2nd International Conference on Emerging Trends in Materials, Computing and Communication Technologies
International Journal of Scientific Research inScience, Engineering and Technology
Print ISSN: 2395-1990 | Online ISSN : 2394-4099 (www.ijsrset.com)

A Survey on IOT Security : Application Areas, Security Challenges, Privacy Preservation Methods

Meenakshiammal R[1], Dr.Bharathi R[2], Dr.P.Krishnakumar[3]

[1]Assistant Professor, Department of CSE, Rohini College of Engineering & Technology, Kanyakumari, Tamil Nadu, India

[2]Assistant Professor, Department of ECE, University College of Engineering, Nagercoil, Tamil Nadu, India

[3]Professor, Department of CSE, VV College of Engineering, Tisayanvilai, Tamil Nadu, India

ABSTRACT

Internet of things is ruling today's world. IoT refers to large network of networks which are able to connect smart devices. They are widely used in various applications like Smart City, Public Health, Waste Management etc. The main challenge with IoT architecture is misuse of personal and private information of customers. This paper provides a clear survey on existing privacy preserving approaches which are widely used in cloud computing environment and the shortcomings of applying same approaches in the context of IoT.

Key Words: IoT, Privacy preserving, Cloud Computing

I. INTRODUCTION

In our day to day life we have an enormous increase in the count of connected devices there by increasing a number of challenges. Challenges may vary from minor connectivity to major security. Hence we need to protect IoT network from various attacks. Resource limited nature of IoT devices further proves inefficiency in traditional security schemes and communication protocols.

The main application areas of IoT include Smart Homes, Smart grids, Smart Retail, Smart agriculture etc. Now a day devices are not only connected to the Internet and other local devices, they can also be able to communicate with other devices also. With the wide spread use of IoT in day to day life leads us to Security and privacy issues. Security and Privacy are the two main components in IoT services and applications.

II. APPLICATION AREAS

Security is most important factor in all IoT applications.

1. Smart Cities

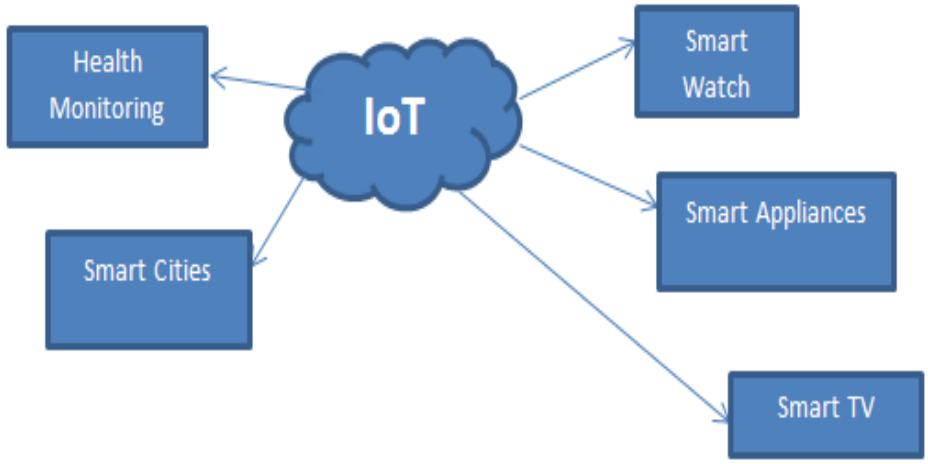
To improve the easiness and quality in life of people tends to the invention of Smart cities. It generally includes Smart traffic management, Smart homes, Smart utilities etc. Even Smart cities improves quality of life of people, it comes with the security challenge i.e a threat to the privacy of people. For example, Smart card services disclose card details and behaviour of customers in purchasing etc.

2. Smart Environment

It includes fire detection in forests, Snow level monitoring, Detection of earth quakes, Monitoring Pollution ets. These applications are directly influenced with people and animals. False positives and false negatives lead to wrong results in these applications.

3. Home Automation

It is one of the most widely used applications. It includes controlling of electrical appliances from remote places, Monitoring Systems etc. By comparing normal behaviour of users we can detect security breaches.



III. SECURITY CHALLENGES

The four layers of IoT application include sensing layer, network layer, middle ware layer and application layer. Each layer is vulnerable to various security threats.

Threats in IoT are different from Conventional threats in normal networks. IoT devices normally have limited memory and computing power. So we can't apply traditional security methods in IoT devices. IoT devices handles variety of data formats, so we can't use standard security protocol.

Data involved in IoT applications may be user's identity information, multimedia conversation or anything. If an unauthorized person access these information leads to violation of Confidentiality, Integrity, or availability. Confidentiality directly affects privacy.

Privacy attacks include Eavesdropping, Impersonation, Sniffing, Tampering, Data Leakage etc.

IV. PRIVACY PRESERVATION METHODS

In traditional networks only the users who are using the Internet are affected by privacy issues but in IoT environment whether the user is using the service or not, if he is present in that environment he will be affected by privacy issues. IoT environment must consider privacy of each and every individual in care and it must use collected personal data from various IoT devices only for its intended purpose. It must store data only when it is absolutely needed in future.

Proposed Solutions:

(i) Authentication and authorization
(ii) Edge computing and plug-in architectures
(iii) Data anonymization
(iv) Digital forgetting and data summarization

Authentication and Authorization

- Light weight cryptographic systems were proposed.
- Lee et al. [9] proposed secure key establishment. Here XOR based encryption method is used. Proposed system establishes mutual authentication procedure in a typical RFID system.
- Porambage et al. [10] propose authentication mechanism for WSNs using PAuth Key protocol

Edge computing and plug-in architectures

- Davies et al. [2] considers data privacy in IoT networks, following Geoffrey Moore's warning [3] about the discontinuity awaiting every new technology. In this work, a plug in mediator is introduced to overcome privacy issues. Data privacy controls are implemented in this architecture example Deletion, Inference, Anonymization etc.
- Langheinrich [4] proposes a privacy-aware system (pawS) to overcome the privacy concerns. It ensures data remains private during data collection. In this work users are notified about what type of data is collected and processed from their environment. So user is having direct control over data and actions. This system ensures privacy preserving in ubiquitous computing [5]. but, proximity, negotiation, and locality are not executed in this system.
- Bag¨u´es et al. [6] proposes a privacy preserving framework for smart homes. To preserve private data user centric approach is used here. Privacy policies are defined by user. Five components are used I this work to ensure privacy
- Seong et al. [7] proposed a decentralized architecture , where Cloud Butlers are used for personal data indexing. To provide privacy control they configured Butler for each user.
- To secure private data in augmented reality applications the system [8] used on device sensor abstractions

Privacy Preservation in IoT Device Layer.

- IoT device layer comprises all physical objects that are involved in data collection and control. Heterogeneity and limited resources nature of these objects introduces new challenges in use of privacy preserving techniques.
- Some of the attacks include DoS, Timing Attack, Replay Attack etc. So we must consider several security concerns in this layer.

(i) Access control and authentication: Used to prevent privacy issues arises because of open and unauthorized access.

Juels et al. [11] proposes a model that uses Selective RFID jamming. In inexpensive tags they have implemented this jamming to preserve privacy.

(ii) Data encryption: Used for secure data exchange and also ensures guaranteed delivery of data Wang [12] uses non linear key algorithm for data encryption. Advantage of this method is it utilizes low power to provide high security.

(iii) Secure channel using IPSec

(iv) Cryptography technology: Used for providing privacy protection. Digital Signatures and hash values are used for providing data integrity.

Privacy Preserving Machine Learning

- ML tasks involve 3 entities namely owner of the input, receiver of output and computation node. We have multiple threats in this. During transmission of data from owner to computation node we need encryption to preserve privacy.

PPML

- Privacy preserving machine learning simulates collaborative training of samples without releasing their private data in clear form
- PathumChamikara et al. [13] proposed PriModChain. To provide privacy it uses differential privacy and smart contracts.
- Francesco Restuccia et al [14] proposed a model that classifies security threats and the solutions in SDN using ML algorithms. Data Collection task comprises 3 main steps Authentication, Wireless Networking and Aggregation combined with validation.
- ShailaSharmeen et al [15] proposed a ML model. To train this model they have considered static, dynamic, hybrid features. The drawback of this method is it is limited to one application and can detect one type of threat.
- Kelton A.P. et al [16] reviewed papers from 2015-2018. Latest and traditional ML based algorithms were reviewed for Security & Privacy. It mainly focuses on IDS.
- Liang Xiao et al [17] reviewed threats to privacy. They concluded CNN & DNN as a solution for privacy protection. Drawback is this is limited to one application
- To train ML model, data acting as an important role. Hui Zhu et al [18] proposed eDiag that uses Kernel SVM to classify patient's data. At the same time it does not disclose private data. Previous methods used Homomorphic encryption.

- Qi Jing et al [19] classifies privacy problems in to 2 types. One is learning privacy problem and other is model privacy problem. They proposed OMPE model that does not use complicated encryption methods to protect learned model. Drawback is it concentrates on model privacy alone.
- Xindi Ma et al [20] proposed a cloud based DL model. It uses multiple keys. In their work data is given to cloud for training without knowing the real data by encryption. They proved PDLM preserves privacy when compared to traditional non-private schemes.

V. REFERENCES

[1]. V Hassija, V Chamola, V Saxena, D Jain, P Goyal… - IEEE …, 2019 A survey on IoT security: application areas, security threats, and solution architectures

[2]. N.Davies, N. Taft, M. Satyanarayanan, S. Clinch, and B. Amos, "Privacy mediators: Helping IoT cross the chasm," in Proceedings of the 17th International Workshop on Mobile Computing Systems and Applications, HotMobile 2016, pp. 39–44, USA, February 2016.

[3]. G. Moore, Crossing the Chasm, Harpercollins, 1991.

[4]. M. Langheinrich, "A Privacy Awareness System for Ubiquitous Computing Environments," inUbiComp 2002: UbiquitousComputing, vol. 2498 of Lecture Notes in Computer Science, pp. 237– 245, Springer Berlin Heidelberg, Berlin, Heidelberg, 2002.

[5]. M. Langheinrich, "Privacy by design-principles of privacyaware ubiquitous systems," in Proceedings of the Ubicomp 2001: Ubiquitous Computing, Lecture Notes in Computer Science, pp. 273–291, Springer, Berlin, Germany, 2001.

[6]. S. A. Bag¨u´es, A. Zeidler, F. Valdivielso, and I. R. Matias, "Sentry@Home - Leveraging the smart home for privacy in pervasive computing," International Journal of SmartHome, vol. 1, no. 2, pp. 129–146, 2007.

[7]. S.-W. Seong, J. Seo, M. Nasielski et al., "PrPl: A decentralized social networking infrastructure," in Proceedings of the 1st ACM Workshop on Mobile Cloud Computing and Services: Social Networks and Beyond, MCS'10, Co-located with ACM MobiSys 2010, USA, June 2010.

[8]. J. Vilk, D. Molnar, B. Livshits et al., "SurroundWeb:Mitigating Privacy Concerns in a 3D Web Browser," in Proceedings of the 2015 IEEE Symposiumon Security and Privacy (SP), pp. 431–446, San Jose, CA,May 2015.

[9]. J.-Y. Lee,W.-C. Lin, and Y.-H. Huang, "A lightweight authentication protocol for Internet ofThings," in Proceedings of the 3rd International Symposium on Next-Generation Electronics, ISNE 2014, Taiwan,May 2014.

[10]. P. Porambage, C. Schmitt, P. Kumar, A. Gurtov, and M. Ylianttila, "Pauthkey: a pervasive authentication protocol and key establishment scheme for wireless sensor networks in distributed IoT applications," International Journal of Distributed Sensor Networks, vol. 2014, Article ID 357430, 14 pages, 2014.

[11]. A. Juels, R. L. Rivest, andM. Szydlo, "The blocker tag: Selective blocking of RFID tags for consumer privacy," in Proceedings of the 10th ACM Conference on Computer and CommunicationsSecurity, CCS 2003, pp. 103–111, USA, October 2003.

[12]. X. Yi, Y. Liang, E. Huerta-Sanchez et al., "Sequencing of 50 human exomes reveals adaptation to high altitude," Science, vol.329, no. 5987, pp. 75–78, 2010.

[13]. PathumChamikaraMahawagaArachchige; Peter Bertok; Ibrahim Khalil A trustworthy privacy preserving framework for machine learning in industrial iot systemsPCM Arachchige, P Bertok, I Khalil… - IEEE Transactions …, 2020 - ieeexplore.ieee.org

[14]. Francesco Restuccia, Salvatore DrOro, and TommasoMelodia. 2018. Securing the Internet of Things in the Age of Machine Learning and Software-defined Networking. IEEE Internet of Things Journal 1, 1 (2018), 1–14

[15]. ShailaSharmeen, Shamsul Huda, Jemal H. Abawajy, Walaa Nagy Ismail, and Mohammad Mehedi Hassan. 2018. Malware Threats and Detection for Industrial Mobile-IoT Networks. IEEE Access 6 (2018), 15941–15957

[16]. Kelton A.P. da Costa, João P. Papa, Celso O. Lisboa, Roberto Munoz, and Victor Hugo C. de Albuquerque. 2019. Internet of Things: A survey on machine learning-based intrusion detection approaches. Computer Networks 151 (2019), 147–157. https://@doi.org/10.1016/j.comnet.2019.01.023

[17]. Liang Xiao, Donghua Jiang, DongjinXu, and Ning An. 2018. Secure Mobile Crowdsensing with Deep Learning. China Communications 15 (2018), 1–11. http://arxiv.org/abs/1801.07379

[18]. Hui Zhu, Xiaoxia Liu, Rongxing Lu, and Hui Li. 2017. Efficient and Privacy-Preserving Online Medical Prediagnosis Framework Using Nonlinear SVM. IEEE Jounral of Biomedical and Health Informatics 21, 3 (2017), 838–850.

[19]. Qi Jing, AthanasiosVasilakos, Jiafu Wan, Jingwei Lu, and DechaoQiu. 2014. Security of the Internet of Things: Perspectives and challenges. Wireless Networks 20 (11 2014), 2481–2501

[20]. Xindi Ma, Jianfeng Ma, Hui Li, Qi Jiang, and Sheng Gao. 2018. PDLM: Privacy-Preserving Deep Learning Model on Cloud with Multiple Keys. IEEE Transactions on Services Computing (2018), 1–13.