International Journal of Research in Economics and Social Sciences(IJRESS)
Available online at: http://euroasiapub.org
Vol. 9 Issue 5, May- 2019
ISSN(o): 2249-7382 | Impact Factor: 6.939 |

Efficiency Analysis of IoT gateways using the Transport Layer Security (TLS) framework and its security issues

MudholkarPankaj Keshavrao[1], Dr. Sudhir Dawra[2]
Department of Computer Science
[1, 2]Himalayan University, Itanagar, Arunachal Pradesh

Abstract-The Internet of Things (IoT) has emerged as one of the Technologies which have attracted the attention of researchers Industry and academia. The Internet of Things idea is Internet interconnection allowed things or devices to be connected to each to reach some common goals, to others and to humans. Nearby futureIoTs will be incorporated seamlessly into our Environment and humanity will depend entirely on that comfort technology, and a comfortable lifestyle. Any safeguards compromise in the system will affect human life directly. Security and privacy of this technology are therefore paramount important problem to solve.

We present a thorough piece in this paper studyingIoT security problems and classifying potential cyber-attacks on any layer of IoT architecture. We do have discussions Challenges to traditional solutions such as cryptographic security Solutions, authentication and key management mechanisms in IoT. A significant area is system authentication and access control OfIoT protection, which has not yet been surveyed. We spent our efforts to bring the state of the art device authentication and access control techniques on a single paper.

Introduction

Security and privacy remains a hot research subject in IoT. In the last few years, it's attracted a lot of interest in research. The IoT network is composed of low-performance resource-constrained and low-power artefacts. Resource limitations are considered in terms of battery capacity, computational power, and memory footprint and bandwidth utilization. Devising new methods and modifying the security protocols available would also be difficult. This is due to the need to maintain a balance between the robustness of the security protocols and limited resource limitations of the IoT system and their access to the legacy Internet. In this study, effective and important lightweight security and privacy solutions regarding authentication, key establishment, and protection of source locations. Such solutions address some of the security challenges confronting IoT. Security analysis and performance assessment show that the suggested approaches have a high level of protection and are sufficient for resource-constrained IoT existence. This study presents a number of significant contributions aimed at resolving IoT security and privacy in the following we present research contributions and possible direction. [1]

1. Transport Layer Security (TLS)-a security protocol for the e-commerce network

The Internet Engineering Task Force (IETF) has developed the Transport Layer Security protocol (TLS) as the standard protocol for the provision of e-commerce security services over the Internet. Global Internet-based e-commerce over TCP / IP requires confidentiality, anonymity, authentication, and non-repudiation protection attributes within the TCP / IP protocol system to be present. Despite the fact that the TCP / IP protocol architecture was undertaken under the auspices of the US Defense Department, the TCP / IP protocols contain major security flaws and are susceptible to many security threats that make the protocols unsafe for Ecommerce applications. The Internet Engineering Task Force (IETF) proposed a long-term solution in the form of the IPSec initiative to the security problems in the TCP / IP protocols around 1995. IPSec is a family of protocols that provide the required security attributes for implementing network layer IPs. Since IPSec is located adjacent to the IP layer, it can provide end-to - end protection and can be used to address a variety of security needs, including secure e-commerce, Virtual Private Networks, access control, private communication between two hosts and many other security needs. However, due to the time delay associated with introducing a robust security protocol such as IPSec, and the related policy of making strong cryptography accessible universally, it was felt that the security protocol for e-commerce would need to be developed separately. Netscape Communications therefore established the Safe Sockets Layer (SSL) protocol, and implemented its support in its browsers. The SSL concept was made public by Netscape too. [2]

2. Things-IOT Internet: Apps, Infrastructure, Supporting Technology, Application & Future Challenges

The Internet of Things refers to a type of network for connecting something to the Internet based on stipulated protocols via information sensing equipment for sharing and communicating information in order to achieve smart identification, locating, tracking, monitoring and management. In this paper we explored briefly what IOT is, how IOT supports various technologies, its design, functionality & implementations, practical view of IOT and what the potential challenges for IOT are. The IOT definition was invented by a member of the technology group Radio Frequency Identification (RFID) in 1999 and has recently become more applicable to the practical world , primarily due to the growth of mobile devices, embedded and omnipresent connectivity, cloud computing , and data analysis. Imagine a world where billions of objects can sense, interact, and exchange information, all in all. All integrated structures have data collected, evaluated and used to facilitate action on a daily basis, providing planning, management and decision-making with a wealth of information. This is the Internet of

Things (IOT) culture. Common concept of the Internet of Things is known as: Internet of Things (IOT) is a network of physical objects. The internet is not only a computer network, but it has developed into a network of devices of all types and sizes, cars, smartphones, home appliances , toys, cameras, medical devices and industrial systems, animals, men, houses, all connected, all communicating and exchanging information on the basis of protocols to achieve smart reorganizations, positioning, tracking, protection.[3]

3. Future Advances to Iot.

Developing enabling technologies such as semiconductor electronics, connectivity, sensors, smart phones, embedded systems, cloud networking, virtualization of networks, and software would be important to allow physical devices to function in evolving environments and to be linked all the time. Although IOT is architect rated into layers, the technologies were divided into three classes. The first development community will affect the computers, the microprocessor chips:

• Low-powered energy and recycling sensors • Sensor Experience in field

• Cpu miniaturisation

• Wireless network of sensors to link to the sensor

Table 4.1 The table below shows future development & research needs to allow IOT technologies

The second category includes technologies that facilitate network sharing and resolve power and latency problems:

• Network networking technologies, such as radios and cognitive networks identified by software.

• Network technology which addresses capacity and latency issues like LTE-A The third category has an impact on the management services that support IOT apps:

• Intelligent technologies for decision taking, such as context-conscious computing systems, predictive analytics, complex event analysis and behavioural analytics.

• Data processing technology speed, for example in memory and streaming analysis.

TECHNOLOGY	FUTURE DEVELOPMENT	RESEARCH NEEDS
Communication Technology	•On chip antennas •Wide spectrum and spectrum aware protocols •Unified protocol over wide Spectrum •Multi-functional reconfigurable chips	•Protocols for interoperability•Multi-protocol chips •Gateway convergence •On chip networks •Longer range (higher frequencies – tenths of GHz)
Network Technology	•Self-aware and self-organizing networks •Self-learning, self-repairing networks •IPv6- enabled scalability •Ubiquitous IPv6-based IoT deployment	•Grid/Cloud network •Software defined networks •Service based network •Need based network
Security & Privacy Technologies	•User centric context-aware privacy and privacy policies •Privacy aware data processing •Security and privacy profiles selection based on security and privacy need	•Low cost, secure and high performance identification/ authentication devices •Decentralized approaches to privacy by information localization

4. BIG DATA CHALLENGES TO SECURITY INFORMATION AND PRIVACY

With the proliferation of devices connected to the Internet and linked to each other, the amount of data collected, stored and processed is that on a daily basis, which also poses new problems in terms of privacy and protection. Furthermore, widely used defense mechanisms, such as firewalls and DMZs, cannot be used in the Big Data infrastructure as security measures should be applied from the periphery of the organization's network to satisfy the user / data usability requirements and the BYOD (Bring Your Own Device) policy.

In light of these emerging circumstances, the key question is what security and privacy policies and approaches are more suitable to resolve the existing top-level challenges to big data safety and privacy (Cloud Security Alliance 2013). These concerns can be grouped into four aspects of Big Data such as network safety (e.g. secure distributed computations using MapReduce), security (e.g. data mining that protects confidentiality / granular access), data management (e.g. safe data provenance and storage), and transparency and reactive safety (e.g. real-time identification of anomalies and attacks). When analysing Big Data there are a number of areas of risk to consider. These include the information lifecycle (provenance, ownership and classification of data), the method of producing and storing data, and the lack of security procedures. In essence, Big Data protection objectives are no different from any other form of data-protecting its confidentiality, integrity and availability**.** [6]

5. Rapid development IoT Design

IoT Technology Trend theIoT is heading off into a new era. In the digital transformation of all industries the IoT plays a significant role. Technological advancement produces huge amounts of connections, significantly increases productivity and makes life more comfortable for people. The IoT business is already booming. Across all sectors the IoT powers digital transformation. Companies, governments, organisations, and societies around the world are working to study and invest in IoT and to gather, analyze , and apply the data generated by it. That will promote the rapid growth of all industries. The IoT, just as the Internet already has, will become part of our lives. The IoT is commonly used for smart house, smart education, smart healthcare, connected devices, the Vehicle Internet (IoV), and other industries. With all connected, it will be of great benefit to individuals and society as a whole. The overwhelming popularity of mobile devices, and the resulting bevy of apps and services that grew up around them, is spurring the IoT market's rapid growth. [6]

6. Conclusion

Throughout this chapter, some of the most significant security and privacy issues that affect Big Data projects and their details will be discussed. Though the activities of information security, Methodologies and resources already exist to guarantee the protection and privacy of the Big Data ecosystem; Different Big Data features make them inefficient when used in an integrated manner. This chapter also provides some solutions to these problems, but does not have a definitive solution the problem solved. It points quite to other directions and technologies that could lead to this solve some of the most important and difficult issues about Big Data protection and privacy. Next, they addressed two separate use cases. All use-cases give certain directions Help solve part of the big Big Data protection and privacy puzzle.

As a vast network, made up of a number of heterogeneous networks and apps, IoT's application areas are growing rapidly and opening up new opportunities for different businesses. It extends from basic logistics to Wireless Body Area Networks (WBANs), industrial manufacturing, and smart infrastructures such as smart grids, smart cities, and smart vehicles. While the number of connected devices is increasing exponentially, the attention they merit is generally not given to developing new, creative business models, security and privacy.

REFERENCES

1) Lin, H., & Bergmann, N. (2016). IoT Privacy and Security Challenges for Smart Home Environments. *Information*, *7*(3), 44. https://doi.org/10.3390/info7030044Gayathri, T., &Durga, N. (2017).

2) A., Mahboob, &Ikram, N.. (2004). Transport Layer Security (TLS)--A Network Security Protocol for E-commerce. Technocrat PNEC Research Journal.
3) Patel, Keyur& Patel, Sunil & Scholar, P & Salazar, Carlos. (2016). Internet of Things-IOT: Definition, Characteristics, Architecture, Enabling Technologies, Application& Future Challenges.
4) Medagliani, Paolo &Leguay, Jeremie&Duda, A. & Rousseau, Franck &Duquennoy, (2014). Internet of Things Applications - From Research and Innovation to Market Deployment.
5) Buttler, P. (2017, July 24). *10 Challenges to Big Data Security and Privacy - Dataconomy*. Dataconomy. https://dataconomy.com/2017/07/10-challenges-big-data-security-privacy/
6) *IoT Application Development – ScienceSoft*. (n.d.). Www.Scnsoft.Com. Retrieved June 4, 2020, from https://www.scnsoft.com/services/iot/development