Journal Homepage: - www.journalijar.com
INTERNATIONAL JOURNAL OF ADVANCED RESEARCH (IJAR)
Article DOI: 10.21474/IJAR01/4549
DOI URL: http://dx.doi.org/10.21474/IJAR01/4549
ISSN NO. 2320-5407

RESEARCH ARTICLE

RESEARCH ON PRIVACY PROTECTION TECHNOLOGY BASED ON IOT.

Zhang Yajie.
Department of information technology, Wenzhou vocational and technical college, Wenzhou, China.

Manuscript Info

Manuscript History

Received: 20 April 2017
Final Accepted: 22 May 2017
Published: June 2017

Key words:-
Smart home, Privacy protection,Iot,Wireless sensor networks

Abstract

The Internet of things technology is leading the wave of information industry revolution and would be widely used in smart home, military and commerce. In Wireless sensor networks, each node sensing, collecting and transmitting information about the perceived objects in coverage areas periodically through collaboration with neighbors. Each sensor node is always resources limited. This paper starting from the hierarchical structure of the internet of things, analyze the privacy and security problems faced by the intelligent home system, then proposed the privacy protection strategy, and designed a privacy protection scheme for smart home systems. This paper constructs the privacy protection model of the internet of things for the intelligent home, gives a detailed model of the process analysis and model of the overall logical structure, improved privacy protection technology for existing legacy networks. Finally , verified the security and practicability of this model.

Introduction:-

With the development of computer and digital communication technology into all areas of life, Internet of things (IOT)came into being. It is widely applied in military,industry,agriculture,traffic,medical health,smart home and other various fields. As one of the typical applications of the internet of things, smart home has greatly changed people's life and brought many conveniences to us. However, with the access to the internet of things such as smart home, privacy issues come with it. Whenever we connect a new electrical appliance to the internet, we generate a group of data about our lives, and those data will be stored on the server of a company. When we login on the smart home system to get the network information, a large number of user personal privacy information, such as IP address, user preferences and network interactive content personal information is easy to be used by a third party. They use of existing technical means to collect such privacy information. In general terms, privacy can be defined as: only expected observers and open objects can view information, and others cannot get it. The data information can be used to build personal digital trajectories and can be used by illegal agencies or hackers. ITU（International Telecommunication Union）points in 2005，it's a great challenge to the development of IOT for the user privacy protection. Lack of users' privacy protection will cause user churn, and it is just one of the drivers of successful development of the IOT.

But the production of smart toilet, smart refrigerator, smart baby monitor Home Furnishing equipment manufacturers generally do not pay special attention to the problem of data security, more consideration is their realization of sensing and transmission function, ignoring the data privacy issues. But often the security holes in these devices can make bad people disrupt family life, steal important personal data, and even use stolen information

Corresponding Author:- Zhang Yajie.
Address:- Department of information technology, Wenzhou vocational and technical college, Wenzhou, China.

to blackmail victims. At present, there are many problems in our smart home system, such as low level of information security and lack of control strategy of information privacy. How to better deal with the privacy protection of smart home network has become a problem to be solved in the smart home network.

The activities within a smart home environment can be identified by analyzing the transmission behavior of the wireless sensors, for example, using WiFi, bluetooth (low energy) and ZigBee technology, and don't even need to see is the transmission of information. Attackers (highly sensitive listening devices) can use this method to destroy life and the environment of wireless sensor deployment in the personal privacy. Against the attack of the most advanced protection mechanism is mainly through the unified transmission time slot to send the sensor data to hide the data transfer mode. This produces the must produce false readings for transport in scheduled time slot without sensor data are available to ensure uniformity. In addition, for the same reason to the slot between the actual data packets must be delayed. Hiding the actual transmission mode can be used to protect is based on the analysis of the transmission, but the protection scheme reduces the availability of smart home technology. False data transmission, for example, can cause considerable energy costs and increasing for battery.

Fundamentals:-

In recent years, smart home technology is developing rapidly, research on privacy protection technology has attracted more and more attentions, many foreign scholars and experts have studied the security of Internet of things. Some researchers summarized the privacy protection technology on data dissemination and data mining , which can be divided into based on data distortion techniques and based on data encryption technology and limited release technology, which limits the release of technology mainly through data anonymization to achieve. Some researchers reviewed from the data query privacy protection technology of wireless sensor networks in several aspects of privacy protection, data aggregation privacy and location privacy protection, respectively introduces the privacy protection method of encryption technology and routing protocol . Latanya Sweeney of Carnegie Mellon University of America proposes k- anonymous model. In order to address privacy protection in location services, Gruteser et al. apply this concept to location privacy, proposed a location k- anonymous model . Domestic scholars put forward a method to protect the RFID anonymous ID user data and location privacy, and proposed based on universally composable model of low cost RFID anonymous authentication protocol by using the pseudo random function to achieve the source.

To resolve the latency issue of periodic transmission method, Shao et al. introduced a probabilistic distribution-based transmission (PDT) method. The key idea of this method is to schedule transmission intervals that are random in length based on a probabilistic distribution, ensuring complete randomness of the entire traffic. Compared with periodical transmission, PDT minimizes the latency of real data transmissions through much frequent transmission schedules, while ensuring near perfect privacy. On the other hand, although such protection method achieves minimum latency, utilizing frequent fake data transmissions causes energy efficiency issues. The problem of energy efficiency is critical because most sensor nodes are battery-powered and the energy cost for data transmission is one of the most significant ones. In fact, frequent fake data transmissions are not favorable for the longevity of the network. On the other hand, if we consider immediate transmission of real data for optimal QoS for smart home environment applications, the privacy of the resident would be totally compromised by the adversaries. To protect privacy of the residents while real data transmissions are made with no delays, we can adopt source simulation concept introduce by Mehta where fake data transmissions are made following the PDT method to obscure real data transmission patterns[3].

This paper[5,6] introduces the method of constructing the shared key between the sensor nodes and ensures the security of the communication process by encryption. Some researches proposed to prevent tampering and theft of privacy data data fusion program. Under the layer node must encrypt the privacy data itself before sending the data, so the intermediate node needs to be frequent to decrypt the received data, in order to reduce the computational overhead of the decryption operation. Girao and Castelluccia et al. Proposed a homomorphic encryption scheme based on the rational lattice. The intermediate node in the scheme does not need to decrypt the received data, and can directly perform the data fusion operation and send it to the upper node after encryption. He and other researches proposed a data fusion algorithm PDA (Privacy-preserving Data Aggregation), which contains two algorithms CPDA and SMART. CPDA algorithm uses data perturbation technology to add private random number to private data to hide sensitive information. Based on the SMART algorithm, the algorithm allocates random time slices for nodes to avoid collisions of data between the same layers, and reduces the impact of data loss on the fusion results. Both algorithms have better protection of privacy, but CPDA uses polynomial algebraic properties,

computational overhead is relatively large, and SMART data fragmentation led to a large amount of data traffic.SMART divides raw data into J slices, randomly selects J-1 neighbor nodes in the neighbor set and exchanges data with them , each node makes SUM processing for all received slices as its own data. Yang Geng et al. Proposed a low-power privacy protection algorithm ESPART based on the SMART algorithm.

For privacy protection in smart home system is increasingly attracting the attention of the researchers, the privacy of data fusion technology, the integrity verification mechanism in the private data in the transmission of research is going to be in the next few years the focus of international scholars study.

Analysis of privacy protection:-

A. needs of privacy protection

The temperature sensor and luminance sensor in the home sensor system collect the surrounding environment information, which is non-sensitive information and can be shared at any time. However, the heart rate sensor captures the user's private health data information, which requires proper protection. In addition, the sound sensor to capture sound information data, and similar acceleration sensor and pressure sensor, these data are generally little attention, the user is not regarded as sensitive data, but if these data sharing on the outside in a public platform is not always safe. For example, an attacker can analyze the data collected by these three sensor nodes to determine the rules of the user's work and rest, and then select opportunities for burglary. As shown in.

Table 1:--Privacy levels for each node.

Privacy level	nodes
public	Illumination,humidity, temperature,etc
Sensitive but not clearly stated	Voltage, current, current, etc
protect	Sound, pressure, etc
private	Heart rate, video,etc

Needs of security Assessment:-

According to the 0CTAVE Allegro method, the security requirements of the important information assets in the home sensor system mainly include three aspects: confidentiality, integrity and availability. As shown in.

Table 2:- Security requirements for node Data.

Security requirement	descriptions
confidentiality	Node data and user information data are readable only by family members. Only the authorized user of the system can access to it.
integrity	Only authorized family members can update or modify node information and user information. For data stored in the nodes, only through the data storage services provided by the system itself, it is updated under certain privacy controls.
usability	Node data and user data must be available to home users.
others	The node data also contains information useful to the public, and the information cycle is uploaded to a platform or server. These system assets have specific protection requirements.

In view of the above privacy protection and security evaluation requirements, the information entropy privacy grade formula is introduced to describe the information privacy level of the system and to evaluate it. This conclusion leads to the idea of sensor node characteristics, and is based on the analysis of the characteristics of each node to design the privacy protection strategy of the system.

Equipment and Analysis:-

In smart home, some sensor nodes have periodic silent time (that is, the node does not send packets outside that time), or has a cycle of active cycles. For example, the light sensor nodes and sound sensor node, the sound sensor node as an example, it can perceive the changes of user's voice, so when people voice activity is frequent, it will send more packets. Thus, when family members are talking or engaging in family activities, an active cycle occurs, and when a person is absent, a silent period of nature is reflected. If the data is stolen, it is easy for the thief to deduce whether someone is in the house. In this project, a feature removal strategy is designed to remove the

features of these nodes and generate false signals or packets during the silent period of the nodes. Furthermore, the time is taken as a seed to generate a random value that is included in the virtual packet as virtual data.

Establishment of privacy information protection model for Internet of things in smart home:-
This paper is research on Intelligent Home Furnishing networking privacy information protection model is applied to various research networking applications may leak user privacy threats against these threats continue to improve the model, complete the analysis and design of the main structure of the model. Taking the smart home environment as an example, this paper describes the specific process of the privacy protection model. Model implementation is shown as Figure 1.

Application of privacy information protection model of Internet of things for smart Home:-
This paper is research on network environment for intelligent Home Furnishing as an example, under the premise of ensuring the interaction of information communication smoothly under the protection of user privacy information better, to establish a user control center to protect their sensitive personal information, to avoid passing too direct interaction to send its important identity information, but also to avoid privacy protection model the information obtained by unrelated sensitive user information is not necessary, all kinds of interactive analysis in the network, the model can be widely applicable to the network environment of other application scenarios in the Internet of things.

This paper simulates the flow of the model with the example of smart home users ,using the daily running process of the smart home system. The overall model implementation such as Figure 1.

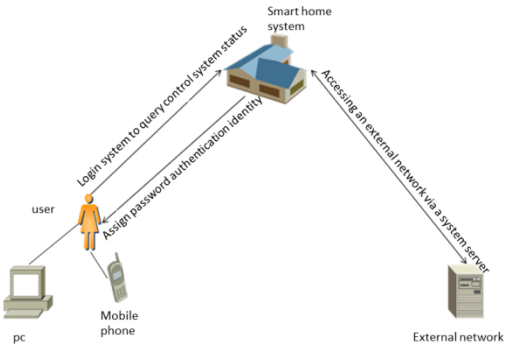

Figure 1:- Model implementation.

The main structure of the model is designed in the observation, control and management module of the smart home system. The observation module provides real-time monitoring data or images according to the user's application information. Real time monitoring data or images are displayed on the user's handheld or PC terminal. The user can remotely control the state of the home equipment. The user can also set personal preferences for the home system to facilitate management. For example, modifying home real time data reporting intervals, closing and opening security system time, or setting room temperature, etc.. The verification module verifies the observation request through the Internet Home Furnishing family intelligent system data information storage module and the applicant, the applicant's information for comparison, correct, then send the real-time monitoring information or data, or as illegal requests rejected. The main function of the module is the real-time inquiry and remote control of the smart home system through the smart phone or home PC. Using B/S structure, using the Internet of things, smart home members can apply smart home systems at any place and at any time through different terminals. It can also realize self-maintenance of client and reduce maintenance cost.

Smart home users need to login system to query the status of the home system, allowing users to login through a variety of terminals login home intelligent home system, real-time inquiry and operation system or change settings. Smart home users enter the system according to the system login name and initialization password. After login successfully, personal information can be searched, such as personal information, authorization operations, etc.. An authorized person logs into the system, and the system requires the user to enter the user ID and the key, thus verifying whether the user is the authorized user of the system. When authorized users for the system can identify archived users, then enter the system, set up personal information, and participate in system inquiries, operations and other activities. When the user is not authorized to log in to the system, allowing the first applicants fill in the

personal data, the system user information and user authorization list and compare the information for verification, if the user information from the family system administrator authorization or new application user information has been recorded in the system, the distribution of the new user password, allows the user to enter the system. If the login person enters an error password or input information for a non-family member, the user is denied access and sent an alert message to the home user. User A login home system real-time operation interface, you can see the home system operation module, the user A to set the temperature, humidity, lights, timing, open and other operations privacy preferences.

Intelligent Home furnishing system will weaken between user A and he needs service, to the maximum extent to meet the needs of the user privacy protection, based on the traditional attribute based access control model based on role based access control model, protect user privacy A. When the user A sets an electrical device on and off time, the system protects and replaces the privacy of the user's A. If users find landing home system is slower, you can determine whether there is malicious; third parties use the Internet to attack home service. home furnishing intelligent user login system, write personal privacy preferences, privacy protection module of the intelligent home furnishing system will make trust evaluation based on user trust model of family intelligent system of authorization, Home furnishing home furnishing intelligent monitoring points selected real-time monitoring information collection computing privacy information, according to the trust evaluation results, such as the judgment of users in the home or office network security etc. then, send the user the required system monitoring Home Furnishing real-time data, if the user judgment in the market or the airport is in network environment, can ensure network eavesdropping situation, then choose to replace the library information on selected collection of smart home furnishing real-time information for the replacement, to ensure the security of user privacy.

Conclusion:-

Although some research achievements have been made in the research of privacy protection for smart home, there are still many achievements to be improved because of my knowledge level and energy limit. Moreover, due to the continuous progress of related technologies, application scenarios facing network privacy protection technology is more complex, in these scenarios needs research on privacy protection mechanism and key technology is also more sensitive to urgent, such as multimedia sensor network application system of the privacy protection study. Data convergence reduces network power by reducing the amount of network traffic, but there is often a lot of energy overhead to protect data privacy. Therefore, the research needs to further explore the data fusion in the realization of the value of privacy protection and the energy consumption between the pros and cons of the balance between the two issues. At the same time, it is the focus of further research to study the data fusion privacy protection technology which satisfies different fusion functions. In short, user privacy protection networking issues will be the focus of the development of the networking industry, whether in theory or in the technical level, Internet privacy protection have a lot of problems need further study and discussion.

Acknowledgements:-

This research was supported by Public welfare science and technology project of Wenzhou in 2014(G20140035),Research on privacy protection technology based on Internet of things in smart home and General scientific research project of Wenzhou vocational and technical college in 2014(WZY2014030), Research and implementation of network privacy protection strategy for smart home.

References:-

1. Zhang Y, Chen X, Li J, et al. Ensuring attribute privacy protection and fast decryption for outsourced data security in mobile cloud computing. Information Sciences, 2016.
2. Yuan X, Peng S. A research on secure smart home based on the Internet of Things[C]// International Conference on Information Science and Technology. IEEE, 2012:737-740.
3. Park H, Park T, Son S H. A comparative study of privacy protection methods for smart home environments[J]. International Journal of Smart Home, 2013, 7.
4. He Y. Research on the development and tendency of smart home based on Internet of things[J]. Wireless Internet Technology, 2016.
5. Eschenauer L, Gligor V D. A key-management scheme for distributed sensor networks[C]. ACM, 2002.
6. Liu D, Ning P, Li R. Establishing pairwise keys in distributed sensor networks[J]. ACM Transactions on Information and System Security (TISSEC). 2005, 8(1): 41-77.

7. M. Shao, Y. Yang, S. Zhu and G. Cao, "Towards Statistically Strong Source Anonymity for Sensor Networks", Proceedings of the 27th Conference on Computer Communications, INFOCOM, IEEE, (2008), pp. 51-55.
8. Lao F, Li G X. Design and Realization of Gateway Node for the Smart Home System Based on Internet of Things. Advanced Materials Research, 2014, 912-914:1218-1221.
9. Li F, Wan Z, Xiong X, et al. Research on Sensor-Gateway-Terminal Security Mechanism of Smart Home Based on IOT. Communications in Computer & Information Science, 2012, 312:415-422.
10. K. Mehta and D. Liu, "Protecting Location Privacy in Sensor Networks against a Global Eavesdropper", IEEE Transactions on Mobile Computing, TMC, vol. 11, no. 2, IEEE, (2012), pp. 320-337.
11. Liu Z, Pan Y, Cao Q, et al. Security and Privacy Protection of Smart Home Based on IPv6. Atlantis Press, 2014.
12. Homin Park H, Basaran C, Park T, et al. Energy-Efficient Privacy Protection for Smart Home Environments Using Behavioral Semantics[J]. Sensors, 2014, 14(9):16235-16257.
13. Tian Y, Song B, Hassan M M, et al. The Distributed Pub-Sub System with Privacy Protection in Smart Home Environments[J]. International Journal on Information, vol.16(vol.16): 2013,pp.663-667.
14. Wu J, Liu J, Hu X S, et al. Privacy protection via appliance scheduling in smart homes[C]// International Conference on Computer-Aided Design. ACM, 2016:106.
15. Kabir M H, Hoque M R, Yang S H. Development of a smart home context-aware application: A machine learning based approach[J]. International Journal of Smart Home, 9(1):2015, 217-226.
16. Ni Q, Hernando A B G, Cruz I P D L. A Context-Aware System Infrastructure for Monitoring Activities of Daily Living in Smart Home[J]. Journal of Sensors, (2016-3-15), 2016, 2016:1-9.
17. Amiribesheli M, Benmansour A, Bouchachia A. A review of smart homes in healthcare[J]. Journal of Ambient Intelligence and Humanized Computing, 6(4): 2015, 495-517.
18. Chua S L, Marsland S, Guesgen H. A supervised learning approach for behaviour recognition in smart homes[J]. Journal of Ambient Intelligence & Smart Environments, 2016, 8(3):259-271.
19. Das B. Machine learning challenges for automated prompting in smart homes[J]. Dissertations & Theses - Gradworks, 2014.
20. Schweizer D, Zehnder M, Wache H, et al. Using Consumer Behavior Data to Reduce Energy Consumption in Smart Homes: Applying Machine Learning to Save Energy without Lowering Comfort of Inhabitants[C]// IEEE, International Conference on Machine Learning and Applications. IEEE, 2015:1123-1129.
21. Apthorpe N, Reisman D, Feamster N. A Smart Home is No Castle: Privacy Vulnerabilities of Encrypted IoT Traffic[J]. 2017.
22. Dorri A, Kanhere S S, Jurdak R, et al. Blockchain for IoT Security and Privacy: The Case Study of a Smart Home[C]// IEEE PERCOM WORKSHOP ON SECURITY PRIVACY AND TRUST IN THE INTERNET OF THING. IEEE, 2017.
23. Abrishamchi M A N, Abdullah A H, Cheok A D, et al. A probability based hybrid energy-efficient privacy preserving scheme to encounter with wireless traffic snooping in smart home[C]// Mobility Iot. 2016.
24. Yoon S, Park H, Yoo H S. Security Issues on Smarthome in IoT Environment[M]// Computer Science and its Applications. Springer Berlin Heidelberg, 2015.
25. Wang X, Zhang J, Schooler E M, et al. Performance evaluation of Attribute-Based Encryption: Toward data privacy in the IoT[C]// IEEE International Conference on Communications. IEEE, 2014:725-730.