume 67, April 2018, Pages 566-578.
[14] Mohamed H. Eldefrawy, *et al.*, "Key Distribution Protocol for Industrial Internet of Things Without Implicit Certificates," *IEEE Internet of Things Journal*, Volume: 6 , Issue: 1 , Feb. 2019.
[15] Al-Ghaili A.M., *et al.*, "Smart Verification Algorithm for IoT Applications using QR Tag," *Computational Science and Technology*. Lecture Notes in Electrical Engineering, vol 481. Springer, Singapore.
[16] Arwa Alromih, *et al.*, "A Randomized Watermarking Technique for Detecting Malicious Data Injection Attacks in Heterogeneous Wireless Sensor Networks for Internet of Things Applications," *Sensors* 2018, 18(12), 4346; https://doi.org/10.3390/s18124346.
[17] Yassine Chahid, *et al.* "Internet of Things Security," *IEEE* 2017.
[18] Aafaf Ouaddah, *et al.*, "Access control in the Internet of Things: Big challenges and new opportunities," *www.elsevier.com/locate/comnetReviewarticle* 2017.
[19] S Rajashree, *et al.*, "*Security with IP Address Assignment and Spoofing for Smart IOT Devices*," International Conference on Advances in Computing, Communications and Informatics (ICACCI) 2018.
[20] N. Park, *et al.*, "Mutual authentication scheme in secure internet of things technology for comfortable lifestyle," *Sensors* 6 (1) (2016) 20-20.
[21] M.H. Ibrahim, "Octopus: An edge-fog mutual authentication scheme," *Internat. J. Netw. Secur. 18 (6)* (2016).
[22] Tianbo Gu, *et al.*, "*BF-IoT: Securing the IoT Networks via Fingerprinting-Based Device Authentication*," 2018 IEEE 15th International Conference on Mobile Ad Hoc and Sensor Systems (MASS) 2018.
[23] OlivierBrun[ab] *et al.*, "*Deep Learning with Dense Random Neural Network for Detecting Attacks against IoT-connected Home Environments,"* Procedia Computer Science Volume 134, 2018, Pages 458-463.
[24] Wahid, *et al.*, "A Survey on attacks, Challenges and Security Mechanism In wireless Sensor Network," *JIRST- International Journal for Research in Science & Technology*, Volume 1, Issue 8, pp. 189-196, January 2015.
[25] Kimberly Hengst, "*DDoS through the Internet of Things, An analysis determining the potential power of a DDoS attack using IoT devices*,"-Twente Student Conference on IT 2016.
[26] F. Ahmed, *et al.*, "Mitigation of black hole attacks in Routing Protocol for Low Power and Lossy Networks*," Secur. Commun. Netw.* 9 (18) (2016).
[27] M. Wazid, *et al.*, "Design of sinkhole node detection mechanism for hierarchical wireless sensor networks," *Sec. Commun. Netw.* 9 (17) (2016) 4596-4614. http://dx.doi.org/10.1002/sec.1652.
[28] Adeilson Marques da Silva Cardos, "*Real-Time DDoS Detection Based on Complex Event Processing for IoT*," 2018 IEEE/ACM Third International Conference on Internet-of-Things Design and Implementation (IoTDI) 2018.
[29] Jyoti Deogirikar *et al.*, "*Security Attacks inIoT: A Survey*," International conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud) I-SMAC 2017.
[30] J. Milosevic, *et al.*, "Malware Threats and Solutions for Trustworthy Mobile Systems Design," *Hardware Security and Trust, Design and Deployment of Integrated Circuits in a Threatened Environment, Switzerland: Springer*, 2017, pp. 149-157.
[31] Qi Zhang, *et al.*, "Spoofing Attack Detection Wireless Networks using Advanced KNN," *International Journal of Smart Device and Appliance*, Vol. 4, No. 1 (2016), pp.1-8.
[32] Y. Chen, *et al.*, "*Detecting and localizing wireless spoofing attacks*," 4th Annual IEEE Communications Society Conference on Sensor, Mesh and Ad Hoc Communications and Networks, 2017, pp. 193-202.
[33] Sohail Abbas, "*An Efficient Sybil Attack Detection for Internet of Things,"* World Conference on Information Systems and Technologies, 2019.
[34] Md. I. Abdullah, *et al.*, "Detecting Sinkhole Attacks in Wireless Sensor Network using Hop Count," *I. J. Computer Network and Information Security*, pp. 50-56, 2015.
[35] OWASP, Top IoT Vulnerabilities. *URL https://www.owasp.org/index. php/Top_IoT_Vulnerabilities*. 2016.
[36] Mohamed Sarrab, *et al.*, "*Critical Aspects Pertaining Security of IoT Application Level Software Systems*," IEEE 9th Annual Information Technology, Electronics and Mobile Communication Conference (IEMCON) 2018.
[37] G. Peretti, *et al.*, "*BlinkToSCoAP: An end-to-end security framework for the Internet of Things*," 7th International Conference on Communication Systems and Networks (COMSNETS), 2015.
[38] S. R. Moosavi *et al.*, "End-to-End Security Scheme for Mobility Enabled Healthcare IoT," *Future Generation Computer Systems*, 2016.

BIOGRAPHIES OF AUTHORS

Maria Imdad is a PhD candidate at Faculty of Computer Science and Information Technology, Universiti Tun Hussein Onn Malaysia. She did her Masters in Information Security from Air University Islamabad, Pakistan in 2017. She did her undergrad in Software Engineering from Riphah International University Islamabad, Pakistan in 2013. Her research interests are, WSN, Information Security, Cloud Computing and Software Engineering.

Deden Witarsyah Jacob received an M.Eng degree from Curtin University of Technology, Australia, in 2006 and Ph.D in 2018 from University Tun Hussein Onn Malaysia. He is the Head of the Open Data Research Center of Industrial Engineering Faculty and Senior Lecturer in the Information System Department of Telkom University, Indonesia. His main research interests include e-government, information technology master planning, e-services, decision-making models, decision support system, and information system project management.

Hairulnizam Mahdin is an Associate Professor at Department of Information Security and Web, Faculty of Computer Science and Information Technology, Universiti Tun Hussein Onn Malaysia. He completed his Ph.D. thesis in 2012 and was conferred a doctorate degree from Deakin University Australia in the same year. His research focuses on the area of data management, IoT, RFID, information security, software engineering and web technology. He has published his research in both ISI and Scopus-indexed journals.

Zirawani Baharum finished her doctorates degree for Doctor of Philosophy in Computer Science in 2017. She received her B.Sc in Computer Science majoring in Modelling and Insudtrial Computing from Universiti Teknologi Malaysia (UTM), in 2003. Then, she received MSc in Information Technology from UTM in 2005. She received her Ph.D in Computer Science from UTM in 2017. She is currently a senior lecturer in Technical Foundation section, Universiti Kuala Lumpur, Malaysian Institute of Industrial Technology (UniKL MITEC). Her research interests are in thecomputer modelling and simulation, intergrted model development, computer science and information and communication technology (ICT).

Shazlyn Milleana Shaharudin is a senior lecturer at the Department of Mathematics, Faculty of Science and Mathematics, Universiti Pendidikan Sultan Idris (UPSI). She graduated with a bachelor science degree in Industrial Mathematics from Universiti Teknologi Malaysia, in 2010. During her PhD journey, she developed an interest in multivariate analysis, specifically in finding patterns which deals with big data. She had published her research in Scopus indexed journal and presented her work in various local and international conferences.

Mohd Sanusi Azmi received BSc., Msc and Ph.D from Universiti Kebangsaan Malaysia (UKM) in 2000, 2003 and 2013. He joined Department of Software Enginering, Universiti Teknikal Malaysia Melaka (UTeM) in 2003. Now, he is currently a Associate Professor at UTeM. He is the Malaysian pioneer researcher in identification and verification of digital images of Al-Quran Mushaf. He is also involved in Digital Jawi Paleography. He actively contributes in the feature extraction domain. He has proposed a novel technique based on geometry feature used in Digit and Arabic based handwritten documents.