International Journal of Research Publication and Reviews

Journal homepage: www.ijrpr.com ISSN 2582-7421

Enhanced Security Framework for Real-Time Detection of Cyber Attacks and Binding Solutions in IoT Environments

Preeti

Research Scholar, Department of Computer Science and Applications
Kurukshetra University, Kurukshetra
Preeti.sen50@yahoo.com

ABSTRACT

A new age of interaction has been brought about by the widespread use of Internet of Things (IoT) devices, which allow for the seamless integration of digital and physical surroundings across a variety of disciplines. But because of their interconnection, IoT ecosystems are vulnerable to a wide range of cyberthreats, from distributed denial-of-service (DDoS) assaults to device hijacking and data breaches. This study offers an enhanced security framework designed to identify cyberattacks in real time and provide binding solutions in Internet of Things settings in response to these issues. Advanced threat detection techniques, which include behavior analysis, anomaly detection, and machine learning algorithms to find malicious activity in IoT networks, are essential parts of the system. Furthermore, the framework creates binding security solutions and conducts thorough vulnerability evaluations to address the attack surface of IoT ecosystems. Through the provision of a comprehensive framework for IoT security, this study helps to build strong and resilient security solutions that protect the availability, confidentiality, and integrity of IoT services and data from ever-changing cyber threats.

Keyword: IoT Security, Cyber Attacks, Threat.

1. INTRODUCTION

The internet of things (IoT) paradigm refers to the network of physical objects or things embedded with electronic, software, sensors, and connectivity to enable objects to exchange data with servers, centralized system, and other connected devices. The IoT is gaining increasing attention. Due to the growing interest in IoT, the number of platforms designed to support IoT has risen considerably. As a result of different approaches and standards there is a wide variety and heterogeneity of IoT platforms. The term of IoT was first invented in 1998 which is a network of networks where typically, many objects or sensors are connected through communications and information infrastructure to provide value-added services. It assured in creating a world where all the objects around us are connected to the internet and therefore the communication to each other with minimal human intervention. The aim is to create a better world for human beings, where the objects around us understand our desire and hence act accordingly without any explicit instructions. The future is not going to be people talking to people, but it is going to be machines talking to other machines on account of the user. The era of IoT in where new forms of interaction between human and things, and between things themselves is going to be realized, therefore adding a new aspect to the world of information technology and communication. The things are heterogeneous and have low memory, less processing power.

Various IoT applications focus on automating different tasks and are trying to empower the inanimate physical objects to act without any human intervention. The existing and upcoming IoT applications are highly promising to increase the level of comfort, efficiency, and automation for the users. To be able to implement such a world in an ever-growing fashion requires high security, privacy, authentication, and recovery from attacks. In this regard, it is imperative to make the required changes in the architecture of the IoT applications for achieving end-to-end secure IoT environments.

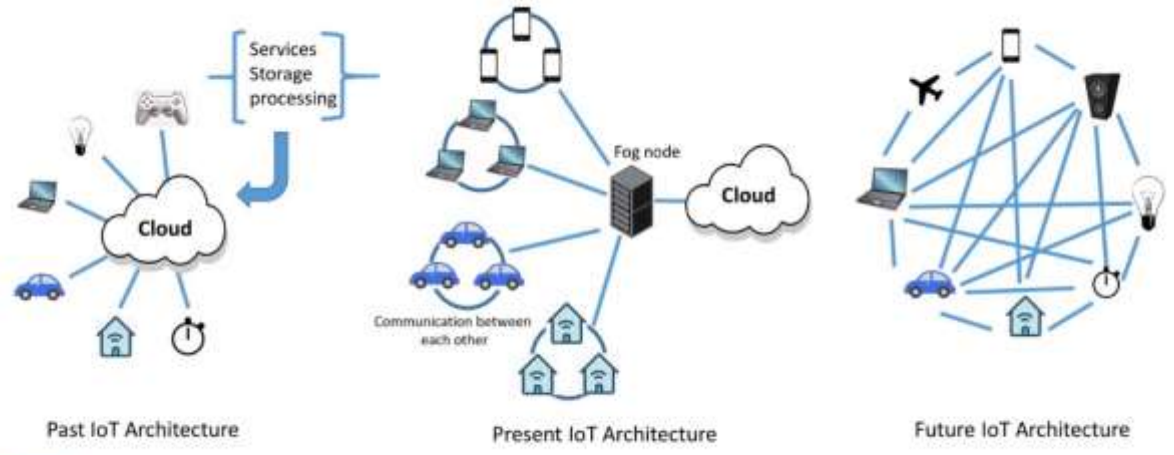

FIGURE 1. Present and future architecture of IoT.

1.1 Technologies of IoT

During initial days of IoT, RFID served as the foundation technology, which allows user to send or receive information using radio - frequency signals. The connected device should be attached with RFID tags, which contains reader and transmitter. With the help of RFID reader, people can locate and monitor the devices. The main application of RFID is transportation.

Later, wireless sensor networks (WSN) served as a building block for IoT. Here sensors/actuators will be attached to the devices with in the network. Sensors are used to sense the data and using actuators data will be transmitted. The main application of WSN includes health-care. With the advancement of RFID and WSN, there is a significant growth in the development of IoT. IoT finds its main applications in the fields of tracking & monitoring, health - care, home automation, environment monitoring, building, agriculture, aqua - culture and others. With the advancement of smart phones, communication protocols, sensor networks technologies; it is possible to connect more objects in a network.

The key technologies of IoT are classified in to two broad categories.

1) Identification Technology: As the name indicates these types of technologies are used for locating and monitoring purpose. The examples include RFID, WSN, QR code, barcodes and Intelligent sensors etc. RFID connected devices contain a reader to collect the information, and a transmitter to transmit the information. RFID are costly when compared to other technologies like WSN.

2) Communication Technology: These will provide guidelines to be followed data transfer. Examples include Zig bee, Z wave, MQTT, Bluetooth, Li-fi, Wi- fi, Near FieldCommunication (NFC), Power line area network and others.

- *Zigbee* is follows IEEE 802.15.4 standard. It is a short range (around 20meters) protocol, used to create a small network. It is generally used in home automation.
- *Z Wave* is long range wireless protocol (approx. 100 meters). Each Z wave network will have a unique ID called Network ID, and each device in a Z Wave network will have a node ID. It is also used in home automation. Unlike Wi-Fi it can transfer data at high speed.
- *Bluetooth* is a short-range protocol, generally used in our day-to-day applications. For example, in our smart phone using Bluetooth we will transfer the information to the paired device. It follows IEEE 802.15.1 standard.
- *Li – Fi (light fidelity)* is also a short-range wireless protocol. Here the transfer of data takes place in the form of light.
- *Wi-Fi* follows IEEE 802.11 standard. It is a medium range network, generally used in local area network. The scalability is more.
- *Near field communication (NFC), is* very short-range networking protocol (appox. 4meters). It provides point to point connectivity between communicating devices. For example, using NFC we can share screen of our smart phone with smart TV.
- *Power Line area network*, is a long range wired communication network. It makes use of power lines for transmitting the data.

These all technologies of IoT makes use of either IPv4 or IPv6 for addressing.

However, while on one side, IoT makes many applications possible, on the other side increases the risk of cyber security attacks. IoT systems are at high security risks for several reasons. They do not have well defined perimeters, are highly dynamic, and continuously change because of mobility. In addition, IoT systems are highly heterogeneous with respect to communication medium and protocols, platforms, and devices. Nowadays, we are witnessing many types of malicious software that exploit the various vulnerabilities of IoT devices and services. Due to high number of IoT devices, this fact can represent a huge security risk, example malicious software on devices can initiate a massive distributed denial of service (DDoS) attack against the target web site or information system. For this reason, security is a very important research topic in the IoT area. The researcher into IoT security is in its early stages and many work focus on potential threats,

due to all these issues and vulnerabilities, the IoT applications create a fertile ground for different kinds of cyber threats. There have been various security and privacy attacks on the already deployed IoT applications worldwide.

1.2 Frameworks of IoT

The Internet of Things (IoT) Framework can be described as being an ecosystem, comprising of several connected devices that communicate with each other, over the Internet. These connected devices usually work to transfer and sense data over the Internet, while requiring very little human intervention. The IoT framework is what makes it possible for the connected devices to have smooth communication over the Internet. Different frameworks are proposed for IoT. Depending on the type of application, particular framework can be opted.

Following are some of the leading frameworks:

i)Cisco: Cisco IoT Cloud Connect provides robust, automated, and highly secure connectivity for the enterprise. IoT data management is done by the Cisco Kinetic IoT platform to extract, move and compute the data. As Cisco is very famous for its security services, it protects IoT deployment against threats with a secure IoT architecture.

ii)Azure: Without the Microsoft Azure solution, a cloud service giant with AWS and Google Cloud platform, the comparison of our IoT platform will be not complete. The Microsoft Azure IoT Suite provides preconfigured solutions and the ability to personalize and develop new solutions to meet the project requirements. The strongest safety mechanisms, superb scalability and simple integration with your current or future systems are achieved through Microsoft Azure Internet of thing Suite.

iii)KAA: This IoT framework open source is most popular for its efficiency and the ‘rich’ services it offers. The KAA IoT is a cloud platform that allows the users to materialize and implement all the smart product concepts that they may be having. While on the KAA IoT framework, the user could manage as many connected devices as they prefer. This ability to manage the unlimited number of devices is made possible by the cross-device interoperability of this platform.

iv)ThingsWorx: is one of the earliest frameworks. ThingsWorx is aimed at the development and deployment of the IoT solutions with another booming IT field – AR (augumented reality). This solution is based on ThingModel which provides for a real time peek into physical devices.

v) AWS: (AWS) is an IoT platform provided by Amazon. This IoT platform provides cloud computing, database, and security services through the AWS Console. There are so many other services such as Regions, Availability Zones, and Virtual Private Clouds (VPCs). It helps to ease out the improving durability, distribution, availability of the application. It provides Registry for recognizing devices, Secure Device Gateway, Compatible Software Development Kit for devices which AWS partnered with HW manufacturers like Intel, Texas Instruments, Broadcom, and Qualcomm.

vi)GE Predix: The GE PREDIX open-source framework is mainly built around the concept of cloud foundry. Even though this IoT framework open source was developed for the internal operations of the GE, it has now become one of the most popular and successful IoT platforms available. The GE PREDIX open source allows for a user to efficiently manage assets, ensure the security and real-time of connected devices, as well as facilitate the acquisition, storage, and access of large chunks of data.

3. Security Issues in IoT Environment

Any IoT application can be divided into four layers:

(1) Sensing layer

(2) Network layer

(3) Middleware layer

(4) Application layer

Each of the layers in an IoT application uses diverse technologies that bring a few issues and security threats. Figure 2 shows various technologies, devices, and applications at these four layers. This section discusses various possible security threats in IoT applications for these four layers. Figure 3 shows the possible attacks on the four attacks. The special security issues associated with the gateways that connect these layers**.** In any IoT ecosystem or environment, there are four important layers. The first layer includes the use of various sensors and actuators to perceive the data or information to perform various functionalities. Based on that, in the second layer, a communication network is used to transmit the collected data. Most of the evolving IoT applications deploy the third layer, called a middleware layer, to act as a bridge between network and application layer. Finally, on the fourth layer, there are various IoT based end-to-end applications like smart grids, smart transport, smart factories, etc. All of these four layers have security problems specific to them. Apart from these layers, various gateways connect these layers and help in the data movement. There are certain security threats specific to these gateways as well.

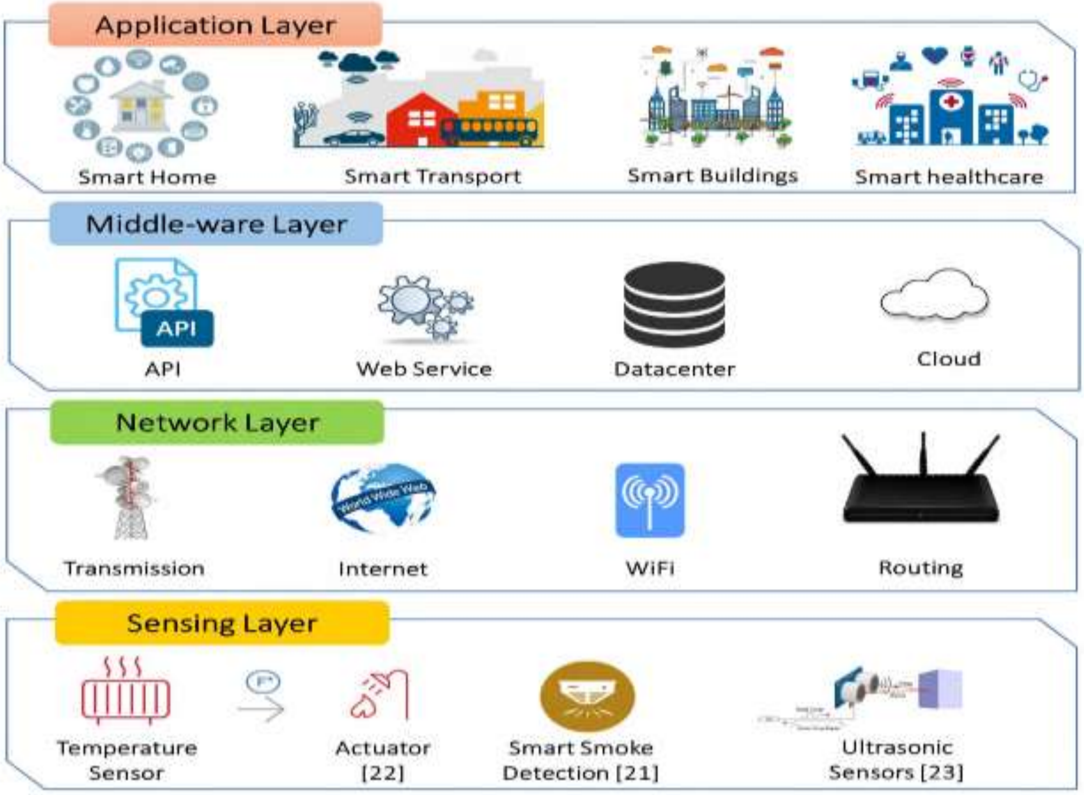

FIGURE 2. Layers in IoT system.

3.1 SECURITY ISSUES AT SENSING LAYER

The sensing layer mainly deals with physical IoT sensors and actuators. Sensors sense the physical phenomenon happening around them [11]. Actuators, perform a certain action on the physical environment, based on the sensed data. There are various kinds of sensors for sensing different kinds of data, e.g., ultrasonic sensors, camera sensors, smoke detection sensors, temperature sensors etc. Various sensing layer technologies are used in different IoT applications like RFID, GPS, WSNs etc. Major security threats that can be encountered at the sensing layer are as follows:

i) Node Capturing: IoT applications comprise of several low power nodes such as sensors and actuators. These nodes are vulnerable to a variety of attacks by the adversaries. The attackers may try to capture or replace the node in IoT system with a malicious node.[14].

ii) Malicious Code Injection Attack: The attack involves the attacker injecting some malicious code in the memory of the node. Using such malicious code, the attackers may force the nodes to perform some unintended functions or may even try to access the complete IoT system.

iii) False Data Injection Attack: Once the node is captured, the attacker may use it to inject erroneous data onto the IoT system. This may lead to false results and may result in malfunctioning of the IoT application. The attacker may also use this method to cause a DDoS attack.

iv) Side-Channel Attacks (SCA): Apart from direct attacks on the nodes, various side-channel attacks may lead to leaking of sensitive data. The microarchitectures of processors, electromagnetic emanation and their power consumption reveal sensitive information to adversaries. Side channel attacks may be based on power consumption, laser-based attacks, timing attacks or electromagnetic attacks. Modern chips take care of various countermeasures to prevent these side-channel attacks while implementing the cryptographic modules.

v) Eavesdropping and Interference: IoT applications often consist of various nodes deployed in open environments [15]. As a result, such IoT applications are exposed to eavesdroppers. The attackers may eavesdrop and capture the data during different phases like data transmission or authentication.

vi) Sleep Deprivation Attacks: In such type of attacks the adversaries try to drain the battery of the low-powered IoT edge devices. This leads to a denial of service from the nodes in the IoT application due to a dead battery. This can be done by running infinite loops in the edge devices using malicious code or by artificially increasing the power consumption of the edge devices.

vii) Booting Attacks: The edge devices are vulnerable to various attacks during the boot process. This is because the inbuilt security processes are not enabled at that point. The attackers may take advantage of this vulnerability and try to attack the node devices when they are being restarted. As edge devices are typically low powered cycles, it is thus essential to secure the boot process in devices.

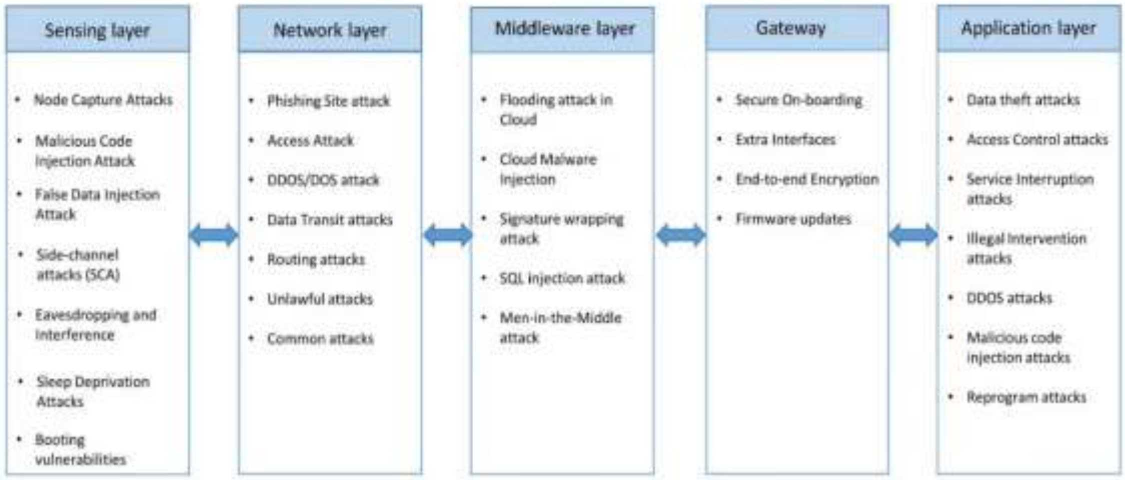

FIGURE 3. Types of attacks on IoT.

3.2 SECURITY ISSUES AT NETWORK LAYER

The key function of the network layer is transmitting the information received from the sensing layer to the computational unit for processing. The major security issues that are encountered at the network layer are as follows.

i) Phishing Site Attack: There is a possibility of encountering phishing sites in the course of users visiting web pages on the Internet. Once the user's account and password are compromised, the whole IoT environment being used by the user becomes vulnerable to cyber-attacks. The network layer in IoT is highly vulnerable to phishing sites attacks [16].

ii) Access Attack: Access attack is also referred to as advanced persistent threat (APT). This is a type of attack in which an unauthorized person or an adversary gains access to the IoT network. The attacker can continue to stay in the network undetected for a long duration. The purpose or intention of this kind of attack is to steal valuable data or information, rather than to cause damage to the network [17].

iii) DDoS/DoS Attack: In this kind of attacks, the attacker floods the target servers with a large number of unwanted requests. This incapacitates the target server, thereby disrupting services to genuine users. If there are multiple sources used by the attacker to flood the target server, then such an attack is termed as DDoS or distributed denial of service attack. Such attacks are not specific to IoT applications, but due to the heterogeneity and complexity of IoT networks, the network layer of the IoT is prone to such attacks [18].

iv) Data Transit Attacks: IoT applications deal with a lot of data storage and exchange. Data is valuable, and therefore it is always the target of hackers and other adversaries. Data that is stored in the local servers or the cloud has a security risk, but the data that is in transit or is moving from one location to another is even more vulnerable to cyber-attacks. In IoT applications, there is a lot of data movement between sensors, actuators, cloud, etc. Different connection technologies are used in such data movements, and therefore IoT applications are susceptible to data breaches.

v) Routing Attacks: In such attacks, malicious nodes in an IoT application may try to redirect the routing paths during data transit. Sinkhole attacks are a specific kind of routing attack in which an adversary advertises an artificial shortest routing path and attracts nodes to route traffic through it. A worm-hole attack is another attack which can become serious security threat if combined with other attacks such as sinkhole attacks. A warm-hole is an out of band connection between two nodes for fast packet transfer. An attacker can create a warm-hole between a compromised node and a device on the internet and try to bypass the basic security protocols in an IoT application.

3.3 SECURITY ISSUES AT MIDDLEWARE LAYER

The role of the middleware in IoT is to create an abstraction layer between the network layer and the application layer. Middle-ware can also provide powerful computing and storage capabilities [19]. This layer provides APIs to fulfill the demands of the application layer. Middleware layer includes brokers, persistent data stores, queuing systems, machine learning, etc. Although the middleware layer is useful to provide a reliable and robust IoT application, it is also susceptible to various attacks. Database security and cloud security are other main security challenges in the middleware layer. Various possible attacks in the middleware layer are discussed as follows.

i) Man-in-the-Middle Attack: The MQTT protocol uses publish-subscribe model of communication between clients and subscribers using the MQTT broker, which effectively acts as a proxy. This helps in decoupling the publishing and the subscribing clients from each other and messages can be sent without the knowledge of the destination. If the attacker can control the broker and become a man-in-the-middle, then he/she can get complete control of all communication without any knowledge of the clients.

ii) SQL Injection Attack: Middle-ware is also susceptible to SQL Injection (SQLi) attacks. In such attacks, attacker can embed malicious SQL statements in a program [20]. Then, the attackers can obtain private data of any user and can even alter records in the database.

iii) Signature Wrapping Attack: In the web services used in the middleware, XML signatures are used [24]. In a signature wrapping attack, the attacker breaks the signature algorithm and can execute operations or modify eavesdropped message by exploiting vulnerabilities in SOAP (Simple Object Access Protocol).

iv) Cloud Malware Injection: In cloud malware injection, the attacker can obtain control, inject malicious code or can inject a virtual machine into the cloud. The attacker pretends to be a valid service by trying to create a virtual machine instance or a malicious service module. In this way, the attacker can obtain access to service requests of the victim's service and can capture sensitive data which can be modified as per the instance.

v) Flooding Attack in Cloud: This attack works almost the same as DoS attack in the cloud and affects the quality of service (QoS). For depleting cloud resources, the attackers continuously send multiple requests to a service. These attacks can have a big impact on cloud systems by increasing the load on the cloud servers.

3.4 SECURITY ISSUES AT APPLICATION LAYER

The application layer directly deals with and provides services to the end users. IoT applications like smart homes, smart meters, smart cities, smart grids, etc. lie in this layer. This layer has specific security issues that are not present in other layers, such as data theft and privacy issues.

Major security issues encountered by the application layer are discussed below.

i) Data Thefts: IoT applications deal with lot of critical and private data. The data in transit is even more vulnerable to attacks than data at rest, and in IoT applications, there is a lot of data movement. The users will be reluctant to register their private data on IoT applications if these applications are vulnerable to data theft attacks. Data encryption, data isolation, user and network authentication, privacy management, etc. are some of the techniques and protocols being used to secure IoT applications against data thefts.

ii) Access Control Attacks: Access control is authorization mechanism that allows only legitimate users or processes to access the data or account. Access control attack is a critical attack in IoT applications because once the access is compromised, then the complete IoT application becomes vulnerable to attacks.

iii) Service Interruption Attacks: These attacks are also referred to as illegal interruption attacks or DDoS attacks in existing literature. There have been various instances of such attacks on IoT applications. Such attacks deprive legitimate users from using the services of IoT applications by artificially making the servers or network too busy to respond.

iv) Malicious Code Injection Attacks: Attackers generally go for the easiest or simplest method they can use to break into a system or network. If the system is vulnerable to malicious scripts and misdirection due to insufficient code checks, then that would be the first entry point that an attacker would choose. Generally, attackers use XSS (cross-site scripting) to inject some malicious script into an otherwise trusted website. successful XSS attack can result in the hijacking of an IoT account and can paralyze the IoT system.

v) Sniffing Attacks: The attackers may use sniffer applications to monitor the network traffic in IoT applications. This may allow the attacker to gain access to confidential user data if there are not enough security protocols implemented to prevent it.

vi) Reprogram Attacks: If the programming process is not protected, then the attackers can try to reprogram the IoT objects remotely. This may lead to the hijacking of the IoT network.

4. LITERATURE SURVEY

This section provides the review on the major issues related to security in IoT. The literature is reviewed from two viewpoints. First section deals with review of the machine learning techniques. The second section deals with overview of the past research work involving block chain techniques.

4.1 Review on Security Issue Address using Machine Learning

The machine learning is a technique to perform computational intelligently. The model needs to design and test using different learning methods. Some of the application requirement is decision should be taken before the actual event occurs. For example, predicting the fire in a kitchen or any industrial area and alarm the sound to prevent the fire. This could be possible if machine learning technologies are used in IoT applications. An efficient framework [27] is required to process and compute the huge data collection using a machine learning technique. An intrusion detection and mitigation framework called IoT-IDM, to provide a network level protection for smart devices deployed in home environment The main contribution in framework is advent of SDN technology, OpenFlow protocol, machine learning technique for detection attack pattern and Java module Floodlight for implementation. They used host-based intrusion and detection instead of network -based system. In order to demonstrate the applicability of framework they selected Philips Hue bulb which accept command from user via HTTP protocol. A concept to secure IoT edge device within gateway using ANN machine learning technique. R programming tool is used to create ANN. While making testbed Ardunio Uno device are used to emulate edge devices which connect to WiFi chip and temperature sensor and Raspberry pi model 3 to implement gateway which is credit card size micro controller and low power consumption, technical specification detailed in. The neural network used five -layer with three hidden layer and input to network model are sensor value, device ID and time stamp as features. SDN based secure IoT framework called SoftThings used with machine learning algorithm. The core idea is based on SDN controller which dynamically control the traffic flow also separate the control plane and data plane. Support Vector Machine (SVM) and SVM: non-linear machine learning algorithm is used which classifies the attack in normal and abnormal traffic. The main component of framework is IoT devices, SDN switch, SDN controller and Master SDN controller. SDN controller consist three main module i.e learning module which analyze the flow pattern, classification module for classify the network traffic and flow management module to control the network flow. The seven multiple hybrid model to detect intrusion in network, since single algorithm strategy model shows high rate of false alarms. The strategy is based on two approaches first is use of supervised learning, which in the context of detection of 10 known attack, 10 second is to use unsupervised learning for the detection unknown and new attacks. The hybrid model increases the high hit rate compare to single algorithm model. The algorithm used are Neural Network (NN) and Support Vector Machine (SVM) for supervised learning, K-mean for unsupervised learning. As feature selection technique Principal Component Analysis (PCA) and Gradually Feature Reduction (GFR) are used. IoT sentinel which is capable to identify new introduced device in network. Authors does so by controlling the network traffic flow of vulnerable devices. IoT sentinel restrict the communication so that adversary is not able to connect vulnerable device to exploit. They use major component i.e Security Gateway and IoT security service provider (IoTSS). Security gateway is SDN based to monitor the profile of individual device and send fingerprint to IoTSS. IoTSS is used here to assess the vulnerability of device. IoTSS uses machine learning classification to check whether fingerprint match or not of individual device. For mitigation strategy they implement concept of network isolation, traffic filtering and user notification. For device identification device fingerprint is used, which is observation of passive network history log i.e source address, time stamps, propagation time etc. It helps to extract the features which is further used in machine learning classifier. Three new Intrusion Detection Systems (IDSs) for IoT i.e K-means clustering unsupervised learning-based IDS, decision tree based supervised IDS, and a hybrid two stage IDS that combines K-means and decision tree learning approaches. All the three IDS are centralized and scalable approaches. The K-means approach achieves 70-93% detection rate for varying sizes of random IoT networks. Decision tree-based IDS achieves 71-80% detection rate and the hybrid approach attains 71-75% detection rate for the same network sizes. A framework to detect android malware application based on permission asking by them using machine learning techniques. Since android allow many other open sources such as torrent, Google play store and direct download make it more prone to attack. Authors classified malware after extracting the permission database stored in file Androidmenifest.XML. Different machine learning techniques viz. Naïve Bayes, J48, Random Forest, Multiclass classifier and multilayer perceptron applied on sample data and performance evaluation is done by confusion matrix. It shows Multilayer perceptron computation complexity is very poor among all machine learning techniques. Multiple hybrid machine learning model for intrusion detection in computer network. They used supervised learning for known attack, and for unknown attack unsupervised is used. Here two terms are used i.e. Multiple and Hybrid, hybrid refers more than one category of machine learning is used and multiple more than one algorithm is used of either supervised or unsupervised learning. Supervised learning SVM and NN are used, in unsupervised learning K-mean used. In their implementation, model uses NN and SVM in first level where known attack is identified and K-mean in the second level where unknown attack is identified. 11 NSL-KDD dataset are used as testing and training dataset. DoS, Normal, Probing, R2L and U2R are the supervised output label, Normal & Attack are two class for unsupervised. PCA and GFR are used as feature selection technique. ANN technique is used to detect Botnet attack. A botnet is a computer network consisting of infected devices controlled by malware. Traditionally, botnets consisted mainly of compromised personal computers, but a low level of information security of IoT devices. The botnet Mirai is considered the largest botnet in the history, containing a huge number of compromised IoT devices. In order to demonstrate the applicability author used Arduino which is lightweight structure. It detects traffic data and send to server for feature extraction. A method to classify DDOS attack which overload the server by sending large volume request to make service unavailable to user. The work is based on packet shipping ratio (PSR) to find the malicious node which may additionally temper a number of packets and make verbal exchange fail. The method used SVM machine learning that analyze IoT malware received from numerous IoT device, SVM create a model for normal and abnormal binary classification. They used XOIC tool for emulate DDOS attack to send traffic from multiple source to single destination address, Wireshark tool used to capture and analyze the packets and 12 Python is used to implement the algorithm. A cloud-based Intrusion Detection System (IDS) using machine learning techniques. All analysis performed in cloud so that IoT environment would not affect. Random forest and neural network used for intrusion detection and intrusion category detection respectively. While gathering traffic module Tshark is used. Tshark is a network protocol analyzer which is capable of capturing packet data from live network connection. Bro-IDS tool is used for mine the features, (Bro-IDS) which is open-source traffic analyzer, considered as security monitor and malicious activity inspector. MySql technology is used to store the extracted features. 12 While proposing they used UNSW-NB15 dataset, which is modern labeled dataset for evaluating NIDS that contains over 2.5 million record and 49 feature. An Intrusion Detection System (IDS) against various attack viz. backdoor, SQL injection and command injection using machine learning technique i.e Random Forest along with evaluate the performance. The system is built for Supervisory control and data acquisition (SCADA) which is largest subset of Industrial Control System (ICS) the integral part of Industrial Internet of Things (IIoT). Modbus communication protocol is used between Human Machine Interface (HMI) and programmable Logic Controller (PLC) which is earliest and most commonly used in IIoT. This protocol does not provide confidentiality, integrity and authentication (CIA) and attacker can easily sniff out the packet. Authors reviewed potential features and chose 23 features that are common in network flows some of these are source port, destination port, source packet etc. Machine learning is used to just classify to decide whether traffic is normal of attack. A machine learning classifier for abnormality determination is generated at each node using learning data. The packet is capture at each node, when it judged to abnormal, the packet data 13 recorded into log and send to monitoring node. Address Resolution Protocol (ARP) is used for topology visualization. ARP protocol is used to extract MAC from IP address. Authors used protocol type, packet size, and number of sending packets to same host in last two seconds as learning data for random forest machine learning classifier. Random forest classifier is plurality of random decision trees are generated from same data learning and the majority decision of the output result of each decision tree is taken as final output result. Machine learning technique to identify IoT devices. They identify IoT devices based on their message packet. Transmission Control Protocol (TCP) & User datagram protocol (UDP) packet is used for analyzed. Low level scanner Network Mapper (NMAP) is used to collect message packets from IoT devices in specified range. To recognize the devices, they used port number above 1024, as first 1024 port are well known and used by standard services. In author’s scenario every IP has port ranging from 0 to 65535. Twenty-three binary features are identified from TCP/IP packets according to their correlation i.e. device type, device model and 13 device manufacturer and used them as label to train the machine learning model. Decision tree are used as classifier model.

4.2 Security issue address using blockchain technology

Blockchain technology is a decentralized/distributed network where each is connected to others in some way. The message is broadcast in the Blockchain network. A block consists of lots of valid transaction and its associated attributes. The Blockchain network uses different consensus algorithm [89] to meet the consensus among the nodes. A secure framework for the internet of things applications based on a distributed system.

A distributed Blockchain-based model proposed system one miner is used to control the communication within the smart home as well as an external source. The framework is secure against fundamental security goals and evaluated the feasibility of using blockchain nodes on IoT devices. A distributed ledger-based blockchain (DL-BC) technology to address security and privacy issues in IoT, such as spoofing, false authentication. A distributed intelligence that performs instance decision making and reduces unnecessary data transfer to the cloud, addressing various security challenges in the IoT paradigm. a blockchain-based secure scheme to resolve the issue of time announcements in IoT.

A blockchain-based scheme to assure the security during time synchronization in IoT.

Specifically, a publicly verifiable ledger is utilized to record and broadcast time, which can minimize many attacks from external environments. The use of multiple time sources can avoid the vulnerabilities caused by the centralized generation of accurate time. Moreover, the decentralized structure of this scheme has the advantage of adapting the changes of network topology. By employing an improved Practical Byzantine Fault Tolerance (PBFT) consensus mechanism, time synchronization can be implemented efficiently.

The Named Data Networking (NDN) of Things architecture and the blockchain solution to deal with the security attacks in this. Named Data Networking (NDN to resolve the challenges of IoT, by taking the advantage of named data paradigm, in which all things including hosts and data are named by the naming schemes, and the data dissemination switched from host-to-host manner to data-oriented communication. In such manner, the network disseminates named data and forward directly on names carrying application semantics. A blockchain-based high-level security management scheme for various IoT devices.

The device classification methods by applying machine learning algorithms on the data stored in the blockchain network which in turn helps to enhance the security of IoT environment by detecting unauthorised devices. A trust management framework for providing secure and trustworthy access control and also detecting and removing malicious and compromised nodes in a decentralized IoT. A blockchain based Trust and Reputation System (TRS) for IoT access control, which progressively evaluates and calculates the trust and reputation score of each participating node to achieve a self-adaptive and trustworthy access control system. Trust and reputation are explicitly incorporated in the attribute-based access control policy, so that different nodes can be assigned to different access right levels, resulting in dynamic access control policies. A Secure Private Blockchain-based framework (SPB) using which negotiations can be done among the energy prosumers over the energy price and trade energy in a distributed manner for a smart grid IoT application. A permissioned blockchain based framework to find provenance of supply chain products. A three-layered trust management framework - Trust Chain, based on consortium blockchain for tracking the interactions among supply chain participants and based on these interactions it dynamically assigns trust and reputation scores. A noble blockchain-based framework for providing a private and secure communication model for smart vehicles so that they can trust the data they receive are generated by a trusted node. The Permissioned blockchain architecture to handle the most expensive computation in pairing-based cryptographic protocols i.e., secure outsourcing of bilinear pairings (SOBP). An IoT application, privacy is a significant concern for the end-users. The blockchain-based encryption techniques are proposed by different authors to solve the privacy preservation issue. The device authentication is one of the important factors for secure communication in the IoT network. The different methods, like mutual authentication, PSO-AES, and distributed authentication, are used for IoT device authentication using blockchain techniques. The management of devices accessibility in the IoT system is essential as critical information is sense using different smart things. The attribute-based access control and blockchain-based permission delegation access control techniques are proposed by the researcher to manage the accessibility of the vital information securely.

References

[1] H. Harun et al.—” A Study using Internet of Things Concept toward Engineering Educational”, VolumeNo.6, June2015.

[2] D. Bandyopadhyay, and J. Sen, “Internet of things: applications and challenges in technology and standardization,” *Wireless Personal Communications*, vol.58, no.1, pp.49-69, 2011.

[3] Kiran Jot Singh, "A Survey of IoT platforms. Create your own Internet of Things," *IEEE consumer electronics magazine*,2017.

[4] Pallavi Sethi," Review Article: Internet of Things: Architectures, Protocols, and Applications," *Journal of Electrical and Computer Engineering*, vol 2017.

[5] A. Mosenia, N. K. Jha, A comprehensive study of security of internet-of-things, IEEE Transactions on Emerging Topics in Computing 5 (4) (2016)586–602.

[6] L. Liu, Z. Ma, W. Meng, Detection of multiple-mix-attack malicious nodes using perceptron-based trust in IoT networks, Future Generation Computer Systems 101 (2019) 865–879.

[7] L. Atzori, A. Iera, and G. Morabito, "The Internet of things: a survey," *Computer Networks*, vol.54, no.15, pp.2787-2805, 2010.

[8] R. Roman, P. Najera, and J. Lopez, "Securing the Internet of Things," Computer, vol.44, no.9,2011, pp.51-58.

[9] A. H. Ngu, M. Gutierrez, V. Metsis, S. Nepal, Q. Z. Sheng, Iot middleware: A survey on issues and enabling technologies, IEEE Internet of Things Journal 4 (1) (2016) 1–20.

[10] V. Casola, A. De Benedictis, A. Riccio, D. Rivera, W. Mallouli, E. M.de Oca, A security monitoring system for Internet of Things, Internet of Things 7 (2019) 100080.

[11] Bridgera. IoT System | Sensors and Actuators. Accessed: Feb. 9, 2019. [Online]. Available: https://bridgera.com/IoT-system-sensors-actuator/

[12] P. I. R. Grammatikis, P. G. Sarigiannidis, I. D. Moscholios, Securing the internet of things: challenges, threats and solutions, Internet of Things.

[13] V. Hassija, V. Chamola, V. Saxena, D. Jain, P. Goyal, B. Sikdar, A survey on iot security: Application areas, security threats, and solution architectures, IEEE Access 7 (2019) 82721–82743.

[14] S. Kumar, S. Sahoo, A. Mahapatra, A. K. Swain, and K. K. Mahapatra, ''Security enhancements to system on chip devices for IoT perception layer,'' in Proc. IEEE Int. Symp.Nanoelectron. Inf. Syst. (iNIS), Dec. 2017, pp. 151–156.

[15] C.-H. Liao, H.-H. Shuai, and L.-C. Wang, ''Eavesdropping prevention for heterogeneous Internet of Things systems,'' in Proc. 15th IEEE Annu. Consum. Commun. Netw. Conf. (CCNC), Jan. 2018, pp. 1–2.

[16] APWG. Phishing Activity Trends Report. Accessed: Feb. 12, 2019. [Online]. Available: https://docs.apwg.org/reports/apwg_trends_report_q4_2017.pdf .

[17**]** C. Li and C. Chen, ''A multi-stage control method application in the fight against phishing attacks,'' in Proc. 26th Comput. Secur. Acad. Commun. Across Country, 2011, p. 145.

[18] C. Kolias, G. Kambourakis, A. Stavrou, and J. Voas, ''DDoS in the IoT: Mirai and other Botnets,'' Computer, vol. 50, no. 7, pp. 80–84, 2017.

[19] S. Bandyopadhyay, M. Sengupta, S. Maiti, and S. Dutta, ''A survey of middleware for Internet of Things,'' in Recent Trends in Wireless and Mobile Networks. Springer, 2011, pp. 288–296.

[20] R. Dorai and V. Kannan, ''SQL injection-database attack revolution and prevention,'' J. Int. Commercial Law Technol., vol. 6, no. 4, p. 224, 2011.

[21] M. Frustaci, P. Pace, G. Aloi, and G. Fortino, ''Evaluating critical security issues of the IoT world: Present and future challenges,'' IEEE Internet Things J., vol. 5, no. 4, pp. 2483–2495, Aug. 2018.

[22] A. Mosenia and N. K. Jha, ''A comprehensive study of security of Internet-of-Things,'' IEEE Trans. Emerg. Topics Comput., vol. 5, no. 4, pp. 586–602, Dec. 2017

[23] Y. Yang, L. Wu, G. Yin, L. Li, and H. Zhao, ''A survey on security and privacy issues in Internet-of-Things,'' IEEE Internet Things J., vol. 4, no. 5, pp. 1250–1258, Oct. 2017.

[24] J. Kumar, B. Rajendran, B. S. Bindhumadhava, and N. S. C. Babu, ''XML wrapping attack mitigation using positional token,'' in Proc. Int. Conf. Public Key Infrastruct. Appl. (PKIA), Nov. 2017, pp. 36–42.

[25] S Mandal, "Internet of Things (part 3)," devices and technologies, [online], source: http://www.c-sharpcorner.com/UploadFile/f88748/internet-of-things-iot-part-3, 2015.

[26] Q. Jing, A. V. Vasilakos, J. Wan, J. Lu, D. Qiu, Security of the internet of things: perspectives and challenges, Wireless Networks 20 (8) (2014) 2481–2501.

[27] I.Kotenko, I.Saenko, A.Branitskiy, Framework for Mobile Internet of Things Security Monitoring Based on Big Data Processing and Machine Learning, IEEE Access 6 (2018).