iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 5 **Issue:** VI **Month of publication:** June 2017

DOI:

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)

A Survey on Data Privacy and Security in Internet of Things

Sheeba P[1]
[1]Assistant Professor, Department of Computer Science and Engineering, New Horizon College of Engineering

Abstract*: The Internet of Things (IoT) is the use of intelligently connected devices and systems to use and manage data collected by embedded sensors and actuators in devices. The internet of things allows devices to be controlled remotely across existing network. According to the Gartner, by year 2020, 260 million objects will be connected and monitored. As the Internet of Things evolves, the proliferation of good connected devices supported by mobile networks, providing pervasive and seamless connection, can unlock opportunities to provide life-enhancing services for customers as well as boosting productivity for enterprises. For consumers, property provided by the IoT may enhance their quality of life in multiple ways. Within the home, the combination of connected sensible devices and cloud-based services can facilitate address the difficulty of energy efficiency and security. IoT security is the area dealing with protecting connected devices and networks in the Internet of things. A recent study regarding the foremost widespread devices in some of the foremost common IoT niches reveals alarmingly high average variety of vulnerabilities per device. On average, twenty five vulnerabilities were found per device. Multiple attacks have already been reported within the past against totally different embedded devices and that we will expect several a lot of within the IoT domain. This paper, is a survey on internet of things, security vulnerabilities and solutions.

Keywords*: IoT, Data privacy, Security, Embedded,

I. INTRODUCTION

The Internet of Things may be a novel paradigm shift in IT. It's a network of networks that consists of several non-public, public, academic, business, and government networks, of native to world scope, that square measure coupled by a broad array of electronic, wireless and optical networking technologies . Internet of Things is maturing and continues to be the latest, most hyped concept in the IT world[1]. Over the last decade the term Internet of Things (IoT) has attracted attention by projecting the vision of a global infrastructure of networked physical objects, enabling anytime, anyplace connectivity for anything and not only for any one [2].

The Internet of Things can also be considered as a global network which allows the communication between human-to-human, human-to-things and things-to-things, which is anything in the world by providing unique identity to each and every object [3]. IoT describes a world where just about anything can be connected and communicates in an intelligent fashion that ever before. Most of us think about “being connected” in terms of electronic devices such as servers, computers, tablets, telephones and smart phones. In what’s called the Internet of Things, sensors and actuators embedded in physical objects from roadways to pacemakers are linked through wired and wireless networks, often using the same Internet IP that connects the Internet. These networks produce huge volumes of data that flow to computers for analysis. When objects can both sense the environment and communicate, they become tools for understanding complexity and responding to it swiftly. What’s revolutionary in all this is that these physical information systems are now beginning to be deployed, and some of them even work largely without human intervention.

The IoT's anyplace, anything, anytime nature might simply modification these benefits into disadvantages, if privacy aspects wouldn't be provided enough. As an example, if anybody will have access to any personal services and knowledge, or if the knowledge of a many individuals is reached by the surroundings automatically, the IoT wouldn't have a reliable setting. There is not any adequate backbone to outline management and knowledge policies for interaction among completely different users and devices. Also, solutions for various security needs have direct impact on the value and time to promote [4]. Moreover, each resolution has its own business needs which can or might not be as strict.

However, while on one side, IoT will make many novel applications attainable, on the opposite aspect IoT will increase the risk of cyber security attacks. In addition, as a result of its fine-grained, continuous and pervasive knowledge acquisition and control capabilities, IoT raises considerations regarding privacy and safety.

II. SECURITY AND DATA PRIVACY CHALLENGES IN IOT

The 3 core problems with the IoT are

Privacy for humans
Confidentiality of business processes
Third-party dependabilityWithin the IoT setting, there are four interconnected and interacting elements (people, devices, software and hardware) that communicate over public, untrusty networks. These are sure to be confronted with security, privacy and open trust issues. Therefore, queries relating to users, servers and trusty third parties must be addressed. The different types of threats that target IoT are discussed below:

A. Attacks in IoT

1) *Denial-of-service attacks (DoS):* In this kind of attack, an attempt is made to make a machine or network resource unavailable to its users. Due to lesser memory capabilities and limited computation resources, the majority of devices in IoT are susceptible to these attacks. The majority of defense mechanisms require high computational overhead, and are subsequently not suitable for resource- constrained IoT. DoS attacks in IoT can sometimes prove very costly, hence researchers have made an arrangement to identify different types of such attacks, as well as developed strategies to secure against them. DoS attacks that can be launched against the IoT are jamming channels, consumption of computational resources like bandwidth, memory, disk space, or processor time, and disruption of configuration information (such as node information)[5].
2) *Physical attacks:* This attack damages the hardware components of IoT devices. Due to the unattended and dispersed nature of IoT, most devices typically operate in external environments, which are highly susceptible to physical attacks
3) *Attacks on privacy*: Since IoT makes large volumes of information easily available through remote access mechanisms, privacy protection in IoT is become increasingly challenging. The attacker need not be physically present to monitor, but information gathering can be easily done anonymously with very low risk. The most common attacks on user privacy are as follows:

a) Eavesdropping and passive monitoring: In this attack, if messages are not protected by encryption, an attacker could easily understand the content
b) Traffic analysis: Through effective traffic analysis, an attacker can easily identify certain information with special methods and activities in IoT devices
c) Data mining: This enables attackers to query information that is not expected in certain databases[6].

B. Security and Privacy Challenges in the IoTs

The Internet of Things is a multi-domain environment with a large number of devices and services connected together to exchange information. Each domain can apply its own security, privacy, and trust requirements. In order to establish more secure and readily available IoT devices and services at low cost, there are many security and privacy challenges to overcome. Among those challenges are:

1) User privacy and data protection: Privacy is a vital issue in IoT security on account of the worldwide character of the IoT atmosphere[7]. Things are connected, and information is communicated and changed over the net, rendering user privacy a sensitive subject in several analysis works. Though a plenty of analysis has already been planned with regard to privacy, several topics still would like more investigation. The research gaps in IoT security includes privacy in information assortment, also as information sharing and management, and knowledge security matters.

2) Authentication and identity management: Authentication and identity management are a combination of processes and technologies geared toward managing and securing access to data and resources[8]. Identity management unambiguously identifies objects, and authentication entails substantiate the identity institution between 2 human action parties. It is essential to contemplate a way to manage identity authentication within the IoT, as multiple users and devices got to demonstrate one another through trustable services.

3) Trust management and policy integration: in IoT, Trust plays an important role in establishing secure communication between things. Two dimensions of trust should be considered in IoT: trust in the interactions between entities, and trust in the system from the user's perspective. In order to gain user trust, there should be an effective mechanism of defining trust in a dynamic and collaborative IoT environment. The main objectives of trust research in the IoT framework are the following: first, the conception of new models for decentralized trust; second, the implementation of trust mechanisms for cloud computing; third, the development of applications based on node trust (e.g., routing, data aggregation, etc.). Trust evaluation must be automated and preferably

autonomous[9].

4) Authorization and access control: Authorization enables determining if the person or object, once identified, is permit- ted to have the resource. Access control means controlling access to resources by granting or denying according to a wide range of criteria. Authorization is typically implemented through the use of access controls. Authorization and access control are important in establishing a secure connection between a number of devices and services. The main issue to be addressed in this scenario is making access control rules easier to create, understand and manipulate.

5) End-to-End security: Security at the endpoints between IoT devices and Internet hosts is likewise important. Applying cryptographic schemes for encryption and authentication codes to packets is not sufficient for resource-constrained IoT. For complete end-to-end security, the verification of individual identity on both ends, protocols for dynamically negotiating session keys (such as TLS and IPsec)[10], and algorithms (for example AES and Hash algorithms) must be secure[11].

C. Security requirement for IoTs

IoT has become one of the most significant elements of the future Internet with a huge impact on social life and business environments. A larger number of IoT applications and services are increasingly vulnerable to attacks and information theft. To secure IoT against such attacks, advanced technology is required in several areas. More specifically, authentication, confidentiality, and data integrity are the key problems related to IoT security. Authentication is necessary for making a connection between two devices and the exchange of some public and private keys through the node to prevent data theft. Confidentiality ensures that the data inside an IoT device is hidden from unauthorized entities[12]. Data integrity prevents any man-in-the- middle modification to data by ensuring that the data arriving at the receiver node is in unaltered form and remains as transmitted by the sender. Table 1 shows a number of security components influencing IoT security functionality.

Vermesan and Friess [14] discussed security and privacy framework requirements in dealing with IoT security challenges, as follows:

1) Lightweight and symmetric solutions to support resource- constrained devices.
2) Lightweight key management systems to enable the establishment of trust relationships and distribution of encryption materials using minimum communication and processing resources, consistent with the resource- constrained nature of many IoT devices.
3) Cryptographic techniques that enable protected data to be stored processed and shared, without the information content being accessible to other parties.
4) Techniques to support (”Privacy by Design”) concepts, including data identification, authentication and anonymity.
5) Keeping information as local as possible using decentralized computing and key management.
6) Prevention of location privacy and personal information inference that individuals may wish to keep private by observing IoT-related exchanges.

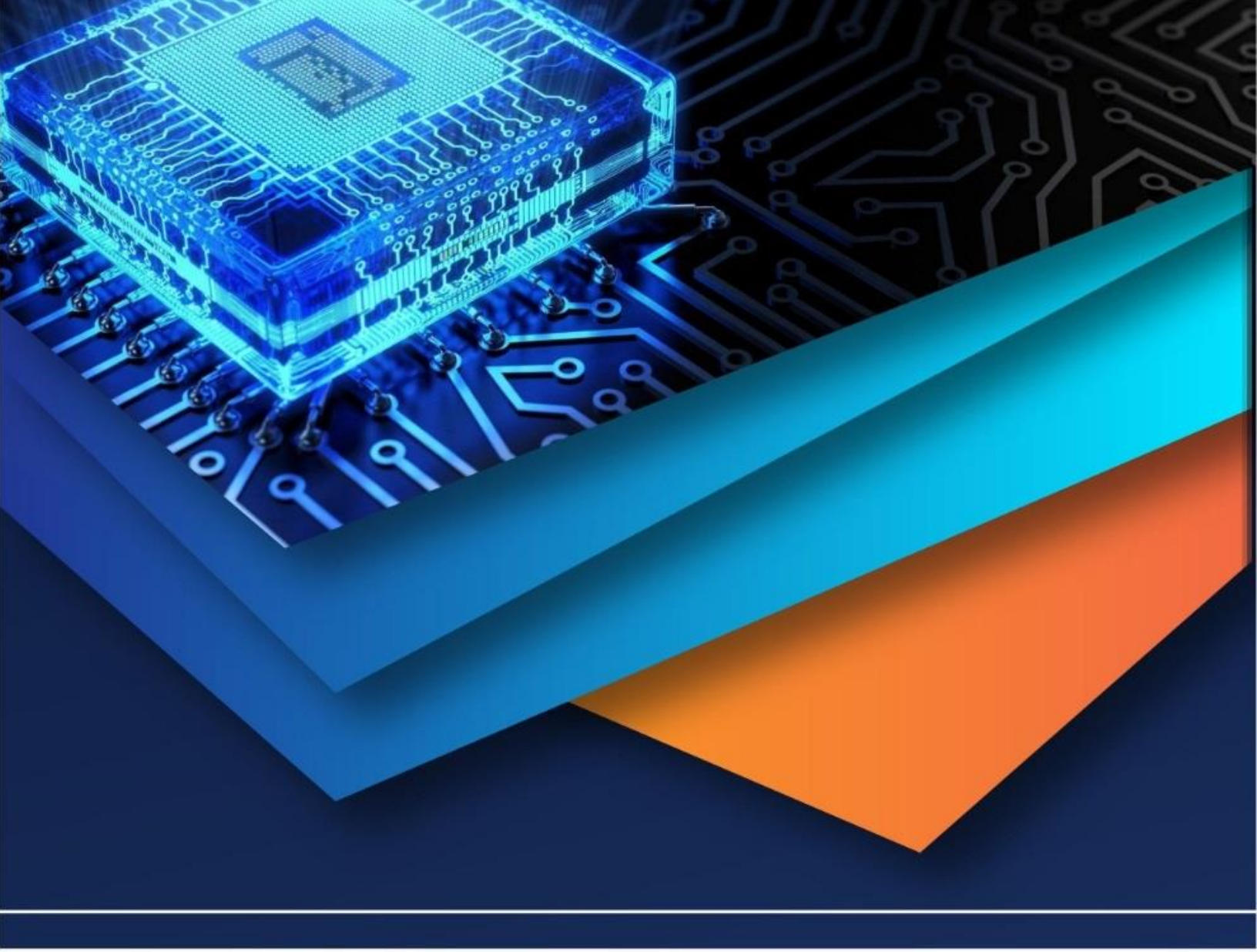
III.CONCLUSIONS

The main aim of this paper was to provide an explicit survey of the most important aspects of IoT with particular focus on the vision and security challenges involved in the Internet of Things. The vision of IoT will allow people and things to be connected anytime, anywhere, with anything and anyone, ideally using any path/network and any services. While Radio Frequency Identification techniques (RFID) and related technologies make the concept of IoT feasible, there are several possible application areas for smart objects. The major IoT targets include creating smart environments and self- configurable/autonomous devices[15]. Several difficulties and challenges related to IoT are still being faced. Challenges like assuring interoperability, attaining a business model in which hundreds of millions of objects can be connected to a network, and security and privacy challenges, such as authentication and authorization of entities are introduced. In the next few years, addressing these challenges will constantly be the focus and primary task of networking and communication research in both industries and academics.

REFERENCES

[1] J. Gubbi, R. Buyya, S. Marusic, and M. Palaniswami, “Internet of things (iot): A vision, architectural elements, and future directions,” Future Generation Computer Systems, 2013.
[2] L. Atzori, A. Iera, and G. Morabito, “The internet of things: A survey,” Comput. Netw., vol. 54, no. 15, pp. 2787–2805, Oct. 2010. [Online]. Available: http://dx.doi.org/10.1016/j.comnet.2010.05.010
[3] D. Bandyopadhyay and J. Sen, “Internet of things: Applications and challenges in technology and standardization,” Wireless Personal Com- munications, vol. 58, no. 1, pp. 49–69, 2011.

[4] D. Miorandi, S. Sicari, F. De Pellegrini, and I. Chlamtac, “Internet of things: Vision, applications and research challenges,” Ad Hoc Networks, vol. 10, no. 7, pp. 1497–1516, 201
[5] O. Vermesan and P. Friess, Internet of Things: Converging Technologies for Smart Environments and Integrated Ecosystems. River Publishers, 2013
[6] O. Mazhelis, H. Warma, S. Leminen, P. Ahokangas, P. Pussinen, M. Rajahonka, R. Siuruainen, H. Okkonen, A. Shveykovskiy, and J. Myllykoski, “Internet-of-things market, value networks, and business models : State of the art report,” 2013.
[7] M. Covington and R. Carskadden, “Threat implications of the internet of things,” in Cyber Conflict (CyCon), 2013 5th International Conference on, 2013, pp. 1–12.
[8] R. Roman, P. Najera, and J. Lopez, “Securing the internet of things,”Computer, vol. 44, no. 9, pp. 51–58, 2011.
[9] H. Suo, J. Wan, C. Zou, and J. Liu, “Security in the tnternet of things: A review,” in Computer Science and Electronics Engineering (ICCSEE), 2012 International Conference on, vol. 3. IEEE, 2012, pp. 648–651
[10] G. Yang, J. Xu, W. Chen, Z.-H. Qi, and H.-Y. Wang, “Security characteristic and technology in the internet of things,” Nanjing Youdian Daxue Xuebao(Ziran Kexue Ban)/ Journal of Nanjing University of Posts and Telecommunications(Natural Nanjing University of Posts and Telecommunications(Natural, vol. 30, no. 4, 2010
[11] A. de Saint-Exupery, “Internet of things, strategic research roadmap,”2009.
[12] C. Yuqiang, G. Jianlan, and H. Xuanzi, “The research of internet of things’ supporting technologies which face the logistics industry,” in Computational Intelligence and Security (CIS), 2010 International Conference on, 2010, pp. 659–663.
[13] S. William and W. Stallings, Cryptography and Network Securiton Education India, 2006
[14] M. Watkins and K. Wallace, “Ccna security official exam certification guide (exam 640-553),” 2008.
[15] D. Dolev and A. C. Yao, “On the security of public key protocols,”Information Theory, IEEE Transactions on, vol. 29, no. 2, pp. 198–208,1983.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY