# Dealing with security issues in IoT

Radhika Sreedharan[1]

*Computer Science and Engineering, Presidency University*
*Bangalore, India*
[1]radhika.sreedharan@presidencyuniversity.in

***Abstract*— IoT (Internet of Things) is related to design of a lot of inter-related "contrived" gadgets having finite capacities with regard to memory and processing power and design is like an Internet. These are frequently battery-driven, raises requirement for adopting environment-friendly techniques. Between the noteworthy ultimatum that establishing interrelated smart objects accompanies are uniformity and coordination. Many smart objects are presumed to develop and addresses of IPv4 are normally utilized. IPv6 is recognized as a possibility for smartobject transmission.**

**Internet of Things (IoT) is a global network of physical and virtual 'things' connected to the internet. All objects have unique IDs that are utilized for identification. IoT is the emerging technology which can change the way we communicate with devices. Hereafter almost every electronic device will be a smart device that will be able to compute and communicate with handheld and other infrastructure gadgets. The Internet of Things utilization builds a lot of security problems, which arises from**

- **Smart objects essence: utilization of cryptographic algorithms which are delicate, with regard to requirements of processing and memory.**
- **Quality protocols utilization and the requirement to reduce the data quantity swapped among nodes.**

**An IoT usage which accumulates or handles consumer distinctive data like bank particulars require a foremost rank of security, while a sensor linked to a station area will have a low rank. It need not be costly to carry out fundamental security steps; but it is significant to determine a security strategy and incorporate recuperation measures in the security problems incidents. The main aim of this topic is to describe mechanisms which can help to deal with IoT security issues.**

***Keywords*— IoT, security, processes, hackers, privacy**

## I. INTRODUCTION

IoT is exposed to risks through bots and malicious attackers because of the shortage of low-powered and uniform security qualities in IoT and a greater number of devices. For this layout, encryption can be a logical response. An important portion of these gadgets is shortage of the capacities of storage and computation which are needed to support complicated mathematical functioning, which come with encryption. For security, certain creators set a built-in password. The built-in password is momentarily beneficial in a few finite schemes. But attackers have sufficient means for cracking such regular passwords, that incorporates the entire system. IoT is unrestricted to low-powered devices. These gadgets with less power in due course get connected to isolated platforms like cloud/fog/server. Acquiring network access or faraway framework by compromising the gadgets with a low power is a truth in current technical domain. Exposure to attacks like flooding, phishing, denial of service, man in-the-middle attacks etc. will be able to activate anomalies chain that can upset the entire network resource.

### Types of IoT Security Issues

Following are types of IoT Security Issues:

1. **Improper Testing and Updating:** Manufacturers of IoT are focussing only on their sales instead of focusing on their problems of testing and protection. Thus, the manufacturing unit needs to be more careful for designing the device-security systems.
2. Default Passwords issues: Few government websites give user default password and login, which can be prone to attack for reading, writing and stealing the data.
3. IoT Ransomware: The ransomware attacks the device and steals the users' data digitally, simultaneously, it disables the devices functioning.
4. IoT Hackers Targeting Cryptocurrency:
   Blockchain is resistant for hacking, however the number of victims is increasing daily. Social engineering has to be educated for settingt strong passwords and private keys. Monero is a popular open-source cryptocurrency, and many digital currencies are designed using IoT devices.
5. Data Security and Privacy: Information is purposefully transmitted and received by a range of IoT devices such as smart devices, printers, speakers, etc. Thus, it is a committed system which has to hold powerful acceptance and secrecy regulations which should never expose any confidential data. Even cache data needs to be strike out frequently.

6. Minimal IoT Attack for escaping Detection: Rather big bombs, a simple needle is sufficient for inserting a virus and damaging the system. Correspondingly, a small path is sufficient for dragging sufficient user information into the hacker zone.
7. Artificial Intelligence and Automation: Autonomous devices make a spontaneous resolution which can affect billions of mechanisms healthcare, power, and locomotives might be too risky. A single code is also sufficient for destroying the whole framework. It can also assist IoT administrators for detecting the malicious pattern in the beginning.
8. Home Intruders: This is comparable to the theft, which can invoke criminal outfits and can lead to invasion of home. Every house has a unique IP address which is effortlessly obtainable for hackers for entering your house.
9. Remote Vehicle Control: The major victims of hackers are smart car. They can effortlessly attack, hijack and access the car. This will turn into a frightening situation when a stranger escorts the user to lethal crimes.
10. Untrustworthy Connections: Some IoT devices transmit messages to devices or networks in the absence of encoding. For overcoming these, developers need to utilize standard TLS or transport encryption. It is also efficient for utilizing an individual isolation system for individual connections. It needs to be double-checked that data should be sent in a confidential way.
11. Management of device update: The protection and secrecy issues in IoT can refer to security problems because of management of device update as well. Unprotected firmware or software could usually cause IoT security risks. Even if a manufacturer provides a gadget with the current software update, you will experience new vulnerableness. Thus, updates are favourably significant to ensure security on IoT devices, which needs to updated promptly once the new vulnerableness are discovered. The utilization of IoT devices in the absence of requisite updates could increase the threats to their security. Additionally, update management can be dangerous because of the fact that devices will send backups to the cloud. In the absence of suitable encryption for the connection and protection for updated files, any malicious agent will be able to obtain confidential information.

## II. ELEMENTS OF SECURITY

*1) Management of access and identity: every feature of identification and way in for IoT usage comprising the subsequent:*

- User access manages approved users and levels of access to elements of service.
- Security procedures need to be executed for restricting access to login and password\3PP session security steps to visible IT systems which can access services or data needed to comprise supervising.
- Management of key and certificate issues procedures for executing and managing keys and certificates which are significant security procedures.
- Management of identity accumulated data protection and when it is imparted is often viewed and has to be taken into consideration for every tasks.

*2. Middleware security:*

- Protection of data controls the life cycle management's security of individualized and secure data. It comprises of sensitivity, truthfulness and accessibility of data at rest, in transfer and service utilization.
- Management of device permits actions for detecting and taking steps with regard to untrustworthy/thieve gadgets or gadgets that are carrying out illegal actions
- API security is executed using encryption and authentication, which will be primitive for transmission among all elements. Tasks do not have the most fundamental encryption even it is economical to execute and managed. The layer 7 B2B gateway issues API communication control. It issues complete safeguarding for service utilization of web and XML in contrary to inner misuse as well as outer abuse.
- In the design and establishment of middleware, the different communication mediums for broad scale IoT deployments have to be considered.

*3. Physical security is related to hardware, and it comprises of infrastructure and devices.*

- Protection of infrastructure includes the features which are utilized for securing the platform internally at the data center and also at the data center itself. Data centers are ISO270001 manageable as a minimal, however other standards like SSAE 16, SOC1 and SOC2 can be taken into consideration.
- In the data center, infrastructure access should be supervised and verified to make sure it is appropriate, particularly when it is in organized surroundings with other companies.

- Protection of network considers separation at level of network among dissimilar internal and external fragments of network. Server nodes and gadgets need to be strengthened so that it can comply with requirements of service.
- Virtualization security is needed whenever software is executed on a virtual machine in a cloud. It is related to strengthening the platform of virtualization and safeguarding the form of virtual and logical network using level of network separation.
- Uninterrupted security is obtained with the help of generic bootstrap architecture (GBA). GBA determines to issue distributed keying material among service user and the device/sensor/gateway so that they can transmit in a secure manner.

## III. PROTECTION OF DATA

The data protection plans conduct the subsequent security features supervision:

- Accumulation and relocation of data
- Channel discarding
- Secrecy and accumulated data protection

The service provider secures the ethics of every data element comprising the subsequent:

- Analytical data
- Application-level information accumulated on the policy
- Rationality of firm method
- Evidence of invoice and charging which includes metadata of every invoice
- Consumer connection information
- Grant data connected with dissimilar policy users
- Settlement and parcel information

## IV. SECURITY RISKS IN IOT

i. Smart objects replication by unapproved makers ii. Smart objects spiteful replacement of smart things at the time of installing.

iii. Violent act due to firmware substitution iv. Security restrictions withdrawal (smart things are not protected physically).

v. Intruding violent acts when transmission means are unprotected

vi. Man-in-the-middle attacks at the time of substitution of keys. vii. Routing violent acts viii. Denialofservice attacks ix. Secrecy risks.

Risks (i) to (iv) are associated with tangible character of smart objects, that are commonly utilized in widespread regions and will not be continuously monitored which leads to potential security issues. Risks (v) to (viii) are examples of security issues arises through requirements for objects to communicate with each other. Risks (v) and (i) are linked with reality that smart objects may distribute confidential information, which, if attacked by forbidden parties, may cause truthful and secrecy issues.

When it is feasible to manage problems which arise due to objects 'physical nature by adopting measures of safe supply and installation like avoided untrusted installers and manufacturers, and attempting to safeguard smart objects at guarded regions, remaining security risks can be faced by accepting measures like secure transmission protocols and algorithms of cryptography.

These measures enforce the following basic security properties:

i. Sensitivity: Communication end-points can read the transmitted data.

ii. Accessibility: the end-points of transmission can always be appeared and cannot be made isolated iii. Truthfulness: Received data are not interfered at the time of transmission; otherwise, any change can be detected.

iv. Authoritativeness: Transmitters of data

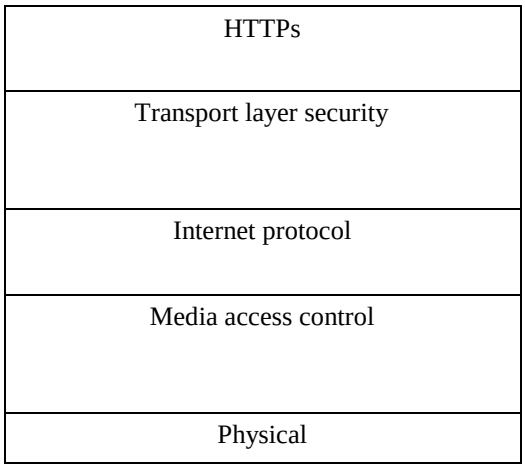
## V. SECURITY PROCESSES

**Traditional vs Lightweight security:**

| CoAP |
|---|
| Datagram<br>Transport layer<br>Security |
| Internet protocol |
| Media access control |
| Physical |

Internet of

Things




Internet

CoAP application protocol is utilized for request/response operations among smart objects or among intelligent objects and non-contrived (quality) node of Internet at the application layer in IoT protocol stack. CoAP alone will not issue primitives to authenticate and protect data, hence those tasks should be executed precisely at that application/service later (by straight away protecting the data which the CoAP encapsulates and swaps) or any of the fundamental layers. Validation, truthfulness and sensitivity of data can be issued at bottom layers like physical or Media Access Control.

Uninterrupted security will not be promised in the absence of high level of certainty on in-between nodes. But because of the exceedingly energetic character of the wireless multihop communications awaited to be utilized to set up the path of routing among nodes at distant end, this type of security is insufficient. That's why, security processes at levels of network, application or transport should be taken into consideration in preference to PHY and MAC level processes.

i. **Network layer:** A node of IoT can secure data swapping in a quality manner utilizing Internet Protocol (IPsec) at the network layer. IPSec was initially established for IPv6, however build extension arrangement, initially, as an IPv4 addition, into which it was decompiled. The necessary part of base IPv6 protocol suite was IPSec, but it is made non-compulsory since that time. IPSec is utilized to protect data flows among a pair of hosts, among security gateways pairs, or among a host and security gateway. For each IP packet, IPSec will be able to issue sensitivity, truthfulness, validation of origin of data and protection in case of rerun attacks. Those tasks of security are executed using two IPSec protocols: Authentication Header (AH) and Encapsulation Security Payload (ESP). AH issues truthfulness, validation of originality of data, and by choice anti-rerun capacities. ESP issues sensitivity, validation of data originality, integrity, and anti-rerun capacities. ii. **Transport layer**: Data swapping among application nodes will be able to be secured in transport layer with the help of quality Transport Layer Security (TLS) as well as Datagram Transport Layer Security (DTLS) rules in recent architecture of IP. The most common secure protocol is TLS. It runs on top of TCP. It issues identical association and stream-oriented interface to application layer. TCP/ TLS issues entire secure transmission with the help of

- peer-entity authentication and exchange of key (with the help of asymmetric cryptography)
- authorization, truthfulness and anti-rerun of data using message authorization code • sensitivity (utilizing symmetric encryption).

The major benefit to secure connections in transport later along-with DTLS comprises in permitting more accurate restriction of access. Functioning in transport layer permits applications for selecting what type of security task needs establishment in an easier way. DTLS permits for the reuse of the side experience benefitted at the time of TLS implementations.

However, there are certain problems to be faced for making DTLS very helpful for strained equipment. The very significant are analogous to the packet of finite size which the fundamental protocols like IEEE 802.15.4 will require. DTLS launches an overhead at the time of both handshake and transport of data phases for IPSec. DTLS leads to division in the handshake layer, and it adds an important overhead. The other explanation may be to utilize the division issues in IPv6 or the layer of 6LoWPAN. A frame development and procedure for compression can be launched for reducing DTLS overhead. DTLS issues a datagram-oriented transmission task, it develops a pointtopoint secure interconnection which is incompatible with multi-cast transmissions.

iii. **Application layer:** When security in transport or internet protocol layer is issued, it has several benefits. They are:

- The same quality process and all the applications divide up the same execution which results in re-utilization of code as well as decreased size of code.
- There is no need for programmers to handle any security process implementation; this remarkably clarifies the applications establishment whenever secure transmissions are needed.

Transport Layer Security and Internet Protocol security have their own obstacles. First if the impossibility to make sure the whole uninterrupted security whenever transmissions of application are indicated by intermediate nodes that perform at the level of application like proxies.

Here, uninterrupted security can be issued using transportorInternet Protocol level 202.5 privacy and security in IoT process, however only in the existence of proven intermediate systems. But here, the broad security is complex by the control of those hop-by-hop management of trust.

A distinct method for issuing entire uninterrupted security is to necessitate security distinctly in the level of application. This clarifies the needs for concealed layers, and apparently decreases the price, with regard to size of packet and processing of data, as application data only needs to be safeguarded, and according to data but not according to packet overhead is launched. Furthermore, at the level of application, multicasting transmission and ininterconnection accumulation of date in encrypted domains are simpler to execute.

The key drawbacks to issue security at the level of application are the obstacles launched for establishment of application and the complete size of code produced by faculty software code repurpose. This is because of deficiency of precise and approved secure protocols at the level of application. S/MIME and SRTP are guidelines utilized for this motive. S/MIME (Secure/Multipurpose Internet Mail Extensions) is a rule to issue validation, truthfulness of message, origin's authentication, and application data's sensitivity. S/MIME was initially established to secure MIME data among email clients, not limited to mail and utilized to secure any application data and can be encased between any transport and application protocol.

The secure transmission protocol which issues sensitivity, validation of message and rerun protection to application data is SRTP (Secure Real-Time Transport Protocol). It is the continuation of Real- Time Transport Protocol (RTP) established to handle real-time data transmissions (e.g., voice or video transmission), however can be re-purposed in further utilization alternatives.

**a. Lightweight Cryptography:** A small calculating gadgets have less abilities of calculation, less memory and finite life of battery are smart objects**.** A very attractive area of research, objective to depict recent ciphers that may satisfy needs of smart objects is lightweight cryptography (LWC). LWC refers to a connection of algorithms of cryptography having lesser trace, lesser power utilization, and less measurable power requirements. LWC constitutes a cryptography customized for restrained gadgets, that needs to cope up with the difference between level of security, cost and working. Algorithms based on Symmetric-key cryptography utilize the identical key to encrypt a plaintext and decrypt a cipher text. The encryption key constitutes a portion undisclosed among parties connected in secure communication. Public key (asymmetric) cryptography needs public key and a private key utilization. Public keys can be linked with the identification of a node by constituting them in a public certificate. Certification authority signs public certificate can be asked to check the certificate.

**b. Homomorphic encryption schemes:** The type of encryption that permits specified kinds of calculation to be implemented on cipher texts for giving an encrypted solution is called homomorphic encryption. Encrypted solution is the cipher text of solutions of work done on the plain text. By symbolizing E{.} as the function of homomorphic encryption and f(.) as the function of computation, it sustains that

$$E\{f(a, b)\} = f(E\{a\}, E\{b\})$$

Homomorphic encryption is utilized for preserving confidentiality between uninterrupted communication points, and made feasible for in-between nodes for processing information, without decrypting data before processing, Homomorphic cryptosystems need computation top levels of computation and require extended keys for obtaining an equivalent level of security compared to symmetric-key algorithm.

## VI. PRIVACY PROBLEMS IN THE IOT

**Role of Authorization:** An unlocked protocol for permitting safeguarded authority from mediator applications in an easy and consistent manner is known as Open Authorization (OAuth). The OAuth protocol issues a layer of authorization for service APIs which are on the basis of HTTP, normally on upper part of a secure transport layer, like HTTP-over-TLS.

The three main responsibilities are described by OAuth:

- The user is the system which generates data.
- The provider of service presents the information which the user generates and makes it obtainable with the help of APIs.
- The consumer of service also known as the "Client application", access the information which the provider of service accumulates for its own utilization.

For complying with security and privacy needs, user needs to provide a direct deal which certain client application will be able to access information an account of them. When the client is granted an access token which contains the identities of user and service consumers, this is obtained. Identities of user and

service consumers should be explored in each requisition as evidence of authorization. The development of initial OAuth protocol is OAuth 2.0 protocol. The OAuth 2.0 protocol determines for enhancing client development clarity by explaining outlines to authorize web, mobile and desktop applications. Connection is an easy task for client application developers in case of existent online services. Executing an authorization process which is on the basis of OAuth, on the side of service provider is a more complex, prolonged, and assured, and all-inclusive task. Furthermore, it comprises of users' and client applications' registrations, and authorizations which users permit to applications of service consumer, and their combination with authentication services.

## VI.SECURITY ARCHITECTURE OF IOT

It is split into three layers:

i. Layer of Perception ii. Layer of Transportation iii. Layer of Application

The main aim of layer of perception is the data collection, control and perception of object. Layers of perception are classified into perception node and perception network. The function of perception node is control and acquisition of data and perception network is to transfer the collected data into the network gateway.

Layer of transportation can be classified into three layers: access network, core network and LAN. The aim of access network is to issue the access environment for perception layer. Access network incorporates Ad hoc network, wireless network and others. Wireless network may be divided into center and non-center network. Base station is utilized to communicate between the mobile nodes in the center network. The example of center network is wireless local area network and cellular network.

The main objective of core network of IoT is to data broadcast. The main core network is the Internet. 6LowPAN are proposed to utilize to issue the IP address to large number of sensor nodes.

IEEE802.15.4 PHY and MAC layer are utilized in 6LowPAN and transportation layer uses IPv6 protocol.

The security problems in Local area network are leakage of data and protection security of server. Security management must be strengthened in LAN for the same. Some of the important transportation problems are given below:

i. Heterogeneous network convergence problems of transport layer analysis ii
ii. Attacks problems of transportation layer analysis.

The application support layer supports business services and realizes allocation of resources in choosing, screening and data processing and smart computation. This layer identifies spam data, malicious data and true data and filters them when required. The organization of application support layer relies upon specific services and applications. M2M, middleware, cloud computing platform are technologies utilized in application support layer. Security processes have been established against the attacks in cloud computing like DDOS attack.

Application layer comprises of various specific individual applications or integrated applications. There are some specific security problems in application layer that cannot be handled by other layers of IoT. This is special security demand of application layer.

Privacy protection, location privacy and query privacy are very crucial in application. RFID systems are utilized in intelligent transportation application of IoT. The most crucial data security threat in RFID system is leakage of information. Data encryption methods can be used to prevent data theft in RFID. The other solution is to store tag ID information in RFID tag and do not store important and sensitive data in tag. The emerging application of IoT is smart home. Network control technology, mobile terminal technology and communications technologies are utilized in smart home. There are different problems with respect to the specific applications of IoT. Various kinds of cyber-attacks have been launched and different defence algorithms have been proposed in smart grids and Advanced Metering Infrastructure (AMI).

## VII. SIGNIFICANCE OF MACHINE LEARNING IN IOT SECURITY

ML techniques are utilized for privacy, security, detection of theft and attack, and analysis of malware. Supervised learning algorithms are utilized for applications of IoT security, issues of localization, and assessment of channel. For supervised learning, regression and categorization procedures are utilized. Techniques of categorization which comes under supervised learning procedures do the modelling and supervising of data set. Procedures of regression comprise of nearest neighbors and logistics regression.

Naïve bayes categorization algorithm is utilized for multiclass and binary surroundings and works finest with distinct data types. This algorithm is helpful to detect issues of intrusion and anomaly.

Unsupervised learning procedures are helpful to detect anomalies, intrusions and faults, balancing of load of clustering of cell. Unlabeled data is handled in a useful way.

## VIII. FUTURE SCOPE

There is a requirement for providing the precis IoT security architecture which has results to the issues of security of different lightweight applications of IoT. One of the ways is to split the need of security and requirement of application computation into many levels. usual applications of IoT. The future research is going on the light-weight security methods of IoT challenges like key management, access control, access authentication and others. The lightweight solutions must give solutions of

## REFERENCES


[1] WileyJ, "Internet of Things- Concepts and applications"

[2] Sudip Misra, Anandarup Mukherjee, Arijit Roy, "Introduction to IoT"

[3] Barry Haughian M, Design," Launch and Scale IoT services"

[4] Mirza Abdur Razzaq, Sajid Habib Gill, Muhammad Ali Quresshi, Saleem Ullah,, "Security Issues in the Internet of Things (IoT): A Comprehensive Study", International Journal of Advanced Computer Science and Applications,Vol. 8, No. 6, 2017

[5] Seokung Yoon, Haeryong Park1,and Hyeong Seon Yoo, "Security Issues on Smart home in IoT Environment "

[6] Mayuri A. Bhabad,, Sudhir T. Bagade ,Internet of Things: Architecture, Security Issues and Countermeasures

[7] Lo'ai Tawalbeh ,Fadi Muheidat,Mais Tawalbeh and Muhannad Quwaider, "IoT Privacy and Security: Challenges and Solutions", Appl. Sci. 2020, 10(12), [8], International Journal of Communication Networks and Information Security (IJCNIS) Vol. x, No. x, November 2016

[8] Aqeel-ur-Rehman, Sadiq Ur Rehman, Iqbal Uddin Khan, Muzaffar Moiz and Sarmad Hasan, " Security Issues in the Internet of Things (IoT): A Comprehensive study", (IJACSA) International Journal of Advanced Computer Science and Applications,Vol. 8, No. 6, 2017

[9] Navod Neranjan Thilakarathne, International Journal of Engineering and Management Research e-ISSN: 2250-0758 | p-ISSN: 2394-6962 Volume-10, Issue-1 (February 2020)

[10] Ashvini Balte, Asmita Kashid, Balaji Patil, "Security Issues in Internet of Things (IoT): A Survey", International Journal of Advanced Research in Computer Science and Software Engineering ,Volume 5, Issue 4, 2015 ISSN: 2277 128X

[11] Ashok Kumar Reddy, "Security issues in using IoT enabled devices and their impact",International Engineering Journal For Research & Development Vol.4 ,Issue 2,E-ISSN NO:-2349-0721

[12] Mardiana binti, Mohamad Noor, Wan HaslinaHassan, " Current research on Internet of Things (IoT) security: A survey", The International Journal of Computer and Telecommunications Networking, Computer Networks ,Volume 148, 15 January 2019, Pages 283-294

[13] R. Shantha Mary Joshitta1, L. Arockia, "Security in IoT Environment: A Survey", Int. Journal of Information Technology & Mechanical Engineering - IJITME, Vol.2 Issue. 7, July- 2016, pg. 1-8 ISSN: 2349-2865

[14] Denver Braganza* and B. Tulasi, : RFID Security Issues in IoT: A Comparative Study", Oriental Journal of Computer Science & Technology ISSN: 0974-6471,March 2017, Vol. 10, No. (1): ,Pgs. 127-134