IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

SECURE AND EFFICIENT MODEL FOR DATA COLLECTION AND STORAGE IN INDUSTRIAL IOT

[1]Aatish Brian D Silva, [2] Dr. K S Jasmine
[1]Student, [2]Associate Professor
[1] Department of Master of Computer Applications
[1]RV College of Engineering, Bengaluru, India

Abstract: With the increase of scope and use of IoT in industrial systems, issues of security and efficiency quickly show up. As the sensors and actuators at the edge location themselves only have minimal security features, security at the edge and over the network must be taken care of without harming the performance of the system as a whole. This paper proposes a system using edge gateways to divide the work instead of letting a central server collect the data thereby decreasing the large amounts of data a single server has to take care of while also providing data security to classify and manage data at these edge gateways. Along at the edge gateway level the concept of data aggregation is also implemented so that the data at the edge gateway level itself can be divided based on their sensitivity reducing extra work to secure non-sensitive data.

***Keywords*— Industrial Iot, Edge Gateways, TrustZone.**

I. INTRODUCTION

The Industrial Internet of Things (IIot) uses the power of industrial internet or IoT 4.0 standards with a large number of sensors, wide networks to collect and work with data in an industrial setting in real time. With the increase in the implementation of IIoT, the amount of data generated at different sources is increasing exponentially. Global analysis shows the IIoT market is expected to grow from USD 77.3 billion in 2020 to USD 110.6 billion by 2025, at an annual growth rate of 7.4% during the forecast period. The growth of the IIoT industry is driven by factors such as technological advancements in semiconductor and electronic devices, increased use of cloud computing platforms. As the scope and adoption of IIoT increases the need for a real time system which addresses real time concerns of performance, coexistence, interoperability, and security and privacy is required. But storing all that raw data brings about its own concerns with respect to security and efficiency as the end devices themselves has minimal storage space and they can be over a large area and be vulnerable for attacks in remote, unsecure areas. Though various security measures are used, there is no unified system to deal with internal or external attacks. This paper proposes a system with utilizes a combination of data segregation and decentralizing data collection methods to solve the requirements of efficiency of and data security.

II. LITERATURE REVIEW

In the paper titled "A Unified Trustworthy Environment Establishment based on Edge Computing in Industrial IoT" published in the 2019 IEEE Transactions on Industrial Informatics, the authors Tian Wang, Pan Wang, Shaobin Cai, Ying Ma, Anfeng Liu, Mande Xie talk about the lack of a unified and tested system for use in IIoT. The authors go on to propose of system of service selection methods based on edge computing technology. The data from the end devices are collected and sent over a trusted network from reliable service providers to improve on the feasibility of creating a trustworthy environment. Further in the paper titled "Secure Data Storage and Searching for Industrial IoT by Integrating Fog Computing and Cloud Computing", from IEEE Transactions on Industrial Informatics of the year 2018, the authors Jun-Song Fu, Yun Liu, Han-Chieh Chao,Bharat K. Bhargava, Zhen-Jiang Zhang present an idea of collecting data at edge servers which collectively make up the main server. The authors suggest a system of preprocessing the raw data form the end devices and divide them into time-sensitive and non-time sensitive data so that the time sensitive data are stored locally and the rest is sent to the cloud server. A series of experiments concluded that this system can greatly improve the efficiency and security of data storage and retrieval in IIoT.

III. METHODOLOGY

3.1 Data Classification Based on Weight

Data collected from end devices can vary in terms of sensitive and non-sensitive data based on weight. For example, the collected from devices monitoring patients in hospitals and incredibly sensitive and personal. It cannot be lost or be modified by external attackers while can cause huge risks to the said patient and hospital. But at the same time, historical data collected for analysis of diseases are not as sensitive, although they need to be secure, the overhead of using security measures like encryption can slow down the system as a whole. Weights can be set to various devices based on the sensitivity of data. This sensitivity can be calculated based on data confidentially, reliability and integrity by the organization implementing the IIoT System.

3.2 Data Collection by Edge Servers

In the proposed system data is collected by Edge Servers rather than a central server. With the increase in the amount of raw data that has to be collected and processed using a single server has large overheads. Instead multiple devices at a location is connected to a server which collects the data and classify them. Device monitors collect data from non-sensitive sources are stored either locally in the general execution space or sent to the central server or cloud for further use. Whereas the sensitive data will be managed by a Sensitive Data Manager which includes the servers ARM TrustZone technology with Encryption API to encrypt the data for security

IV. BLOCK DIAGRAM

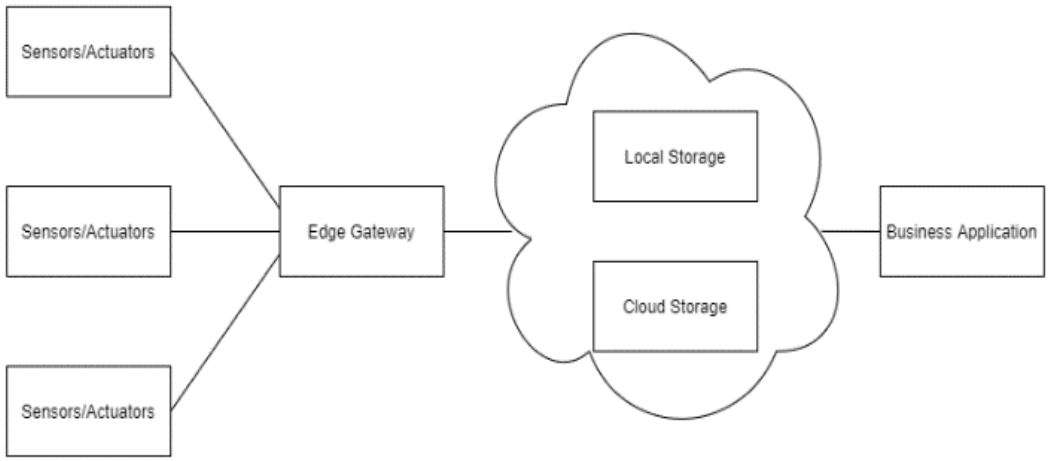

figure 1. block diagram for the system

In the proposed system the edge gateways are used to collect data from a set of sensors. Data will then be classified at the edge gateway server and stored securely based on requirements. Non-sensitive large amounts of data will be offloaded to the cloud server efficiently.

V. ARM TRUSTZONE

Encryption of data becomes easier with the classification of data into sensitive and non-sensitive data. However, a trusted environment is required for encryption. The proposed system suggests using TrustZone technology. TrustZone is a hardware security solution supported by devices and servers build using the ARM architecture. It divides the system into normal world and secure world. In a TrustZone execution environment, a processor is shared by both worlds at different times which makes it seem as if both worlds are isolated, giving an isolated, safe and programmable environment to safely encrypt data. A general Linux operating system will run on the normal world. Non-sensitive data will be managed by this OS. A customized secure version of Linux with encryption API will run on the secure world creating what will be known as a Trusted Execution Environment which is isolated from the rest of the system and isn't prone to attacks.

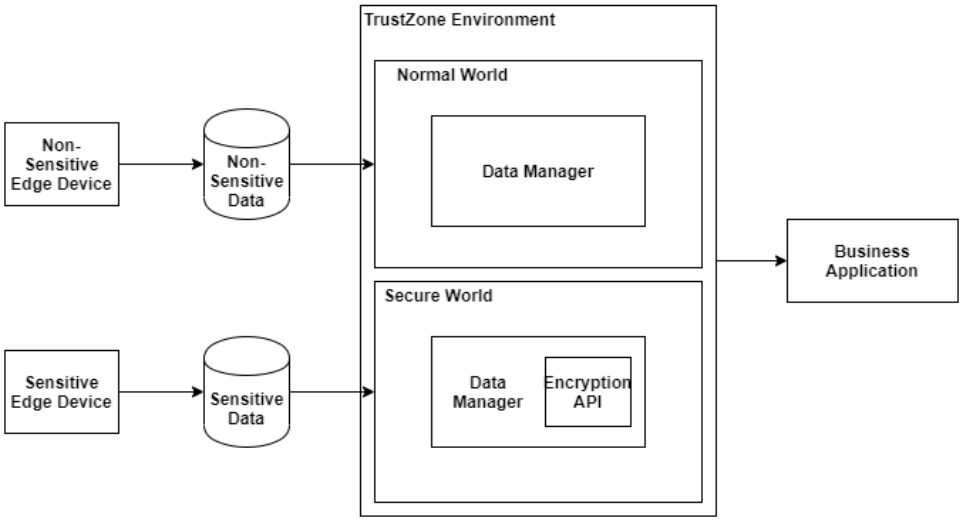

figure 2. architecture for trustzone based data classification system

VI. EXISTING WORKS

LEGIoT: A Lightweight Edge Gateway for the Internet of Things

LEGIoT System is an architecture designed to deal with bandwidth requirements and security in IoT environment. It works by implementing container in IoT network using edge gateways with the inclusion of variety of IoT protocols for optimal efficiency. It has been implemented in real time networks to demonstrate its scalability and sustainability in a wide range of networks. However, LEGIoT was designed and tested with IoT in mind, in the scale of larger buildings. But the amount of data generated in future IIoT settings will increase drastically and the cost of maintaining and adding a larger number of Edge Gateways won't be sustainable. To decrease the load put on these gateways, this paper suggests the idea of data classification. Not all the data generated in an IoT setting need to have prime priority and not having to securely store them using TrustZone improves the performance of the gateways.

VII. CONCLUSION

This paper proposes a system of using edge gateways to classify data in sensitive and non-sensitive data. Sensitive data is encrypted and stored safely. Non-sensitive data is not worked on too much increasing the efficiency of the system even when collected large amounts of data.

REFERENCES

[1] Tian Wang, Pan Wang, Shaobin Cai, Ying Ma, Anfeng Liu and Mande Xie, "A Unified Trustworthy Environment Establishment based on Edge Computing in Industrial IoT", IEEE Transactions on Industrial Informatics (Volume: 16, Issue: 9, Sept. 2020), DOI: 10.1109/TII.2019.2955152

[2] Jun-Song Fu , Yun Liu , Han-Chieh Chao , Bharat K. Bhargava and Zhen-Jiang Zhang, "Secure Data Storage and Searching for Industrial IoT by Integrating Fog Computing and Cloud Computing", IEEE Transactions on Industrial Informatics (Volume: 14 , Issue: 10 , Oct. 2018), IEEE, 2018, DOI: 10.1109/TII.2018.2793350

[3] Sandro Pinto, Tiago Gomes, Jorge Pereira, Jorge Cabral and Adriano Tavares, "IIoTEED: An Enhanced, Trusted Execution Environment for Industrial IoT Edge Devices", IEEE Internet Computing (Volume: 21, Issue: 1, Jan.-Feb. 2017), IEEE, 2017, DOI: 10.1109/MIC.2017.17

[4] Jacob Wurm, Khoa Hoang, Orlando Arias, Ahmad-Reza Sadeghi and Yier Jin, "Security analysis on consumer and industrial IoT devices", 2016 21st Asia and South Pacific Design Automation Conference (ASP-DAC), Macau, China, 2016, DOI: 10.1109/ASPDAC.2016.7428064

[5] Zhaozong Meng, Zhipeng Wu, Cahyo Muvianto and John Gray, "A Data-Oriented M2M Messaging Mechanism for Industrial IoT Applications", IEEE Internet of Things Journal (Volume: 4, Issue: 1, Feb. 2017), 2017, DOI: 10.1109/JIOT.2016.2646375

[6] Rodrigo Román-Castro, Javier López and Stefanos Gritzalis, "Evolution and Trends in IoT Security", 2016 3rd International Conference on Computing for Sustainable Global Development, 2016, DOI: 10.1109/MC.2018.3011051

[7] Shivaji Kulkarni, Shrihari Durg and Nalini Iyer, "Internet of Things (IoT) security", 2016 3rd International Conference on Computing for Sustainable Global Development (INDIACom), New Delhi, India, 2016, INSPEC Accession Number: 16426642

[8] Israr Ahmed, A. P. Saleel, Babak Beheshti, Zahoor Ali Khan and Imtiaz Ahmad, "Security in the Internet of Things (IoT)", 2017 Fourth HCT Information Technology Trends (ITT), Al Ain, United Arab Emirates, 2018, DOI: 10.1109/CTIT.2017.8259572

[9] Rwan Mahmoud, Tasneem Yousuf, Fadi Aloul and Imran Zualkernan, "Internet of things (IoT) security: Current status, challenges and prospective measures", 2015 10th International Conference for Internet Technology and Secured Transactions (ICITST), London, UK, 2015, DOI: 10.1109/ICITST.2015.7412116

[10] Syed Rizvi , Andrew Kurtz , Joseph Pfeffer and Mohammad Rizvi, "Securing the Internet of Things (IoT): A Security Taxonomy for IoT", 2018 17th IEEE International Conference On Trust, Security And Privacy In Computing And Communications/ 12th IEEE International Conference On Big Data Science And Engineering (TrustCom/BigDataSE), New York, NY, USA, 2018, DOI: 10.1109/TrustCom/BigDataSE.2018.00034

[11] Jihad DAZINE, Abderrahim MAIZATE and Larbi HASSOUNI, "Internet of things security", 2018 IEEE International Conference on Technology Management, Operations and Decisions (ICTMOD), Marrakech, Morocco, 2019, DOI: 10.1109/ITMC.2018.8691239

[12] Zhi-Kai Zhang, Michael Cheng Yi Cho, Chia-Wei Wang, Chia-Wei Hsu, Chong-Kuan Chen and Shiuhpyng Shieh, "IoT Security: Ongoing Challenges and Research Opportunities", 2014 IEEE 7th International Conference on Service-Oriented Computing and Applications, Matsue, Japan, 2014, DOI: 10.1109/SOCA.2014.58

[13] Israr Ahmed, A. P. Saleel, Babak Beheshti, Zahoor Ali Khan and Imtiaz Ahmad, "Security in the Internet of Things (IoT)", 2017 Fourth HCT Information Technology Trends (ITT), Al Ain, United Arab Emirates, 2017, DOI: 10.1109/CTIT.2017.8259572

[14] Jian Zhang, Huaijian Chen, Liangyi Gong, Jing Cao and Zhaojun Gu, "The Current Research of IoT Security", 2019 IEEE Fourth International Conference on Data Science in Cyberspace (DSC), Hangzhou, China, 2019, DOI: 10.1109/DSC.2019.00059

[15] Jack Whitter-Jones, "Security review on the Internet of Things", 2018 Third International Conference on Fog and Mobile Edge Computing (FMEC), Barcelona, Spain, 2018, DOI: 10.1109/FMEC.2018.8364059