Applied Mechanics and Materials Vols. 433-435 (2013) pp 1752-1755 *Online: 2013-10-15*

doi:10.4028/www.scientific.net/AMM.433-435.1752

Research on Data Security Technology in Internet of Things

ZHAO Yanling

Leshan Vocational and Technical College, Leshan 614000, China

lszhaoyl@yeah.net

Keywords: Internet of Things, Information Security, Data Security

Abstract. The Internet of Things is currently the most popular field of communication and information research directions. Their application in the amount of information involved, are extremely large amount of data. How to ensure the transmission efficiency of business information under the premise of improving networking applications data security to protect the user's privacy data will be particularly important. Paper uses a custom data packet encapsulation mechanism, reducing the overhead of data resources; another based on their cross-platform communication features, combined with secure encryption and decryption, signature and authentication algorithm, the establishment of a secure communication system of things model for the differentiation of things communications environment, providing a standard packet structure, namely smart business security IOT application Protocol intelligent Service Security Application Protocol(ISSAP).

Introduction

Internet of Things collected data to be transferred to the data center, users in different locations to be able to query the use of these data, as well as the identification of these sensing devices and management. The transmission of data will be needed for a variety of wired or wireless network, in order to ensure real-time data transmission and accuracy, which requires a new protocol to accommodate heterogeneous network of heterogeneous networks. However, the application layer Internet of Things the most basic elements - business security application protocol Internet of Things have not formed a unified standard. About Internet of Things Smart business security application protocol research, still in its infancy, there is a huge space for theoretical research and application prospects. Therefore, IOT application protocols for smart business security key technology research and related research implementation, optimization of theoretical innovation and forward-looking, it is smart business Internet of Things foundation and guarantee the normal operation, determine the future Internet of Things technology development and progress. Internet of Things agreement ISSAP secure smart business applications is to provide intelligent business applications Internet of Things indispensable basic condition, it will provide a huge Internet of Things equipment and a wide variety of businesses to provide fast, convenient and simple smart business development and runtime environment, and is a large-capacity high-performance business data fusion, interconnection and secure communications to provide basic protection to meet the Internet of Things requirements of complex business systems to expand coverage and improve Internet of Things business application development capabilities.

Internet of Things overall platform architecture design

Internet of Things construction business support platform's main purpose is integrated networking industry chain on the core technology, to achieve standardization Internet of Things application standards, networking application service automation allocation, scheduling and achieve information sharing. Figure 1 is a networking platform for the location of the Internet of Things.

As an extension of the Internet of Things, which must be composed by a large number of heterogeneous networks, manage and control such a large amount of network equipment will be facing new problems and challenges. So, things should have a flexible platform for autonomy, in a timely manner to make the distribution, management, restoration of function, and according to

changes in the environment have to make adjustments spontaneous. This autonomy refers platform able to follow the needs of developers and business purpose to implement, and ultimately achieve business development, deployment and implementation.

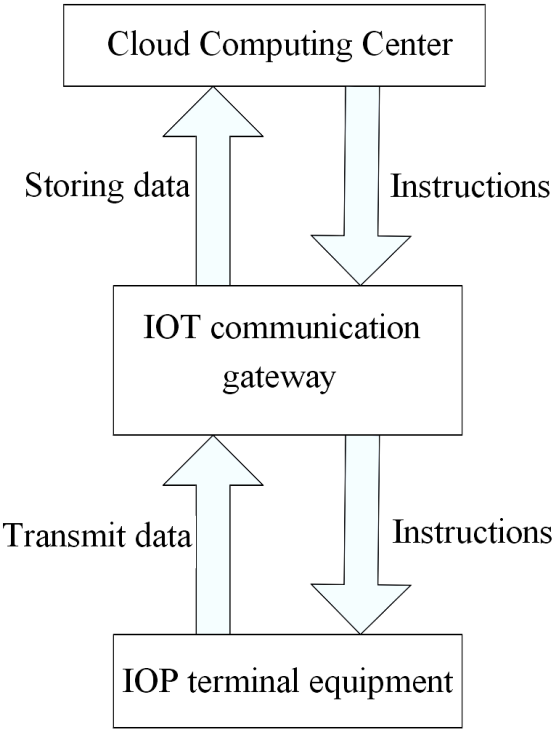

Figure 1 Data communications IOT platform architecture

Networking platform in which the network is complex, a variety of wired or wireless network combined into a heterogeneous network. Open network allows malicious attackers have an opportunity, they are able to take advantage of this loophole in any way for the network to attack and try to get the platform user's personal privacy and confidentiality requirements of a strong some information. Some of the information once it has been such a malicious attacker access, use or distribute will give the social stability and personal and national security to bring a strong influence and impact.

IOT data security architecture

Typically the sensor nodes in complex environments in which or unattended. Therefore, in addition to its general wireless networks face information tampering, disclosure, denial of service attacks and other threats, is also facing the sensor nodes are malicious attackers physical manipulation or even destruction danger.

IOT network layer security issues. IOT layer transport network can be divided into core-aware network transmission and the transmission network in two parts. Typically, sensor nodes faster energy consumption, so that they can not have a complex security mechanisms; core networks, although a relatively complete security protection, but due to a large amount of information data IOT features in the process of transmission, need to transfer large amounts of data will make the network congestion, resulting in denial of service attacks.

IOT support layer security issues. Support layer is the application layer to provide service support, when the support layer different applications simultaneously handle multiple requests, bound to the same time a large number of different types of intelligent data processing and decision analysis. This layer is primarily related to the safety of the platform safe operation of the database data, the task scheduling and handling safety and physical security platform server. IOT application layer security issues. Application layer is to provide users with the application; users will be faced with the threat of

loss of privacy. User's private information including location information and personal information, including location privacy refers to the user location information on their own ability to control.

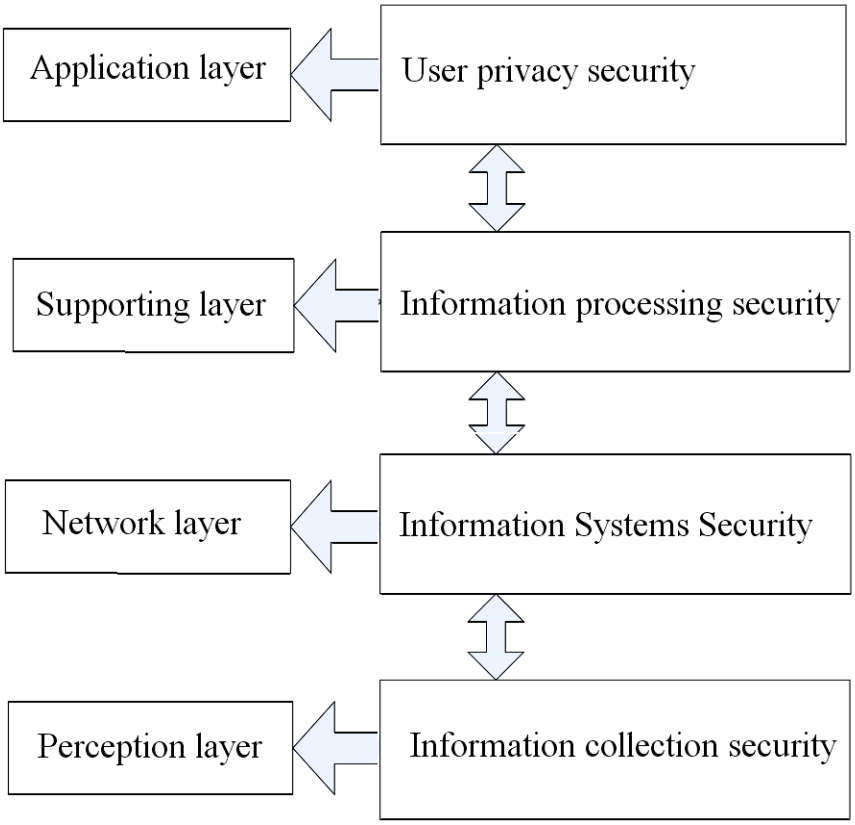

Figure 2 Security architecture of IOT

Refers to the ability to control the user can decide whether to publish their current location information, or to see who published this information, as well as how specific location information released. Location privacy is often overlooked, in fact, the disclosure of location privacy most immediate danger is likely to be criminals use to track the parties, resulting in a threat to personal safety. Home address of the leak may give users a spam problems. Personal privacy inherent in the content is very broad, and for different people, different cultural nationalism, privacy is not the same connotation. Generally speaking, personal privacy, including personal information, physical condition, and property and so on.

Data security technologies of IOT

Security protocol on the protection of network security and personal privacy plays a vital role. Only protect the security of network communications and the user's privacy, users can rest assured that the use IOT brought about by the application of a variety of convenient services, otherwise, the application of things into people's lives difficult, not to mention widespread popularity the. Therefore, the security of the Internet of Things application protocol for the development of networking plays an important role, how to design to protect user privacy and security of communications standard IOT protocols business applications will be the key to further development IOT.

ISSAP protocol mainly used USPIOT platform for business communications and is used to build client and service platform server or server business platform for communication between a business application protocols. Through standardized data formats and communication platform for various system interfaces, sensing devices for heterogeneous centralized data processing to maximize the interaction of both communication efficiency, establish an open USPIOT business platform, in a transparent manner to provide users with differentiated with QoS guaranteed IOT smart Business. TLV encoding means for Tag, Length and Value encoded bit stream to form a packet; decoding and

encoding are two reciprocal processes, it is from the bit stream packet parsing restore the original data in the process.

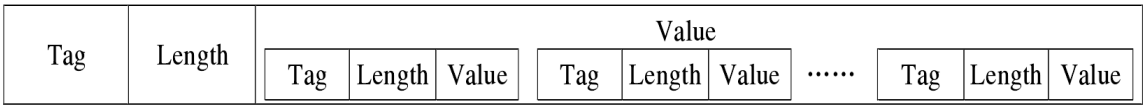

Figure 3 ISSAP TLV of nested code

ISSAP agreement characterized by the largest group of teachers and members of the project self-defined data frame format, which is based on ASN.1 abstract syntax markup language designed with traditional Extensible Markup Language (XML)-based data frame compared to this Agreement defined data frame has occupied bandwidth is small, easy to read the message format, the packet packet high flexibility, cross-platform communication, user and IOT USPIOT business platform interoperability features.

Conclusion

This paper is based on the development of networking and security issues facing the business protocol for secure communications strong demand, made IOT safe intelligent business application protocols - ISSAP agreement, then, explains things based platform application protocol ISSAP application scene and its characteristics, it is used to create client and server or between business platform for communication between a server platform for business applications protocol. From the information security and privacy protection point of view, IOT to bring life easier, but also increases the risk of exposure to such information. To keep the data falls in the hands of a malicious user, the Internet of Things will be even more important to the security of communication. IOT communication needs for security, business intelligence is bound to IOT Application Protocol ISSAP security challenges, which requires ISSAP agreement must be in a secure application protocols.

References

[1] M. Kumar: International Journal of Network Security, Vol.11 (2010), p. 89-93.

[2] J. H. Song, W. S. Vincent: Mobile Network Application, Vol.15 (2010), p.160-171.

[3] M. Eltoweissy, M. Moharrum: IEEE Communications Magazine, Vol. 44 (2006), p.122-130.

[4] L.Chunand, T.Hwang: ComputerS & Security, Vol.22 (2003), p.68-72.

[5] M. Peyravianan: Computer Communieations, Vol.29 (2006), p.660-667.

[6] L. Atzoria, A. Giaeomo: The International Journal of Computer and Telecommunications Networking, Vol.54 (2010), p.2787-2805.

Advances in Mechatronics and Control Engineering II
10.4028/www.scientific.net/AMM.433-435

Research on Data Security Technology in Internet of Things
10.4028/www.scientific.net/AMM.433-435.1752

DOI References
[2] J. H. Song, W. S. Vincent: Mobile Network Application, Vol. 15 (2010), pp.160-171.
http://dx.doi.org/10.1007/s11036-009-0167-4
[3] M. Eltoweissy, M. Moharrum: IEEE Communications Magazine, Vol. 44 (2006), pp.122-130.
http://dx.doi.org/10.1109/MCOM.2006.1632659
[5] M. Peyravianan: Computer Communieations, Vol. 29 (2006), pp.660-667.
http://dx.doi.org/10.1016/j.comcom.2005.07.025