Journal Homepage: -www.journalijar.com
INTERNATIONAL JOURNAL OF ADVANCED RESEARCH (IJAR)
Article DOI:10.21474/IJAR01/7839
DOI URL: http://dx.doi.org/10.21474/IJAR01/7839
ISSN NO. 2320-5407

RESEARCH ARTICLE

PRIVACY ISSUES IN SMART HOME DEVICES USING INTERNET OF THINGS – A SURVEY.

Dr. D. Usha and M. Bobby.
1. Assistant Professor,Department of Computer Science, Mother Teresa Women's University, Kodaikanal.
2. Research Scholar, Department of Computer Science, Sri Adi Chunchanagiri Women's College,Cumbum.

Manuscript Info

Manuscript History
Received: 8 August 2018
Final Accepted: 10 September 2018
Published: October 2018

Keywords:-
Internet of Things,Privacy,Smart Home

Abstract

With the use of smart sensor technology, any electronics devices or appliances can be designed to connect to internet.Most of the people thinks that life can be even better with new advancement in modern technology like IoT. Applying security in Internet of Things environments has been identified as one of the top hurdles for realizing the vision of smart, energy-efficient homes.The nature of smart homes unavoidably raises security and privacy concerns. As all the smart home appliances, industrial machinery, public sector services and many other devices all are connected to the Internet, a lot of information is available on it. This information is prone to attack by hackers.In this paper, we present a SURVEY of the privacy issues directed towards the smart home devices.

Introduction:-

Internet of Things

The internet of things (IoT) has been described as the infrastructure of the information society. All these "things" connect to the Internet via Wi-Fi and then "talk" to each other.It is the modern world network of device such as home appliances, vehicles, and other physical devices. These devices are interconnected over the network provided.They are embedded with required software, actuators, sensors, and network connectivity. Each of these devices are uniquely identified over the network and exchange data.IoT is an advanced automation and analytic system which exploits networking, sensing, big data, and artificial intelligence technology to deliver complete systems for a product or service. These systems allow greater transparency, control, and performance when applied to any industry or system.

IoT systems have applications across industries through their unique flexibility and ability to be suitable in any environment. They enhance data collection, automation, operations, and much more through smart devices and powerful enabling technology.

Traditionally, the ingredients necessary for IoT are sensors, Wi-Fi, and a control panel, which in the simplest of cases can be a smart phones or PC. The sensors pick up the information, the Wi-Fi transfers this information to a repository, while the control panel can respond when the data flag problems, either fixing them automatically, or the problems can be fixed manually.

Corresponding Author:- Dr.D.Usha.
Address:- Assistant Professor,Department of Computer Science, Mother Teresa Women's University, Kodaikanal.

In order to provide users with valuable output, the IoT architecture should guarantee the suitability and trustworthiness of the processed data. This is a major requirement of such systems in order to guarantee robustness and reliability at the service level and able to support security.

Smart Home Devices

Smart home is one in which the various electric and electronic appliances are wired up to a central computer control system so they can either be switched on and off at certain times or if certain events happen.Most homes already have a certain amount of "smartness" because many appliances already contain built-in sensors or electronic controllers.There are three broadly categorized components of an IoT automated house: hardware, software, and communication protocol. These three components are indispensable as each of these are crucial for building a smart home. Equipping the IoT network with right hardware ensures successful IoT prototype development. It will also help in coping with technological changes.It is crucial to select the right communication protocol. A well designed and tested protocol will help in avoiding performance bottlenecks and issues with device integration. Along with the communication protocol, another crucial component of the IoT network is the firmware.It would be very disastrous if private and confidential information is accessed by unauthorized intruders.With all of this IoT data being transmitted, the risk of losing privacy increases.Millions of devices interconnected and concerns over privacy increased more than ever. Data encryption is very much necessary for maintaining the privacy of the data that is shared over the internet.

Review of the Contributions:-

Freddy K Santoso, Nicholas C H Vunpresent an approach to incorporate strong security in deploying Internet of Things (IoT) for smart home system, together with due consideration given to user convenience in operating the system. The IoT smart home system runs on conventional Wi-Fi network implemented based on the AllJoyn framework, using an asymmetric Elliptic Curve Cryptography to perform the authentications during system operation. A Wi-Fi gateway is used as the center node of the system to perform the system initial configuration.It is then responsible for authenticating the communication between the IoT devices as well as providing a mean for the user to setup, access and control the system through an Android based mobile device running appropriate application program.

Noah Apthorpe, Dillon Reisman, Nick Feamste examine four IoT smart home devices (a Sense sleep monitor, a Nest Cam Indoor security camera, a WeMo switch, and an Amazon Echo) and find that their network traffic rates can reveal potentially sensitive user interactions even when the traffic is encrypted. These results indicate that a technological solution is needed to protect IoT device owner privacy, and that IoT-specific concerns must be considered in the ongoing policy debate around ISP data collection and usage.

Biljana L.Risteska StojkoskaKire V.Trivodaliev propose a holistic framework which incorporates different components from IoT architectures/frameworks proposed in the literature, in order to efficiently integrate smart home objects in a cloud-centric IoT based solution. We identify a smart home management model for the proposed framework and the main tasks that should be performed at each level. We additionally discuss practical design challenges with emphasis on data processing, as well as smart home communication protocols and their interoperability. We believe that the holistic framework ascertained in this paper can be used as a solid base for the future developers of Internet of Things based smart home solutions.

Tianyi Song,Ruinian Li,Bo Mei,Jiguo Yu,Xiuzhen Cheng propose an improved energy-efficient, secure, and privacy-preserving communication protocol for the (Smart Home Systems) SHSs. Data transmissions within the SHS are secured by a symmetric encryption scheme with secret keys being generated by chaotic systems. Meanwhile, They incorporate message authentication codes to our scheme to guarantee data integrity and authenticity. They also provided detailed security analysis and performance evaluation in comparison with their previous work in terms of computational complexity, memory cost, and communication overhead.

Huichen Lin andNeil W. Bergmann identifies key future requirements for trusted Smart Home systems. A gateway architecture is selected as the most appropriate for resource-constrained devices, and for high system availability. Two key technologies to assist system auto-management are identified. Firstly, support for system auto-configuration will enhance system security. Secondly, the automatic update of system software and firmware is needed to maintain ongoing secure system operation.

Dimitris GeneiatakisIoannis Kounelis,Ricardo Neisse set up the scene for a security and privacy threat analysis for a typical smart home architecture using off the shelf components. To do so, we employ a smart home IoT architecture that enables users to interact with it through various devices that support smart house management, and we analyze different scenarios to identify possible security and privacy issues for users.

Pawani PorambageMika Ylianttila Corinna Schmitt propose as members of the always-connected paradigm of the massive IoT world, people can scarcely control the disclosure of their personal information. The biggest challenge is to allow users to experience the best utilization of IoT-based products and services with the fewest privacy threats and failures. This article provides a holistic view of the challenges of and issues related to preserving IoT privacy, as well as the existing solutions. Privacy by design (PbD) is identified as the key solution for many IoT privacy issues.

Conclusion:-

Our conventional devices and appliances will get smarter, our lifestyle can be changed with modern technology.Smart home technology and the IoT will deliver the insight needed for people to live better lives—longer, healthier, and happier.Security and privacy at the device level, protecting the user and encrypting communication links are critical to the secure operations of IoT. Privacy principles dictate that users should be able to keep control of their data as well as to be able to opt out of the "smart" environment without incurring negative consequences.

References:-

1. R. Roman, P. Najera, J. Lopez, "Securing the Internet of Things,"*Computer* , vol.44, no.9, pp.51,58, Sept. 2011
2. Alcaide, A., Palomar, E., Montero-Castillo, J., & Ribagorda, A. (2013). "Anonymous authentication for privacy-preserving IOT target-driv-en applications." Computers & Security, 37, 111–123Al
3. Roberto Minerva, Abiy Biru, "Towards a Definition of the Internet of Things,"*IEEE IoT Initiative white paper.*
4. J. Liu, Y. Xiao, and C. L. P. Chen. "Authentication and Access Control in the Internet of Things," In *IEEE 32nd InternationalConference on Distributed Computing Systems Workshops*, June2012.
5. S. Raza, H. Shafagh, K. Hewage, R. Hummen, and T. Voigt, "Lithe: Lightweight Secure CoAP for the Internet of Things," in *IEEESensors Journal*, Vol. 13(10), 2013.
6. H. S. Ning, H. Liu; Y, L.T. "Cyberentity Security in the Internet of Things,"*Computer*, vol.46, no.4, pp.46,53, April 2013
7. Santoso, Freddy K., and Nicholas CH Vun. "Securing IoT for smart home system." In Consumer Electronics (ISCE), 2015 IEEE International Symposium on, pp. 1-2. IEEE, 2015.
8. Lindsay, Greg, Beau Woods, and Joshua Corman. Smart homes and the internet of things. Atlantic Council, 2016.
9. Brown, Eric. "Who needs the internet of things?." Linux. com. Retrieved 23 (2016).
10. Porambage, Pawani, Mika Ylianttila, Corinna Schmitt, Pardeep Kumar, Andrei Gurtov, and Athanasios V. Vasilakos. "The quest for privacy in the internet of things." IEEE Cloud Computing 2 (2016): 36-45.
11. Lin, Huichen, and Neil W. Bergmann. "IoT privacy and security challenges for smart home environments." Information 7, no. 3 (2016): 44.
12. Song, Tianyi, Ruinian Li, Bo Mei, Jiguo Yu, Xiaoshuang Xing, and Xiuzhen Cheng. "A privacy preserving communication protocol for IoT applications in smart homes." IEEE Internet of Things Journal 4, no. 6 (2017): 1844-1852.
13. Geneiatakis, Dimitris, Ioannis Kounelis, Ricardo Neisse, Igor Nai-Fovino, Gary Steri, and Gianmarco Baldini. "Security and privacy issues for an IoT based smart home." In Information and Communication Technology, Electronics and Microelectronics (MIPRO), 2017 40th International Convention on, pp. 1292-1297. IEEE, 2017.
14. Stojkoska, Biljana L. Risteska, and Kire V. Trivodaliev. "A review of Internet of Things for smart home: Challenges and solutions." Journal of Cleaner Production 140 (2017): 1454-1464.
15. Apthorpe, Noah, Dillon Reisman, and Nick Feamster. "A smart home is no castle: Privacy vulnerabilities of encrypted IoT traffic." arXiv preprint arXiv:1705.06805 (2017).
16. Yang, Heetae, Wonji Lee, and Hwansoo Lee. "IoT Smart Home Adoption: The Importance of Proper Level Automation." Journal of Sensors 2018 (2018).