JETIR.ORG ISSN: 2349-5162 | ESTD Year : 2014 | Monthly Issue
JOURNAL OF EMERGING TECHNOLOGIES AND INNOVATIVE RESEARCH (JETIR)
An International Scholarly Open Access, Peer-reviewed, Refereed Journal

# Security Challenges and Countermeasures for the Internet of Things (IoT)

**Dr. Mahesh Sharma**[1]

**Dr. Seema Nath Jain**[2]

Vice Principal[1], Ideal Institute of Management and Technology [GGSIPU], Karkardooma, Delhi, India.

Principal[2], Ideal Institute of Management and Technology [GGSIPU], Karkardooma, Delhi, India.

***Abstract:*** This paper presents a survey as well as an investigation and analysis of the current state of Internet of Things (IoT) security. The Internet of Things aims to connect anybody with anything, anyplace. In contrast to the fixed Internet, an IoT connects a huge number of machines, resource- constrained devices, and sensors via various wired and wireless networks. The realization, network, and

application layers are the three hypothetical layers that make up an IoT. This paper describes the security issues that exist inside and between these layers. There are also several security ideas that need be implemented at each tier. Previous work on ensuring security for each IoT layer, as well as related countermeasures, is also examined. Finally, the report discusses potential IoT acquisition strategies.

***Keywords:*** *Integrity, Policies, Availability, Confidentiality.*

## Introduction

The Internet of Things (IoT) is a collection of networked items, services, people, and devices that can communicate, share data, and information in order to achieve goals in a variety of fields and applications. Transportation, agriculture, healthcare, energy generation and distribution, and many more fields that require things to connect over the Internet to execute business assignments intelligently without human involvement can all benefit from IoT. Devices that join the Internet of Things often use an Identity Management (IM) solution to be identified among a set of similar and dissimilar devices. In the Internet of Things, an area is defined by an IP address, but each entity within that region is identifiable by a unique ID.

In recent years, IoT techniques have witnessed fast expansion, with additional technologies such as Radio Frequency Identification (RFID) and Wireless Sensor Networks being published (WSN). RFID qualifies the tagging or labelling of each and every gadget, serving as the IoT's primary reorganization mechanism. Each "thing" (people, equipment, etc.) becomes a wirelessly distinct object that may interact between the physical, cyber, and digital worlds thanks to WSN.

The remainder of this work is arranged in the following manner. The three-layer IoT structure and architecture are described in Section 2. Section 3 discusses security issues relating to various security principles and the characteristics of IoT devices. This section also discusses the security issues that are linked to each layer of the IoT. Section IV addresses recent research efforts aimed at demonstrating countermeasures to IoT security concerns. Section 5 gives a broad overview of all the IoT security-relatedresearch that has been done. Section 6 discusses possible future directions in light of the current state of IoT security.

## Architecture

Each layer in an IoT architecture is explained by its functions and the devices that it employs. In the IoT, there are various viewpoints on the number of levels. However, many researchers believe that the Internet of Things is based on three layers: perception, network, and application. Each layer of IoT has its own set of security concerns. The core three-layer architectural structure of IoT, as well as the devices and technologies that surround each layer, is depicted in Fig. 1.

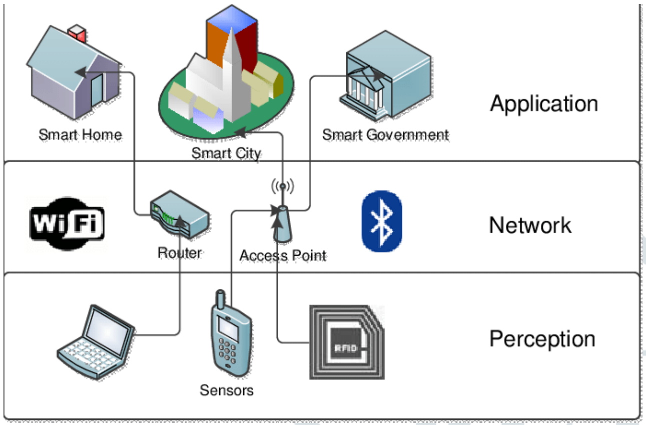

**Figure 1: IOT 3 Layer Architecture**

## Perception Layer

In the Internet of Things, the perception layer is also known as the "Sensors" layer. The goal of this layer is to use sensors to collect data from the environment. This layer monitors, collects, and analyses sensor data before sending it to the network layer. In addition, in local and short-range networks, this layer may conduct IoT node combination.

## Network Layer

The network layer of the Internet of Things handles data routing and communication between multiple IoT hubs and devices. At this layer, Internet gateways, switching, and routing devices, among others, provide desperate network services by utilizing cutting-edge technologies such as WiFi, LTE, Bluetooth, 3G, and Zigbee. By aggregating, filtering, and transferring data to and from various sensors, network gateways act as a mediator between distinct IoT nodes.

## Application Layer

The data's validity, integrity, and confidentiality are all ensured by the application layer. The goal of IoT, which is to create smart surroundings, is carried out at this layer.

## Security Issues in IoT

To check the security of IoT, the same basic security objectives of Confidentiality, Integrity, and Availability that should be provided for any interactions utilizing computers and networks are required. However, the IoT has a number of constraints and limitations in terms of components and devices, computing and power resources, and even the diverse and ubiquitous nature of the IoT, all of which necessitate additional research in order to organize security. This section is divided into two parts: the IoT's common security characteristics and the security issues unique to each tier of the IoT.

Security Features of IoT

IoT security difficulties can be classified into two categories: technological and security concerns. The technology problems arise from the diverse and widespread nature of IoT devices, whereas the security difficulty stems from the ethics and utility that must be adopted in order to achieve a secure network. IoT security should be considered throughout the development and operation of all IoT devices and hubs. The security principles that should be followed in order to build a secure interaction framework for people, software, processes, and things in an IoT are listed below.

Confidentiality – It is critical to guarantee that data is secure and accessible only to authorized users. Because the Internet of Things is based on exchanging data and information between many different typesof devices, it's critical to ensure that the data is accurate, that it's coming from the right sender, and that it's not being tampered with during transmission due to intentional or unintended interference.

Availability – The goal of the Internet of Things is to connect as many smart devices as possible. Users of the Internet of Things should have access to all data at all times. However, data is not the only module employed in the IoT; devices and services must also be approachable and accessible when needed in a timely manner if the IoT predictions are to be realized.

Authentication – In the Internet of Things, each object must be able to unambiguously identify and verify other things. However, because of the nature of the IoT, this process might be challenging; numerous entities are mixed together (devices, people, services, service providers and processing units). Furthermore, objects may occasionally need to communicate with other objects for the first time (objects they do not know). As a result, a technique for mutually authenticating entities in every IoT conversation is necessary.

Lightweight Solutions – All of the previously discussed security goals are not unique to IoT, however it may add unique traits and limits to each of them. In general, however, confidentiality, integrity, availability, and authentication are considered fundamental goals in computer and network security.

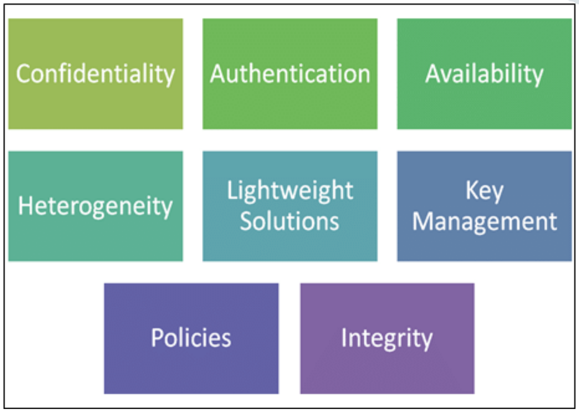

**Figure: IoT Security Principles**

Heterogeneity – The Internet of Things connects a variety of entities with varying potential, complexity, and vendors. The devices have a variety of release dates and versions, use a variety of technical interfaces and bitrates, and are meant for a variety of purposes. As a result, responsibilities must be defined in order to work on a range of devices and in various settings. The Internet of Things (IoT) strives to connect device to device, human to human, and person to human, and as a result, it connects many things and networks. Another issue to consider in IoT is that the environment is constantly changing (dynamics), thus a device may be linked to an entirely different group of devices at one time than it is at another. Furthermore, an effective cryptography system with proper key management and security protocols is required to assure security.

Policies – There must be regulations and standards in place to ensure that data is managed, safeguarded, and transported efficiently, but more significantly, a process must be in place to ensure that every entity follows the rules. Every service that is engaged must have unambiguous Service Level Agreements (SLO). The application of such rules will encourage human users to trust the IoT paradigm, resulting in its growth and scalability in the future.

Key Management Systems – To establish data secrecy in the Internet of Things, devices and IoT sensors must exchange encryption materials. For this purpose, all structures must have a lightweight key management system that can enable trust between different things and supply keys while using the device's minimum capacity.

**Security Issues in Each Layer**

Each IoT layer can be managed in terms of security threats and assaults. These might be aggressive or passive, and they can come from external or internal sources in response to an Insider attack. The active attack interrupts the service, whereas the differential type monitors IoT network data without interfering with it. IoT devices and services are vulnerable to Denial of Service (DoS) attacks at each layer, which render the device, resource, or network unavailable to authorized users. Table 2 lists the security issues at each tier, and a brief examination of these issues is provided below for each layer.

**Perception Layer**

In the IoT perception layer, there are three security issues. The first factor is the impact of wireless signals. Signals are typically exchanged between IoT sensor nodes via wireless technology, which might be weakened by convulsing waves. Second, because IoT nodes are typically run in exterior and outdoor environments, physical attacks on IoT sensors and devices, in which an attacker can interfere with the device's hardware components, the sensor node in IoT devices can be attacked not only by the owner but also by attackers. The third aspect is the dynamic nature of the network model, as IoT nodes are frequently shifted around. Sensors and RFIDs make up the majority of the IoT perception layer, therefore their storage, power, and compute capabilities are severely constrained, rendering them vulnerable to a variety of threats and attacks.

Replay Attacks, which include faking, changing, or replaying the identification information of one of the IoT devices, can easily compromise this layer's confidentiality. Or, in what is known as a Timing Attack, the attacker may obtain the encryption key by reviewing the needed time to conduct the encryption. Another threat to confidentiality is when an attacker takes control of a node and seizes all information and data, which is known as a Node Capture attack. By delivering Malicious Data, an attacker can add another node to the network, jeopardizing the integrity of the data in this layer. This can also result in a DoS attack, as it consumes the energy of the system's nodes and prevents them from going into sleep mode, which they utilize to conserve energy. The above-mentioned security vulnerabilities at the perception layer can be addressed via encryption (point-to-point or end-to-end), authentication (to authenticate the sender's genuine identity), and access control. The next section contains additional security procedures and processes to address this problem.

**Network Layer**

As previously stated, DoS attacks can be managed at the network layer of the Internet of Things. Apart from DoS attacks, the adversary can also compromise network confidentiality and privacy through traffic analysis, eavesdropping, and passive monitoring. Because of remote access mechanisms and device data interchange, these attacks have a high probability of occurring. Man-in-the-Middle attacks, which can be followed by eavesdropping, are very manageable at the network layer. The secure interaction channel will be completely weakened if the devices' keying material is intercepted. In the Internet of Things, the key exchange method must be secure enough to prevent eavesdropping and identity theft.

### Application Layer

There are numerous security issues in the IoT because there are yet no comprehensive policies and standards in place to oversee communication and application expansion. Different authentication systems exist in different software and apps, making unification of all of them difficult to provide data privacy andidentity authentication. The high number of connected devices sharing data will result in a significant increase in the number of applications that analyze the data, which can have a significant impact on service availability.

### IoT Security Solutions

At all three layers of the IoT, security computations are required: at the physical layer for data collection, at the network layer for overpower and dispatch, and at the application layer for confidentiality, authentication, and integrity. The state-of-the-art security computes that address the unique characteristicsand security intentions of IoT are covered in this part.

### Measures of Authenticity

Zhao et al. published a change authentication approach for IoT systems and terminal nodes in 2011. Hashing and characteristic extraction are the foundations of the strategy. To avoid collision attacks, the feature extraction was combined with the hash function. This strategy truly assigns a good authentication solution in the IoT. The features extraction technique has the properties of irreversibility, which is desirable for security, as well as light weight, which is advantageous in IoT. When the platform tries to transfer data to terminal nodes, the strategy concentrates on the authentication process, not the other way around. While the technique will increase security while reducing the quantity of data delivered, it is based solely on theory, with no experimental proof of concept to back it up.

Wen et al. provide another technique for ID authentication at IoT sensor nodes. It's a request- reply mechanism-based one-time one cypher approach. For security, creating precise access controls is just as important as authentication, and the two-work hand in hand in safeguarding IoT. Mahalle et al. introduced an Identity Authentication and Capability based Access Control (IACAC) for the IoT to address these functionalities. This study attempts to fill a vacuum in the market for a combined protocol that accomplishes both authentication and access control in order to achieve reciprocal identity establishing in the Internet of Things. The model employs a public key approach that is compatible with IoT devices' lightweight, mobile, distributed, and computationally restricted characteristics, as well as existing access technologies such as Bluetooth, 4G, WiMax, and Wi-Fi. It protects against man-in-the- middle attacks by encrypting the authentication message between the devices with a timestamp that serves as the Message Authentication Code (MAC).

The technique is broken down into three stages: first, a secret key is created using the Elliptical Curve Cryptography – Diffie Hellman algorithm (ECCDH), then identity is built using one-way and mutual authentication protocols, and last, access control is implemented. Due to the usage of Elliptic curve cryptography, the shared secret key is begun by a combination of a public key and a private parameter, and it has a small size and minimal computational cost (ECC). Each IoT device stores an expert with access rights, a device identifier, and a random number to allow admission. The hashing of device ID with access rights yielded this random number. The IACAC paradigm isn't perfect in terms of preventing DoS assaults. However, it reduces it because only one ID can access a resource at a time.

### Trust Creation

Because items or devices in the Internet of Things can physically migrate from one owner to another, trustbetween the two owners is required to begin a seamless transition of the IoT device in terms of access control and permissions. By providing an item-level access-control framework, the work in presents a shared belief for inter-system security in IoT. It establishes confidence across the IoT development, operation, and dispatch phases. Two techniques establish this trust: the creation key and the token.

### Mediated Architecture

It's difficult to keep track of security in the IoT since there aren't any standardized procedures or standards for controlling the design and execution of algorithms. To address the heterogeneity of diverse devices, softwares, and protocols, it is critical for IoT to have a unified architecture that supports internal autonomy or a centralized unit. The study in advocated a clarification for coupled IoT, and a methodologyfor access control delegation is offered based on that concept. The approach described takes into account the fundamental properties of IoT systems: adaptability and scalability. Another attempt was made in to create a framework for critical infrastructures called Secure Mediation GateWay (SMGW). This satisfies an IoT hypothesis because it may be applied to any type of distributed infrastructure that is entirely heterogeneous in nature and function. SMGW can recognize and allocate all necessary information from various nodes, overcome the heterogeneity of heterogeneous nodes, whether they are telecommunication, electrical, or water distribution nodes, and exchange all messages and information over an untrusted Internet network. This study qualifies the continuation of another federated strategy, which was presented in to give the Smart Home structure based on the SMGW.

It is not enough to have procedures and standards in place to ensure security; enforcement measures are also required. Neisse et al study's addresses this issue by merging SecKit, a security toolkit, with the MQ Telemetry Transport (MQTT) protocol. Because of the dynamic nature of IoT, established techniques may not be successful. The proposed method mechanism has the potential to have a positive impact on IoT security, but it adds to the process's duration.

### Security Understanding

The knowledge and review of human users who are a member of the IoT network is another important security factor for the success and expansion of the IoT structure. The authors used real data to describe the consequences of not safeguarding the IoT. These IoT devices (SCADA devices, web cams, traffic control devices, and printers) were accessible to the general public using no password or the default password. The collected data was fascinating, revealing that many of these technologies were truly feasible. If individuals continue to be unconcerned about security and employ the bare minimum of security, such as the default password that comes with the product, the IoT will bring more harm than good. If one of the network's devices isn't secure, hackers will have more opportunities to attack the entirenetwork.

### The Overview Picture

The various elements and security integrities stated earlier stress on IoT security, and the issues that IoT security faces have been the focus of many studies for a long time. In this section, an assessment of some comparable work is provided, as well as the paper's offerings. In a survey study presented by Roman et al., a full introduction to the Internet of Things (IoT) and security issues, as well as the necessity for IoT standards, is explained. However, no solutions are presented for the security threats that have been identified. Following this, the survey resolution was completed, which included solutions for all security threats.

## Future Tracks

In recent years, IoT has advanced rapidly in fields such as telemedicine platforms, intelligent transportation systems, logistics monitoring, and pollution monitoring systems, among others. Some analysts anticipate that by 2020, the total number of things will have increased to 26 billion units. However, the IoT's security threats must be addressed in order for it to grow and mature. The following are future research directions for making the Internet of Things more secure.

## Standards (Architecture)

IoT now uses a variety of devices, services, and duties to accomplish a shared goal. However, there must be a set of criteria that must be followed from the micro to macro levels of IoT recognition in order to accommodate a network of IoT structures in order to accomplish a larger structure, such as forming a smart town by joining many smart homes.

## Identity Management

In the Internet of Things, identity management is accomplished by exchanging discovering information between devices for the first time connection. This process is susceptible to overhearing, which can result in a man-in-the-middle attack, posing a threat to the entire IoT infrastructure. As a result, some pre- defined identity management entity or hub is required to monitor the device relationship process using encryption and other techniques in order to prevent identity theft.

## Session Layer

The three-layer architecture of IoT, according to most researchers, does not include the opening, closing, and controlling of a session between two items. As a result, there is a need for requirements that may solve these issues while also simplifying device interaction. In IoT design, an abstract session layer should be included as an additional layer that may specifically manage the connections, obligations, and sessions between interacting devices.

## 5G Protocol

IPv4 will undoubtedly fall short of containing the massive quantities of IP-identifiable items required to implement IoT. That is why there is a push to implement IPv6, which can accommodate 3.4x1038 devices. However, such a big number of devices will generate a lot of traffic, which will cause further delays and necessitate more bandwidth. The goal of the next generation of communication (5G) is to deliver speeds of 10-800 Gbps, which is a significant improvement over the current technology (4G), which provides speeds of 2-1000 Mbps. 5G should be able to handle the traffic generated by IoT devices. IPv4/IPv6 structure translation is intended to be used in 5G technology to accommodate both IPv4 and IPv6.

## Conclusion

At each tier, the IoT framework is vulnerable to assaults. As a result, there are several security concerns and needs that must be addressed. The current state of IoT research is primarily focused on authentication and access control protocols, but with the rapid advancement of technology, it is becoming increasingly important to consolidate new networking protocols such as IPv6 and 5G in order to achieve the progressive mash-up of IoT topology.

The biggest IoT advancements are mostly on a small scale, such as within enterprises and in a few niche industries. Various security concerns must be addressed in order to scale the IoT structure from a single organization to a discipline of multiple companies and systems. The Internet of Things has a lot of potential to change how we live today. However, security is the most important discipline in recognizing truly smart structures. If security disciplines such as privacy, confidentiality, authentication, access control, end-to-end security, trust management, global rules, and standards are fully abandoned,the Internet of Things can be used to transform everything in the near future. New identification, wireless, software, and hardware technologies are required to address the present open research vulnerabilities in IoT, such as device standards, key management and identity setup systems, and trust management hubs.

**References**

1. M. Abomhara and G. M. Koien, "Security and privacy in the Internet of Things: Current status and open issues," in Int'l Conference on Privacy and Security in Mobile Systems (PRISMS), 1-8, 2014.

2. K. Zhao and L. Ge, "A survey on the internet of things security," in Int'l Conf. on Computational Intelligence and Security (CIS), 663-667, 2013.

3. L. Atzori, A. Iera, G. Morabito, and M. Nitti, "The social internet of things (siot)–when social networks meet the internet of things: Concept, architecture and network characterization," Computer Networks, vol.56, 3594-3608, 2012.

4. M. Leo, F. Battisti, M. Carli, and A. Neri, "A federated architecture approach for Internet of Things security," in Euro Med Telco Conference (EMTC), 1-5, 2014.

5. P. N. Mahalle, B. Anggorojati, N. R. Prasad, and R. Prasad, "Identity authentication and capability based access control (iacac) for the internet of things," J. of Cyber Security and Mobility, vol. 1, 309-348, 2013.

6. M. Farooq, M. Waseem, A. Khairi, and S. Mazhar, "A Critical Analysis on the Security Concerns of Internet of Things (IoT)," Perception, vol. 111, 2015.

7. R. Roman, P. Najera, and J. Lopez, "Securing the internet of things," Computer, vol. 44, 51-58, 2011.

8. R. Roman, J. Zhou, and J. Lopez, "On the features and challenges of security and privacy in distributed internet of things," Computer Networks, vol. 57, 2266-2279, 2013.

9. Q. Wen, X. Dong, and R. Zhang, "Application of dynamic variable cipher security certificate in internet of things," in Int'l Conference on Cloud Computing and Intelligent Systems (CCIS), 1062-1066, 2012.

10. G. Zhao, X. Si, J. Wang, X. Long, and T. Hu, "A novel mutual authentication scheme for Internet of Things," in Int'l Conference on Modelling, Identification and Control (ICMIC), 563-566, 2011.

11. N. Koblitz, "Elliptic curve cryptosystems," Mathematics of computation, vol. 48, 203-209, 1987.

12. J.-Y. Lee, W.-C.Lin, and Y.-H. Huang, "A lightweight authentication protocol for internet of things," in Int'l Symposium on Next-Generation Electronics (ISNE), 1-2, 2014.

13. Y. Xie and D. Wang, "An Item-Level Access Control Framework for Inter-System Security in the Internet of Things," in Applied Mechanics and Materials, 1430-1432, 2014.

14. B. Anggorojati, P. N. Mahalle, N. R. Prasad, and R. Prasad, "Capability-based access control delegation model on the federated IoT network," in Int'l Symposium on Wireless Personal Multimedia Communications (WPMC), 604-608, 2012.

15. M. Castrucci, A. Neri, F. Caldeira, J. Aubert, D. Khadraoui, M. Aubigny, et al., "Design and implementation of a mediation system enabling secure communication among Critical Infrastructures," Int'l Journal of Critical Infrastructure Protection, vol. 5, 86-97, 2012.

16. R. Neisse, G. Steri, and G. Baldini, "Enforcement of security policy rules for the internet of things," in Int'l Conference on Wireless and Mobile Computing, Networking and Communications (WiMob), 165- 172, 2014.