ECONSPEAK: A Journal of Advances in Management IT & Social Sciences,
Vol. 8, Issue 12, December 2018 Impact Factor 5.132 ISSN: (2231-4571)
www.skirec.org Email Id: skirec.org@gmail.com

Output Review of IoT Gateways for Big Data Protection System using TLS and its security challenges

Mudholkar Pankaj Keshavrao[1], Dr. Sudhir Dawra[2]

Department of Computer Science

[1, 2]Himalayan University, Itanagar, Arunachal Pradesh

Abstract

This article presents the performance analysis of big data protection IoT gateways using Transport Layer Security (TLS) system and its security challenges in the solution offered; the IoT gateways provide additional protection by securing data using Transport Layer Security (TLS). Real-time experimental assessments have demonstrated the applicability of the proposed mechanism relating to security assurance and the target IoT devices' consumed resources. In the original TCP / IP protocol used on the Internet, mechanisms such as secure socket layer or TLS (Transport Layer Security) are added. Until now the IP protocols have been taken into account in many concerns. But in securing each IoT solution the nature of IoT devices and IoT architecture is faced with its own challenges.

Concept and implementation of the initial Internet of Things (IoT) appeared as timely as the 1980s and ended up popular in the late 1990s. Continuous advances in many important areas, including computing, wireless sensor networks, embedded systems, and small-scale electromechanical (MEMS) systems, have driven the development of the Internet of Things (IoT). Right now, IoT technologies are occurring in almost every area and are taking on an inexorably important role in our daily lives (e.g., medical services systems, building and home mechanization, ecological screening, board base, board strength and transport systems).**Introduction**

Transport Layer Security (TLS) is a protocol that ensures privacy and data respectability between two applications that are imparted. It is the most commonly distributed security protocol used today and is used by Web programs and various applications that allow data to be exchanged safely over a network, such as exchanges of information, VPN partnerships, text and voice over IP. TLS developed from Netscape's Secure Sockets Layer (SSL) protocol and has largely supplanted it, despite the fact that the terms SSL or SSL / TLS are still used occasionally. Key contrasts between SSL and TLS that make TLS a progressively secure and effective protocol are message validation, key material age and the retained figure suites, with TLS supporting more current and increasingly secure calculations. TLS and SSL are not interoperable, but \ TLS offers some retrogressive resemblance to inheritance systems as of now.

TLS is made from two layers according to the detail of the protocol: TLS Record Protocol and TLS Handshake Protocol. The Record Protocol provides security for the association, while the Handshake Protocol allows the server and customer to verify each other and arrange encryption calculations and cryptographic keys before trading any data. Implementation imperfections of any encryption technology have been consistently a major problem, and TLS is no special case. [1]

1. Securing Big Data System using protection of transport layer

Every organization needs to gather troves of business intelligence (BI), as much data as executives, marketers and every other department inside the organization can get their hands on. But once you have this data, the trouble lies not only in analyzing the massive data lake to find the key insights you are looking for (without being inundated by the sheer volume of information) but also in securing all that data. And while the IT department and data scientists at your organization run predictive analytics algorithms, data visualizations, and use a variety of other data processing techniques on the Big Data you've collected, your business needs to make sure there are no leaks or weak points in the reservoir.

The long list of best practices is distributed in 10 categories, so we've whittled down the best practices to 10 tips to help lock the IT department's key business data. These tips employ a variety of data storage, encryption, management, tracking and security techniques. Non-relational databases such as NoSQL are common but vulnerable to attacks such as NoSQL injection; the CSA lists a number of countermeasures to defend against that. Begin by encrypting or hashing passwords and ensure end-to - end encryption using algorithms including advanced encryption standard (AES), RSA, and Secure Hash Algorithm 2 (SHA-256) to encrypt data at rest. Converter layer security (TLS) and secure socket layer encryption (SSL) are also useful. [2]

2. Safe communication through IoT and Big Data using TLS

The data integrity has to be enforced via an application or middleware layer. At rest and in transit, passwords should never be left in the open, but should rather be encrypted or hashed using protected hazing algorithms. Similarly, data which is stored in the database will never be left open. Given the already weak authentication and authorization strategies employed, it is important to keep the data encrypted while in repose due to the related performance impacts. Hardware-based encryption / decryption and bulk file-based encryption are faster and will alleviate some anxiety about the performance effects of encryption. Of course, hardware-based encryption is not without its own criticism because it sometimes contributes to a lock-in vendor, a low-strength key used in encryption / decryption that can be abused by attackers.

Thus, malicious users who gain access to the file system may directly extract sensitive data from the file system. In order to preserve confidentiality while in transit, it is a good practice to use SSL / TLS to create connections between client and server and also for communication across participating cluster nodes. Adopting these mechanisms for the sharing of mutually verifiable keys and maintaining trust will guarantee data confidentiality when data is in transit. The NoSQL architecture will support pluggable authentication modules that can implement protection at all levels as the situation demands.

Considering the money-related growth of technology and the potential for new business openings, it is projected that the Internet of Things will produce net income of $14.4 trillion over the next two decades for efforts. Associations have started designing and introducing their own IoT procedures with the thought process to capture the open door this new time the Internet of Things (IoT) offers empowers any machine to connect with any other computer that uses the Internet. To feature every computer perspective, the term internet of all is similarly used. The Internet of Things is connected to the gathering of data from various sources and make it useful in ways that improve the direction we take. The immense amount of data that will come in from devices demonstrates a monumental challenge for IoT solutions providers. Big Data solutions will overcome this check by allowing us to dissect data and find examples and trends of interest.[3]

3. IoT impacts on Big Data

In essence, IoT and big data are two-growths which can be considered as sides of a similar coin. Today the business world faces the tremendous challenge of handling and collecting valuable knowledge in IoT condition from the big data. Big data is a wording which is eluded to the huge measures of data produced by associated technology. Big data is a tool used by numerous business associations in today's focused world to make their advertising and other advertising efforts increasingly viable. Utilizing the notable data for expectation and investigation of certain circumstance isn't new, yet what's happening is the huge measure of data is accessible with us because of the Internet of Things (IoT). Big data and IoT are therefore truly linked and should be used together while considering the components of security. What effect does IoT have on Big Data? The correct response is IoT change the way organizations use big data for research purposes.

IoT and big data both develop the field and are set to influence numerous business zones and day-to-day regular existence. Which segments would likely feel the IoT / big data disturbance first, however? In its 2015 Internet of Things expectations, as per IDC, more than half of the IoT movement focuses on assembly, transportation, smart city, and customer applications, but all businesses will have taken off IoT activities within five years.

New IoT and Big Data Applications are required to address explicit business solutions that require, for example, precautionary maintenance, unfortunate counteractive action, resource use, stock uptake, calamity arrangement and recovery, downtime minimisation, advancement of vitality use, adequacy of device execution, executive network execution, usage limitation, quantification of scope, request The big data at that point were prepared by using big data examination which undertakings can further use for their deliberate choices and expand their business execution. [4,5]

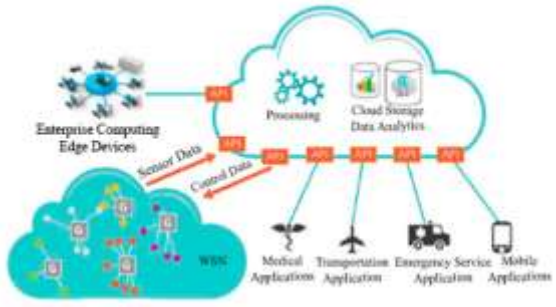

Figure 4.1 Internet of things

4. IoT stability issues In protection layer for transport

Transport Layer Security is the prevalent HTTP encryption protocol but the implementation of TLS is overcomplicated for resource-confined IoT devices. To secure communications, CoAP employs Transport Layer Security as its security protocol. DTLS offers the same security infrastructure as TLS do. The key difference between TLS and DTLS is that TLS is based on TCP protocol, and that DTLS is based on UDP protocol. The CoAP specification stipulated four different protective modes.

The Internet of Things (IoT) has the details at stake. Everyone claim to be the cleverest thing in the world. Nevertheless, the spread of resources, the lack of climate, with fragmented client meetings, is a gigantic test for the fast-growing market. This research discusses the security problems when companies start moving sensitive information into a Big Data Vault. The biggest security issue in IoT is physical and virtual verification. When we talk about physical inspection, it will be increasingly complicated as the phased security mechanisms are used for the network equipment.

Since firewalls are kept behind the network equipment and data must also flow across business entities, stuff ends up in the complex. Additionally, the virtual test comes into being at the stage where the network devices got to collect the information from various sources through the business association. The primary focus of the IoT-condition security assaults is the entire

process of correspondence between IoT-devices. The parts that concern this contact process are simply the IoT system and the gateways. The gateways are an essential issue which controls the entire network and the related procedures.

If the gateways failed the whole network is a failure, and the whole cycle of communication was affected. When conveying one of the virtual hazards between the IoTarray, the impedance that needs to be treated properly can occur. Obstruction generated in the situation where other undesired information misfits or decimes the data being imparted due to the inhabitancy of the physical system. In IoT condition, in some cases, a long-lasting correspondence link must be formed which persistently conveys traffic flow but is extremely overwhelming in IoT and big data condition due to obstruction of service denial which makes the correspondence assets unavailable. Impedance issue can also arise due to the sticking of physical communication channel between hubs. [6]

5. Conclusion

Big data protection mechanisms such as secure socket layer or TLS (Transport Layer Security) are added on the original TCP/IP protocol used in the Internet. The IP protocols are taken into consideration in many concerns until now. But the nature of IoT devices and IoT architecture is faced with its own challenges in securing every IoT solution. Some new security mechanisms are developed with these kinds of constraints. The requirement of the solution has direct correlation with the cost and time to the market. A consequence of requirements for the IoT is that legacy devices for Transport layer security may become a security and privacy liability. Security vulnerabilities of devices should therefore be monitored and solved. It might be useful to consider a set of devices in the IoT. We surveyed and analyzed a requirement of security issues for IoT system and security challenges for Internet of things. The requirement can be considered for some security options and approach that can be used for IoT solution.

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/info7030044
2. Gayathri, T., &Durga, N. (2017). Security Challenges Associated with High Dimensional Data. *International Journal of Scientific Research in Computer Science, Engineering and Information Technology © 2017 IJSRCSEIT*, *4*(10), 2456–3307. http://ijsrcseit.com/paper/CSEIT1724131.pdf
3. Pathak, Pankaj&Asstt, Sr& Professor, &Vyas, Nitesh& Professor, Asstt& Joshi, Someshwar. (2017). Security Challenges for Communications on IOT & Big Data. International Journal of Advanced Research in Computer Science. 8.

4. Syed, 1, Shahdad, Y., Khan, F., Bilfaqih, S., Sultana, H., &Hussain, M. (2018). *IMPACT OF BIG DATA IN INTERNET OF THINGS (IoT)*. *6*(2), 2320–2882. http://www.ijcrt.org/papers/IJCRT1812372.pdf
5. Jing, Qi &Vasilakos, Athanasios& Wan, Jiafu& Lu, Jingwei&Qiu, Dechao. (2014). Security of the Internet of Things: Perspectives and challenges. Wireless Networks. 20. 2481-2501. 10.1007/s11276-014-0761-7.
6. Jing, Qi &Vasilakos, Athanasios& Wan, Jiafu& Lu, Jingwei&Qiu, Dechao. (2014). Security of the Internet of Things: Perspectives and challenges. Wireless Networks. 20. 2481-2501. 10.1007/s11276-014-0761-7.