Exploration of Various Attacks and Security Measures Related to the Internet of Things

Debajit Datta, Dheeba J

***Abstract*: *In this era of technological advances, it will be impractical to think of a day without the usage of gadgets. Development and popularity of the Internet of Things have helped mankind a lot in several ways, but at the same time, there has also been an increase in attacks invading the underlying security. Advances in studies have resulted in the development of evolved algorithms that can be used in order to reduce the attacks and threats to the Internet of Things. With several advancements in studies and research works, the security measures on various Internet of Things based components and protocols are developing with time, but concurrently more advanced threats and attacks on these components are also evolving. These attacks are not only harmful to the components, but rather they also affect the users and applications that are associated with it, by breaching data, increase in inconsistency and inaccuracy, and many more. This work deals with the study of several attacks that are associated with the Internet of Things and also the approaches to secure the IoT systems. This work will also help in coming up with further up-gradation in the currently implemented security protocols and also in predicting the possible attacks that can be developed against the IoT protocols*.

***Keywords*: *Internet of Things, Security Issue, Cyber Attacks, Protocol, Privacy, Security Measure*.**

I. INTRODUCTION

The Internet is an interconnection of computers, connected in a Wide Area Network that is facilitated with communication at a global level. There are several standards and protocols that are associated with the Internet, that has to be followed and maintained by the applications and actors who have involvement with it. The regulations and protocols that have been developed or are developing, over the years, are highly standardized and globally accepted. The growth of the Internet has led to the emergence and advancement of several cybercrimes, for which many laws have been enforced to punish the violators. According to Donn Parker [26], the crimes related to computers are broadly classified into four types – the crimes where a computer or any other computational device is a victim; the crimes in which it provides an atmosphere wherein the crime is committed; the computers act as a weapon for committing a crime; it is used figuratively to perform perjury or create tension, mostly psychological, in the victims. The expansion of the Internet and its associated applications with time worked as a catalyst in increasing the hopes and demands in the users that it has led to various new inventions and developments in various fields on Computer Science and has also made it possible for fields outside Computer Science to get more exposure globally. One such development, associated with the Internet, is the Internet of Things (IoT) – which is a concept that deals with automation and intercommunication of several hardware products that are interconnected with the Internet. The IoT has gained a lot of popularity since the time, this term was first coined globally. The utility of IoT cannot be counted individually in this era of modernization – be it checking the kind of liquid present in a glass, to measuring happiness in people just using simple hand-bands, to remotely updating the magnitude of fertility, to remotely checking on patients – IoT is still claimed to be just developing in the field Computer Science. With IoT, the Internet becomes a strong base that connects all other components of things into one place, in a single platform. With the development of IoT, there has been a noticeable increase in the efficiency of utilization of the resources along with visible minimization of human effort due to automation. It helps a lot these days to save time and prosper in other fields of Computer Science, including Artificial Intelligence, Big Data, Cloud Computing, High-Performance Computing, Machine Learning, Data Mining, etc. The connectivity is one of the major features of IoT along with integrity with other models and analysis of data. Every IoT devices have a unique identity and they exhibit a beautiful advantage of having low-power embedded systems that work efficiently without the consumption of more battery power; they are also self-configuring which helps them adapt to changes on their own in a dynamic fashion. The physical architecture that is common for all IoT devices includes a sensor that captures the minor or major changes in the surroundings and an actuator that provide a set of outputs on the basis of the conclusion drawn from the sensed data. Like any other network and communication-oriented concept, IoT also has several protocols that are associated with it - the Link Layer protocol of IoT informs the manner in which data can be physically sent over the network or the coding and decoding paradigms for packets; the Network layer plays an essential role in the transmission of IP datagrams over the source and destination network by performing tasks to address the host and to properly route a packet; the Transport layer is, on the other hand, responsible to cater an end-to-end transfer of

Revised Manuscript Received on July 22, 2020.

Debajit Datta, Undergraduate B.Tech., Vellore Institute of Technology, Vellore, India. E-mail: debajit.datta2000@gmail.com

Prof. J. Dheeba, Associate Professor in School of Computer Science and Engineering, Vellore Institute of Technology, Vellore, India. E-mail: dheeba.j@vit.ac.in

message which is independent of the underlying network; the application layer, under the lower layer protocol, guides in interfacing an application for transmission of data over a given network.

This work studies various IoT technologies, and IoT based protocols. It also focuses on the determination of the security issues and several other attacks that are associated with the protocols, and it also highlights the security measures, which are already available over several protocols or externally, to eradicate several security issues on the protocols.

II. IOT PROTOCOLS

The IoT protocols can be broadly divided into four main layers namely, the physical and MAC layer, the network layer, the transport layer and the application layer as shown in Fig. 1. The physical and data link layer consists of protocols like Bluetooth, ZigBee, Wi-Fi. The network layer consists of RPL, CORPL, CARP, 6LoWPAN protocols.

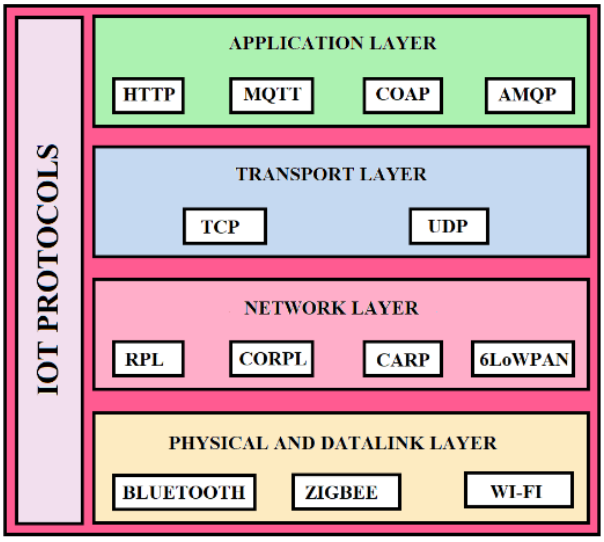

Fig. 1. Architecture of layers of protocol in IoT.

The transport layer consists of TCP and UDP protocols. And the application layer includes HTTP, CoAP, MQTT, AMQP protocols. These protocols are used for providing a proper transmission of communication.

A. Physical and Data Link Layer

- **Bluetooth**

  With the revolutionization of the Internet of Things, the main module which is responsible for generating a wireless connection amongst the several components, that can cover a wide area, is also developing. Bluetooth is one of the widely used communication technology that provides a wireless mode of communication. Bluetooth is cheap and is also known for the consumption of low power. Bluetooth is widely used for ad-hoc communication for transmitting data and voice over a short-range [27]. The radio range which is associated with it is approximately 2.45 GHz and the bandwidth which is achievable ideally is around 1 Mb/s. The physical layer and the link-layer for Bluetooth are standardized by the IEEE802.15 committee.

- **ZigBee**

  Like Bluetooth, ZigBee is also a technological standard for IoT. It is designed mainly for supporting the control networks and the sensor networks, ZigBee is developed to perform operations in mainly the Personal Area Networks (PAN) and the device-to-device networks, since the connectivity that is established is between the small-packet devices. It is standardized by the globally accepted committee, the IEEE802.15.4 committee. Like Bluetooth, ZigBee is also reliable and is cheap, and it is known for the consumption of low power which is ideal for the small IoT devices which do not have a high-power storage capacity [28]. ZigBee provides good scalability since it exhibits a design which is flexible for several applications. It provides transmission in a short-range only.

- **Wi-Fi**

  Wi-Fi stands for Wireless Fidelity which is also used for a monetarily reasonable, high-speed wireless communication. Wi-Fi is versatile and compatible with various Internet Protocol (IP) networks and provides scalability over a larger network. It does not require too much effort or complications in order to install it within a system, rather it can be installed faster than many others. This has been standardized under the IEEE802.11 committee. Wi-Fi provides a strong association when it comes to a scenario where a client requires to have an association with the main access point [29]. It also comes with an authorization feature for providing security.

B. Network Layer

- **RPL**

  Routing over Low Power and Lossy Networks (RPL) typically consists of several embedded devices that have limitations for power and memory. The nodes are organized with formations of Directed Acyclic Graph (DAG) under the surveillance of RPL protocol which has loop detection mechanisms and Destination Oriented DAG (DODAG) repair mechanisms. It helps in controlling and managing the traffic flows between the nodes resulting in point to point, point to multipoint and multipoint to point traffic flow, using the inbuilt distance vector protocol and source routing protocols. The traffic routing is handled by several control messages like the DODAG information object (DIO) which is multi-casted downwards, the DODAG information solicitation (DIS) when a node wants to join a DODAG, DODAG advertisement object (DAO) for requesting child to join DODAG and an acknowledgement message (DAO-ACK).

- **CORPL**

  The Cognitive RPL or CORPL is an extension and modification of the existing RPL protocol that

uses DODAG topology which is known for the usage of a packet forwarding mechanism within the nodes, called the opportunistic forwarding [33]. The opportunistic forwarding provides better support with high-priority delay that utilizes two different techniques to improve the performance. CORPL also helps in providing a practical solution for cognitive Advanced Metering Infrastructure (AMI) networks.

- **CARP**
  The Channel-Aware Routing Protocol (CARP) is a distributed routing protocol for the network layer that is mainly designed for underwater [34] communication. The protocol is oriented with the packets that are lightweight in nature. Overall, the protocol performs various functionalities that are based on initialization of the network and forwarding of data throughout the network, without coverage of support for the data that are collected previously. With CARP, packets of various sizes are allowed to be transmitted, different ratios of transmission and propagation delays are supported by this protocol.

- **6LOWPAN**
  6LoWPAN is an IPv6 address prefixed over Low-power Wireless Personal Area Network. It is generally associated as a fundamental aspect of the transport protocol, which is further defined by the IEEE802.15.4 standard. The nodes present in this are small in size, thus, they are easily controlled by microcontrollers of 8-bit, or the ones with 16-bit, or the one with 32-bit. The packet size of the data to be transmitted is in octets, having 127 bytes. 6LoWPAN is known for its small packet size and reasonably cheap cost [30]. It is generally associated with ad-hoc networks having a star and mesh topology with limited accessibility, powered by low bandwidth.

C. Transport Layer

- **TCP**
  The Transmission Control Protocol (TCP) is based on a three-way handshaking and acknowledgement. The protocol provides several functions like error control where the packets that are received are filtered on the basis of duplication and inconsistency – the duplicate packets are discarded, whereas, the packets that are lost in a transmission are retransmitted in order to maintain consistency of the system. TCP also provides reliability even though the transmission is segmented. It is responsible for the flow control as well as congestion control of the entire transmission.

- **UDP**
  The User Datagram Protocol or UDP is another transport later protocol, where there is no concept for acknowledgement after a transmission. The protocol has no three-way handshaking mechanism either. It is useful for the applications that are time sensitive and do not require a guaranteed transmission delivery.

D. Application Layer

- **HTTP**
  Hypertext Transfer Protocol (HTTP) is an application layer protocol that is suitable for providing several hypermedia resources which is carried out in a method, similar to that of a synchronous request and response model, over the Internet. In IoT, HTTP is not widely used for the reason of being a heavyweight protocol that requires huge amount of energy and power for the IoT, where both are limited. Moreover, the HTTP protocol is ideally designed for at a time communication between two systems. This protocol is also known for utilization of a heavy system of resources, where the advanced Wireless Sensor Networks (WSNs) fail to meet the expectation of being provided with sufficient power [31]. However, the IoT network deals with two broad categories namely the telemetry, which involves data transmission from sensors to server; the other ones is telecommand where the commands are sent across entire networks to control the IoT devices.

- **COAP**
  Constrained Application or CoAP is specifically designed to suit the computer systems that do not have processors that are exceptionally powerful or storage space that is literally unlimited. This provides service to the embedded devices that are bound with very limited power for processing and limited resources too. CoAP has been defined in RFC7252, which provides utility to small and constrained embedded systems having low bandwidth networks. It fulfills all the criteria and requirements to serve machine-to-machine (M2M) communication using a stateless HTTP mapping [29][31]. The transport layer of CoAP is supported by UDP binding which results in lower overheads of the headers that are present. CoAP is based on fixed-length headers which are short in nature and in binary language.

- **MQTT**
  MQTT stands for Message Queuing Telemetry Transport, which provides a communication protocol over lightweight messages for devices in a machine-to-machine (M2M) network. The messages that are transmitted in low network bandwidth and the relative footprint of the associated code is also small in size, such messages are termed as a lightweight [29][31]. This protocol mimics a mechanism similar to that of a publisher-subscriber mechanism. The telemetry data is transmitted without any barrier from a device and it is served to a broker or a server.
  Overall, MQTT provides efficiency over the associated bandwidth and it is also known for utilizing bare

minimum power, which is ideal for embedded systems [32]. Unlike a paradigm that is based on the concept of a request and response, the protocol that is based on a publish-subscribe architecture provides event-driven mechanisms and also provides messages that can be pushed to the clients.

- **AMQP**
  The Advanced Messaging Queuing Protocol (AMQP) is an application layer protocol that is mostly used for business messaging application. The AMQP protocol in a transmission provides provision of point-to-point as well as a publisher-subscriber models.

The protocol is responsible for maintaining a proper routing and queuing protocol. The broker of an AMQP [31] can facilitate receival of messages from the publishers. The broker is also responsible for routing the messages over the available connections to the consumers, who have subscribed to the topics, through messaging queues.

III. ATTACKS AND SECURITY ISSUES

There are several attacks which are enacted on the Internet of Things system that can harm the components associated with the IoT and also the actors or data who are dependent on the system. Hardware Trojan is one of the attacks that is made against the nodes of Radio Frequency Identification (RFID) which performs computations [1][3][13]. There are other attacks on the RFID nodes as well, like the non-network side-channel attack where information that are critical, are retrieved from the nodes; or a Denial of Service (DoS) attack [2][4]. The attacks are generally executed in distributed manner. The edge nodes of an RFID are susceptible to physical attacks and node replication attacks too [1][9][13]; the attacker may succeed in inserting a forged edge node that camouflages and harms the system. The physical attacks can be brutal enough to damage the devices as well as the whole system belonging to IoT. The RFID are susceptible to the problems created by sudden interruption or modification in the system [23]; cloning where a carbon copy of data from RFID is made by the attacked onto a tag created by Electronic Product Code (EPC); snooping attack on the readers of RFID can be utilized in order to skim through the data that is stored. RFIDs are interfered with the help of alteration of the radio frequencies. They can also be vulnerable to interception and fabrication of the system [3]. The forging attacks provides the attackers provision to steal an identity by taking the information taken for authentication to give the network a proof of genuineness of the attacker through the identity. Shim, Kyung-Ah [14] in the work has taken a certificateless signature scheme, L-OOCLS which is lightweight, to mimic a possible universal forgery attack on it. It concludes that the scheme cannot be claimed to a flawless signature for IoT since it can be easily forged. Node tempering and faking the identity [13][19] of a node are carried out by the attackers are targeted mainly to fetch illegally the sensitive information and alter them. Malicious node injection is a kind of node attack where the attacker successfully injects different sorts of malicious nodes. The collision occurs at the victim node, where the watchdog nodes are affected by the announcement of several incorrect messages [19], along with introduction of malicious nodes within the IoT system. There are several issues that are common to mainly the application layer like the malicious code attacks where information is retrieved from several sources by altering the interfaces, the attackers may also mess with mostly the node-based applications in order to alter the consistency of overall system. Sniffers and other attackers can also eavesdrop into the available node data and may create noises by tangling it mainly in the perception layer [2][13]. On creation of an authenticated connection does not perfectly help in eradication of many of the security issues. Attackers take over their threatening moves, faking and hiding their identities as in a masquerade attack. The attackers also successfully impersonate an internal node in order to get access to the confidential information within the network. The attacks that deals with theft [4] of an identity are tricky to identify since they pretend to be authorized nodes. Another common attack is the man-in-the-middle attack where the attacker breaks into a network with an intention to gather information that are exchanged through communications within the nodes in a network. The attacks on several components in the system generates illegal access [8] to private and sensitive information that can control the overall transmission of the system. Studies related to social engineering [10] over various social interactions say that it can be used for influencing a person or a group of persons to forcefully agree upon a request or a set of requests that are made by one or more attackers. Attacks associated with social engineering can be an email phishing or a telephonic vishing or smishing via SMS. Over the years, the vulnerability due to baiting has also increased along with a reverse social engineering. These attacks are very challenging, and most of the time the victim is unaware of the trap, or the mail culprit associated with the work. It has been seen that with proper programming by the attackers, some nodes are made to send wrong and false recommendations which are transmitted to other nodes in their neighbors [11], so that the true nodes get low measure of trust value creating a threatening scenario termed as badmouthing attack. Auditing of the clouds by breaking into the cloud services provided by the vendors in spite of the underlying security alliance [13] with the help of illegally gaining user trust, can be one of the vicious attacks. A software-defined IoT network can be a prey of the Distributed Denial of Service (DDoS) attack where the denial of service is created for the users in a distributed fashion [17]. Packets in huge amount can be sent to the controller pool of a software-defined (SD) IoT controller, depriving the SD-IoT from functioning. In the inter-domain Software Defined Network (SDN) system, the vulnerability of getting affected by DDoS attacks are more. The Link Layer Discovery Protocol (LLDP) are practiced by the SDN controllers that can discover various topologies of the underlying networks making them

susceptible [20] to easy leaks of data over the inter-domain links. In the Wireless Sensor Network (WSN), most of the attacks are based on the channels amongst the nodes present. Jamming attacks, where the communication channels are purposefully disordered, and Tampering attacks, where the nodes are damaged and access is fiddled [5][13], are highly associated with the WSN physical layer. To the WSN data link layers, the main threats include collision over nodes, that ends up with a mismatch over checksum value, and exhaustion of resources that occurs mainly when recklessly the requests or data transmission are repeated in a WSN. The network layer of the WSN is susceptible to Sybil attack where a malicious node can pretend to have multiple identities, making it difficult to detect. Another attack where heavy power is transmitted by hello flood attack broadcasting over the network. A flooding memory exhaustion in the transport layer can alter the network by making several requests for setting up a connection, over and over.

A desynchronization can be established by breaking and destroying the connection that has been creating for preventing the transmission of data. Eavesdropping attacks are carried by several sniffing tools like the packet sniffers [13] which are intended mainly for gathering private information from the WSNs. Since, the WSNs are, for most of the time, used in order to collect data from several sources [21], physical challenges that are associated with it include storage problem. The WSN are vulnerable to sleep deprivation attacks as well, where repetitive requests [23] are sent by the attacker on the node to finish up the power it has.

In the Wireless Sensor Network (WSN), most of the attacks are based on the channels amongst the nodes present. Jamming attacks, where the communication channels are purposefully disordered, and Tampering attacks, where the nodes are damaged and access is fiddled [5][13], are highly associated with the WSN physical layer. To the WSN data link layers, the main threats include collision over nodes, that ends up with a mismatch over checksum value, and exhaustion of resources that occurs mainly when recklessly the requests or data transmission are repeated in a WSN. The network layer of the WSN is susceptible to Sybil attack where a malicious node can pretend to have multiple identities, making it difficult to detect.

Another attack where heavy power is transmitted by hello flood attack broadcasting over the network. A flooding memory exhaustion in the transport layer can alter the network by making several requests for setting up a connection, over and over. A desynchronization can be established by breaking and destroying the connection that has been creating for preventing the transmission of data. Eavesdropping attacks are carried by several sniffing tools like the packet sniffers [13] which are intended mainly for gathering private information from the WSNs. Since, the WSNs are, for most of the time, used in order to collect data from several sources [21], physical challenges that are associated with it include storage problem. The WSN are vulnerable to sleep deprivation attacks as well, where repetitive requests [23] are sent by the attacker on the node to finish up the power it has.

There are several attacks on other protocols like Wi-Fi where there are Address Resolution Protocol (ARP) spoofing where packets are transmitted over the routes. Bluetooth devices are vulnerable to DoS, passive listening attack and man-in-the-middle attack [18]. Bluetooth protocols can also be a target of bluejacking and blue-snarfing attack, where the attackers are able to send unwanted messages to the devices that are present in the zones and are able to get private information as well. ZigBee is vulnerable to attacks where the keys are theft for binding the systems of certificate. There are encryption attacks like the side-channel attacks that are on various IoT based devices [19][30], because the cryptanalysis attacks with ciphertext only attacks, known or chosen plaintext attacks, ciphertext attack and man-in-the-middle attack. The keylogger is coded by the attackers [23] for coming up with an interface similar to that of the original, which can be confused of being the legitimate interface by the users. The attackers in this way captures the details of the key punches in order to fetch the data, which is usually authentication data that can be used for further breaking into the system. Based on the research work of Ronen, Eyal, and Adi Shamir [25], the attackers behavior can be classified as the one where the functionality of the device is ignored by them; or the functionality is intentionally reduced by them; or the functionality is misused by them or the functionality is extended by them – in their research work, they studied the case of hacking LED lights in order to come up with a possible scenario where data leakage is taken place without the involvement of any sort of wireless connection, from just an air-gapped and Tempest protected networks. In the MQTT protocol [32], the overall security of the system is totally dependent on how the user is going to use it, since it comes with an authentication system with username and password, along with TLS based handshaking property.

There are some challenges to the Bluetooth technologies as well, where the attackers can illegally view the different links that are associated with different Bluetooth versions, and even modify them [27]. Apart from that, the Bluetooth encryption technologies can also be deciphered if the length of the encryption key is not a complex one. Unlike Bluetooth, the 6LoWPAN networks suffer from security issues that are generated through congestions [30], because of heterogenous devices in large quantities. Attacks are not only confined to the protocols in the Internet of Things, rather they are targeted on the devices and the users as well. The Internet of Things has a wide range of applications, and thus all those applications are vulnerable to attacks and threats as well. A research work [21] has revealed that the data that is collected from devices installed into smart home, in a continuous fashion, can leak some private and sensitive activities of the people inside the house; similarly, in a smart grid, attackers can break into the system and alter the integrity and consistency of the data by falsifying the collected data measures or, changing the overall billing.

Another study has stated that there are several devices in the market that are vulnerable to be attacked by the attackers and which can also put the users into danger. Smart toys for children as mentioned in the research by Valente et al. [12] can be altered by attackers in order to have private conversations with the children playing with them and can grab personal information about the household, lifestyle and worse, can affect the mental growth of children. There are also IoT based drones and intimate devices that can be altered in order to attack the users physically and mentally without their affirmative consent about the same. The research states that during their research period, some applications and products like some surveillance camera, drones, etc., [12] were vulnerable to being tampered. On being tampered, the attackers might have a purpose of fetching details about user without their consent and also can assault them as well.

Some of the products lack the requirement of having a user authentication on the device or on the application, or may be on both. Some products are also vulnerable to disclosure of session token and proper encryption of data. A device scanning attack can be done on some IoT devices [16] since many users who use the devices do not change the password that has been set as default, so, the attacker can easily set an authentication message breaking the security and get the whole MAC address of the system. A device spoofing attack can also be initiated where the attacker selects the target MAX address and registers a spoofed plug, ending up into the victim's close vicinity like a smartphone or application. A firmware attack is also quite possible in an IoT device, where malicious firmware is loaded onto the victim's system, which can be used to decode or get information about the password and other sensitive data or even modify the system data.

IV. SECURITY COUNTERMEASURES

Over the years, there has been drastic advancement for providing more security to the components of the Internet of Things. There are many measures that are taken for analyzing the side-channel which can help in the detection of Trojan and identifying the malicious software or firmware within a system [1]-[3]. A Trojan activation method can also be undertaken that can provide easy detection of Trojan. There are mechanisms which are based on various policies that can also be utilized in order to detect various kinds of intrusion on the different systems. Along with IDS, there are some cryptographic schemes that are used for strong encryption for facilitating a secured communication in efficient way. There are also methods which undergoes de-patterning of the network that also decentralizes the nodes [1] within the network. There has been development of Keep in Touch and Closed Loop Hierarchy that can be implemented into the networks in order to enhance the services that are provided by mainly the RFID and Near Field Communication (NFC). There are approaches that extends the Domain Specific Metrics (DSM) that provides better analysis of the incoming threats and maturity of the system [2].

Some principles are proposed that uses a defense frame for providing security in a dynamic fashion by analyzing and computing the incoming threats and danger. Message Authentication Code (MAC) is used for verification [8] of the data integrity and also check the authenticity of the users and nodes. A secured and encrypted protocol of communication can be implemented for security or a mutual authentication system between the nodes and the server can also limit many attacks. An anti-bot mechanism which is used widely these data, can also be used to mitigate the attacks which are based on brute force [16] or and Intruder Detection System can also be installed. An edge layer security service can associated with the RFID tags [21] so that the security management tasks can be promoted from the end devices having comparatively less capability to the ones having comparatively higher capability and power, which can be integrated with the intrusion detection algorithms in order to be able to identify whenever an attack is made on the system.

The work of Mishra et al. [22] deals with a system that can predict sybil attacks, which are of two types – the one where entire set is simultaneously used for attacking, and the one where the attacker is trained enough to alter the overall set of identities that could have been used to predict an attack under process. The algorithm is implemented with machine learning algorithm, K-mean clustering in order to have an interpretable visualization of the way an attacker is set to launch the location selection process, which is fed to the launching phase of the system that uses an identity replacement model in order to disclose the forged identity.

Encryption algorithms are mixed and strengthened to come up with better algorithms [3] that provides integrity amongst the data by securing the overall transmission like the usage of the Advanced Encryption Standard (AES), which is known for its simplicity and reliability, with that of the Elliptic Curve Cryptography (ECC) in the field of information security. The Secure Mediation Gateway (SMGW) has been developed to facilitate managing of a secured connection for the communication amongst the nodes within the network and for that of the nodes amongst various SMGW networks. The password-based authentication is widely used method for verifying the authenticity of a user or a node as an authentication mechanism in the IoT. There is also a token-based authentication system as a part of the authentication mechanism [4] which is further divided into soft and hard tokens. There are methods including smartcard, ECC, hashing technologies, password and RFID, biometric cryptography, Diffie-Hellman, AES, Rivest Shamir Adleman (RSA) algorithm for providing security within a system. The security of ZigBee can be provided with keys, the RF fields are of Near Field Communication (NFC) have inbuilt security in them along with other security levels in Bluetooth [18] and WPA2 certification for Wi-Fi security. There are also backup networks [23] that are used to aid the underlying network by providing a outages-free cellular network for the system built across WLAN networks. End-to-end communication for the

Internet of Things [21] is essential for safety enhancements which are associated with the Internet based applications. Symmetric encryption algorithms like AES and other hash functions are utilized in the Physically Unclonable Function (PUF) hardware in order to have a better security solution. IP based security using end-to-end protocol can be categorized into 6LoWPAN based and IPv6 based security solutions, wherein there is a two-way authentication before transmission of data. For the network layer of IoT there has been several security measures like it is provided with encryption algorithms like the Cyclic Redundancy Check (CRC) for monitoring [23] the overall integrity of the system; followed by payload security integrated with digital signatures for verification of identities and minimizing the fake identity threats by the attackers; the routing of the packets of data that are transmitted within the network, are tracked by a technique, termed as Delap Per Hop Indicator (Delphi) which identifies the packers throughout the transmission.

According to the work of Wang et al. [28], AES-128 encryption in ZigBee technology can be helpful in securing the protocol stack structure along with the associated the individual characteristics and functions of them. Their study has studied the overall performance of the encryption system and has analyzed the achievable optimization from the round operation optimization algorithm to the column confusion optimization algorithm. The work of Al-Kashoash et al. [30] proposes mechanism to gain control over the congestions in data channel of 6LoWPAN and WSN.

The proposed algorithm begins with detection of congestion within several data channels, by consideration of the load, losses and delays that are associated with the transmission; next an implicit or and explicit congestion notification is sent either via piggybacking or through separate overheads; finally the congestion is controlled by controlling the traffic, and considering other parameters like throughput, fairness, latency, etc. On controlling congestions, the malicious packets can also be reduced over the data channels.

WSN are blessed with several security aspects like the SVELTE for detection of any form of intrusion within the system in a sophisticated manner [5] that majorly deals with IPv6 over the technologies having 6LoWPAN. A RIDES is a Robust Intrusion Detection System which is a part of the Intrusion Detection System (IDS) that can simulate the properties of NS2 in order to provide the concept of Bloom filter and CUSUM charts. The DEMO protocol can be used for determining the DoS detection on the systems in a WSN. IoT security can be improved by implementing machine learning algorithms [9] can be implemented for detection of threats and provide solution for the security issues. Classification learning with the Support Vector Machine (SVM), Bayesian Theorem, K-Nearest Neighbor (KNN), Random Forest (RF), Association Rule (AR) can be applied on to the system for determination of several parameters for security purpose.

Regression learning like Decision Tree (DT), Neural Network (NN), Ensemble Learning (EL) can be used for detection of present anomalies or malware in the system and awareness of intrusion [9]. Unsupervised learning under machine learning can also be utilized like the Principle Component Analysis (PCA), K-mean Clustering for feature selection in order to provide better security. Reinforcement Learning can be adopted for authentication and jamming attacks along with malware detection. The research work of Ahmed et al. [20] devote towards identifying the anomalies that occur in the traffic that occurs while transmitting data over an SDN. A Gaussian function is proposed that can be implemented to the Self Organizing Maps (SOMs) to help in cover the topologies faster. In the work, the SDN feature has been highlighted where it offers to delegate network security tasks in order to provide the users of the host network complex security management tasks.

The system proposed by Li et al. [6] is specifically designed to detect any sort of abnormality in dissipation of power pattern which are generally caused either by the physical attacks or maybe from some cyber related attacks as well. Using deep learning algorithms, the model is trained to preprocess the input energy pattern of a system, which has put Convolutional Neural Network (CNN) with a rectified linear unit (ReLU) activation function. The overall dispute and anomaly can be detected by mapping an ideal graph with that of the graph obtained which provides information about the attacks on the system. This proposal is said to correctly predict the anomalous behavior which are cyber or physical oriented.

The work of Zhang et al. [7] proposes a secured system of transmission which is Relay-Aided Vectorized (RAV) in order to provide a secured communication within the IoT network under a Bit Error Rate (BER) of 0.5 irrespective of channel. The algorithm focuses on mainly the downlink of a communication which can be from the controllers of a system to the system-actuators. The system claims to prove its effectiveness and high-end security through various security analysis. Reddy et al. [11] propose a system that resolves the problem of attacks in IoT based on badmouthing by taking both direct and indirect trust through their proposed algorithm. The algorithm computes the measure of direct trust through measures like the data members called packet sent and packet forward, similarly the indirect trust is measured completely based on their algorithm finally they calculate the total measure for node trust where a weight is multiplied with both the trust values and added.

The system of Doshi et al. [15] propose a machine learning based detection of DDoS attacks. In the system, the traffic data is collected which are worked onto the next module of the system, which extracts features which are involved with predicting DDoS. K nearest neighbors, linear kernel based SVM (LSVM) are used along with DT, RF and NN to come up with the selection of optimized hyperparameters that can be used to predict the attacks of DDoS. The precision and recall of the system are high, thus the F1 score which is the harmonic mean of these two metrics, are also high.

The work of Yin et al. [17] deals with a system that can be used for detection of a DDoS attack by taking the cosine similarity of the vectors produced by taking the packet-in rate of input port and distributing them as separate vectors X and Y of k length. If the found cosine similarity has a value higher than that of the normal flow, it is concluded that there has been a DDoS attack, and the corresponding packet can be rejected. The work of Yan et al. [24] deals with a multilevel DDoS mitigation framework (MLDMF) where the entire system is broadly categorized as the edge computing level that consists of SDN-based industrial IoT Gateways (SDNIGWs); the next level of the system is the fog computing level that industrial IoT management control unit (IMCU) for securing the controllers and the applications which are based on the SDN; the final level is the cloud computing level dealing with the cloud services and big data technologies.

The authentication techniques are evaluated on various parameters like the average response time which is taken care by the server, the time taken to complete the handshaking process between the nodes present in a network. The memory consumption is also one parameter that can be used for assessing the overall authentication system. The overall delay and throughput of the transmission can also serve as evaluation criteria [4]. The cost of a transmission with respect to size of the message that is needed to be paid for transmission, can be considered as a parameter for evaluating the technique, in association with the memory, storage and energy costs. The proposed Lightweight Distributed Access Control system with Keyword Search (LDAC-KS) can be utilized along with integration with the pairing-based cryptography [8] and it also helps in retrieving the keyword search that are based on ciphertext that are stored within the cloud server.

This system can also provide support in getting data without data confidentiality. A secure application code can technically help in reducing attacks on the application layer, along with educating the system users in order to complicate the password [13][16][23], which cannot be easily guessed or backtracked using the mechanisms like the brute force algorithm. The agreements that are to be facilitated should be key-based along with an enabled log monitoring and database monitoring system that should be able to surveil the systems in the absence of the human.

Firewalls, antivirus software and antimalware software are being installed to protect the system from direct attacks onto the system by the attackers; some access to a network are also given only after the permission is granted by the Access Control Lists (ACL) [23], which can also be used to monitor the some sort of intrusion detected within the network, or some suspicious activities around the network. The work of Ronen, Eyal, and Adi Shamir [25] has proposed that usage of security protocols that are standardized, or a TLS protocol where the certification is focused on in order to establish a secured connection.

V. CHALLENGES TO BE ADDRESSED IN FUTURE

There are still a few challenges related to the overall security of the system that are yet to be worked on and solved in the future in order to save the IoT systems, data associated with them and the users of the systems. Most of the present security measures for the IoT devices are based on a fixed number of users, but the evolving challenges come up when the overall users increase or decrease unexpectedly or have a sudden increase in the count of links that are potentially weak and vulnerable to attacks [1][3]. Apart from these, there are other physical damages that can be done into the Internet of Things components along with insisted cut off of power or hardware failure [2] and tampers that are done on the physical components.

The further challenges in IoT include the target of several integrated modules belonging to the system which includes the foremost standardization of the entire system, which is then followed by the deployment challenges and preservation of confidential data. The Distributed Denial of Service (DDoS) attacks [5][15][20] are a threat of the entire community which is based on the Internet. The algorithm proposed to detect DDoS using machine learning algorithms, are still theoretical, and not tested under an actual environment where the traffic is not constant and keeps on changing all the time, thus making it unpredictable in nature. Examining the flow of the packets at the domains of the intermediate SDN need to be efficiently mitigated so that the victim systems of the network are not affected with the DDoS attacks [20]. The algorithms and techniques that are already present for the several components of the IoT systems [19], should be lightweight and effective, so that, the IoT devices are secured. The PUF hardware technology and end-to-end protocols [21] can be useful for securing the systems up to certain extent, but thereafter further challenges arrive including the overall safety of the device at the ends, because the system only has a two-way authentication, thus minimum protection can only be provided to the end devices. Moreover, the end-to-end protocol is a heavy method that requires proper storage space and power supply, which is difficult to provide when it comes to the IoT devices.

VI. RESULTS

In the theory proposed for the end-to-end protocol, the heterogeneity of the devices and underlying network is ignored, but in a real-time application, there are ought to be variation with the networks or the devices, developing problem in communication. The fields that are associated with IoT like big data analytics, blockchain technologies [24], cloud computing, data mining, etc. must also be protected since these fields are also vulnerable to attacks, and can affect the entire system including the IoT. The routing attacks are also evolving, like the sinkhole attack where, in a Wireless Sensor Network (WSN), the data which is collected from various nodes with their sensors are forwarded to the sink node instead of the main sub-branch of the WSN.

Another important attack to be addressed is the guessing attack wherein, the attacker tries to predict the actual authenticated password from the server in order to authenticate themselves [4] as a valid user. It is hard to achieve since the tries are either achieved through algorithms of pretty high complexity, like the dictionary attack and brute force attack. Development in Quick Response (QR) codes provide a great impact on the security of the authentication system. Though systems have been developed to manage potential pilot contamination attacks on the system [7], intelligent eavesdropper problems, which can come up with different strategies suiting a scenario the best, are yet to be addressed. Several algorithms have been developed for securing the cyber transmissions including Rivest Shamir Adleman (RSA), Secure Hash Algorithms (SHA), and many more, but the problem exists in implementing the same within the IoT systems that are aided with limited power and storage capacity. Moreover, these algorithms are very time-consuming to execute [13], thus these are not feasible to secure the transmission of real-time data over the networks. The security that is provided by various encryption algorithms is not completely secured because of the fact that the attacker can crack an obfuscation algorithm [16] by a simple eavesdrop into the plaintext. The algorithm proposed in [22] is claimed to achieve a coverage of 48.7% which is comparatively less along with the fact that it has assumed a hypothetical situation where only single node that is compromised, which is not a real-life scenario, thus, the system can further be improved. The IoT proposals mostly focus on the interoperability [29], but the usage of semantic web technologies and the interworking API is still to be mined for better grasp over a network, and in order to come up with more security. Even though machine learning algorithms have been integrated and implemented to support the security of the overall system, but it should be kept in mind that the dataset to be used for training the system must be clean and clear and reliable for observation of various attributes that are present and can be related in order to fetch a proper output [9].

The data must also be relevant and consistent and must be sufficient for the associated predictions. The attacks made with the help of social engineering are unpredictable in nature, making it difficult for the system to understand a forthcoming attack. Since the attacker uses reverse social engineering, along with other power moves, it becomes almost impossible to identify them, since the confidentiality is breached under the presence of the victim over a secured middleware [10]. These kinds of attacks are yet to be addressed, but they provide a wide range of associated attacks along with it. There are many ideas and algorithms that are proposed theoretically and tested in a simulated environment but are yet to have physically experimented on the actual systems in an actual environment. These algorithms are accepted after a small-scale experiment need not be proactive and dynamic in nature when it comes to load balancing, which is an important challenge that is needed to be overcome because an IoT device has limited power and memory storage. Some vulnerability in the products' privacy can be used as a weapon to affect the mental and physical health of innocent users of all age groups, irrespective of their genders.

VII. CONCLUSION

There have been several improvements in security that have helped to secure the overall system based on the Internet of Things, but parallelly, the attacks have also increased and mutated over time. One of the greatest reasons of why securing IoT is very challenging is because of the fact that it includes heterogenous modes of communication and devices – the range of functionality provided by the IoT devices are also enormous as a result the amount of data produced by them is also huge and, at some point, unmanageable too. Some of the attacks on the actors of the IoT, are yet to be addressed like that created by social engineering and reverse social engineering; it is because, even if technically one succeeds in securing a cent percent accurate secured system, but there should be ways to control leak of entire confidentiality on an unintentional disclose of a single piece of information by a human being.

IoT is a broad field, thus consists of several associated fields like big data analytics, cloud computing, etc. which must also be addressed while securing IoT, since, these technologies go hand in hand, thus disturbance in one of these, is tend to affect the entire system. The systems can still be made to be highly secured by improving the existing systems, but there are attacks that are targeted on innocent users of the system, who unknowingly end up giving private information about the systems to the attackers. The attackers can try to come close to the vicinity of the victim, pretending to be caring and understanding, but later use their power moves to fetch information and backstab the victim. Therefore, meanwhile, educating the users who are associated directly or indirectly with the Internet of Things systems, should also be taken care.

The users must also be made aware of the underlying securities within the system and must be trained with the possible preventive measures that can help in the reduction of the leak of information from the user side. Some proposed approaches are yet to be tested on actual physical devices and are yet to be experimented under dynamic conditions, in order to conclude the real feasibility of the systems. The IoT can be protected along with the users, if the untouched or open challenges are somehow solved. In future, the issues that are discussed can be addressed and new protocols and security measures can be researched on. Improvements can be made on several aspects of the IoT protocols and layers, along with better routing and monitoring services. Security in the application layer must also be improved to reduce the dirty attacks made by fooling innocent users. The IoT field is growing bigger every single day and is yet to be discovered more.

ACKNOWLEDGMENT

Words are nothing but token of gratitude. We would like to thank our friends and colleagues who have been more than just supportive and encouraging when it was about this work. We would also like to thank other faculty members who guided us with more knowledge and insight in coming up with this successful work. We are also grateful to the other authors who have put in all their efforts in coming up with their researches, without which this project would not have been possible. Their research work has given us a deep insight to the vivid topics of Computer Science, including the Internet of Things and Cyber Security. Numerous facts and figures have come up that we were previously unaware of, and we would always be grateful to know those things.

REFERENCES

1. Mosenia, Arsalan, and Niraj K. Jha. "A comprehensive study of security of internet-of-things." IEEE Transactions on Emerging Topics in Computing 5.4 (2016): 586-602.
2. Kumar, Sathish Alampalayam, Tyler Vealey, and Harshit Srivastava. "Security in internet of things: Challenges, solutions and future directions." 2016 49th Hawaii International Conference on System Sciences (HICSS). IEEE, 2016.
3. Oracevic, Alma, Selma Dilek, and Suat Ozdemir. "Security in internet of things: A survey." 2017 International Symposium on Networks, Computers and Communications (ISNCC). IEEE, 2017.
4. Nandy, Tarak, et al. "Review on Security of Internet of Things Authentication Mechanism." IEEE Access 7 (2019): 151054-151089.
5. Adat, Vipindev, and B. B. Gupta. "Security in Internet of Things: issues, challenges, taxonomy, and architecture." Telecommunication Systems 67.3 (2018): 423-441.
6. Li, Fangyu, et al. "Enhanced cyber-physical security in internet of things through energy auditing." IEEE Internet of Things Journal 6.3 (2019): 5224-5231.
7. Zhang, Ning, et al. "RAV: Relay aided vectorized secure transmission in physical layer security for Internet of things under active attacks." IEEE Internet of Things Journal 6.5 (2019): 8496-8506.
8. Harbi, Yasmine, et al. "A review of security in internet of things." Wireless Personal Communications 108.1 (2019): 325-344.
9. Tahsien, Syeda Manjia, Hadis Karimipour, and Petros Spachos. "Machine learning based solutions for security of Internet of Things (IoT): A survey." Journal of Network and Computer Applications (2020): 102630.
10. Ghasemi, Mohsen, Mohammad Saadaat, and Omid Ghollasi. "Threats of social engineering attacks against security of Internet of Things (IoT)." Fundamental Research in Electrical Engineering. Springer, Singapore, 2019. 957-968.
11. Reddy, Vijender Busi, et al. "A Similarity based Trust Model to Mitigate Badmouthing Attacks in Internet of Things (IoT)." 2019 IEEE 5th World Forum on Internet of Things (WF-IoT). IEEE, 2019.
12. Valente, Junia, Matthew A. Wynn, and Alvaro A. Cardenas. "Stealing, spying, and abusing: Consequences of attacks on internet of things devices." IEEE Security & Privacy 17.5 (2019): 10-21.
13. Ali, Inayat, Sonia Sabir, and Zahid Ullah. "Internet of things security, device authentication and access control: a review." arXiv preprint arXiv:1901.07309 (2019).
14. Shim, Kyung-Ah. "Universal Forgery Attacks on Remote Authentication Schemes for Wireless Body Area Networks Based on Internet of Things." IEEE Internet of Things Journal 6.5 (2019): 9211-9212.
15. Doshi, Rohan, Noah Apthorpe, and Nick Feamster. "Machine learning ddos detection for consumer internet of things devices." 2018 IEEE Security and Privacy Workshops (SPW). IEEE, 2018.
16. Kumar, Sathish Alampalayam, Tyler Vealey, and Harshit Srivastava. "Security in internet of things: Challenges, solutions and future directions." 2016 49th Hawaii International Conference on System Sciences (HICSS). IEEE, 2016.
17. Yin, Da, Lianming Zhang, and Kun Yang. "A DDoS attack detection and mitigation with software-defined Internet of Things framework." IEEE Access 6 (2018): 24694-24705.
18. Chahid, Yassine, Mohamed Benabdellah, and Abdelmalek Azizi. "Internet of things security." 2017 International Conference on Wireless Technologies, Embedded and Intelligent Systems (WITS). IEEE, 2017.
19. Deogirikar, Jyoti, and Amarsinh Vidhate. "Security attacks in IoT: A survey." 2017 International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud)(I-SMAC). IEEE, 2017.
20. Ahmed, M. Ejaz, and Hyoungshick Kim. "DDoS attack mitigation in Internet of Things using software defined networking." 2017 IEEE third international conference on big data computing service and applications (BigDataService). IEEE, 2017.
21. Sha, Kewei, et al. "On security challenges and open issues in Internet of Things." Future Generation Computer Systems 83 (2018): 326-337.
22. Mishra, Alekha Kumar, et al. "Analytical model for sybil attack phases in internet of things." IEEE Internet of Things Journal 6.1 (2018): 379-387.
23. Shah, Sameena, Syed Suhail A. Simnani, and M. Tariq Banday. "A Study of Security Attacks on Internet of Things and Its Possible Solutions." 2018 International Conference on Automation and Computational Engineering (ICACE). IEEE, 2018.
24. Yan, Qiao, et al. "A multi-level DDoS mitigation framework for the industrial internet of things." IEEE Communications Magazine 56.2 (2018): 30-36.
25. Ronen, Eyal, and Adi Shamir. "Extended functionality attacks on IoT devices: The case of smart lights." 2016 IEEE European Symposium on Security and Privacy (EuroS&P). IEEE, 2016.
26. Parker, Donn B. Fighting computer crime. New York, NY: Scribner, 1983.
27. Lonzetta, Angela M., et al. "Security vulnerabilities in Bluetooth technology as used in IoT." Journal of Sensor and Actuator Networks 7.3 (2018): 28.
28. Wang, Yongkang, Chunxia Chen, and Qijie Jiang. "Security algorithm of internet of things based on ZigBee protocol." Cluster Computing 22.6 (2019): 14759-14766.
29. Noura, Mahda, Mohammed Atiquzzaman, and Martin Gaedke. "Interoperability in internet of things: Taxonomies and open challenges." Mobile Networks and Applications 24.3 (2019): 796-809.
30. Al-Kashoash, Hayder AA, et al. "Congestion control in wireless sensor and 6LoWPAN networks: toward the Internet of Things." Wireless Networks 25.8 (2019): 4493-4522.
31. Naik, Nitin. "Choice of effective messaging protocols for IoT systems: MQTT, CoAP, AMQP and HTTP." 2017 IEEE international systems engineering symposium (ISSE). IEEE, 2017.
32. Soni, Dipa, and Ashwin Makwana. "A survey on mqtt: a protocol of internet of things (iot)." International Conference On Telecommunication, Power Analysis And Computing Techniques (ICTPACT-2017). 2017.
33. Aijaz, Adnan, Hongjia Su, and Abdol-Hamid Aghvami. "CORPL: A routing protocol for cognitive radio enabled AMI networks." IEEE Transactions on Smart Grid 6.1 (2014): 477-485.
34. Basagni, Stefano, et al. "CARP: A channel-aware routing protocol for underwater acoustic wireless networks." Ad Hoc Networks 34 (2015): 92-104.

AUTHORS PROFILE

Debajit Datta is currently a third-year undergraduate pursuing Computer Science and Engineering from Vellore Institute of Technology, Vellore. He is an experienced front-end developer with experience of working in the non-profit organization management industry. He has been an active member of the clubs and chapters in the university and has participated is several hackathons at university level. He has been an active member of Developers Student Clubs VIT, a student chapter powered by Google Developers Group and Venturesity VIT, a student chapter. He has industrial exposures from five different industrial internships within the three years of B. Tech. He has also presented a research paper at ic-ETITE'20 conference organized by IEEE and supported by ACM. Email: debajit.datta2000@gmail.com

Prof. J. Dheeba, completed her B.E and M.E in computer Science from Anna University Chennai. She completed her Ph.D from Anna university chennai in the year 2013. Presently she is working as Associate professor in School of computer science and engineering, VIT, Vellore having rich teaching and research experience of 12+ years. Her areas of interests are Algorithms, Medical Imaging, Deep Learning. Email: dheeba.j@vit.ac.in