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

# A Comprehensive Study on IoT, Threats posed by Security Issues, and Abstraction Techniques

[1] Mr. S Manjunatha , [2] Dr. Seshaiah Merikapudi , [3] Mr.Ankit Saurabh
[1]Assistant Professor, [2] Assistant Professor, [3]Student
[1]Computer Science and Engineering,
[1]SJC Institute of Technology, Chickballapur, India

***Abstract :*** In the past, the Internet of Things (IoT) was the focus of research. With the great puissance of IoT, there come many kinds of quandaries at once challenges. Security is one of the main quandaries in IoT technology, applications, and forums. To integrate this consequential IoT feature, this paper updates the progress of IoT research and found that there are a few security issues and challenges that need to be considered and briefly explicated. Efficacious and efficient safety because IoT is required to ascertain data anonymity, confidentiality, integrity, validation, access control, and the facility to identify as well as variability, quantification, and availability, should be considered. Considering these facts, by reviewing some recent research on the IoT domain, the incipient IoT solutions from the technical, edifying, and industrial sides are provided and discussed. Predicated on the findings of this study, the desired IoT solutions need to be designed and distributed, which can ascertain: anonymity, confidentiality, and integrity in different areas.

**Keywords—Internet of Things, Security, Threats, Data, Challenges, Solutions**

## I. INTRODUCTION

Internet of Things (IoT) is an emerging technology and is considered the future of the cyber world. By sanctioning contrivances/objects to acclimate capabilities predicated on prevalent and non-proprietary communication protocols, and utilizing astute communications, over a potent ecumenical network infrastructure. The concept of IoT can be optically discerned as an extension of subsisting interactions between people and applications that communicate in an incipient size. Due to advances in mobile communications, the establishment of Radio Frequency Identification (RFID), and Wireless Network Networks (WSNs), objects and methods in IoT can communicate with another regardless of time, place or situation. The most immensely colossal prosperity of IoT lies in the engenderment of keenly intellective environments: perspicacious homes, perspicacious convey, keenly intellective things, astute cities, perspicacious lives, astute lives, etc. for organizations and companies, including IoT applications and accommodation providers, IoT platform providers and mitigators, telecom operators and software vendors. In additament, IoT will have a consequential impact on the cognition experience; especially in the higher inculcation system.

With the expeditious magnification of IoT application utilization, a few security issues have become very high. As implements and materials become a component of the Internet infrastructure, these issues need to be considered. When virtually everything will be connected on the Internet, these quandaries will arise more; the perpetual ecumenical exposure to the cyber world will expose many security jeopardies. Such security errors will be exploited by malefactors, and in time can be misused in areas that are not controlled by billions of IoT machines. In additament, IoT will adscititiously increase potential areas of assailment on hackers and other cybercriminals.

In fact, when IoT becomes ubiquitous, everyone, even individuals or companies, will be concerned. Adscititiously, contrasts reveal incipient forces of influence and exchange. This leads to incipient potential risks cognate to information security and data aegis, which should be considered. In additament, the lack of security will engender resistance to IoT acceptance by companies and individuals.Safety issues and challenges can be solved by providing opportune training to designers and developers to integrate security solutions into IoT products and thus, inspirit users to utilize the built-in IoT security features on contrivances.

This paper provides an overview of key IoT issues regarding safety and addresses considerations that should be considered afore and during design phases to fill the literature gap on this issue by providing alternative solutions from the three features that include technical, inculcative, and industrial solutions. The main contribution of this paper is to provide the indispensable information on how certain utilizations of such technology can be made with categorical methods and algorithms. This is believed to guide future studies on the application of categorical solutions to a particular quandary predicated on the proposed algorithms and methods of academic researchers' attention..

## II. Security Issues, Challenges and Considerations

IoT has commenced gaining momentum in recent years as a result of the expeditious magnification of Internet-connected contrivances. However, security remains one of the major quandaries of IoT, and the main concerns raised by sundry Internet stakeholders have the potential to truncate its adoption. Consequently, it is considered to be one of the major quandaries that require to be addressed in order to develop IoT in the genuine world. Security is a rudimentary quality of the IoT system and is associated with certain security features that are often the rudimental requisite to enable the Trust and Privacy attributes of the system. IoT Security is a focus area for forfending connected contrivances, data aegis, and Internet of Things objects. Computer equipment and embedded sensors utilized in

astute home systems, and portable contrivances are the driving forces of the IoT.

Impotent security and security breaches need to be considered from the outset as well as robust design, both on individual contrivances and across systems. Billions of adscititious connected contrivances in incipient environments and applications denote that the IoT world has incremented the involution of applications. As the number of IoT-connected contrivances grows, security issues are becoming more and more mundane and there are many security concerns that should be considered as a whole system. In integration, traditional security methods cannot be applied directly to IoT technology due to their designed system i.e. constrained power and these astronomically immense numbers of connected contrivances raise variability and magnification quandaries. The safety and security of such systems can be compromised by a wide variety of jeopardies, both prognosticable and capricious, so the scalability of the system should be a vigorous consideration.

Heterogeneity is one of the most paramount issues, as well as the security measures to be integrated into the IoT and have a paramount impact on the network security resources to be deployed on the IoT. Contrivance contrivances will interact with a wide variety of contrivances directly or through the gates. Heterogeneity requires security in order to surmount the infeasibility of making efficacious algorithms and protocols for all contrivances in IoT system fields. In this case, it is consequential to utilize functional cryptographic algorithms that can provide high performance and comply with lightweight security procedures that provide a secure end-to-end communication channel. These protocols require authentication, so key control systems should be acclimated to disseminate this information and avail in obtaining the required session keys among peers.

Dealing with the decline in IoT distribution is another consequential quandary. The most astronomically immense challenge is to provide reliable solutions, which can contain billions of objects connected to many different local or ecumenical networks. In additament, many of them are portable and locating and verifying felicitous ownership of an object will be a major quandary for IoT infrastructure. Consequently, the development of efficacious strategies that support heterogeneity and balancing, making utilizer data innominate are paramount issues. In integration, providing addressing scalability for immensely colossal IoT deployments is another consequential issue. The most astronomically immense challenge is to provide reliable solutions, which can contain billions of objects connected to many different local or ecumenical networks. Adscititiously, many of them are portable and locating and verifying congruous ownership of an object will be a major quandary for IoT infrastructure. Ergo, the development of efficacious strategies that support heterogeneity and balancing, making utilizer data incognito are

paramount issues. In additament, the provision of flexible enrollment schemes and event management while ascertaining that ratings in reverence of items and users are still considered an open matter.

minority the capacity of the contrivances used is, in fact, physical access to sensors, resources, and openness systems, postulating the contrivances / objects will be wireless communication. Security concerns such as DoS / DDoS attacks, intruder attacks, sundry network quandaries, IPv6 system susceptibilities, WLAN system conflicts withal obviate IoT security applications and application security issues including access to information and utilizer authentication, information. , verbalizer management and more.

In integration, a sizably voluminous number of IoT applications and accommodations are in peril of data larceny or larceny. To bulwark the IoT from such attacks, advanced technology is needed in a number of fields. Information security and network should be equipped with facilities such as identity, confidentiality, integrity and accessibility. More precisely, authentication, confidentiality, and data integrity are consequential issues cognate to IoT security. Verification is required to build connections between contrivances and to exchange public and private key numbers with a node to obviate data larceny. In integration, confidentiality ascertains that data inside the IoT contrivance is encrypted from unauthorized objects, while data integrity obviates any data conversion in the center by averting data that has reached the recipient's location unchanged and is perpetually transmitted to the source.

## III. Trust, Data Confidentiality, and Privacy in IoT

Reliability and security are predicated on tokens or guarantees, provided by trust management infrastructure, embedded and possibly shared between contrivances. These tokens can be symmetric keys or digital certificates. They are serviceable in diverting external attacks initiated by unlicensed businesses, but failing to divert internal attacks, where credentials or nodes with your personal information are in peril. Public key (PKI) infrastructure is utilized to engender and manage certificates. In some critical security environments, reliable field modules are utilized, which provide a hardware-predicated reliability base and a high caliber of authenticity of the patented features that belong to a particular contrivance. Since IoT is a flexible system, steps are habituated to prove the reliability of IoT components for the rest of their lives is compulsory.

Current Identity and Access Management (IAM) solutions for IoT are inhibited in their faculty to habituate to maintain ownership and organizations on an immensely colossal scale.19 This inhibition has led to a lack of layers to integrate IoT-predicated applications. At this time, there is no consummate framework available for the acquisition and management of IoT businesses and their ownership across all different solutions.

The customary approach is to provide circumscribed access predicated on the expected role rather than inhibited access to standard IAM systems. As a result, authentication from the same contrivance may provide different access capabilities predicated on how the utilizer has verified the contrivance.

IoT will require traditional IAM systems to integrate M2M businesses. Typically, IAM platforms will require to be modified to cover ownership of IoT-predicated systems.

The data sent or received by the node can be trusted if its integrity, optionally coalesced with the confidentiality of data by symmetric encryption (utilizing the Advanced Encryption Standard [AES] algorithm as the de facto industry standard), is ensured. For example, in a body area network, a wireless glucometer sends glucose readings to an integrated insulin pump. This information must be bulwarked from maleficent or intentional interference, and consideration of patient privacy requires data encryption. However, there are cryptography challenges for contrivances with integrated applications, for example, 8-bit microcontrollers with constrained RAM. Encryption is mundane and is applied directly to the hardware, while data integrity is provided by message verification codes or cryptographic hashes affixed to the payment of data.

The pump must be able to ascertain that it is connected to a trusted glucometer (and receive data from it) and not to a maleficent contrivance. Proof of accreditation provides proof that a peer has the ascendancy to (a) communicate with other peers and (b) manage a concrete act. In our example, (1) a glucometer receives only data requests from an insulin pump (not a blood pressure quantifying contrivance); in additament, both the glucometer and the pump must be of the same manufacturer; and (2) the reset command sent to the glucometer sensor by the insulin pump (after sensor resetting) should be used only if the insulin pump is in the required authorization level.

Maintaining privacy in IoT is still a significant challenge. Privacy includes the protection of individual information as well as the ability to control what happens with this information. Privacy issues in IoT systems are complicated by the fact that a system is more than the sum of its parts. Privacy

considerations for low-level tools may differ significantly from concerns posed on an application or data analysis level. Also, any level of privacy breach in the system is affected by the entire system.

A plethora of private information can be accumulated from the perspicacious contrivances. Control of this information is impotent in current IoT techniques. In many cases data is accumulated passively and because of it some privacy breaches can go unnoticed for a long time. The question of IoT data ownership – who owns which data and who controls where data goes – engenders major issues from regulatory, ethical, and financial standpoints. End users believe they own all the data. The pristine equipment manufacturers believe they own, or at least have access rights to, the data engendered by their endpoints. The accommodation providers in many cases believe they own the data, as do the application providers. Issues of data ownership become increasingly intricate as more heterogeneous IoT systems with more players from divergent organizations are deployed. Decommissioned old contrivances can still keep an abundance of privacy-sensitive information and data sanitization should be done for them

## IV. IoT Challenges

The security concern is the most immensely colossal challenge in IoT. The application data of IoT could be industrial, enterprise, consumer or personal. This application data should be secured and must remain confidential against larceny and tampering.

For example, the IoT applications may store the results of a patients health or shopping store. The IoT amend the communication between contrivances but still, there are issues cognate to the scalability, availability and replication time. Security is a concern where the data is securely transmitted over the cyber world.

While conveying the data across international border, safety measure act may be applied by regime regulation such as Health Indemnification Portability and Accountability (HIPA)act. Among different security challenges, the most paramount challenges pertinent to IoT are discussed.

1) Data Privacy: Some manufacturers of astute TVs amass data about their customers to analyze their viewing habits so the data accumulated by the astute TVs may have a challenge for data privacy during transmission.

2) Data Security: Data security is withal a great challenge. While transmitting data seamlessly, it is consequential to obnubilate from optically canvassing contrivances in the cyber world.

3) Indemnification Concerns: The indemnification companies installing IoT contrivances on conveyances amass data about health and driving status in order to take decisions about indemnification.

4) Lack of Prevalent Standard: Since there are many standards for IoT contrivances and IoT manufacturing industries. Consequently, it is an immensely colossal challenge to distinguish between sanctioned and non-sanctioned contrivances connected to the cyber world.

5) Technical Concerns: Due to the incremented utilization of IoT contrivances, the traffic engendered by these contrivances is withal incrementing. Hence there is a desideratum to increment network capacity, ergo, it is additionally a challenge to store the immensely colossal quantity of data for analysis and further final storage.

6) Security Attacks and System Susceptibilities: There has been an abundance of work done in the scenario of IoT security up till now. The cognate work can be divided into system security, application security, and network security.

a) System Security: System security mainly fixates on overall IoT system to identify different security challenges, to design different security frameworks and to provide congruous security guidelines in order to maintain the security of a network.

b) Application security: Application Security works for IoT application to handle security issues according to scenario requisites.

c) Network security: Network security deals with securing the IoT communication network for communication of different IoT contrivances.

## V. ANALYSIS OF DIFFERENT TYPES OF ATTACKS AND POSSIBLE SOLUTIONS

IoT is facing a wide variety of attacks including active attacks and passive attacks that can easily impair functionality and eliminate its housing benefits. In a passive attack, an intruder may just sniff the node or purge the information but never physically attack it. However, active attacks physically impair performance. These active attacks are further divided into two categories which are internal

attacks and external attacks. Such hypervigilant attacks can avert conspiracies to communicate intellectually. Therefore, security barriers must be implemented to prevent conspiracies from malicious attacks. This section discusses the attack type, the nature of the attack/deportation, and the attack threat level. The different degrees of attacks are classified into four types according to their behavior and propose possible solutions to threats/attacks.

1) Low-level attack: If an assailant endeavors to assail a network and his assailment is not prosperous.

2) Medium-level attack: If an assailant/intruder or an eavesdropper is just heedfully aurally perceiving the medium but don't alter the integrity of data.

3) High-level attack: If an assailment is carried on a network and it alters the integrity of data or modifies the data.

4) Astronomically High-level attack: If an intruder/assailant attacks on a network by gaining unauthorized access and performing an illicit operation, making the network unavailable, sending bulk messages, or jamming network.

The Table I presents different types of attacks, their threat levels, their nature/behavior, and possible solution to handle these attacks

## VI. CONCLUSION

The main accentuation of this paper was to highlight major security issues of IoT concretely, focusing the security attacks and their countermeasures. Due to lack of security mechanism in IoT contrivances, many IoT contrivances become soft targets and even this is not in the victim's erudition of being infected. In this paper, the security requisites are discussed such as confidentiality, integrity, and authentication, etc. In this survey, twelve variants of assailments are categorized as low-level attacks, medium-level attacks, high-level attacks, and prodigiously high-level attacks along with their nature/demeanor as well as suggested solutions to encounter these assailments are discussed.

Considering the consequentiality of security in IoT applications, it is genuinely paramount to install security mechanism in IoT contrivances and communication networks. Moreover, to forfend from any intruders or security threat, it is withal recommended not to utilize default passwords for the contrivances and read the security requisites for the contrivances afore utilizing it for the first time. Incapacitating the features that are not used may decrease the chances of security attacks. Moreover, it is consequential to study different security protocols utilized in IoT contrivances and networks

TABLE I. A SUMMARY OF DIFFERENT TYPES OF ATTACKS AND THEIR THREAT LEVELS, THEIR NATURE

| Type | Threat level | Behavior | Suggested Solution |
|---|---|---|---|
| Passive | Low | Usually breach data confidentiality. Examples are passive eavesdropping and traffic analysis. Hostile silently listen the communication for his own benefits without altering the data | Ensure confidentiality of data and do not allow an attacker to fetch information using symmetric encryption techniques |
| Man in the Middle | Low to Medium | Alteration and eavesdropping are the examples of this attack. An eavesdropper can silently sense the transmission medium and can modify the data if encryption is not applied and steal the information that is being transmitted. Hostile may also manipulate the data. | Apply data confidentiality and proper integration on data to ensure integrity. Encryption can be also applied so that no one can steal the information or modify the information or encode the information before transmission. |
| Eavesdropping | Low to Medium | The information content may be lost by an eavesdropper that silently senses the medium. For example in medical environment, privacy of a patient may be leaked. | Apply encryption on all the devices that perform communication. |
| Gathering | Medium to High | Occurs when data is gathered from different wireless or wired medium. Examples are skimming, tampering and eavesdropping. Data is being collected to detect messages. Messages may also be altered | Encryption can be applied to prevent this kind of attack. Identity based method and message authentication code can also be applied in order to prevent the network from such malicious attacks. |
| Active | High | Effects confidentiality and integrity of data. Hostile can alter the integrity of messages, block messages, or may re-route the messages. It could be an internal attacker. | Ensure both confidentiality and integrity of data. To maintain data confidentiality, symmetric encryption can be applied. An authentication mechanism may be applied to allow data access to only authorized person. |

| | | | |
|---|---|---|---|
| Imitation | High | It impersonate for an unauthorized access. Spoofing and cloning are the examples of this attack. In spoofing attack a malicious node impersonate any other device and launch attacks to steal data or to spread malware. Cloning can re-write or duplicate data. | To avoid from spoofing and cloning attacks, apply identity based authentication protocols. Physically unclonable function is a countermeasure for cloning attack. |
| Privacy | High | Sensitive information of an individual or group may be disclosed. Such attacks may be correlated to gathering attack or may cause an imitation attack that can further lead to exposure of privacy. | Apply anonymous data transmission. Transmit sample data instead of actual data. Can also apply techniques like ring signature and blind signature. |
| Interruption | High | Affects availability of data. This makes the network unavailable. | Applying authorization, only authorized users are allowed to access specific information to perform certain operation. |
| Routing diversion | High | Only the route is diverted showing the huge traffic and the response time increased. | Ensure connectivity based approach so no route will be diverted. |
| Blocking | Extremely High | It is type of DoS, jamming, or malware attacks. It sends huge streams of data which may leads to jamming of network, similarly different types of viruses like Trojan horses, worms, and other programs can disturb the network. | Turn on the firewall, apply packet filtering, anti-jamming, active jamming, and updated antivirus programs in order to protect the network from such attacks. |
| Fabrication | Extremely High | Affects the authenticity of information. Hostile can inject false data and can destroy the authenticity of information. | Data authenticity can be applied to ensure that no information is changed during the transmission of data. |
| DoS | Extremely High | Malicious user may modify the packets or resend a packet again and again on network. User can also send bulk messages to devices in order to disturb the normal functionalities of devices. | Apply cryptographic techniques to ensure security of network. Apply authenticity to detect the malicious user and block them permanently. In this way, the network is prevented from damage. |

## REFERENCES


[1] J. S. Kumar and D. R. Patel, “A survey on internet of things: Security and privacy issues,” International Journal of Computer Applications, vol. 90, no. 11, 2014.

[2] Mirza Abdur Razzaq, “Security Issues in the Internet of Things (IoT): A Comprehensive Study,” International Journal of Advanced Computer Science and Applications, Vol. 8, No. 6, 2017

[3] Parushi Malhotra and Yashwant Singh, “ Internet of Things: Evolution, Concerns and Security Challenges”

[4] Anca D. Jurcut, Pasika Ranaweera and Lina Xu, “Introduction to IoT Security”

[5] M. Abomhara and G. M. Køien, “Security and privacy in the internet of things: Current status and open issues,” in Privacy and Security in Mobile Systems (PRISMS), International Conference on. IEEE, 2014, pp. 1–8.

[6] S. Chen, H. Xu, D. Liu, B. Hu, and H. Wang, “A vision of iot: Applications, challenges, and opportunities with china perspective,” IEEE Internet of Things journal, vol. 1, no. 4, pp. 349–359, 2014.

[7] L. Atzori, A. Iera, and G. Morabito, “The internet of things: A survey,” Comput. Netw., vol. 54, no. 15, pp. 2787–2805, Oct 2010.