**International Journal of Research Publication and Reviews**

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

# Security Analysis of IOT Things

***T Anil Kumar***

Student, Department of Information Technology, GMR Institute of Technology

**ABSTRACT:**

Internet of things are being used in a variety of fields, including the healthcare industry, smart grid systems, smart cities, and smart homes.. Through a variety of sensors, actuators, transceivers, or other wearable devices, these gadgets send a large amount of data. The IoT environment exposes data to a wide range of hazards, threats, and assaults. Going for deal with assaults, vulnerabilities, security, and privacy issues associated with IoT, a strong security system is essential. Aiming to analyze the security of IoT devices and suggest solutions to security issues and challenges by utilizing mobile computing, a thorough review of the literature has been undertaken in this study. It is a revolutionary way to conduct a thorough and thorough security analysis of IoT gadgets in the environment of mobile computing. In this paper, a detailed review of the security-related challenges such as spoofing, jamming, lack of encryption, lack of trusted executed environment, user interaction, insufficient privacy protection etc. further possible threats in IoT applications. After discussing the security issues, various emerging and existing technologies such as WIFI, Bluetooth, ZigBee, RFID etc.… focused on achieving a high degree of trust in the IoT applications are discussed.

***Keywords - Security, Internet of Things, Security of data, Smart grid system, Smart cities, Information Security, Sensors, Actuators*.**

## I. INTRODUCTION

The Internet of Things (IoT) is a collection of physical items that include sensors, actuators, and controllers and are connected to the online world. The IoT has become a part of contemporary daily life as a result of the low cost of hardware, the popularity of mobile devices, and broad Internet connectivity. IoT device usage is predicted to grow exponentially in the future, and as it does, security concerns will become more important to take into account because all IoT devices are connected to the Internet, making it possible for hackers to access these devices. The expansion of the Internet and Web into the physical world was made possible by a number of factors that go under the general heading of the phrase. IoT has only become a reality because to the development of advanced supporting technologies like cloud computing, data analytics, IP-based networking, ubiquitous computing, etc.; otherwise, the practice of managing things by fusing sensors, computers, "Internet of Things," or IoT, which is a developing subject of economic, social, and technical significance and networks has been around for decades. The word Internet of Things was first introduced by Ashton et al. in 1999while talking of a global network of objects connected to RFID in a supply chain application. Since then, the Internet of Things (IoT) has been expanded to include new application areas, and a plethora of new technologies have appeared in the IoT space, including those for business, agriculture, animal farming, transportation, healthcare, smart homes, smart retail, supply chain, smart wearables, and smart security. IoT and Network of Things (N o T) are frequently used interchangeably.

For instance, in a healthcare IoT application, a compromised sensor may reveal private information or deliver inaccurate heart rate readings, resulting in prescription errors; or in an ITS, if traffic light control is compromised, this may result in a car accident. Therefore, in this context, a security flaw can result in data privacy violations in addition to financial loss, and in the worst cases, it may even cause physical harm to people. While having connectivity for anything and everywhere at any time is alluring and has many benefits, there are also new requirements and challenges that must be taken into account when designing IoT systems and applications.

In an IoT environment, security challenges like privacy, authorization, verification, access control, information storage, and management present significant difficulties. As we will discuss in Section I.A, the huge scale, dynamism, and variety of devices, among other characteristics of the IoT environment, all add to the difficulty of such security elements. Addressing these concerns and providing suitable security solutions is essential for the development and widespread adoption of the IoT paradigm..

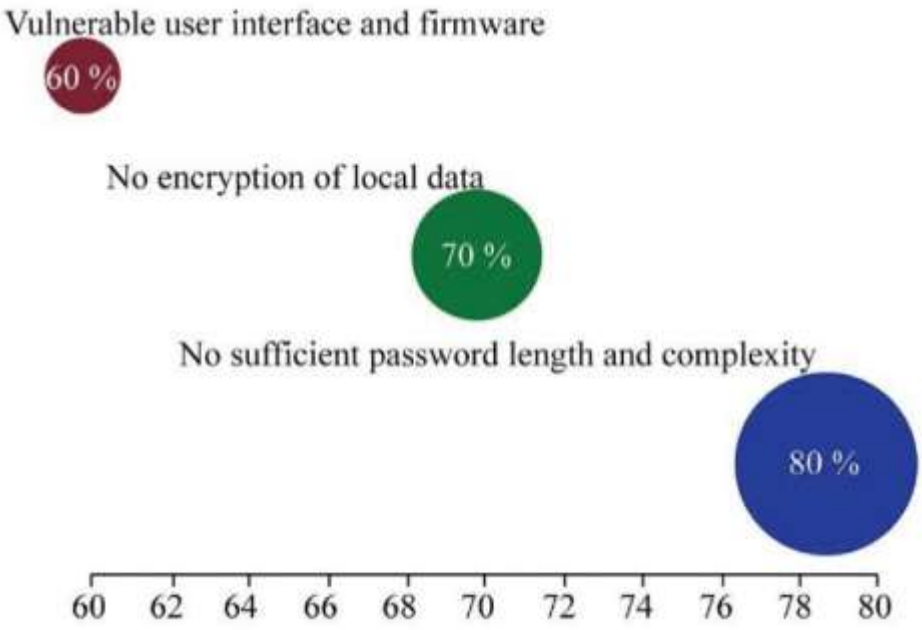



**Figure 1: Percentage of vulnerabilities of IoT**.

## II. LITERATURE SURVEY

In paper [1] Macedo said IoT ecosystems experience the same network-layer vulnerabilities as wireless networks in general, which are made worse by their high dynamism, the need to integrate several technologies, and the existing absence of standards. IoT does not currently use a dominating technology or stack of standardized protocols. This has frequently led to the adoption of proprietary protocols and the creation of ad hoc network architectures, which aren't always focused on providing security solutions at all tiers and can result in vulnerabilities that can be exploited in assaults. The information taken from primary research with a focus on security issues was analysed from the perspectives of general aspects, authentication, access control, and data protection..

In paper [2] F**.** Meneghello and M. Calore survey of practical security vulnerabilities in real IoT devices, We concentrate on the particular issues that arise in the IoT space, where certain hardware may not even handle the most fundamental functions, including random number generation or common encryption procedures. As a result, we focus on the four IoT communication protocols that are most commonly used in business: ZigBee, Bluetooth low energy (BLE), 6LoWPAN, and LoRa WAN. We quickly review the security measures that each protocol supports and then examine the attack surface. We also disclose a number of actual assaults on well-known commercial IoT devices as illustrations of the dangers posed by inadequately designed security mechanisms.

In paper [3] M. Aly said that The IoT using the cloud, including key management, node compromise, layer addition or removal, and privacy of identity and location. The requirement for lightweight cryptographic techniques, privacy, unique object identification, software vulnerabilities, and malware are some of the top IoT security issues covered in a different report. The top 10 vulnerabilities for IoT design are listed by the Open Web Application Security Project (OWASP). Similar to this, the IoT-A project outlines an IoT reference architecture whose compliance necessitates implementation for security, privacy, and trust. The privacy model necessitates the definition of access controls and procedures for data encryption and decryption in order to prevent improper data usage

In paper [4] S. Ammirato, F. Sofo, A. M. Felicetti and C. Raso proposed a methodology to support the adoption of IoT innovation and its application to the Italian bank branch security context. CPS systems have a number of security and privacy problems that could affect their dependability, safety, efficiency, and perhaps prevent widespread adoption. We concentrate on the primary CPS security threats, vulnerabilities, and attacks as they relate to the components and communication protocols in use for CPS systems and their interconnections, including IoT systems.

In paper [5] T. Nandy, M. Y. I. B. Idris, R. M. Noor, L. M. Kiah, L. S. Lun, N. B. A. Juma gave a review on security of Internet of Things authentication mechanism. Attackers aim for a network in order to gain access to it and obtain important data that can be used to either satisfy their needs or be sold on the black market**.**

## III. Security Challenges in IoT

The Internet of Things (IoT), an ecosystem made up of the fusion of many network technologies, not only inherits the security challenges with wireless networks and traditional wired networks, but also includes sensor networks, mobile networks, and other network technologies. Due of its extremely

unique characteristics, additional issues arose. In order to properly coordinate the integration of the offline and online worlds, it is important that we first look at the sensor devices in charge of gathering and monitoring environmental characteristics. It is challenging to implement dependable and complicated security protocols, such as those used for authentication reasons, on sensors nodes because of their constrained computation and storage capacities. The gadgets must integrate lightweight technology, which sometimes do not provide the best levels of protection. Lastly, consider the characteristics that this development has by nature. Opportunistic, ad hoc interactions between devices and humans are typical in an IoT environment. as a result of some specific settings, users. For instance, a mobile device could only let nearby users to use its resources for a set period of time. Therefore, less formal business models are being adopted more frequently than formal agreements between parties. Due to the ad hoc character of contacts, which is a crucial issue, building trust between the involved parties in this situation is a challenging process.

## IV. Context: -

These studies concentrate on particular methods to cover issues with IoT security and do not offer a comprehensive view of crucial factors to provide security at various levels for these systems. These security issues are covered in our study: (i) Access control, authentication, data protection, and (iv) trust. We view them as being extremely thorough and encompassing additional facets. For instance, trust includes accessibility, and data protection includes privacy. Moreover, current research Don't talk about architectural details when referring to the locations where security techniques are used. considering the analysis, we seek to synthesise the studies we found in our literature search. to clarify the methods employed as security remedies and discuss the locations where the aforementioned techniques were used in terms of the IoT systems' architectural stack. We think. that the kind of summary and reflections presented in our paper could aid researchers in seeing opportunities on the most recent developments to pinpoint key issues and knowledge gaps in IoT security research. Additionally, the conversation architectural features may enable the scaling of security solutions based on the constrained computational capacity of IoT devices, assisting IoT system developers in the process. Prior studies include the literature review was done using a variety of research techniques.

## V. Sensor Movement:

IoT devices can move around easily, so it's important to specify the precise processes that handle this feature by re-authenticating devices when they switch locations.

Our architectural design allows for two main types of movement:

- Inter-cluster movement: refers to the movement of sensor from one cluster to another, and between different gateways under the same Health IoT.
- Inter-network: refers to movement between different health IoTs

We assume that a sensor can be either static or dynamic in order to manage sensor movement in a flexible manner. It is forbidden for a static sensor to move. This holds true for a few IoT medical devices, such as humidity controllers and room thermostats. We can define the following movement models for dynamic sensors:

- Intra-cluster movement model: the sensor is allowed to move within a specific gateway and in a defined secure range (SR). For instance, this model applies for the sensors within a surgical robot and sensors determining anaesthetic levels during surgery.
- Intra-H IoT movement model: here the sensor can move between different clusters in a specific H IoT within a defined SR. This may be the case with smart beds that contain pressure and heartbeat sensors, designed to monitor the patient’s condition.
- Intra-network movement model: the sensor is free to move between different clusters and between different H IoTs. For example, smart badges that assist in locating medical personnel and in providing balanced resource allocation around the hospital.

### *5.2 Data Protection*

Essentially, data protection is an issue. He responsibility to enable personal decision-making data flow, taking action after collecting the data

through the dissemination, processing, and storage of data, i.e., through an all-encompassing fine-grained data management. The vast majority of methods used in primary studies are based on encryption to protection for data. In addition to other techniques, ECC is used. For instance, based on the elliptical curve digital signature algorithm, according to (ECDSA)

a method that uses ECC to produce a digital signature for data to allow authenticating it while maintaining overall performance. ECDSA only uses keys that are a certain size.

160 bits is incredibly little compared to pure DSA.

### *5.3 Architecture design*

In the architectural design, To achieve a real-time response and reduce latency, we concentrate on dispersing an authentication system on fog nodes and close to the end IoT devices. In this case, as seen in Figure 1, we suggest a three-layered architecture. These are the layers that make this up:

- Cloud layer: a server or several servers make up this layer. These servers support additional layers for device registration and the creation of secure communication. Additionally, it enables system registration and communication with users.
- Edge layer: the edge layer can be composed of several sub-layers for better distribution. The Home IoT server (H IoT), which is in charge of the area, is what it primarily contains. Each H IoT is in charge of controlling gateway registration and authentication. For purposes of communication and mutual authentication, all H IoT servers must register with the cloud. Several gateways are also present in this layer. The gateway is in charge of using continuous authentication to identify the sensors located in its territory.
- End devices layer: this layer is made up of sensors that are grouped into clusters and are each under the control of a different gateway.

### *5.4 Performance Analysis:*

we evaluated the performance of the proposed protocol in terms of computation and communication costs.

- Computation Cost

We calculate the costs associated with the operations used in the proposed protocol, which consists of static and continuous phases for authentication. The proposed protocol makes use of the XOR operation, concatenation, generate randoms, hashing, and HMAC. We choose to disregard the time spent on concatenation and XOR because their computation costs are lower than those of other operations. To determine how long certain operations—such as hashing, creating random data, and HMAC

- Packet Delivery Ratio

The number of packets transmitted by the sender and the number of packets successfully received at the receiving end are used to determine the packet delivery ratio. It is challenging to test the performance of the network since it depends on a number of variables, including bandwidth, device capabilities, and network setup. The Packet Delivery Ratio can be calculated using the equation.

$$PDR=NRP/NSP$$

## VI. METHODOLOGY

We outline the procedure followed when conducting the selection of the studies to be included in our analysis after conducting a literature search. According to an SLR is based on the selection and subsequent analysis of a number of scientific articles. A clearly defined protocol that allows for the replication, verification, and auditing of the outcomes. Essentially, an SLR consists of three phases. The conducting step entails locating pertinent research, choosing primary studies, evaluating study quality, extracting necessary data, and data synthesis. Researchers create a review report in the final phase, Documenting, and validate it. According Such a strategy offers the advantage of giving an overview. State -of-the-art on the subject under study, which is useful for researchers in need of a current state-of-the-art

first approach to a specific topic. This kind of research trend identification is also made possible by studies, which raise the most contentious issues and unresolved issues while highlighting the research potential in less well-known areas, specifically I Planning, (ii) Conducting the review, and (iii) Documenting and Reporting the review. The review process is executed following the tasks involved in conceiving, developing, and validating research topics during the planning phase.

### *6.2 Description of AES*

The United States National Institute of Standards and Technology (NIST) developed the Advanced Encryption Standard (AES) as a specification for the encryption of electronic data in 2001. Despite being more difficult to build, AES is still commonly used because it is substantially stronger than DES and triple DES. Points to remember

- AES is a block cipher.
- From 128 to 256 bits are used to make keys.
- Blocks of 128 bits each are used to encrypt data.

As a result, from 128 bits of input, it produces 128 bits of encrypted cypher text as an output. The substitution-permutation network principle, which underlies AES operation, involves a series of interconnected operations that replace and shuffle the input data.

***6.3 General Aspects Analysis***

- The vast majority of papers include authentication tactics, which shows a keen interest in research on techniques for using authentication in an IoT setting. Contrarily, very few studies have examined trust-related issues, which are underrepresented in primary studies despite the fact that they are obviously very important in the IoT context. Because there are no formal contracts and the IoT tends to use more flexible commercial practises and scattered transactions, The parties' relationships are crucial. So, we assess the research.
- The need to fill a gap in the literature by developing strategies to deploy trust in the context of the Internet of Things.
- Authentication

Authentication is the process of identifying an authorised entity for a certain application. Device authentication has been found to provide considerable advantages for IoT security architectures, making it one of the most extensively utilised components that are crucial to IoT security ecosystems since authentication is required in order to provide additional security features, claim the authors.

- Access Control

The process of limiting requests to some resources is called access control. Access to a resource obtained from a legitimate source. As per the prescribed guidelines [69]. This feature became apparent as the second-highest number of primary studies, with 49 articles, was found. Access control techniques were widely used in the implementation locations, with implementations at the tiers of Things, Fog, and Cloud. It denotes the absence of any trends. The best location to implement access control solutions. However, the majority of research on healthcare, smart cities, Access control is typically implemented by Industrial IoT applications. External entities. This strategy reveals a clear worry about utilising portable solutions to extend the life of the devices which are sensible, particularly in these kinds of applications. There is no pattern of implementation within each tier. revealed for a particular technique, similar to how within every domain of an application.

- Data Protection

Essentially, data protection is an issue. The responsibility to enable personal decision-making data flow, taking action

after collecting the data through the dissemination, processing, and storage of data, i.e., through an all-encompassing fine-grained data management. The vast majority of methods used in primary studies are based on encryption to protection for data. This could be supported by the idea that In addition to other techniques, ECC is used. For instance, based on the elliptical curve digital signature algorithm, according to (ECDSA) a method that uses ECC to produce a digital signature for data to allow authenticating it while maintaining overall performance.

- Application Domain

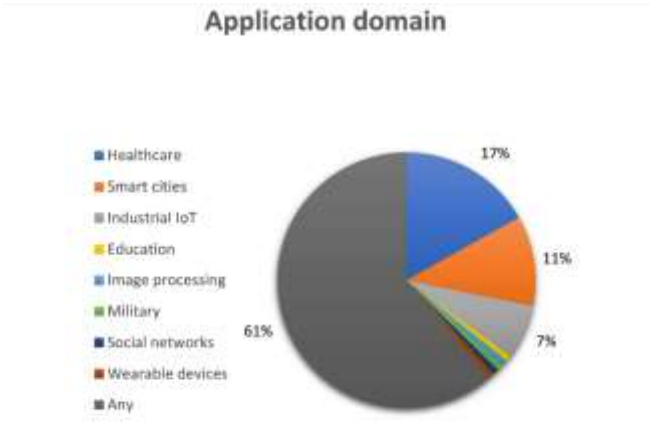



Fig. 4. General application domain.

The majority of primary studies (61%), followed by 17% studies that addressed healthcare and 11% studies that addressed smart city applications, concentrated on solutions that could be used in any application domain

- Deployment of Security Techniques at the Architectural Tiers:

Given the diversity of IoT environments, things' computational resources range from limited devices that have only used more powerful CPU, memory, and power resources. When an application generates a lot of workload when it comes to computational resources, it is typical to transfer a portion of the computational work from resource-limited IoT devices

to other locations. This method is well-known. As a computational offload and the obvious choice to handle the enormous amount's processing and long-term storage. The cloud stores IoT data. IoT and the cloud can work together to create

emerges as an ecosystem with two architectural tiers, with the cloud is the top tier, with the physical/things tier at the bottom.

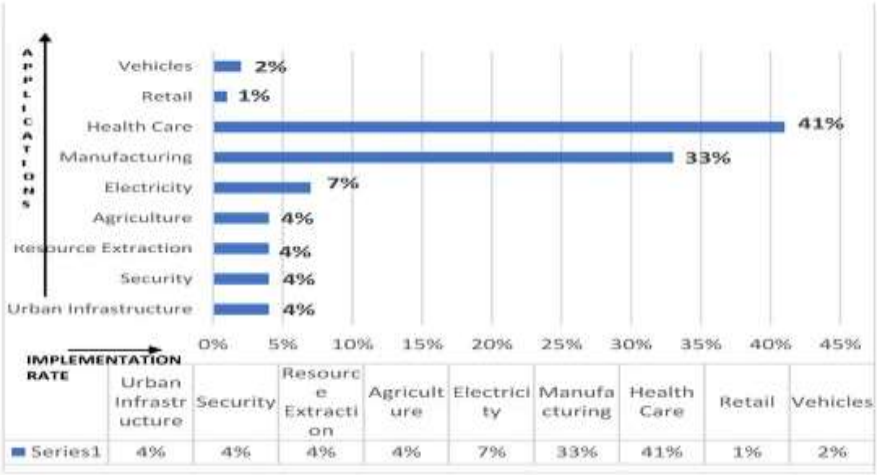
- Description of Different Types of Masquerade Attacks

| Attacks | Description |
|---|---|
| Masquerade Attack | In this attack, adversary counterfeit identity of the legitimate user to get access to the network. |
| Man-in-the-middle Attack | In this attack, attackers inquire impertinently communication between two communicators. |
| DoS Attack | In this attack, attackers flood the network by spreading inconvenient packets and disrupt actual communication to penetrate the network. |
| Forging Attack | In this attack, an adversary emulates a system or authenticated user to gain access to the network. |
| Guessing Attack | In this attack, attackers predict and explore the possibilities of getting advantages over the credentials of legal users. |
| Physical Attack | In this attack, network enemies try to get access to the physical components. In addition, they may penetrate the network or inject malicious scripts into the network, after getting physical access |
| Routing Attack | In this attack, attackers create an improper route to send or receive packets in a network. |

## VII. RESULTS AND DISCUSSION

Analysis of the results showed that there is a research gap regarding trust in Internet of Things, with only a few studies looking into this topic.

this feature. Additionally, a large number of studies that dealt with ECC, "Author Solutions," and the authentication aspect OAuth-based procedures The ECC method is appropriate to appear in this area because it is well-known The "Author Solutions" is a collection of different answers offered by the main study authors. And what some find interesting is the adoption of OAuth-based methods, which was regarded as a freely available standard for assigning API access.




We would like to emphasise the significance of taking a comprehensive approach to security in order to safeguard IoT building blocks and provide. Designing in security. Last but not least, there is a lack of a clearly defined architecture that takes into account security aspects and could act as a reference design for creating IoT security products.

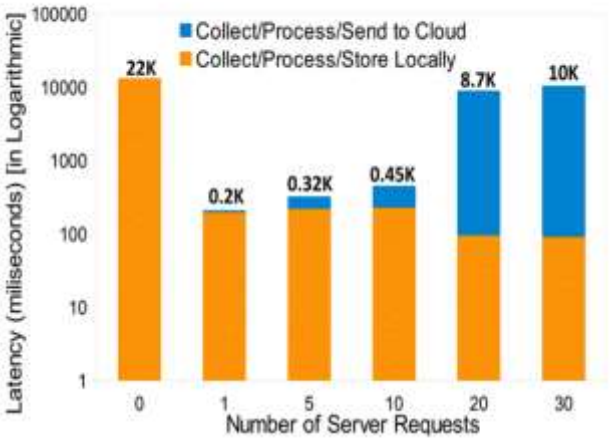



**Fig 2: Graphical Representation of Regression Statistics**

We can see from the findings that Iatency16 also rises as the number of query requests rises. Latency rises to 10 seconds when MOSDEN completes 30 queries. However, combining the data and sending it to the cloud consumes a sizable portion of the overall processing time.

## VIII. CONCLUSION

IoT's significant influence is a result of device connectivity. These devices must be reliable and secure in order to protect this infrastructure. In this study, we developed a device-to-device continuous authentication mechanism for the Internet of Things. By utilising lightweight cryptography methods like hash and HMAC, the protocol continually authenticates each other while taking into account the hardware and software constraints of IoT devices (such as token, battery, and location). By leveraging anonymity and untrace ability, it also protects the privacy of communicating devices. It also sets a secure authorised region for each moving sensor and takes into account various IoT device movement models. The protocol depends on the usage of emergency keys and shadow IDs to re-initiate communication between sensors and gateways in order to prevent a DoS attack that results in momentary synchronisation loss. Sensors can be verified by the closest gateway in the event of a permanent gateway failure.

## IX. REFERENCES

[1]. E. L. C. Macedo, E. A. R. de Oliveira, F. H. Silva, R. R. Mello, F. M. G.Franca, F.C.Delicato,et al.,"On the security aspects of Internet of Things:A systematic literature review", *J. Commun. Netw.*, vol. 21, no. 5, pp. 444-457, Oct. 2019.

[2]. F. Meneghello, M. Calore, D. Zucchetto, M. Polese and A. Zanella, "IoT:Internet of threats? A survey of practical security vulnerabilities in real IoT devices", *IEEE Internet Things J.*, vol. 6, no. 5, pp. 8182-8201, Oct. 2019.

[3]. M.Aly, F. Khomh, M. Haoues, A. Quintero and S. Yacout, "Enforcing security in Internet of Things frameworks: A systematic literature review", *Internet Things*,vol. 6, Jun. 2019.

[4]. S. Ammirato, F. Sofo, A. M. Felicetti and C. Raso, "A methodology to support the adoption of IoT innovation and its application to the Italian bank branch security context", *Eur. J. Innov. Manag.*, vol. 22, pp. 146-174, Jan. 2019.

[5]. T. Nandy, M. Y. I. B. Idris, R. M. Noor, L. M. Kiah, L. S. Lun, N. B. A. Juma'at, et al.,"Review on security of Internet of Things authentication mechanism", *IEEE Access*, vol.7, pp. 151054-151089, 2019.

[6]. Q. Jing, A. V. Vasilakos, J. Wan, J. Lu, and D. Qiu, "Security of the internet of things: Perspectives and challenges," Wireless Netw., vol. 20, pp. 2481–2501, Nov. 2014.

[7]. S. Sicari, A. Rizzardi, L. Grieco, and A. Coen-Porisini, "Security, privacy and trust in internet of things: The road ahead," Comput. Netw., vol. 76, pp. 146–164, Jan. 2015.

[8]. I. Ali and Z. Ullah, "Internet of things security, device authentication and access control: A review," International J. Comput. Science Inf. security, vol. 14, no. 8, Aug. 2016, pp. 456–466.

[9]. F. A. Alaba, M. Othman, I. A. T. Hashem, and F. Alotaibi, "Internet of things security: A survey," J. Netw. Comput. Appl., vol. 88, pp. 10–28, June 2017.