International Journal of Future Generation Communication and Networking
Vol. 13, No. 1, (2020), pp. 1550-1556

Overcoming Privacy and Security Challenges of Internet of Things Applications

Mohammed Imtyaz Ahmed[a], Dr. G Kannan[b]
[a]Ph.D Scholar, B.S. Abdur Rahman Crescent Institute of Science and Technology, ECE Dept, Chennai, India.,
[b]Associate Professor, B.S. Abdur Rahman Crescent Institute of Science and Technology, ECE Dept, Chennai, India.
mdimtyazahmed@gmail.com[a], kannan@crescent.education[b]

Abstract

Internet of Things (IoT) technology paves way for integration of anything with digital world. Radio Frequency Identification (RFID) tags and sensors play crucial role in realizing IoT which has potential use cases like smart home, smart city and healthcare. IoT bestows plenty of advantages like technology driven communication, connected infrastructure, productivity, connected people, connected transportation, automation and control besides saving time. Nevertheless, due to its heterogeneous nature in terms of protocols, devices and standards, IoT applications cause many privacy and security challenges. Its immaturity due to lack of global standards lead to security vulnerabilities. In this paper we investigate privacy and security challenges thrown by IoT integrated applications and possible countermeasures. We also identity issues that need further research in future.

Index Terms – Security issues, privacy issues, Internet of Things, IoT integration, security and privacy solutions

1. INTRODUCTION

IoT helps in integration of physical things (virtually anything) with digital world. In involves sensors, actuators, electronics, software and things identified uniquely with RFID. IoT connected devices are integrated with Internet through a gateway. With sensors embedded into IoT devices, it is possible to monitor environments and integrated IoT with various applications such as healthcare units, transportation systems, inventory management systems and so on [12], [18], [19]. IoT applications are growing faster. It is estimated that, according to International Data Corporation report, 41 billion IoT devices will be in operation by 2020 with market share of $8.9 trillion. The absence of human role is the main difference between IoT and Internet. IoT devices are meant for different applications. IoT services are manifold and users get benefited with IoT integration. For instance, patients can have remote health monitoring facility with IoT integrated with healthcare units. Quality of human life will get increased with IoT applications and the services they render. However, these benefits come for huge price when security and privacy issues are considered.

ISSN: 2233-7857 IJFGCN

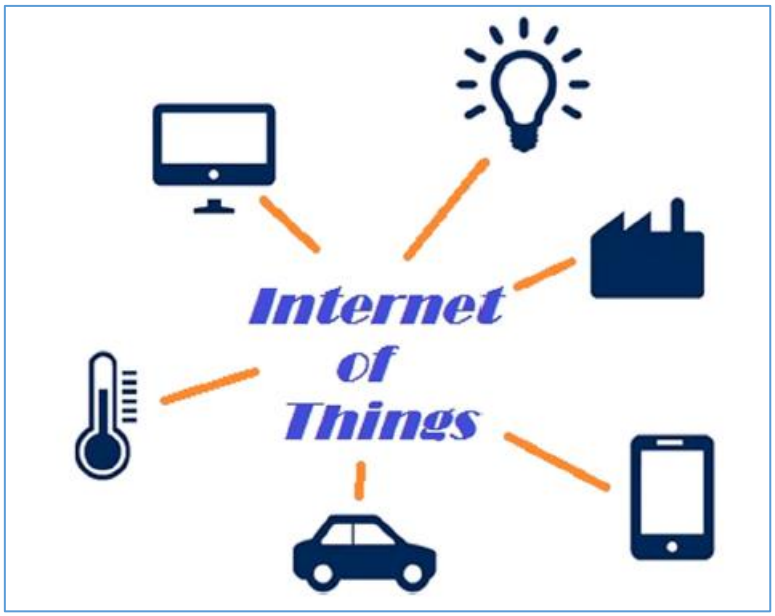

Figure 1: Overview of IoT

As studied in [2] and presented in Figure 1, IoT is used to have integration of digital and physical objects seamlessly for more intuitive environments. This actually shows technological innovation which brings ocean of possibilities. Nevertheless, IoT applications are prone to many security and privacy issues. Investigation into these aspects is very essential. The rest of the sections in this paper focused in security and privacy issues and countermeasures.

2. PRIVACY AND SECURITY CHALLENGES

The connected devices participating in any IoT use case might carry sensitive information. Disclosure of such information leads to potential risks. As IoT technology can be used to avail benefits in every field, it is essential to safeguard critical digital infrastructure from privacy and security attacks. The possible attacks are replay, man in the middle, black hole attack, sinkhole attack, Denial of Service, Distributed Denial of Service (DDoS), encryption attacks and

software attacks.

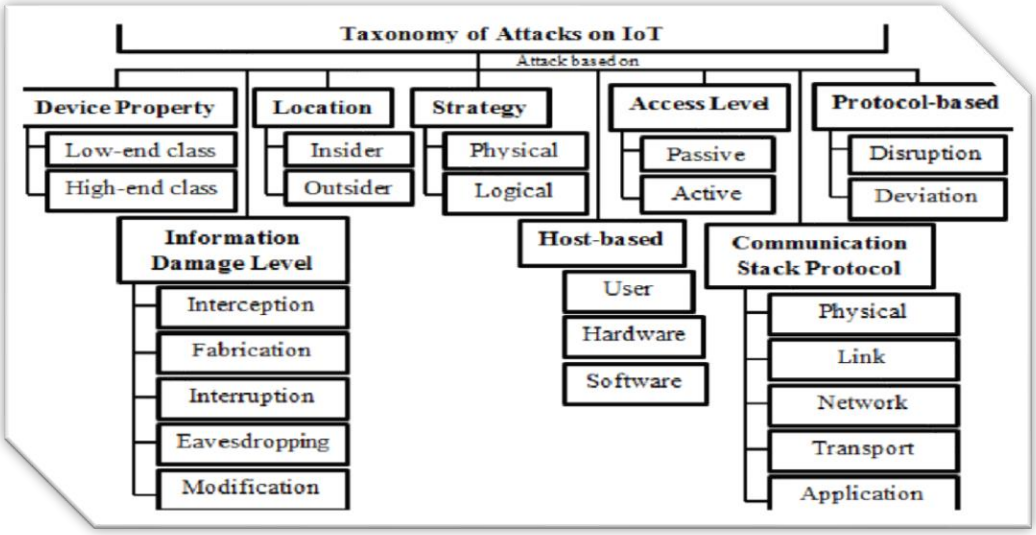

Figure 2: Taxonomy of security attacks on IoT use cases

Taxonomy of IoT is shown in Figure 2. As explored in [17], there are IoT attacks based on device property, protocol-based solution, access-level based ne, strategy, location and device property based. Khan and Salah [3] categorized security issues three groups namely low level, intermediate level and high level. The low level issues include jamming adversaries, sleep deprivation attack, insecure physical interface, low-level Sybil and spoofing attacks and insecure initialization. The intermediate level attacks include replay, RPL routing, insecure neighbour discovery, buffer reservation, sinkhole, wormhole, authentication, transport level security, session establishment and privacy violation. The high level issues include middleware security, insecure firmware, insecure interfaces and CoAP security

The privacy and security issues are investigated in [10]. They include device related issues like tamper resistant packages, headless nature and resource constraints; communication issues such as dynamic characteristics of devices and heterogeneous protocols; service issues like longevity expectation. Yang *et al*. [8] opined that RFID tag carries sensitive data and the disclosure of the same causes potential privacy risk. Privacy leakage while sensing data is another issue. Therefore, privacy in terms of data storage and trustworthy are desired features in IoT [9]. Data collection in IoT applications can lead to privacy leakage [11]. When RFID is used IoT applications are prone to privacy and security issues [12]. RFID enabled healthcare systems integrated with IoT can cause issues related to data security and privacy [13], [19].

3. SECURITY AND PRIVACY PROTECTION METHODS

This section provides privacy and security related methods for IoT. These methods can safeguard communications and also privacy of entities involved.

3.1 Constrained Application Protocol for IoT

The Constrained Application Protocol (CoAP) is a protocol which is used at application level of IoT applications. This protocol provides services to constrained devices. However, this protocol is investigated by Alghamdi *et al*. [14] and found that CoAP has its security limitations. The analysis is made with X.805 standard. The authors opined that these limitations can be overcome with IPSec and DTLS protocols.

3.2 RFID Based Authentication

RFID based authentication is possible in cases of smart applications for controlled access. Gope *et al*. [6] proposed an authentication scheme for both security and privacy. IoT devices and parities will have secure communications and the privacy of communications and devices will be preserved. It has features like secure localization, mutual authentication, privacy, anonymity, forward secrecy and untraceability. However, it does not protect compromised servers or forgery attacks and has no provision for physical security as well.

3.3 Signature Based Authenticated Key Establishment

Challa *et al*. [7] focused on signature based approach for authenticated key establishment for secure communications. They evaluated the scheme with BAN logic. The authentication process involves sensing device, gateway node and user. It has both password and biometric approach besides revocation of smart cared. It supports adding sensing devices dynamically on the fly and ensure secure key establishment. It was implemented in NS-2 simulator.

3.4 Biometric Authentication for Security in IoT Applications

Biometrics such as face, iris etc. have been playing role in many applications. In case of IoT applications, they can be used effectively. In [5], different biometric features are explored for security IoT application. They include physiological features like face, fingerprint, iris, palm print, hand geometry, DNA and hand veins. There are behavioural features like gait, signature, voice and keystroke. The summary of all the features are visualized in Figure 1.

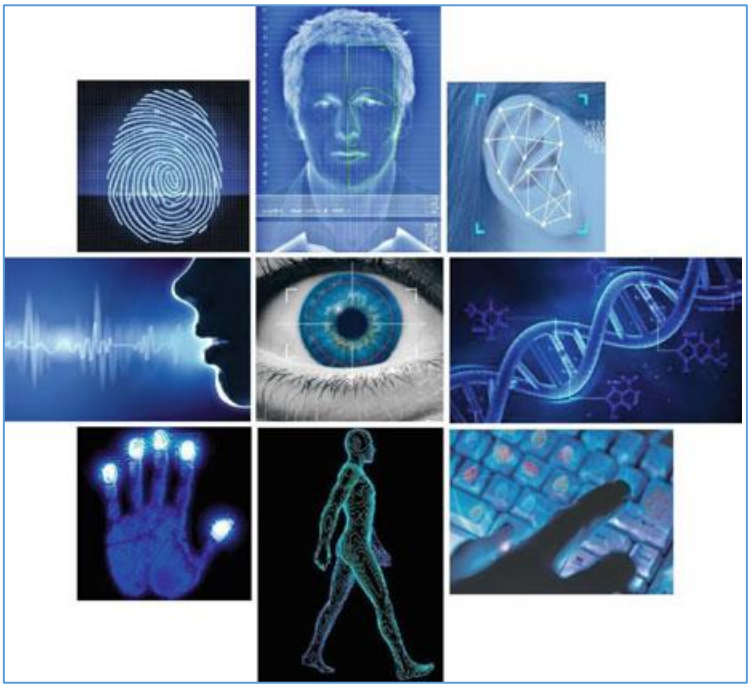

Figure 3: Physiological and behavioural categories of biometrics

Othman and Aydin [4] proposed a method for face recognition. It has many phases like face representation, feature extraction, feature comparison and classification. Face representation includes detection of face with AdaBoost classifier as explored in [16]. Towards feature extraction Local Binary Patterns (LBP) is used. For a pixel with (x, y) coordinates LBP is computed as in Eq. 1 where T denotes texture.

$$T \approx t\big(s(g_0 - g_c),,,,s(g_7 - g_c)\big) \quad (1)$$

Afterwards, the histogram of the face is denoted as LBP(x, y). It is computed as in Eq. 2 where various labels are denoted as *n*.

$$LBPH\ (i) = \sum_{x,y} I\{i, LBP\ (x,y)\},\ i = 0,,,n-1 \quad (2)$$

After this, classification is carried out. In the process face recognition is done based on histogram matching. It is computed as in Eq. 3.

$$d_{x^2}(M,S) = \sum_{i=1}^{B} \frac{(M_i - S_i)^2}{M_i + S_i} \quad (3)$$

Where M and S are histogram objects and each histogram has number of bins denoted as B. It is known as S and M model in order to have comparison of two faces for biometric authentication.

3.5 Secure Mutual Authentication

Mutual authentication is essential among connected components in IoT. Alshahrani and Traore [1] proposed such authentication scheme based on cumulative keyed-hash chain. For the purpose of identity assurance, they used fog computing which is known as edge computing that complements cloud computing. Between sender and receiver challenge and response mechanism is employed for identity. They evaluated protocol using Burrows-Abadi-Needham (BAN) approach. Smart home case study is considered for their empirical study using Cooja contika environment. When cloud is used for storage and processing, IoT can exploit it as well. Stergiou *et al*. [2] explored the approach in which IoT and cloud computing can be integrated.

3.6 Cloud Based RFID Authentication

As RFID became popular, it is widely used in IoT applications for identity and communications. It can be used to have mutual authentication. Xie *et al*. [15] proposed a scheme based on RFID with cloud integration. The scheme includes parities like mobile reader, fixed reader and cloud server. Encrypted Hash Table (EHT) is used to ensure that the confidentiality of the data is not lost. Virtual Private Network (VPN) technology is used between server and fixed reader for secure communications. The final parties included in the scheme are tag owner, verifier, VPN agency and cloud provider. This scheme needs further improvements to make it light weight.

4. CONCLUSION AND FUTUE WORK

In this paper, we investigated different aspects of privacy and security including the schemes available for protection of privacy and security communications in IoT use cases. Due to immature standards and lack of global standards, IoT has still many security and privacy issues. They are discussed in the paper and prevention methods found in the literature are provided. From the existing methods, it is understood that there are certain improvements needed and thus required further research. 1) RFID based authentication needs further investigation to ensure privacy preserving authentication with the assistance of cloud. 2) There is need for secure and lightweight privacy preserving IoT integration for remote patient monitoring as it has potential benefits. 3) Access control mechanisms in IoT applications like smart home can be improved with biometrics.

References

[1] Mohammed Alshahrani, Issa Traore. (2019). Secure mutual authentication and automated access control for IoT smart home using cumulative Keyed-hash chain. *JISA*. 1-20.

[2] Christos Stergiou, Kostas E. Psannis, Byung-Gyu Kim, Brij Gupta. (2016). Secure integration of IoT and Cloud Computing. *ELSEVIER*. 1-13.

[3] Minhaj Ahmad Khan, Khaled Salah. (2017). IoT security: Review, blockchain solutions, and open challenges. *ELSEVIER*. 1-17.

[4] Nashwan Adnan OTHMAN, Ilhan AYDIN. (2018). A Face Recognition Method in the Internet of Things for Security Applications in Smart Homes and Cities. *IEEE*. 1-5.

[5] Mohammad S. Obaidat, Soumya Prakash Rana, Tanmoy Maitra, Debasis Giri, and Subrata Dutta. (2019). Biometric Security and Internet of Things (IoT). *SPRINGER*. 1-33.

[6] Prosanta Gope, Ruhul Amin, S.K. Hafizul Islam, Neeraj Kumar, Vinod Kumar Bhalla. (2017). Lightweight and privacy-preserving RFID authentication scheme for distributed IoT infrastructure with secure localization services for smart city environment. *ELSEVIER*. 1-10.

[7] SRAVANI CHALLA, MOHAMMAD WAZID, ASHOK KUMAR DAS, NEERAJ KUMAR, ALAVALAPATI GOUTHAM REDDY, EUN-JUN YOON, KEE-YOUNG YOO. (2017). Secure Signature-Based Authenticated Key Establishment Scheme for Future IoT Applications. *IEEE*. 5, 1-16.

[8] Yuchen Yang, Longfei Wu, Guisheng Yin, Lijie Li, and Hongbin Zhao. (2016). A Survey on Security and Privacy Issues in Internet-of-Things. *IEEE INTERNET OF THINGS JOURNAL*. 1-10.

[9] Kuan Zhang, Jianbing Ni, Kan Yang, Xiaohui Liang, Ju Ren, and Xuemin (Sherman) Shen. (2017). Security and Privacy in Smart City Applications: Challenges and Solutions. *MCOM*. 1-8.

[10] Joseph Bugeja, Andreas Jacobsson, and Paul Davidsson. (2016). On Privacy and Security Challenges in Smart Connected Homes. *IEEE*. 1-4.

[11] Qi Jing, Athanasios V. Vasilakos, Jiafu Wan Jingwei Lu, Dechao Qiu. (2014). Security of the Internet of Things: perspectives and challenges. *SPRINGER*. 1-21.

[12] Nyoman Adhiarna, Yoon Min Hwangb, Min Jae Park, Jae Jeung Rho. (2013). An integrated framework for RFID adoption and diffusion with a stage-scale-scope cubicle model: A case of Indonesia. *IJIM*. 1-13.

[13] Samuel Fosso Wamba, Abhijith Anand, Lemuria Carter. (2013). A literature review of RFID-enabled healthcare applications and issues. *IJIM*. 1-18.

[14] Thamer A. Alghamdi, Aboubaker Lasebae, Mahdi Aiash. (2013). Security Analysis of the Constrained Application Protocol in the Internet of Things. *IEEE*. 1-7.

[15] Wei Xie, Lei Xie, Chen Zhang, Quan Zhang, Chaojing Tang. (2013). Cloud-based RFID Authentication. *IEEE*. 1-8.

[16] T. Hastie, S. Rosset, J. Zhu, H. Zou, "Multi-class adaboost," Statistics and its Interface, vol. *2*, pp. 349-360, January 2006.

[17] Nawir, M., Amir, A., Yaakob, N., & Lynn, O.B. (2016). Internet of Things (IoT): Taxonomy of security attacks. *2016 3rd International Conference on Electronic Design (ICED)*, 321-326.

[18] Imtyaz Ahmed and G. Kannan (2018). A Review on Present State-of-the-Art on Internet of Things, Journal of Advanced Research in Dynamical and Control Systems, p 352-358

[19] G Kannan and R.Mohamed Thameez (2015). Design and Implementation of Smart Sensor Interface for Herbal Monitoring in IoT Environment, International Journal of Engineering Research, p 469-475.

Biographical Notes

Mohammed Imtyaz Ahmed has 6+ years of experience in IT field as senior quality engineer in various MNC companies in India and he pursed Master of Technology in Telecommunication and software engineering from BITS Pilani, Rajasthan, India in 2015 as part of work integrated programme and Bachelor of Technology in Electronics and communication engineering from Jawaharlal Nehru Technical University, Hyderabad, India in year 2011. He is currently pursuing Ph.D in B.S. Abdur Rahman Crescent Institute of Science & Technology Chennai, India and currently working as senior quality engineer in Infosys, Hyderabad. His main research work focuses on Internet of Things (IoT), Wireless communication.

Dr.GKannan received Ph.D degree from Anna University Chennai, India, an M.Tech Embedded Systems from SASTRA University Thanjavur and B.E Electronics and Instrumentation Engineering from Bharadhidasan University Tiruchirappalli in 2014, 2005 and 2000 respectively. At present he is working as Associate Professor in the Department of Electronics and Communication Engineering of B.S.Abdur Rahman Crescent Institute of Science and Technology Chennai, India. His areas of research include Wireless Sensor Network, System level power management in Embedded systems and Real Time Operating Systems.

ISSN: 2233-7857 IJFGCN