Journal of Theoretical and Applied Information Technology
30th September 2022. Vol.100. No 18

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

THE SECURITY CONCERNS AND SOLUTIONS FOR CLOUD-BASED IOT SYSTEM

MAHENDRA DEORE[1], DEEPAK MANE[2], GOPAL UPADHYE[3], NILOFER KITTAD[4]

[1]MKSSS's Cummins College Of Engineering For Women, Pune-411052, Maharashtra, India

[2]JSPM's Rajarshishahu College Of Engineering, Pune-411033, Maharashtra, India

[3]Pimpri Chinchwad College Of Engineering, Pune, Maharashtra, India

[4]MKSSS's Cummins College Of Engineering For Women, Pune-411052, Maharashtra, India

E-Mail: [1]mdeore83@Gmail.Com, [2]dtmane@Gmail.Com, [3]gopalupadhye@Gmail.Com,

[4]kittadnilofer@Gmail.Com

ABSTRACT

From recent times our day to day life has significantly started to depend on the technological advancements of the Internet of Things. IoT has made it possible to converge the abilities of almost all types of devices ranging from small hand held devices to massive machines. Any system based on IoT infrastructure needs to deal with the issues of collection, storage and analysis of humongous data. Using external cloud servers is more convenient than the other alternative of being responsible for onsite storage but the issue of security and privacy need to be addressed in this case. This paper primarily focuses on the analysis of possible security threats for cloud based IoT systems. The authors have classified the security challenges for such a system and have presented a detailed survey of the techniques of cryptographic solutions to address the identified challenges. The authors have also suggested the security techniques and tools that can be used at each layer of the cloud service provider.

Keywords: *Internet of Things, Cloud, Cryptography, Encryption, Security and Privacy.*

1. INTRODUCTION

Internet of Things (IoT) performs a noteworthy part within all elements of our everyday lives. It covers a wide range of sectors to encompass applications in the zone of keen human services, smart homes, savvy urban communities etc. [3]. Figure 1 depicts the applications of IoT in our various domains. The extensiveness of IoT facilitates some of the regular activities, enhances the manner in which individuals connect with the environment and surroundings, and expands our social associations with other individuals and entities. IoT gives rise to enormous measures of information, and cloud computing provides a mobility route to this information. The cloud has turned out to be an aid to all sorts of IoT based organizations. Many IoT cloud suppliers exist in the market at present to use appropriate and particular IoT based services [4]. It has enhanced the financial effectiveness of several business-critical processes. Cloud is becoming one of the vital sections of the IoT framework.

At the onset of the cloud computing era, organizations were extremely concerned, and legitimately so, about the privacy of the information. This was both, from the point of view of administrative reasons and security. A lot of enterprises refused to allow data that was critical to their business to reside on the servers of an external provider [5]. These obstacles have been largely overcome with the existence of cloud stages that are public and the same rigid levels of security along with rigorous administrative controls that can be found on private clouds or in-house foundations. Various Cloud service suppliers charge a compensation for each utilization, which implies that you pay for the assets that you utilize and nothing else. Economies of scale is another manner by which cloud suppliers can profit from new, smaller IoT businesses and reduce the general expenses of IoT organizations.

Another advantage of Cloud Computing for IoT is that it empowers better merging which is fundamental for engineers today. By enabling engineers to store and

access information remotely, engineers can get to the information promptly and deal with ventures immediately. At long last, storing information in the Cloud, allows IoT organizations to change rapidly in a straightforward manner, and allot assets to various regions.

The entire cloud based IoT architecture consists of various dynamic physical things, sensors, actuators, cloud administrations, particular IoT conventions, correspondence layers, clients, designers, and an undertaking layer and so forth. At a high level, cloud based IoT can be considered as a three-layered architecture comprising: Device Zone, Data Transmission Zone, Gateways and Cloud Services Zone. Figure 2 below describes each zone separated by boundaries. Zones are a comprehensive approach to fragment a solution, every zone maintains its own data, authentication procedures and authorization requisitions. Zones also perform the function of separating the damage and limiting the effect of zones with a low trust on zones with a higher level of security.

The device zone can be defined as the physical space that is immediately in the vicinity of the device. It is in this space that physical access to the gadget is possible along with extra local network distributed computerized access. Gateway is a gadget/apparatus or some broadly

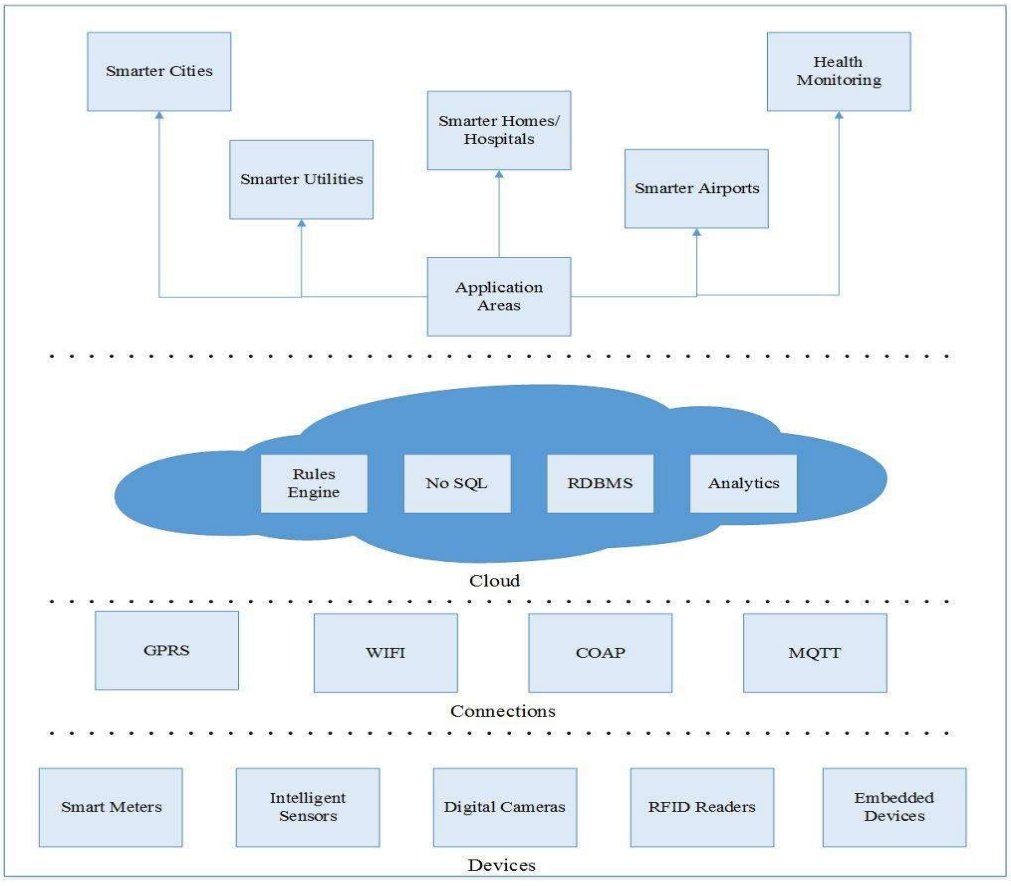

Figure 1: Internet Of Things And Its Various Application Areas

Journal of Theoretical and Applied Information Technology
30th September 2022. Vol.100. No 18

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

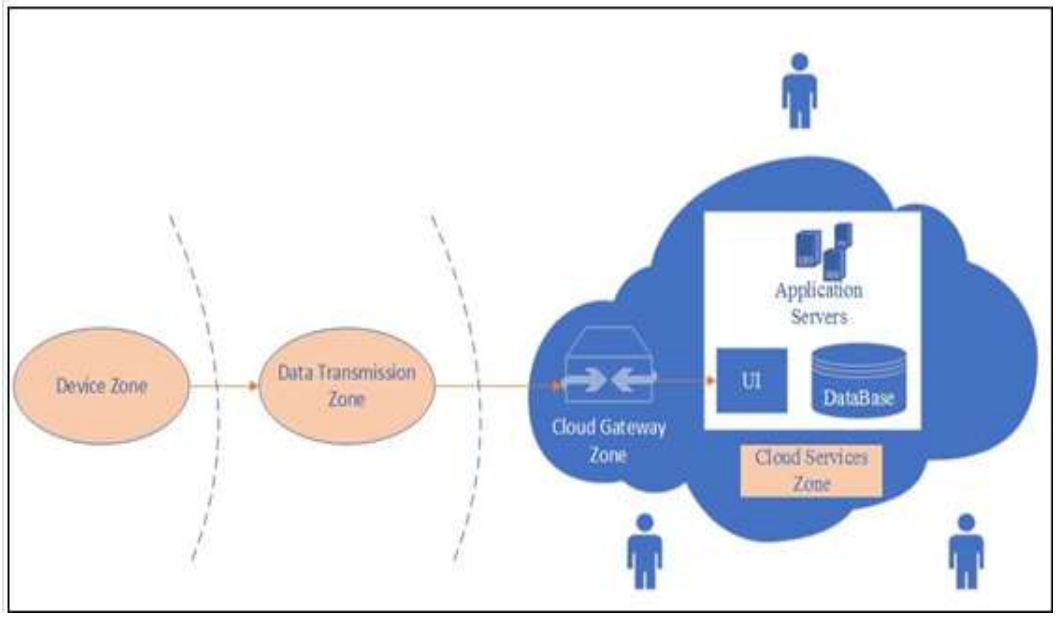

Figure 2: Architectural Model Of Cloud Based Iot.

useful server that functions as an agent empowering correspondence. It can also be a framework of device control and a center point for managing device information. A cloud gateway can be defined as a framework that allows correspondence to and from remote devices, other gateways out in the field or other destinations from across the open network space in a normal process towards a central control center that is cloud-based. Such a center also functions as an information examining framework. A service for this kind of setting is defined as any module or component of a product that interfaces with other devices via a field or through a cloud gateway in order to gather and examine information and also for the purposes of order and control.

1.1. Privacy And Security Concerns

With the evolution of internet communication infrastructure to include sensing objects, suitable procedures are required to protect interactions with these devices. With regards to future IoT applications, the operative security of data from noxious attacks is a crucial yet complicated issue that should be tended to. There has been noteworthy research endeavours put on to sum up the security issues for cloud-IoT framework [7], [8], [9], [10]. Security procedures intended to ensure communications must give fitting affirmations regarding secrecy, reliability, verification and non-revocation of the data streams.

The outflow of client data in IoT environments like, information, location, and utilization, is pulling in the consideration of research groups [11], [12]. Imperative protection issues are the identity and location information of client. Identity security points to the way that the portable IoT client's genuine identity must be very much shielded from the public; then again, when some issue occurs in crisis cases, it can likewise be successfully tracked down by the authorized person. Location security appears to be particularly of importance in IoTs, since the habitually uncovered location protection would unveil the living propensity of the IoT client.

Throughout this survey, the emphasis is on security for communication in the IoT and analyzing solutions available in the context of the various IoT communication technologies.In this paper we mainly focus on the current state of the art and recent developments in the area of cryptographic algorithms to secure the cloud based IoT system.

1.2 Some Security Threats In IoT And Cloud Computing

- Threats at Data
- Data Breaches

- Cloud service misuse
- Insecure Interfaces and APIs
- Malicious Intruders
- Malicious Intruders

While using or developing IoT systems with cloud we should use techniques or methods to avoid such type of threats.

Security issues in IoT and Cloud Today, Cloud of things is emerging area as due to pandemic we all using Iot devices everywhere. The services we use in IoT from cloud provide power to IoT. Cloud helps IoT in improving limitations of devices, increases device capability, provides unlimited data storage and also adds some security measures in it. Although cloud offers various services in IoT, it is also facing security challenges as we are using centralized data storage, as there may be insecure communication between devices or may have authentication and authorization issues while using IoT devices. If IoT system has poor implementation it may carry poor integration with cloud. This will breaks security measures. This may lead to vulnerability attacks. To ensure security:

- Ensure security at the edge of device
- Monitor the data flow and secure it in early stage
- Regular error checking should be done
- Use strong passwords for IoT and Cloud
- Use strong encryption techniques
- Aviod lack of execution environment

According to Shantanu Pal et al. [6], they have present a systematic approach to understand the security requirements for the IoT, which will help designing secure IoT systems for the future. In developing these requirements, they provide different scenarios and outline potential threats and attacks within the IoT. Based on these characteristics of the IoT, the possible threats and attacks are group into five areas, namely communications, device/services, users, mobility and integration of resources. They also examine the existing security requirements for IoT.

Author [71] discuss, and analyze significant security issues (data, network and service, applications, and people-related security) and present the limitations from a general, artificial intelligence and deep learning perspective.

Deepti Rani et al. [72] identify and classify various security challenges faced by IoT users. Several types of security and privacy issues have been addressed presented also classification of security and privacy issues considered in different levels of IoT architecture.

2. LITERATURE SURVEY

With the rapid evolution of IoT, there are multiple IoT applications which have an effect on our daily life. They encompass various routine household devices and conventional equipment that generally contribute towards improving the life of an individual. As the IoT model encompasses different zones to fragment the solution, it needs to focus on issues at each zone. Here we analyze the security threats on the basis of layered architecture i.e., Device Zone, Data transmission Zone, Cloud Gateway and Cloud Services.

2.1 Device Zone

Device layers are mostly concerned with the collection of information, object perception and control. They are affected by types of attacks which focus on the hardware components of the IoT framework. It is possible to sub-divide the device Zone into two parts:

• Device node (sensors or controllers, etc.)

• Device network which interacts with the transportation network.

The function of a device node is data acquisition as well as data control. On the other hand, the device network transmits the data that has been gathered to the gateway or it can also send control instructions to the controller. Each device in IoT is detectable and analyzable through the internet by the means of Radio Frequency Identification (RFID), Wireless Sensor Network (WSN) or some other means. Both RFID and WSN can be utilized to secure reliability and secrecy of information in IoT by password encryption technology [13]. The primary distinction among them is that, RFID is essentially utilized for object identification, whereas

WSN is primarily utilized for the impression of real-world physical parameters related with the surrounding environment [8].

2.1.1 Security issues of RFID tags and solutions:

IoT is made up of many small devices, for example, RFIDs which stay unattended for long periods of times. It is simple for an adversary to access the data stored in the memory of an IoT device [8]. RFID can give basic information about a thing as it is examined. But as per their application, they expose some major harm in IoT. The answers of RFID tags can be pre-determined because of which it is possible to track them. This violates the location privacy in IoT [14]. Even in cases when tags prevent revelation of important information, they can still disclose their own or the holder's identity. There are some other important attacks possible on RFIDs such as:

a. Physical Attacks/Tampering: These sorts of attacks are possible when the attacker has complete physical access to a tag. In this attack, the tags can be physically controlled and adjusted in a laboratory setup. Many physical attacks against RFIDs are known such as probe attacks, material removal through shaped charges or water etching, circuit manipulation, and clock glitching [7]. The purpose behind such attacks is data mining from the tag or altering the tag in order to duplicate it.

b. Tag Cloning: Tag cloning which can also be known as spoofing along with imitating of RFID tags can be tremendously advantageous to hackers on the one hand and extremely dangerous and damaging for the reputation of the organization [15], [69]. Potential harm can be opened up when levels of automation are very high. An attacker may utilize tag cloning to get to confined regions, financial balances, or critical data by means of different attacks like in man-in-the-middle attack or Sybil attack [16]. For instance, a malicious Sybil node in a remote system may send large amounts of connection requests to the access point, to imitate large number of legitimate clients. As a result of this, the legitimate clients are denied access once the malicious node has established connection with access point. So, Sybil attacks totally degrade the IoT usefulness [17], [18].

Solutions:

For intermediate node distance measurement, ranging techniques like Radio Signal Strength Indicator (RSSI), Angle of Arrival (AoA), Time of Arrival (ToA) or Time Difference of Arrival (TDoA) can be used. Received signal strength indication (RSSI) based methodologies are practised in [19], [20] and [21] as they do not require additional hardware. They have concluded that RSSI based methodologies can be combined with other ranging techniques to form a hybrid solution which can be used for localization purposes in IoT.

Spoofing attacks can be avoided by secure trust management and by following proper authentication schemes [22], [23]. In [34] a channel based authentication framework is proposed to detect Sybil attacks in wireless network by exploiting the uniqueness of channel responses in remote environments. Here the statistics are made on the basis of the number of claimed identities, number of access points, whether they are synchronized or not and the Sybil attack strategy used.

2.1.2 Security issues of wsns and solutions:

WSN can play a very important role in IoT [13], [8], [24], [25], [34]. WSN can inspect and trace the status of devices, and transmit this status information to the control centre or sink nodes by means of multiple hops. In this way, WSN can be considered as the further channel between reality and the digital world [26]. As compared to other available technologies, WSN provides many other advantages as in scalability, dynamic reconfiguration, reliability, small size, minimal effort, and low energy utilization. Every one of these benefits helps WSN to be incorporated in different territories with varied prerequisites. In WSNs, during the process of data collection, the data may be routed in a faulty manner, or it may be the object of eavesdropping, the message may be tampered with and the data may face other security challenges [70], as explained below:

a. Node Tampering: The attacker can instigate harm to a sensor node, by physically supplanting the whole node or part of its equipment or even electronically investigating the nodes to get entrance and adjust delicate data, for example, shared cryptographic keys or routing tables.

b. Malicious Code Injection: Here the attacker can harm a node by physically infusing the node with defamatory codes which will give illegal access of the IoT system to the attacker [27], [28].

c. Impersonation: Impersonation involves temporarily altering the identity for collusion attacks, which makes authentication very difficult in the distributed environment [29].

d. Denial of Service (DoS) Attacks: Attackers misuse the processing capacity of the nodes, making them in accessible. There are different types of DoS attacks like battery draining, sleep deprivation, outage attacks and battery draining.

1. Battery draining:

Because of size restrictions, nodes typically need to support little batteries with extremely restricted resource threshold. This in turn has intensified the battery draining attach which may by implication result in severe damages, for example, node blackout or an inability to report a danger.

For instance, once an attacker is able to figure out how to drain the battery of a smoke detector, he will be in a position to enervate the fire discovery system. Such attacks could decimate a system if reviving the nodes is troublesome [7]. Another case of a battery-draining attack is the point at which an attacker sends huge amounts of arbitrary packets to a hub and forces the hub to run its checking systems, similar to verification. Literature discusses many battery-draining attacks [30], [31].

Consider the power utilised by the device while it is active is P_{act} and while sleeping isP_{sl} and the fraction of time the device is active is D. Then, Battery life = P_{act} / P_{sl}. Here, the aim of attacker is to keep the device active as long as possible, to make D = 1.

2. Sleep Deprivation:

Sleep deprivation is a particular sort of DoS attack in that the casualty is a battery-powered node with a restricted resource limit. In such type of attack, the attacker endeavours to send an undesired pack of requests of solicitations that appears to be authentic [8]. As a result it is significantly harder to identify such an attack as compared to a simple battery-draining attack. The study exertion by Martin et al. is one of first productions to nearly analyse the effect of sleep deprivation attacks on restricted resource limit devices [32].

3. Outage Attacks:

The edge outage attack occurs when an edge device cannot exhibit the expected operation. For example, any of the outer devices or an administrative node can mal-function. The cause of these attacks can be because of battery draining, code injection, inaccurate assembly process, sleep deprivation, or it may be because of unallowed physical access to the node. The most popular instance of outage attack is, injecting Stuxnet [33] into Iran's nuclear process control program. Stuxnet modifies the manufacturing process control signals in a way that the affected system fails to gain its power to identify miscellaneous patterns. Thus, this makes the system not able to shut down even in critical situations [7].

E. Node replication attacks:

In this type of an attack, the attacker inserts an additional node, a faulty one, in the current set up of nodes by impersonating one of the existing node's recognition number. A node replication attack results in noticeable decrement in the network performance. Furthermore, an attacker can simply contaminate or misallocate packets arriving at the replica**.** This attack for the most part does serious harm to the framework by empowering the aggressor to get expected access to separate cryptographic shared keys [7]. In addition, node imitations may withdraw approved nodes by executing node repudiation conventions [8].

f. Jamming Adversaries: Jamming attacks on remote devices in IoT objectify weakening of the systems by radiating radio recurrence signals without following a convention [35]. The radio obstruction impacts the system activities extremely and can influence the sending and getting of information by real nodes, bringing about a breakdown or erratic conduct of the framework [36], [8].

g. Insecure Initialization: A safe procedure of instating and arranging IoT at the physical layer guarantees a legitimate working of the whole framework without abusing protection

and interruption of system administrations [37]. The physical layer correspondence likewise should be secured with a specific end goal to make it out of reach to unapproved receivers.

Solutions:

Various resolutions have been proposed for wireless sensor networks that contemplate the sensor as a part of internet associated by means of nodes. Even though in IoT the sensor nodes themselves are considered as the Internet nodes influencing the authentication practise more noteworthy. The reliability of the information likewise turns out to be fundamental and requires exceptional consideration towards holding its consistency. To deal with these security issues for smart devices connected in the IoT environment, there is a growing necessity to practise aspects like cryptographic encryption, key management, secure routing, node trust [38], [13]. Key management involves private key creation, allocation, storage, revision and demolition processes. In secure routing, setting up secure and effective routing protocols is done to prevent attacks. Trust management mechanisms are introduced as a means to ascertain that there is security in wireless sensor networks.

The primary application domains of a wireless sensor network are widespread, that require high information security including information privacy and integrity [39], [40]. This can be achieved by information encryption [18]. Cryptographic algorithms provide a vital technique to guarantee the physical layer network security, and are fundamental for guaranteeing security of the entire system service [13].

2.1.3 Cryptographic Solutions For The Device Zone:

Security for clients is an extremely complex concern since it includes communications with various system components. Operative resolution for these complex concerns can be realised through lightweight cryptographic methods for the device-zone layer. These resolutions are block ciphers, stream ciphers, hash functions, lightweight pseudo random number generator functions, and lightweight public key primitives. [41] Cryptography techniques are usually merged to give the expected level of protection relying upon the affectability of information, network settings, and application and client's prerequisites. Lightweight cryptographic methodologies are designed for WSN, RFIDs, Smart cards and different devices to actualize private and public key administration to settle the issues of verification.

There are two types of encryption strategies. The first type is symmetric encryption algorithms and the second type is the public key encryption algorithms. On the one hand, asymmetric encryption algorithms can furnish a very high level of security. However, resources such as area for memory and power are limited in the sensor nodes making complex and high-power use of asymmetric encryption algorithms very difficult to utilize in wireless sensor networks. Symmetric encryption algorithms on the other hand, are used extensively because of low and simple computation. There are many versions of Asymmetric encryption algorithms available that are able to protect the Cloud-IoT systems from attacks from hostile injections such as Trojan [42] or from various flaw injectors [43]. Though the technology of this algorithm is fairly mature, the strength of the security that it provides is not very high.

However symmetric encryption algorithms have complications that are given below:

- The main exchange protocols that built upon the symmetric cryptosystem are to huge making such encryptions not very scalable.
- In WSNs, nodes are in an unattended environment. Once a node is traded off, it will result in a major security breach to the whole network.
- In a symmetric encryption algorithm, for authentication, message authentication codes are used. These codes amplify the load on the correspondence system and need a lot of storage space, which in turn results in requiring high power utilization [13].

On the basis of above critical issues of symmetric key encryption, public-key encryptions are considered for encryption in wireless sensor networks.

In the case of encryptions using a public key, each node contains its own private key and also the public key of the base station.

The public key of all the nodes is protected by the base stations. A public key algorithm provides decent scalability, exclusive of obscuring the key management protocol. It is suitable for node verification, and it makes sure of the security of the whole network [44]. There are three kinds of algorithms for public key encryption in existence now which are suitable for wireless sensor networks: Rabin's Scheme, NtruEncrypt and Elliptic Curve Cryptography. [45] and [46] recommend a much easier execution of ECC for Cloud-IOT system that handles location secrecy and other private user data. The other two algorithms are explained in the following section.

i.) An **NtruEncrypt** algorithm can be mathematically explained as –

$$PR = (Z(y))/(((y^M\text{-}1), b)) \quad (1)$$

Here, PR represents a polynomial ring and can be set up by using the (M, a, b) parameters. This must follow some properties as:

- The elements of the ring, PR, are all polynomial in nature with the highest degree M-1, wherein M is a prime number.
- We reduce polynomial coefficients to mod a or mod b, taking a and b as polynomials or prime integers.
- *a* is very small compared to b, and the value lies in the range of M/2 and M.
- Polynomials are one variable over y.

Multiplication in ring PR can be referred to as 'Star Multiplication', represented as the ( ) symbol. In other words it can be known as the complex product of two vectors.

$$P(y) = p_0 + p_1y + p_2y^2 + \ldots + p_{M-1}y^{M-1}$$
$$= (p_0, p_1, p_2, \ldots, p_{M-1}) \quad (2)$$

The above-mentioned equation is related to the vector which is formed by the polynomial's coefficient.

Then the coefficients r_k of

r(y) = p(y) _ q(y) mod b, a are each calculated with aggregation of products p_i q_j with $i + j \equiv k \bmod M$.

For Key Generation/ Encryption and for Decryption, b and a will be the modulus for reduction of r_k. An initial security analysis and the detailed explanation of the methodology are mentioned in [46].

Key Generation:

To generate a private key fp(y):

Select any polynomial FP (y) from the ring PR. FP (y) is a small value that can be binary from the set {0, 1} (if value of a= 2) or can be ternary from the set {−1, 0, 1} if value of a= 3 or a= y+ 2

Let: Private Key,

$$fp(y) = 1 + p\,FP(y)^1 \quad (3)$$

The public key h(y) is generated using f(y) as follows:

Select any polynomial g(y) from PR.

Calculate the inverse $f^{-1}(y)$ (mod b).

Finally, calculate the public key

$$h(y) = g(y) \_ f - 1(y)\ (mod\ b) \quad (4)$$

Encryption:

- Encrypt the plaintext into a polynomial by using set {0, 1} or {−1, 0, 1}.
- Select any $\varphi(y)$ from PR.
- Calculate the Encrypted-text polynomial as:

$$r(y) = a\varphi(y) \_ h(y) + m(y)\ (mod\ b) \quad (5)$$

Decryption:

- Private key is used for decryption

M'(y) = c(y) _f(y) (mod a) (6)

- Convert the coefficients of message polynomial to plaintext.

ii.) The simplified version of **Rabin's scheme** can be understood by following mathematically expression:

Key Generation:

- In the very first step, two large prime numbers are chosen.
- Then, m is computed as product of a and b.

$$m = a * b$$

- Select a random number q in the range of 0 to m $(0 \leq q < m)$.
- Here, (m, q) is treated as a public key and (a, b) is treated as the private key for encryption.

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

Encryption:

- Message is represented as an integer value y, where y is in the range of

$$0 \leq y < mn$$

- Cipher text is computed as: Encrypt,

$$q(y) \equiv y(y+q)\ mod\ m \quad (7)$$

We can get a squaring operation Encrypt,

(y) = y2 mod m by putting 0 in place of q in encrypt, q(y).

The difference between Rabin's Scheme of Encryption and RSA is that Rabin's Scheme needs only one squaring while RSA needs several squaring and multiplications. As a result, RSA is much slower than Rabin's Scheme.

Decryption:

Decryption is performed using four square roots value, represents asy1, y2, y3, and y4:

$$c = Encrypt(y) \equiv y2\ mod\ m \quad (8)$$

These three algorithms have been tested on the Mica2 series wireless sensor platform, showing that only when there is an algorithm that has been designed well and the correct parameters that help boost the design are selected, can an algorithm using a public key be utilized in a wireless sensor networks that have limited energy and computing power [13], [47]. To further optimize the application of public key algorithm into WSNs, two most important research aspects are presented. In the part of hardware, customised designs can be created, ensuring less power co-processors to fulfil almost all of the computations of the encryption algorithms. In the aspect of software, well proposed algorithms with right parameters can be used to decrease the amount of computation.

Finally, it can be concluded that both, symmetric, as well as asymmetric algorithms have their advantages and disadvantages and neither type is able to come up with a complete solution to the issues that arise out of network security.

A significant factor that needs to be taken into account by the security facilities is how to make use of the technology for asymmetric encryption algorithms in WSN. Future research can focus on energy usages that result from public key encryption algorithms along with security protocols communication.

IoT devices should make continuous bi-directional associations with the web from the cloud servers. Transport Layer Security (TLS) gives security for exchanging information over the system. The information is encoded to keep anybody from tuning in to and understanding the content. This is achieved by using server certificates that customers must approve. At times, the server likewise approves customer centric certificates. While TLS/SSL is appropriate for information exchange security, however the data in use can't be encoded for evident reasons. This should be decoded, worked upon and after that encoded, which requires a large number of key administration and approval issues. Because of this, the complexity of cloud data management increases and this can result in security issues while relocating data between clouds services which otherwise can be done seamlessly.

In a homomorphic encryption framework, it would be workable for a cloud administration to do a progression of tasks on encoded information while never decoding it, generate outcomes that are never decoded, and send the outcomes to the information's holder for decoding. Despite the fact that managing happens on a third-party platform utilizing that platform's assets, the information remains encoded at each phase all the while.

1. The user will send the encoded data to cloud **(En (n)).**

2. Suppose the user want to perform some function on the data, which is **F (n).**

3. Then cloud should be able to perform the Operation:

$$En\big(F(n)\big) = \{Eval(F, En(n))\} \quad (9)$$

For example, say we perform a query to cloud from one of our IoT devices. In a homomorphic encryption world, the IoT device will send the query to the cloud in an encrypted format and the cloud will perform the operation on the encrypted query and return the results in an encrypted format only. Then the device can decrypt the result and use the result.

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

Fully Homomorphic Encryption (FHE):

The advancement of fully homomorphic encryption is a progressive development, richly spreading the range of calculations which can be applied to process encoded data homomorphically. Primarily, FHE allows random calculations on encoded data.

Lately, an original method based on ring learning with errors is proposed for FHE [48]. As this technique effectively decreases noise and performs far better from the usability point of view, the results obtained are better than many other existing techniques. But there is still a need for more simple and practical execution for FHE methods. Furthermore, various asymmetric FHE methods have been presented recently based on ideal lattices, approximate GCD, etc. For many of the existing applications, a need has arisen for symmetric FHE that is more efficacious and simpler. In [49] an easier method based on n polynomial rings over integers is presented. The algorithm suggests:

Consider X is an integer which is a multiple of another integer Y, then for any n1, n2, $n1 \equiv n2 \; mod \; Y$ stays unaffected if

$n1 \equiv n2 \; mod \; X$ is calculated. This is the method that is utilized to construct a new key. This key is made accessible publicly exclusive of the secret key. The security parameter of the scheme is 1 while message space is MS. The integer message is obtained in its binary form or the message can be a binary number of some bits, if the binary message (M) is of length (l+1) bits.

Algorithm 1. Key Generation

1. Produce the secret key Ks, a prime number of length K bits.

2. Select an even integer a randomly.

3. Refresh key $kr = a * ks.$ (10)

Let M be encoded into message polynomial MP (n) of degree l with coefficients representing each bit of M.

Algorithm 2. Encryption (MP (n), Ks, l)

1. Select a polynomial y(n) of degree l such that,

$MP(n) \equiv y(n) mod Ks.$ (11)

2. Pick a polynomial d(n) of degree 1 randomly.

3. Coefficients of d(n) are integer of length a.

4. Compute $c(n) = y(n) + Ks * d(n)$ (12)

5. $c(n)$is the encrypted message polynomial.

Algorithm 3. Decryption (c (n), Ks, l)

Compute,

$c(n) \; mod \; Ks \; mod \; 2 = MP(n)$ (13)

After a few calculations on the cipher text, the noise that is generated may surpass resulting in incorrect decryption. In the event that this occurs, a one step refresh process is utilized to eliminate the noise.

Algorithm 4. Refresh (c(n), Kr, l)

Compute,

$c'(n) = c(n) mod Kr$ (14)

The proposed scheme provides a much easier method for current day cloud applications.

Commercial Solutions:

Commercial solutions for security threats in the cloud help to further close the gap currently existing in the available human skills set. Security as a Service (SaaS) security from various vendors delivers the required tools at a lower cost of entry and a faster time to value. [50] Illustrates a detailed survey on various tools which are being used by renowned public cloud providers such as Amazon AWS, Microsoft Azure and VMware. Cloud provider capabilities of products developed by third party vendors specialize in security of cloud systems. These work especially when security mechanisms against network-based attacks are implemented at the application level. Cloud Stack, Eucalyptus, OpenStack, Open Nebula are four most common and specialized cloud security software's [51]. This paper evaluates the above software's based on certain parameters which are part of ISO 27001:2005. The results show that Cloud Stack is the best performing software for all open source cloud

environments. Table 1 below demonstrates various security software's which can be used to handle various security issues.

TABLE I: Cloud Security: Emerging Threats And Current Solutions

Security challenges	Tools
Malware Injection	• Barracuda Web App Firewall • DeepSecurity(TrendMicro) • Neutron Network (OpenStack) • Security Onion(OpenStack) • Microsoft Advanced Threat
DoS	• DefenseFlow • OpenDayLight • CDN(Azure) • vShield (VMWare)
Spoofing	• Keystone (OpenStack) • Azure Active Directory IAM • AWS IAM
Sniffing	• AWS DirectConnect • HP Atalla Cloud Encryption • CipherCloud

2.2 Data Transmission Zone:

The data from the sensors of the device zone comes in an analog form. The analog streams that come from sensor nodes, create large volumes of data rapidly. This data needs to be combined and transformed into digital streams for additional processing. Data acquisition systems (DAS) execute these tasks of combining and transforming. This is done by connecting to the sensor network, aggregating the outputs and then performing the analog-to-digital transmission. This data is then further routed through Wi-Fi, wired LANs, or the Internet to cloud gateways. Here, it is very important to build a secure channel between the sensors and the servers in order to guarantee the validity of the collected data. If by any chance the gathered information is altered, the outcome of the analysis will deviate significantly and this may even cause serious damage. Thus, as mentioned above, cryptography solutions are practised to send/receive messages and to ensure privacy and for the authentication of data.

2.3 Cloud Gateway Zone

The gateway layer mostly gives pervasive access condition to the device zone. The principle behind this layer is to pass on the assembled data, collected from the device layer, to a specific data preparing framework over the existing correspondence networks which can be utilized by access networks (3G, Wi-Fi, Ad hoc organize, and so on.) or core networks (Internet) [8]. The gateway layer is a grouping of varied heterogeneous systems; because of this it is vulnerable to get attacked. It can be further partitioned into three layers by utility: the access network, the core network and local area. Here cloud gateway zone security issues are analysed along with possible solutions.

In [52], concise outlines of concerns in wireless networks like cellular networks are discussed. According to this, the public and varied design of IP-based LTE network leads to a strengthened number of safety breaches in distinction of the 3G grid. Mostly, the safety breaches at gateway zone are:

a. Routing Attacks: Here, nodes in direct proximity can modify the appropriate routing path while gathering and forwarding information practice. Such attacks, which interfere with the way the packets are routed, are called routing attacks. They are used by attackers for deception, re-direction, misallocation or dropping packets at the correspondence level.

Altering attack is one of the common types of routing attacks. In an altering attack, the invader deviates the routing data, for example, by creating routing loops or generating incorrect faulty messages. There are many other major routing attacks proposed like Black Hole [7], [53], Gray Hole [53], Worm Hole [54], Hello Flood [55], and Sybil [18, 56]. They are discussed below:

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

1. Black Hole:

This attack is propelled by utilizing a malignant node in the network, which draws attention to the traffic through publicizing information about the briefest path to the destination node. Thus all packets are directed towards the malignant node causing diving of packets by the attacker.

2. Gray Hole:

Gray Hole attacks are an adaption of the black hole attack where in packets are randomly dropped by nodes.

3. Worm Hole:

These attacks are serious attacks which can even be unleashed in situations where legitimacy and secrecy are ensured in all interactions. Here, packets are first recorded at a point and after that they are under passed to an alternative area.

4. Hello Flood:

In Hello Flood, the assault depends on the fact that a given node should send "HELLO PACKETS" to illustrate its existence to its neighbours. The assumption of the receiver nodes is that they are within the correspondence range of the sender. A pernicious node having high communication power is used in this assault for sending "HELLO PACKETS" in the network appearing to be the neighbour node.

5. Sybil

A device or a node in a network may assume multiple illegal characteristics. It does not copy any node, but instead just takes on the identity or another node out of a few other nodes. As a consequence, redundancies are caused in the routing convention. Sybil attacks debase information integrity, security, and asset utilization.

b. DoS Attacks: In IoT, DDos attack [57] is one of the commonest attacks experienced in a network. Generally, modernizing the framework and exercising DoS attack prevention and detection practices works as a solution to this.

c.Data Transit Attacks: During communication in the network, numerous attacks are possible targeting secrecy and reliability of information, for example, sniffing, and man-in-the-middle.

d. ARP vulnerabilities: In this scenario, the attacker incorrectly directs the in/out movement of a casualty VM to a flawed VM by manipulation of the fact that the protocol for address resolution has no need of proof of existence.

e. DNS poisoning attack: In this type of an attack the fact that the network is susceptible to redirection of all the traffic towards malicious servers and away from authentic ones is taken advantage of.

f. Sniffer attack: Deliberately tuning into exchanges that are confidential that is transmitted over the communication links is what is known as sniffing or snooping. This is done at the correspondence level [58]. Consequently, the attacker is in possession of highly confidential data after decryption. The sniffer may be able to obtain crucial data like node settings, node qualifier and common network keywords in instances where the packets carry access control data. This information may be misused to plan other attacks.

As an example, if the attacker is able to extricate data that will enable the addition of another node to the arrangement of approved nodes, it will be very easy for the attacker to add a malevolent node to the framework.

g. Man in the middle: In this instance, the attacker installs him/herself in the middle of a communication going on between two devices thereby imitating both sides and has access to data that the two devices are sending back and forth.

Solutions:

To solve the network security issue, access control and network encoding practices are present. In access control, legitimate users can exclusively access the Wi-Fi network as per the IEEE802.11 specifications. In network encryption, only the real receivers can rightly decrypt and can understand the information content. The encryption methods for network layers are TKIP and AES [13], [29].

As high numbers of devices access the internet, resulting in more IP addresses, IPv4-based Internet cannot fulfil the requirement of so many devices. Thus IPv6-based Internet comes into picture. To apply IPv6 sensor systems with minimum power utilization for a heterogeneous combination, 6

Lowpan techniques are considered to solve the issue of IPv6 addresses.

Granjal et al. [59] have suggested an approach that provides secure inter-communication prototype and procedure which guarantees assured assimilation and safety among WSNs and internet. To assist to and fro security among sensor nodes and hosts on the Internet, the proposed system uses 6LoWPAN safety headers and a procedure to handle the disbursed power consumption along with safety computations on WSN.

Jara et al. [60] compared the prerequisites and desired characteristics for assisting agility in IoT, and came up with a procedure for constrained systems based on active IPv6 and IPSec. Their analysis proves that active IPv6 and IPSec are suitable for constrained systems and further they have built and examined the same. The presented approach takes care of the essentials of IoT and provides appropriate resolution for dynamic ecosystems in measures of effectiveness and safety.

Kothmayr et al. [61] suggested the first ever totally built co-operative verification method for IoTs, based on current conventions of internet, especially the DTLS convention. The presented security module is examined in a completely authenticated DTLS handshake and is relied on the interchange of X.509 certificates in the form of symmetric key interchange. They function on conventional correspondence stacks which provide UDP/IPv6 organizing for 6LoWPANs. Raza et al. [62] came up with a contracted 6LoWPAN header for DTLS.

2.4 Cloud Services

Service layers gives assistance as and when requested by the clients. For example, the service layer can impart required information like temperature and humidity estimations to the customer accessing this service. The significance of this layer for the IoT is that, it provides the ability to give high superiority resources to meet client requirements. Various IoT contexts (i.e. acute city, healthcare and factory) are executed inside this layer; in addition, an Application Support Sub-layer (ASS), to maintain wide range of merchandise facilities and to acknowledge smart estimation and resource distribution can be actualized all through particular middleware and distributed computing platforms.

The common issues of cloud computation services are service interruptions like data backup, system shutdown and not able to reach data centre. Also, DDoS attacks [63] can be possible on cloud services, which prevent legitimate users from accessing the services, by making important cloud services use more resources like memory, storage space, and network bandwidth. As a result, the response of the cloud services turns out to be very slow or they may even become unresponsive.

IoT can be applied to a varied range of provinces, comprising of many day-to-day domains that we deal with like healthcare (for tracking body health), environment (for automated handling of assets), energy control, weather controlling and many more. Most of the current IoT devices include manageable implanted computer frameworks. A few of them, seem like approximately utilizable computers, consequently they are prone to similar security breaches just like normal computers. At instances when associating with the Internet, they can get tainted by Trojan like infections [65], [66].

IoT is instigating an innovative surrounding where in malware will be utilised for devising prominent botnets. A freshly exposed component of Linux malware i.e., Mirai [64], is getting utilised for binding IoT devices into botnets. Here in Mirai, it is possible to get shell access of telnets or SSH accounts by using regular passwords. After gaining access to an account, serious damage can be caused like process adjourning, file corruption, or other malwares can also be planted on the system. The affected devices then come under Mirai's dominance and anticipate commands to attack in the way of DDoS attack.

The tremendous web blackout in October 2016 was a consequence of a DDoS assault utilizing traded off IoT assets executing the Mirai malware. Subsequently, the study of safety analysts of Malware Must Die presented another malware group called IRC Telnet. This malware was deliberately created for infecting IoT frameworks and

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

further generating botnets out of them for targeting huge attacks like DDoS [67]. Similar to Mirai, IRC Telnet uses generally fixed passwords. It includes an IoT gadget by attacking its Telnet ports and sullying the gadget's working system. By then, the IoT gadget transforms into a hub of the botnets.

Solutions:

DDoS requests generally include similar type of insignificant content. To prevent DDoS attacks in the network, in [68] a methodology is proposed where in, the algorithm identifies the sender is malicious or not as per the uniformity of the content in the data packets it sends. If the attacker continuously sends requests with similar content then it will be considered as an attacker. Thus, after receiving a request from such a malicious sender, the legitimate node will disprove this request and will save the bandwidth for serving further requests.

In [1], a new methodology based on a SDN/NFV framework to prevent DDoS attack is presented. Here the number of devices affected by a malicious hacker produces packets directing a web server. But the web servers are built with a defence system versus the DDoS attack. For this, network service functions (NSF) are used to set detailed rules by network administrators or web administrators.

With the progression of Software Defined Networking (SDN), a prevention methodology to prevent DDoS attempts has brought up a new way for the cloud computing environment [2]. In SDN, softwares are approved to run separately from underlying hardware i.e., virtualization. SDN presents many well-defined features to propose solutions for mitigating DDOS attacks. These features include, separation of control and data plane, controller centralization, fully automated operation, traffic tunnelling etc. A simple categorization of security concerns for Cloud-IoT is presented in figure 3 along with its possible solutions.

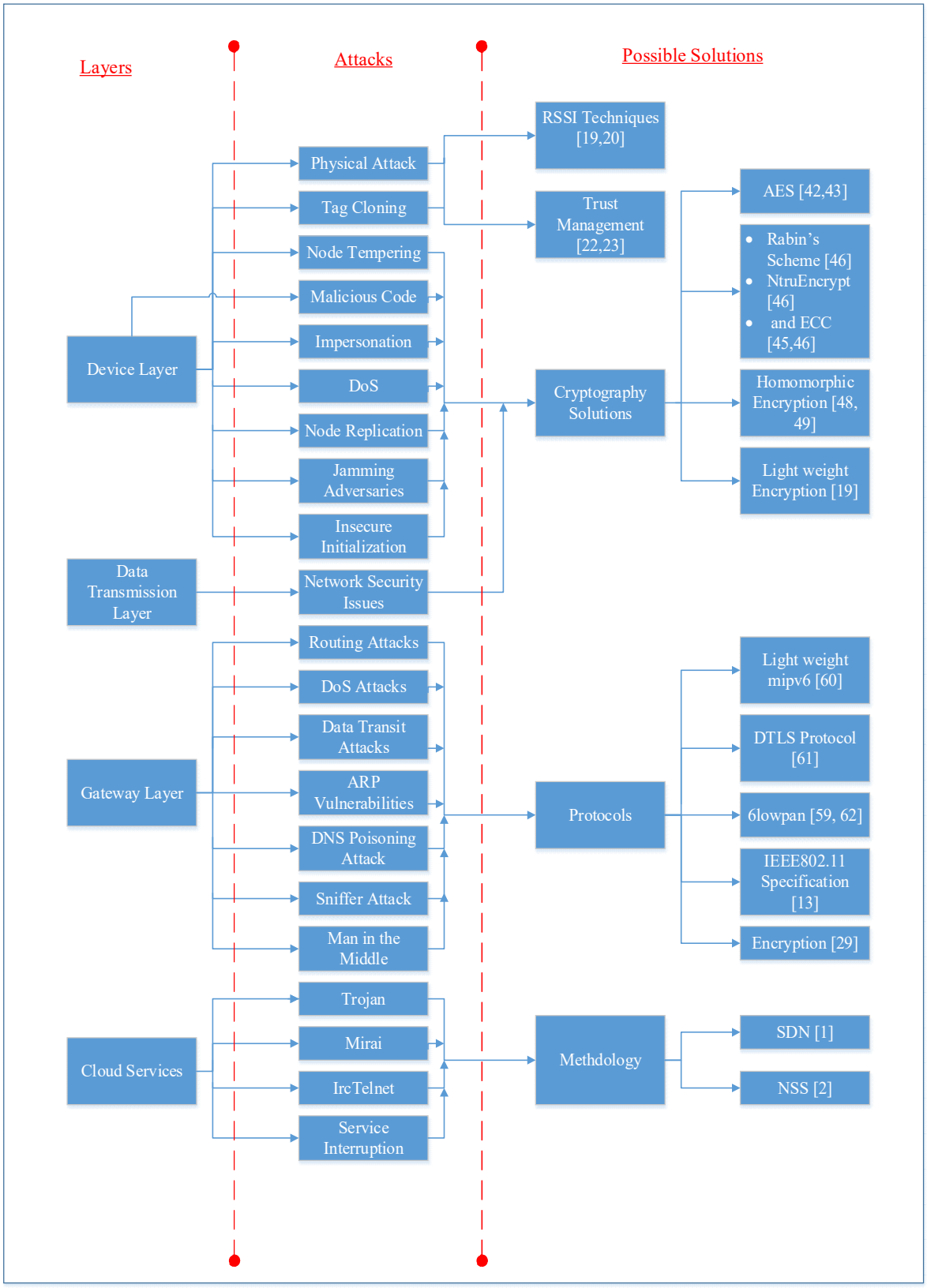

Figure 3. Layer Wise Security Issues And Possible Solutions For Cloud-Iot

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

3. COMPARATIVE ANALYSIS

Table III shows comparative analysis of security concerns and solutions mentioned in the literature.

Table Iii: Comparitive Analysis Of Security Solutions.

Sr. No	Security concern	Solutions	Benefit
1	RFID tags	Use of soft blocker security scheme, use proper authorization and authentication	Saves data leakage from RFID tags
2	Wireless Sensor Networks	Key Management, Trust Management, use of effective routing protocol	Prevent IoT system from attacks
3	Device level attacks	Use of cryptographic devices	provides security at device level
4	Cloud Gateway	Use of 6LoWPAN safety headers,	Protects from attacks at cloud gateway level

The main objective of cloud computing security is to minimize the risks.

- Data breach and IP theft/ loss
- Identity theft
- Unauthorized access to mission-critical assets
- Malware infections
- DDoS attacks
- Financial damage and revenue losses

Once the data is stored in the cloud, it is easier to get back-up and restore that data using the cloud. Cloud allows us to quickly and easily access store information anywhere, anytime in the whole world, using an internet connection. Security of the data is biggest advantages of cloud computing. Cloud offers many advanced features related to security and ensures that data is securely stored and handled.

In case of wsn it is scalable and hence can accommodate any new nodes or devices at any time. It uses different security algorithms. In RFID devices may be able to read and even change data on tags without the knowledge of the person who owns the object. Side-channel attacks can pick up RFID data as it passes from a tag to a reader, which could give the attacker access to passwords or information that should be secure.

4. CONCLUSION

New technological developments in the field of cloud-IoT have proved that it is necessary to build a thread resistant procedure for the security for the communication between the devices and cloud storage. The different issues in all the four layers of layered architecture of IoT namely Device zone, Data transmission zone, cloud gateway and cloud services have been characterized in this article. Risk mitigation techniques along with the direction for achieving more efficient solutions for the frequently occurring risks at each layer have been suggested here. Some commonly used cryptography techniques used to achieve secure data transmission between machines in networks which can be distributed networks have also been discussed here. Achieving secure transmission for a cloud based IoT framework is a topic of research and still many advancements need to be done in this domain in order to address all the wide range of threats.

REFERENCES

[1] Daeyoung Hyun, Jinyoug Kim, Dongjin Hong, and Jaehoon Jeong, “SDN-based Network Security Functions for Effective DDoS Attack Mitigation”, International Conference on Information and Communication Technology Convergence (ICTC), 2017.

[2] T. Tamanna, T. Fatema and R. Saha, SDN, “A research on SDN assets and tools to defense DDoS attack in cloud computing environment”, International Conference on Wireless Communications, Signal Processing and Networking (WiSPNET), pp. 1670-1674, Chennai, 2017.

[3] J. Venkatesh, B. Aksanli, C. S. Chan, A. S. Akyurek and T. S. Rosing, "Modular and Personalized Smart Health Application Design in a Smart City Environment", in *IEEE Internet of Things Journal*, vol. 5, no. 2, pp. 614-623, April 2018.

[4] Partha Pratim Ray, "A survey of IoT cloud platforms", Future Computing and Informatics Journal, Volume 1, Issues 1–2, Pages 35-46, 2016.

[5] Mahmoud Ammar, Giovanni Russello, Bruno Crispo, "Internet of Things: A survey on the security of IoT frameworks", Journal of Information Security and Applications, Volume 38, Pages 8-27, 2018.

[6] Shantanu Pal, Michael Hitchens, Tahiry Rabehaja, Subhas Mukhopadhyay, "Security Requirements for the Internet of Things: A Systematic Approach", MDPI Journal, Sensors, 20, 5897, 2020.

[7] A. Mosenia and N. K. Jha, "A Comprehensive study of Security of Internet-of-Things," in *IEEE Transactions on Emerging Topics in Computing*, vol. 5, no. 4, pp. 586-602, Oct.-Dec. 1 2017.

[8] J. Lin, W. Yu, N. Zhang, X. Yang, H. Zhang and W. Zhao, "A Survey on Internet of Things: Architecture, Enabling Technologies, Security and Privacy, and Applications", in *IEEE Internet of Things Journal*, vol. 4, no. 5, pp. 1125-1142, Oct. 2017.

[9] M. Asplund and S. Nadjm-Tehrani, "Attitudes and Perceptions of IoT Security in Critical Societal Services", in *IEEE Access*, vol. 4, pp. 2130-2138, 2016.

[10] Zhou, Jun & Cao, Zhenfu & Dong, Xiaolei & Vasilakos, Athanasios, "Security and Privacy for Cloud-Based IoT: Challenges", IEEE Communications Magazine, pp: 26-33, 2017.

[11] L. Chen *et al*., "Robustness, Security and Privacy in Location-Based Services for Future IoT: A Survey", in *IEEE Access*, vol. 5, pp. 8956-8977, 2017.

[12] D. He, R. Ye, S. Chan, M. Guizani and Y. Xu, "Privacy in the Internet of Things for Smart Healthcare," in *IEEE Communications Magazine*, vol. 56, no. 4, pp. 38-44, APRIL 2018.

[13] Jing, Q., Vasilakos, A.V., Wan, J. et al., "Security of the Internet of Things: perspectives and challenges", Springer Science + Business Media New York, 2014.

[14] M. E Beqqal and M. Azizi, "Classification of major security attacks against RFID systems," *2017 International Conference on Wireless Technologies, Embedded and Intelligent Systems (WITS)*, Fez, pp. 1-6, 2017.

[15] L. Roselli, C. Mariotti, P. Mezzanotte, F. Alimenti, G. Orecchini, M. Virili, and N. B. Carvalho, "Review of the present technologies concurrently contributing to the implementation of the internet of things (iot) paradigm: Rfid, green electronics, wpt and energy harvesting", In *Proc. of 2015 IEEE Topical Conference on Wireless Sensors and Sensor Networks (WiSNet)*, January 2015.

[16] K. Zhang, X. Liang, R. Lu, and X. Shen, "Sybil attacks and their defences in the internet of things", *IEEE Internet of Things Journal*, pp:372–383, 2014.

[17] I. Andrea, C. Chrysostomou, and G. Hadjichristofi, "Internet of things: Security vulnerabilities and challenges", In *Proc. of IEEE Symposium on Computers and Communication (ISCC)*, July 2015.

[18] Minhaj Ahmad Khan, Khaled Salah, "IoT security: Review, blockchain solutions, and open challenges", Future Generation Computer Systems, Volume 82, Pages 395-411, 2018.

[19] E. R. Naru, H. Saini and M. Sharma, "A recent review on lightweight cryptography in IoT", International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC), Palladam, pp. 887-890, 2017.

[20] A. Mohsen Nia, S. Sur-Kolay, A. Raghunathan and N. K. Jha, "Physiological Information Leakage: A New Frontier in Health Information Security", in *IEEE Transactions on Emerging Topics in Computing*, vol. 4, no. 3, pp. 321-334, July-Sept. 2016.

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

[21] A. Brandt and J. Buron, "Home automation routing requirements in low-power and lossy networks." [Online]. Available:https://tools.ietf.org/html/rfc5826.

[22] Babu, P. & Bhaskari, Lalitha & CH. Satyanarayana,. (2011). A Comprehensive Analysis of Spoofing. International Journal of Advanced Computer Sciences and Applications. Jan 2011.

[23] Bojjagani, Sriramulu & Brabin, Denslin & Rao, P.V.. (2020). PhishPreventer: A Secure Authentication Protocol for Prevention of Phishing Attacks in Mobile Environment with Formal Verification. Procedia Computer Science. 171. 1110-1119. 10.1016/j.procs.2020.04.119.

[24] S. C. Padwal, M. Kumar, P. Balaramudu and C. K. Jha, "Analysis of environment changes using WSN for IOT applications",2nd International Conference for Convergence in Technology (I2CT), Mumbai, pp.27-32, 2017.

[25] M. Tellez, S. El-Tawab and M. H. Heydari, "IoT security attacks using reverse engineering methods on WSN applications", *IEEE 3rd World Forum on Internet of Things (WF-IoT)*, Reston, VA, pp. 182-187, 2016.

[26] K. O'Flaherty, "Securing the internet of things", SC Magazine UK, 2015.

[27] S. Sharmeen, S. Huda, J. H. Abawajy, W. N. Ismail and M. M. Hassan, "Malware Threats and Detection for Industrial Mobile-IoT Networks", in *IEEE Access*, vol. 6, pp. 15941-15957, 2018.

[28] W. Yu et al., "A Survey on the Edge Computing for the Internet of Things", in IEEE Access, vol. 6, pp. 6900-6919, 2018.

[29] M. Frustaci, P. Pace, G. Aloi and G. Fortino, "Evaluating critical security issues of the IoT world: Present and Future challenges", in *IEEE Internet of Things Journal*, 2017.

[30] M. Khouzani and S. Sarkar, "Maximum damage battery depletion attack in mobile sensor networks," IEEE Trans. Automatic Control, vol. 56, no. 10, pp. 2358–2368, 2011.

[31] E. Y. Vasserman and N. Hopper, "Vampire attacks: Draining life from wireless ad-hoc sensor networks," IEEE Trans. Mobile Computing, vol. 12, no. 2, pp. 318–332, 2013.

[32] T. Martin, M. Hsiao, D. Ha, and J. Krishnaswami, "Denial-of-service attacks on battery-powered mobile computers," in Proc. IEEE 2nd Conf. Pervasive Computing and Communications, 2004, pp. 309–318.

[33] A. Matrosov, E. Rodionov, D. Harley, and J. Malcho, "Stuxnet underthe microscope", ESET LLC, Tech. Rep., 2011.

[34] L. Xiao, L.J. Greenstein, N.B. Mandayam, W. Trappe, Channel-Based detection of sybil attacks in wireless networks, IEEE Transa. Inf. Forensics Secur. 4 (3) (2009) 492–503.

[35] S. Amuru, H. S. Dhillon, and R. M. Buehrer, "On jamming against wireless networks," IEEE Trans. Wireless Commun., vol. 16, no. 1, pp. 412–428, Jan. 2017.

[36] S. Bhattarai, S. Wei, S. Rook, W. Yu, R. F. Erbacher, and H. Cam, "On simulation studies of jamming threats against LTE networks," in 2015 International Conference on Computing, Networking and Communications (ICNC), pp. 99–103, Feb 2015.

[37] S. H. Chae, W. Choi, J. H. Lee and T. Q. S. Quek, "Enhanced Secrecy in Stochastic Wireless Networks: Artificial Noise With Secrecy Protected Zone", in *IEEE Transactions on Information Forensics and Security*, vol. 9, no. 10, pp. 1617-1628, Oct. 2014.

[38] Singh, S., Sharma, P.K., Moon, S.Y. "Advanced lightweight encryption algorithms for IoT devices: survey, challenges and solutions", J Ambient Intell Human Comput , 2017

[39] Z. Ling, K. Liu, Y. Xu, Y. Jin and X. Fu, "An End-to-End View of IoT Security and Privacy," *GLOBECOM 2017 - 2017 IEEE Global Communications Conference*, Singapore, pp. 1-7, 2017.

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

[40] D. Schinianakis, "Alternative Security Options in the 5G and IoT Era", in *IEEE Circuits and Systems Magazine*, vol. 17, no. 4, pp. 6-28, Fourthquarter 2017.

[41] Arbia Riahi Sfar, Enrico Natalizio, Yacine Challal, Zied Chtourou, "A roadmap for security challenges in the Internet of Things", Digital Communications and Networks, 2017.

[42] Filippos Pirpilidis, Kyriakos G. Stefanidis, Artemios G. Voyiatzis, Paris Kitsos, "On the effects of ring oscillator length and hardware Trojan size on an FPGA-based implementation of AES", Microprocessors and Microsystems, Volume 54, Pages 75-82, 2017.

[43] Hassen Mestiri , Fatma Kahri , Belgacem Bouallegue and Mohsen Machhout , "A High-Speed AES Design Resistant to Fault Injection Attacks", *Microprocessors and Microsystems,* 2015.

[44] Singh, S., Sharma, P.K., Moon, S.Y. et al., "Advanced lightweight encryption algorithms for IoT devices: survey, challenges and solutions",Journal of Ambient Intelligence and Humanized Computing,pp 1–18, 2017.

[45] Ioannis Chatzigiannakis, Andrea Vitaletti, and Apostolos Pyrgelis, "A privacy-preserving smart parking system using an IoT elliptic curve based security platform", Computer Communications, Volumes 89–90, Pages 165-177, 2016.

[46] Gunnar Gaubatz, Jens-Peter Kaps, and Berk Sunar, "Public key cryptography in sensor networks—revisited. In Proceedings of the First European conference on Security in Ad-hoc and Sensor Networks" (ESAS'04), Claude Castelluccia, Hannes Hartenstein, Christof Paar, and Dirk Westhoff (Eds.). Springer-Verlag, Berlin, Heidelberg, 2-18, 2004

[47] Li, M., Li, Z., & Vasilakos, V. (2013)., "A survey on topology control in wireless sensor networks: Taxonomy, comparative study, and open issues", Proceedings of the IEEE, 2013.

[48] Xiaojun Zhang, Chunxiang Xu, Chunhua Jin, Run Xie, Jining Zhao, "Efficient fully homomorphic encryption from RLWE with an extension to a threshold encryption scheme, Future Generation Computer Systems", Volume 36, 2014.

[49] Maranika Dasgupta, S.K. Pal, "Design of a polynomial ring based symmetric homomorphic encryption scheme", Perspectives in Science, Volume 8, 2016.

[50] Luigi Coppolino, Salvatore D'Antonio, Giovanni Mazzeo, Luigi Romano, "Cloud security: Emerging threats and current solutions", Computers & Electrical Engineering, Volume 59, 2017.

[51] S. Ristov and M. Gusev, "Security evaluation of open source clouds", Eurocon 2013, Zagreb, pp. 73-80, 2013.

[52] X. Yang, X. Wang, Y. Wu, L. Qian, W. Lu and H. Zhou, "Small-Cell Assisted Secure Traffic Offloading for Narrow-Band Internet of Thing (NB-IoT) Systems," in *IEEE Internet of Things Journal*, 2017.

[53] B. Revathi and D. Geetha, "A survey of cooperative black and gray hole attack in MANET," Int. J. Computer Science and Management Research, vol. 1, no. 2, pp. 205–208, 2012.

[54] O. Garcia-Morchon, S. Kumar, R. Struik, S. Keoh, and R. Hummen, "Security considerations in the IP-based Internet of Things." [Online]. Available: https://tools.ietf.org/html/draft-garcia-core-security-04

[55] L. Wallgren, S. Raza, and T. Voigt, "Routing attacks and countermeasures in the RPL-based Internet of Things," Int. J. Distributed Sensor Networks, vol. 2013, 2013.

[56] K. Zhang, X. Liang, R. Lu, X. Shen, "Sybil attacks and their defenses in the internet of things", IEEE Internet Things J, pp. 372–383,2014.

[57] S. U. Maheswari, N. S. Usha, E. A. M. Anita, and K. R. Devi. "A novel robust routing protocol raeed to avoid dos attacks in wsn", In *Proc. of 2016 International Conference on Information Communication and Embedded Systems (ICICES)*, February 2016.

[58] A. Mukherjee, "Physical-layer security in the Internet of Things: Sensing and communication confidentiality under

resource constraints", Proceedings of the IEEE, vol. 103, no. 10, pp. 1747–1761, 2015.

[59] J. Granjal, E. Monteiro, and J. S. Silva, "A secure interconnection model for ipv6 enabled wireless sensor networks," in 2010 IFIP Wireless Days, Oct 2010, pp. 1–6.

[60] A. J. Jara, D. Fernandez, P. Lopez, M. A. Zamora, and A. F. Skarmeta, "Lightweight mipv6 with ipsec support", in Mobile Information Systems, 2014.

[61] T. Kothmayr, C. Schmitt, W. Hu, M. Bryunig, and G. Carle, "Dtls based security and two-way authentication for the internet of things", Ad Hoc Netw., vol. 11, no. 8, pp. 2710–2723, Nov. 2013.

[62] S. Raza, D. Trabalza, and T. Voigt, "6lowpan compressed dtls for coap," in 2012 IEEE 8th International Conference on Distributed Computing in Sensor Systems, May 2012, pp. 287–289.

[63] K. Sonar and H. Upadhyay, "An Approach to Secure Internet of Things Against DdoS", Springer Singapore, pp. 367–376, 2016.

[64] Wikipedia,"Mirai,"https://en.wikipedia.org/wiki/Mirai_(malware), 2016.

[65] A. N. Nowroz, K. Hu, F. Koushanfar, and S. Reda, "Novel techniques for high-sensitivity hardware Trojan detection using thermal and power maps," IEEE Trans. Computer-Aided Design of Integrated Circuits and Systems, vol. 33, no. 12, pp. 1792–1805, 2014.

[66] M. Tehranipoor, H. Salmani, and X. Zhang, "Hardware Trojan detection: Untrusted manufactured integrated circuits," in Integrated Circuit Authentication. Springer, pp. 31–38, 2014.

[67] Swati Khandelwal, "New iot botnet malware discovered; infecting more devices worldwide", http://thehackernews.com/2016/10/linux-irciot-botnet.html, 2016.

[68] C. Zhang and R. Green, "Communication security in internet of thing: Preventive measure and avoid ddos attack over iot network", in Proceedings of the 18th Symposium on Communications & Networking, ser. CNS '15. San Diego, CA, USA: Society for Computer Simulation International, pp. 8–15, 2015.

[69] Y. Chen, W. Trappe and R.P. Martin, "Detecting and localizing wireless spoofing attacks", in: 2007 4th Annual IEEE Communications Society Conference on Sensor, Mesh and Ad Hoc Communications and Networks, pp. 193–202, 2017.

[70] K. Angrishi, "Turning Internet of Things (IoT) into Internet of Vulnerabilities (IoV): IoT Botnets," arXiv preprint arXiv, 2017.

[71] Waqas Ahmad, Aamir Rasool , Abdul Rehman Javed, Thar Baker and Zunera Jalil ,"Cyber Security in IoT-Based Cloud Computing: A Comprehensive Survey", MDPI Journal, Electronics, 11, 16, 2022.

[72] Deepti Rani, Nasib Singh Gill, Preeti Gulia, "Classification Of Security Issues And CyberAttacks In Layered Internet Of Things", Journal of Theoretical and Applied Information Technology, Vol. 100. No 13, 2022.