International Journal of Engineering & Technology, 7 (2.19) (2018) 26-30

International Journal of Engineering & Technology

Website: www.sciencepubco.com/index.php/IJET

Research paper

Emprical Study of Iot Solution for The Security Threats In Real Life Scenario: State of The Art

C Bala Murugan[1]*, S Koteeswaran [2]

[1] Research Scholar,
Department of Computer Science and Engineering, School of Computing,
Vel Tech Rangarajan Dr. Sagunthala R&D Institute of Science and Technology,
Avadi, Chennai-62, TamilNadu, India.
and
Assistant Professor,
Department of Computer Science and Engineering,
V V College of Engineering, Tirunelveli – 627657, TamilNadu, India.
[2] Associate Professor,
Department of Computer Science and Engineering, School of Computing,
Vel Tech Rangarajan Dr. Sagunthala R&D Institute of Science and Technology,
Avadi, Chennai-62, TamilNadu, India.
**Corresponding author E-mail: balu_manoj85@yahoo.co.in*

Abstract

IoT technology and applications represents security as a significant issue for facilitating the tremendous implementation. Devoid of IoTs technology ensures the device level confidentiality, privacy and authenticity. The applicable users are not going to undertake answers for security in IoT in huge scale. The earlier stage deployments of IoT devices are primarily based on RFIDs technology which results in simplest, security solutions inside the principal been devised in an advert hoc manner [8]. This brings the fact that such deployments were typically vertically incorporated, with all additives beneath the manage of a single administrative entity. In the angle of an IoT eco-system, in which unique person may be worried in a given software state of affairs. One person owing the physical operations of sensors, one stakeholder deals with the statistics and processing them and other numerous stakeholders supplies different services based totally on such statistics to the customers. This leads to numerous variety of safety demanding situations and security for the IoT. In this paper, we address the revisited security issues and discuss the critical safety protection conditions of Internet of Things era into a mainstream. To support this, the three key problems requiring cutting-edge techniques includes are data confidentiality, privacy and trust.

In this review, we presented net factors with architectural design goals of IoT. We surveyed security and privacy issues in IoTs. Also the discussion on several open issues based on the privacy and security is addressed. Many real time applications of IoTs in real life treats the security issues of IoT as a main factor. Thus the IoT of complicated security issues have been anticipated the researchers to address.

Keywords: *of things (IoTs), Privacy, Security, eHealth monitoring systems, Data confidentiality.*

1. Introduction

IoT technologies are transitioning from monolithic boards of sensors or actuators toward modular home equipment focused many real time applications that fulfill actual-life wishes. Currently, IoT has developed into an atmosphere made from specialized hardware, network connectivity, and with open cloud numbers which are all well designed to facilitate information collection and processing. The quick development of IoT technologies might also from time to time leave users vulnerable, unaware, and in lots of cases not able to protect against privacy and security risks that twig from the usage of IoT products and frameworks [1][3].

In IoT scenarios, Data confidentiality represents a fundamental issue which indicates the guarantee that authorized entities can get admission to and modify sensed data. This is mainly relevant in the employer context, in which facts can also constitute an asset to be blanketed to shield competitiveness and market values. Inside the IoT context not only the handiest customers are used, but additionally legal objects may additionally get proper to get entry to the information. This requires addressing vital additives: first, the definition of an get entry to manipulate mechanism and the second is the device identification and authentication system.

As many applications are IoT based real time applications, ensuring the data confidentiality are more important factor of data security. For instance, consider the data sensed by the biosensors for the bacterial composition of the product used for guaranteeing the desired exceptional in the food enterprise. This information is actually confidential in business point of view which brings violent advantage over competing organizations. As an example, consider the environmental monitoring applications which act as an earlier warning system to indicate the rise of earthquake and tsunamis and so on. These situations are treated very secretly under the civil protection department .The leakage of such information brings a panic situations among the people groups.

Copyright © 2018 C Bala Murugan, S Koteeswaran . This is an open access article distributed under the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

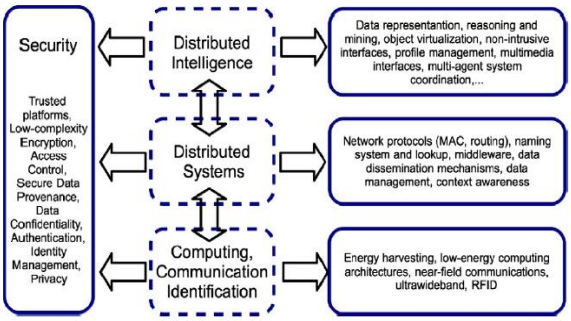
The regular solution of ensuring the data confidentiality under the IoT environment is not a proper solution [4]. Hence secure access control mechanism and device identifier is needed to properly chosen for ensuring the security in many knowledge based information systems. The best example is Role-Based Access Control (RBAC), an standard approach which ensures confidentiality in the IoT environments.

2. Background Study

Security implications of IoT and its programs have already become hurdles for its wider adoption. on the one hand, as the scale of the IoT marketplace grows, so does its attack floor due to the fact new interconnected gadgets are delivered to the chain; each of that may turn out to be the brand new weakest link for an adversary to exploit. furthermore, the extended call for and adoption might also make it tough for the industry to evaluate vital elements of IoT safety and privacy. as an example, new, IoT specific protocols are being designed constantly but they'll no longer were very well examined to prove their trustworthiness[5]. Finally, IoT has come to be an umbrella term for many specific applications and industry use cases every having its personal security requirements but counting on the same essential IoT technology. Designing security that encompasses and applies to all the use instances may be a frightening challenge, and requirements and exceptional practices committees are nevertheless figuring out the way to cope with this task.

Security implications on the IoT and its hurdles are explained by many researchers. Alternatively, the growth in the IoT market brings the issues about the data confidentiality since all the IoT devices are connected in chain. Moreover, the increased demand and adoption may make it hard for the industry to assess critical aspects of IoT security and privacy. For example, the emerge of various new IoT protocols are being designed constantly, but they will no longer were very well examined to prove their trustworthiness. Finally, IoT has come to be an umbrella term for many specific applications and industry use cases every having its personal security requirements but counting on the same essential IoT technology[6][7].

Many use cases are available to learn about the potential pitfalls of IoT applications and components as applied to the excellent use cases. Our primary intention is to raise consciousness regarding deficiencies in current practices and absence of standards relating IoT safety and privacy and their viable implications to the public and large adoption. To give up the same, an excellent use case related to the health care namely e-healthcare is discussed under this section. The implementation methodologies of the IoT application type are always simple and achieve a desired functionality using commercial off-the-self components. But the difficulty arises in the place of easy to abuse, security and privacy threats that exist in simple IoT use cases. The causes for the IoT threats are due to the following factors including the emanation of records relative to consumer vicinity, the leakage of sensitive information and the remote exploitation of device functionality by unauthorized users. Figure 1 shows the nomenclature of the research areas relevant to Internet-of-Things.



. **Fig 1**. Nomenclature of research focus relevant to Internet-of-Things.

3. Security Concerns in Internet of Things

Internet of Things genuinely is a system of real world applications with real time interactions. Machine to Machine (M2M) communications is the improvement in the initial level of IoT which is having unique traits with the deployment contexts and contribution [9]. The best networking is the Wireless Area Network (WAN) which works without human intervention [12][13]. The varieties of threats within the security of IoT are shown in the figure 2.

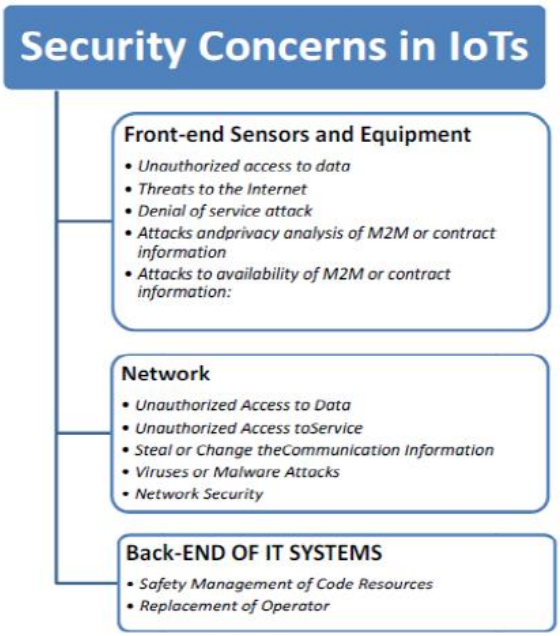


Fig 2. Security Threats in IoT

The front-end sensors and device gets records through the included sensors. Then they transmit the information using gadget to machine devices, for that reason achieving networking offerings of a couple of sensors. This technique involves the safety of machines with commercial organization implementation and node connectivity. Most devices are extra frequently dispensed within the absence of tracking situations. An outsider can effects get admission to those gadgets which propose damage or unlawful movements on the ones nodes may be done. Viable threats are analyzed and are labeled to unauthorized get entry to to information, threats to the internet and Denial of Service (DoS) attack. Wireless Sensor Network (WSN) plays an crucial role supplying a more complete interconnection capability, effectualness and thriftiness of connection, as well as true notable of company in IoTs. When you consider that a big range of machines sending data brings network congestion, large range of nodes and organizations exist in lots can be resulted in denial of provider assaults. IoT systems paperwork a gateway, middleware, which has excessive protection necessities, and amassing, examining sensor infor-

mation in real time or pseudo real-time to boom commercial corporation intelligence. The security of iot systems has seven essential requirements such as data privacy safety, getting access to manipulate, user authentication, communication layer protection, data integrity and data confidentiality and data availability at any time.

4. Internet of Things –Privacy Conceren

IoT privacy refers to the right of an entity, performing in its private behalf to determine the degree to which it's going to engage with its surroundings, collectively with the diploma to which the entity is inclined to share data approximately itself with others. Commonly in IoTs, the surroundings is sensed via way of linked gadgets. They then broadcast the accrued facts and particular occasions to the server which includes out the software program not unusual sense. Privateness ought to be protected within the tool, in garage at some point of communication and at processing which permits to disclose the touchy facts .The privateness of users and their data protection were recognized as one of the important challenges which need to be addressed inside the IoTs. Under IoT applications the privacy is mainly focused on four levels such as privacy in device level, privacy during communication level, privacy in storage and privacy at processing. The details explanation of these four levels is shown below coming sections.

4.1. Privacy in Device

The confidential data are leaked through the unauthorized manipulation or through the maintenance of hardware and software in IoT devices. For example, by means of reprogramming in the a surveillance digital camera, the data captured is not send to the valid users and it also sends to the intruder. Hence, here plays a vital role of maintaining the privacy of the device for accumulating the sensitive information robustness and tampering the resistance. This pays the path for lot of privacy issues and it is needed to protect the private records in case of misuse of device.

4.2. Privacy in Communication

To guarantee information confidentiality at some point of the transmission of the data, the maximum not unusual method is encryption. Encryption on positive activities provides statistics to packets which provides a manner for tracing like security parameter index, and many others.

4.3. Privacy in Storage

Defensive privacy of information garage, following principal should be taken into consideration.

• Handiest the least possible quantity of records needed to be stored.
• Only on obligatory case the best private facts are retained.
• The information is delivered out on the premise of whenever want-to-recognize.

4.4 Privacy at Processing

During the processing stage, the privacy on the public information is paid more attention. First of all, non-public information needed to be treated in a way that it should be considered with the supposed motive. Next, without any specific recognition and the information of the statistics proprietor, their non-public facts ought to not be disclosed to the third party. The privacy during the processing is handled with the data annotation schema which is shown in figure 3.

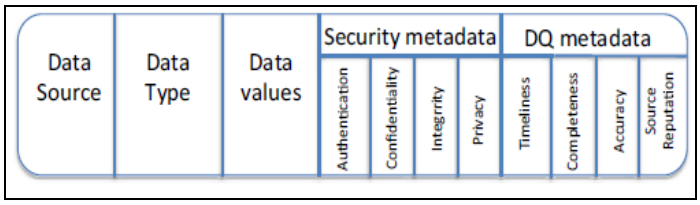


Fig3 Data Annotation Schema

5. Security and Privacy Requirements of Real Life Scenarios

In this section, the real time scenario like eHealth tracking systems is considered for discussing the essential safety and privacy necessities for such systems. The terms data y security and data privacy plays a vital role. The term data security refers the process of securely storing and communicating data to other entities. On other hand data privacy means the data is accessing of data by the authorized persons. In such a way the eHealth monitoring systems is developed with the ultimate goal of users investing in healthcare domain. In building healthcare systems, security and privacy requirements are maintained under four different level as shown in Figure 4.

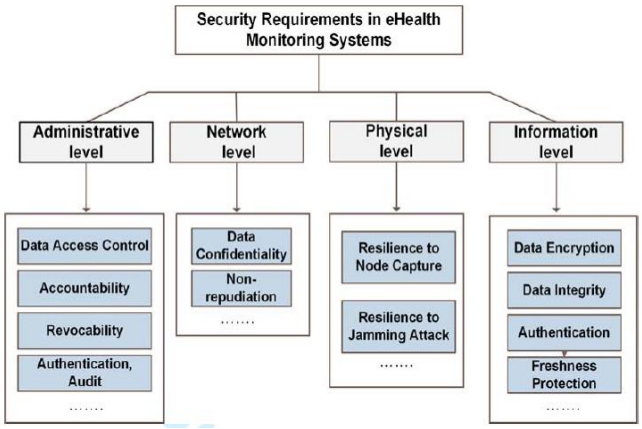


Fig 4.: IoT Security requirements in eHealth Monitoring systems

5.1 Administrative level security

Under the Administrative level security, the protocol for the access control is well defined for the secure access of patients' health data[10]. Data access control is aiming at preventing the illegal access to the patients' personnel data .since the patient's health record are admittance by the multiple persons such as doctors, senior nurses, lab analysts and so on leads to a risk of misusing the personal information which is more sensitive. Doctors and nurses may have exceptional get right of entry to privileges to the affected person's health record in line with their duties, while insurance groups might be allowed to get right of entry to most effective the facts associated with the reimbursements of scientific bills. Furthermore, numerous access authorization ranges ought to be granted to the records related totally on their position in regards to the treatment of the patient that is the physician chargeable for the affected person's health repute may have complete get admission to patient health information, even as different doctors may additionally have restricted and provide access privileges depending at the background and occasions. Every other aspect duty is applied in ehealth monitoring structures [11] goals to achieve greater efficient usage of the affected character's health facts by the use of the legitimate customers, and save you any capacity misuse that may threaten the affected individual privateness. Revocability includes shielding for a given system from compromised entities and clients. Therefore at administrative level safety must consist of sturdy authentication measures and normal audit of all concerned administration entities. This can honestly save from eavesdropping threats which is probably the various principal

motives which could cause the failure of eHealthcare tracking systems.

5.2 Network level of security

The network level of security plays a main role in make suring the safety of the entire eHealth tracking device as it offers secure transmission of the records from the sensing gadgets in the direction of the faraway data servers and from the ones latter to the cease individual in conjunction with clinicians. Safety in network level encompasses also securing the network devices in opposition to tampering attacks. The information privateness which leads to the disclosure of personal health information to unwanted users. The components of the eHealth monitoring systems transmit very sensitive records about the patients who normally do now not get hold of sharing it with others, because it famous shows their fitness conditions which include diabetic, drug-addicted, early diploma of pregnancy and many others. To defend the clients privateness, all communications in healthcare systems have to be encrypted. Information encryption in traditional sensors is commonly completed with the beneficial useful resource of encrypting the data before sending it, using a mystery key shared on a at ease communication channel hooked up the numerous speaking entities. in case of inter device communications, the extra appropriate manner for encryption is the use of flow cipher algorithms, on account that in such algorithms the size of cipher text is exactly much like plaintext, and no extra facts desires to be transmitted.

5.3 Physical level security

The safety efforts at sensor stage are devoted to the safety of eHealth monitoring device from threats targeted at the physical sensor devices, with the intention to ensure the accuracy and trustworthiness of the records they generate. Because of this, threats like sensor node seize and jamming assaults need to be effectively mitigated. The two essential forms of bodily sensors may be excellent in eHealth monitoring structures, specially, sensors placed at the patients frame, and the IoT sensors deployed in health center premises or embedded in some structures which encompass the health facility clever beds. The former sensors are chargeable for measuring the affected person's vital symptoms, while the latter measures the environmental situations. Without strong bodily degree safety mechanisms, attackers can without issues seize a specific sensor node, retrieve its cryptographic keys and protocol statistics, and finally clone it with the intention to redeploy more than one malicious sensor within the network. Such sensors can be placed into the ehealth monitoring tool, main to devastating impact at the entire device.

6. Security Threats in Ehealth Monitoring Systems

In eHealth care tracking gadgets, there are various capability safety threats that may notably degrade the overall system normal overall performance and its trustworthiness level. The disclosure threats can be launched thru any malware or document sharing gadget and even by means of intentional or unintentional password sharing. It's far a long way extensively recognized that the eHealth tracking tool is susceptible to numerous different threats in particular because of the inherited vulnerabilities from wi-fi networks. Actually, the wi-fi channel, used as important verbal exchange assist, is susceptible to several varieties of safety attacks starting from eavesdropping, data change and injection to jamming and Denial of Service (DoS) assaults. The tiny sensors used inside the eHealth monitoring system are much less tamper resistant in comparison to first rate wi-fi devices and they could outcomes without problems be compromised. Despite the fact that records saved in sensor node further to on the community server is encrypted collectively with its encryption key, compromising the tool will absolutely purpose the disclosure of the facts. The ehealth tracking systems are particularly dynamic in nature because of their scalability from WBANs to the cell crowd sensing [2]. Due to the accidental failure or malicious activities, nodes can depart and be part of the community regularly. Furthermore, some nodes may also additionally deleted because of the exhaustion of their battery strength, therefore an attacker can launch assaults via the usage of masquerading real main nodes.

Due to the truth eHealth care packages contain no longer simplest scientific but additionally personal data; safety and privateness upkeep of such facts are main problems in this context. Some key measures which could protect the facts from numerous threats consists of

- Information encryption: suitable slight-weight statistics encryption techniques can save statistics from the disclosure within the transit.
- Data integrity: every other serious factor of the safety is the right integrity test of the exchanged information to prevent any exchange of its content material cloth whilst in transit.
- Data authentication: suitable authentication schemes also could make information more comfortable. It's far an efficient degree to keep away from impersonation assaults.
- Data protection: This protection company prevents an attacker from replaying outdated data.

6. Conclusion

The IoT technology attracts huge modifications in each person's normal lifestyles. Inside the IoTs technology, the quick-range mobile transceivers may be implanted in kind of every day requirements. The connections amongst human beings and communications of humans will expand and amongst objects to objects at on every occasion, in any place. The performance of data control and communications will rise as much as a brand new excessive degree. The dynamic surroundings of IoTs introduce unseen opportunities for verbal exchange, which might be going to change the perception of computing and networking. The privateness and safety implications of such an evolution should be cautiously considered to the promising technology. The safety of statistics and privacy of customers has been recognized as one of the key traumatic situations within the IoT.

References

[1] K. Zhao and L. Ge. "A Survey on the Internet of Things Security," *Proc. 9th Int'l Conf. Computational Intelligence and Security* (CIS), 2013,pp. 663–667.

[2] Q. Jing et al., "Security of the Internet of Things: Perspectives and Challenges," Wireless Networks, vol. 20, no. 8, 2014, pp. 2481–2501.

[3] H. Feng and W. Fu, "Study of Recent Development about Privacy and Security of the Internet of Things," Proc. Int'l Conf. Web Information Systems and Mining (WISM), 2010, pp. 91–95.

[4] D. Puthal et al., "A Dynamic Prime Number Based Efficient Security Mechanism for Big Sensing Data Streams," to be published in Computer and System Sciences, 2016; http://dx.doi.org/10.1016/j.jcss.2016.02.005.

[5] J. Gubbi et al., "Internet of Things (IoT): A Vision, Architectural Elements, and Future Directions," Future Generation Computer Systems, vol. 29, no. 7, 2013, pp. 1645–1660.

[6] L. Atzori, A. Iera, and G. Morabito, "The Internet of Things: A Survey," Computer Networks,vol. 54, no. 15, 2010, pp. 2787–2805.

[7] Hewlett Packard (HP), Internet of Things Research Study. 2015. DOI: http://www8.hp.com/h20195/V2/GetPDF. aspx/4AA5-4759ENW.pdf

[8] Jung T. K. 2013. Analyses of Integrated Security Framework with Embedded RFID System for Wireless Network Architecture. Journal of Convergence Information Technology Vol 8. No. 14 2013.

[9] S. K. Datta, C. Bonnet, and N. Nikaein, "An IoT gateway centric architecture to provide novel m2m services," in Proceedings of the World Forum on Internet of Things (WF-IoT). IEEE, 2014, pp. 514–519.

[10] D. Lake, R. Milito, M. Morrow, and R. Vargheese, “Internet of Things: Architectural framework for ehealth security,” Journal of ICT Standardization, River Publishing, vol. 1, 2014.
[11] H. Abie and I. Balasingham, “Risk-based adaptive security for smart IoT in eHealth,” in Proceedings of the 7th International Conference on Body Area Networks. ICST, 2012, pp. 269–275.
[12] Perrig, J. Stankovic, and D. Wagner, “Security in wireless sensor networks,” Communications of the ACM, vol. 47, no. 6, pp. 53–57, 2004.
[13] S. Sastry, S. Sulthana, and S. Vagdevi, “Security threats in wireless sensor networks in each layer,” Int. J. Advanced Networking and Applications, vol. 4, no. 04, pp. 1657–1661, 2013.