INTRODUCTION TO INTERNET OF THINGS - COMP6121-112

Assignment I

Report of paper selection

Complete by

P2213046 王榮勝 Rongsheng Wang, Mark

P2213913 詹澤齊煒 Zeqiye Zhan, Janzen

P2213983 李俊蓉 Junrong Li, Rachel

P2212990 李宇昆 Yukun Li, Leo

Sep 26, 2022

I. Introduction

After 2003, the number of sensors has grown substantially. According to the latest report (The global sensor market) released by the market research agency ReportLinker, the global sensor market is expected to reach US$128.56 billion by 2025. The rapid growth of sensors makes a smarter and better city. The rise of the number of sensors, which have characteristics as low-power, long-life devices, in order to data collection, storage, etc. Therefore, cyber attackers prefer to attack these sensors. And these IoT objects are developed based on the traditional TCP/IP model, so they are not designed for such a large number of connected devices, that's why the blockchain concept needs to be introduced, we need a more powerful distributed solution to solve the security problem of a large number of sensors in edge computing.

A large number of sensors collect specific data and send it to the client (CPE). So how to communicate? The characteristics of the communication technology used by sensors are different. For example, low-power transmission will use technologies such as Bluetooth and RFID, while long-term transmission requires the use of various cloud-based protocols, which require higher data transmission rates and higher power consumption.

Cloud computing is the framework of smart cities, and a new technology called fog computing/edge computing is based on cloud computing.

The difference between these two technologies is calculation method. Cloud computing is biased towards central computing, while fog computing will distribute the calculation to all fog nodes. After calculating all the data, the data is transported by application layer for people use, Cloud computing provides interfaces to software, and uses software defined network.

II. Smart city layered architectures and adversaries

The smart city architecture can be classified into layers based on the assets operating in a physical cyberspace environment. smart city architecture can mainly be divided into three-layered architecture: application layer, transmission layer and sensing layer:

The application layer provides platforms for people to use, this layer provides a path for the interaction using received information from the transmission layer. It executes commands based on data from the devices at the sensing layer.

And the transmission Layer is responsible for the communication among the devices between the upper and lower layers, the transmission technologies such as 5G, or satellite play an important role in data transfer. Routers and switches use communication and transmission technologies to route the data. The transmission layer has the responsibility to identify things and collect the information from sensors, there are many types of sensors attached to objects to collect information. The sensors are chosen according to the requirement of applications. There are corresponding attacks according to the different layers. as for the application layer adversaries. when IoT is used in order to make a smart home, it introduces many threats and vulnerabilities from the inside and outside. The most common attacks at this layer are injection attacks, parameter tampering. The transmission layer can be targeted by obstructing the network resources and bombarding the fake data. It can lead to serious consequences such as distributed denial of service attacks.

For the sensing layer, there are many sensors in this layer, due to the low power and low calculation of the sensors, network security and authentication issues arise. It can lead to serious consequences such as physical attacks and port scanning attacks.

III. Blockchain of IoT in Smart Cities and Authentication

One of the core highlights of this paper is that the distributed system is applied to the smart devices of the Internet of Things in the smart city, and the accompanying authentication scheme and a whole series of theories and concepts. First of all, a distributed system is a system composed of a group of computer nodes that communicate through a network and coordinate their work to accomplish a common task, but in the Internet of Things, it is composed of nodes at various perception layers. These nodes have independent storage space, and can complete most of the required calculations locally. They will communicate only when the results are uploaded, authentication, which require the participation of the server. This method is called fog computing. Since each node has an independent storage space, they can request to act as a local server and make the system a distributed system through a series of registration and verification mechanisms.

Because IoT devices require authentication, they are vulnerable to intrusion attacks. The author's workaround is to use the blockchain only as a distributed data repository, leaving the decentralized OAuth2-based implementation of authentication and authorization logic outside the blockchain.
In addition, the author also proposes an Ethereum-based edge computing smart contract as a low-cost, low-overhead tool for computing resource management by SmartEdge; using the Blockchain of Things Sentry framework to integrate blockchain with IoT networks, it can enhance network security by analyzing network traffic patterns of devices obtained from data stored in the blockchain; And a blockchain-based authentication mechanism, the BCTrust framework, designed for those equipment with resource constraints(such as compute, storage, and energy consumption constraints). These technologies can effectively improve the performance, security, and practicability of the Internet of Things based the blockchain.

IV. Future improvements

Furthermore, in smart city infrastructure, the data is transmitted from multiple CPSs to the security operations center (SOC) over the internet, posing security threats in different communication architectures of the smart city. Therefore, IoT technology must establish a strong security mechanism in the future. Firstly, building a blockchain-based Internet of Things, with the help of the underlying DLT and the consensus mechanisms, to provide robust security for communication. Secondly, bringing tokens to the Internet of Things. Guaranteed that the use of tokens can be used to identify and verify ownership of assets in smart city infrastructure and trade through the unique method of identifying non-fungible tokens. Finally, address the limitations of consensus network to securely store and manipulate privately encrypted data through a decentralized key management system. In addition, more reliable and lightweight encryption algorithms are also necessary, which can not only better protect the integrity and privacy of communications, but also meet the requirements of low-level device usage.

The IoT based on decentralized system and blockchain is stronger and better. It also has higher efficiency and less delay performance compared to normal IoT system. It is a better suitable solution for Smart Cities.