ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 9, September 2016

A Study on Privacy and Security concerns in Internet of Things

Samiksha Ravindra Suryawanshi

Assistant Professor, Department of I.T., Karmaveer Bhaurao Patil College, Vashi, Mumbai, Maharashtra, India

ABSTRACT: Information Security, privacy and data protection are closely related and narrowly linked to each other due to the overlapping requirements. The promises made by Internet of Things materialize in our day to day lives so challenges in efficiency of current data privacy are very often as they support the pervasive components at play in IoT. The privacy and security concerns in IoT applications show themselves as threat to the end-user utility and also have negative impact in trust among end-users. The paper introduces some terminologies related to Internet of Things (IoT), which identifies and connects worldwide physical objects into a unified system. In IoT serious concerns are raised over access to personal information related to device and individual privacy. This paper presents a study report on the security and privacy concerns in Internet of Things.

KEYWORDS: Internet of Things; Privacy Protection; Security in IoT; Denial of Service; WSN; Threats

I. INTRODUCTION

With the advancement in Internet technology and communications technology, our everyday lives are led into an imaginary space of virtual world. People can chat, work, and go shopping, keeps pets and plants in the virtual world which is provided by the network. But, human beings live in a real world and perhaps human activities cannot be implemented with the help of services in the imaginary space. The limitation of imaginary space is that it restricts the development of Internet to provide better services. To overcome these constraints, a new technology is required that integrates imaginary space and real-world on a same platform called as Internet of Things (IoTs). Taking into consideration the large number of sensors and wireless communication, the sensor network technology puts up new demands to the Internet technology. This might bring huge changes to the future society, as it might change our way of life and business models. Apart from various benefits of IoTs, there are also several security and privacy concerns at different layers which are the Front end, Back end and Network. This paper surveys several privacy and security concerns related to Internet of Things (IoTs) by defining some open challenges.

II. RELATED WORK

In the recent attempts seen at establishing privacy and security frameworks for supporting trust management in pervasive systems, a comprehensive model that builds trust among the target users of these emerging technologies is yet to achieve wide acceptance [1]. Itani et al. [2] has described a set of security protocols in cloud computing scenario that safeguard privacy and compliance of end-user data. Yau et al. [3] discussed at performance and security tradeoffs in SOA. The Ponemon Institute [4] has shared an insightful research report detailing the proactive steps for protecting sensitive information in the cloud.

Numerous studies have put forward the privacy and security frameworks for protecting data in specific domains like mobile health monitoring [5], self-improving smart spaces [6], location privacy in mobile computing [7], privacy protection in web services [8], privacy enhancement in platform as a service in cloud computing scenarios [9], and more. This can challenge the trend by proposing a holistic view to the problem throwing light on protecting the privacy and security of end-user data while promoting trust in new and old technology solutions that are willing to adopt these standards.

Cloud Computingreference architecture has been proposed by NIST [10] and Itani et al. [2] have explored a reference framework for privacy in cloud computing scenarios. Studies have focused on legal compliance and the

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 9, September 2016

technical implementation of trust models, frameworks and protocols. Langheinrich [11] addressed key privacy concerns in ubiquitous systems.

Recent studies in this domain can be categorized as either high-level frameworks (with a focus on legal compliance and risk assessments) or low-level frameworks (with a focus on technical implementation of access controls to data). Neither of these approaches offers a solution.

III. CONNECTIVITY TECHNOLOGIES AND INTERACTION AMONGST INTERNET OF THINGS (IOT) DEVICES

The main objective of Internet of Things is to allow automatic exchange of information between two systems without any manual input. The automatedinformation exchange between two devices can take placethrough some of the following specific communication technologies,

A. *WIRELESS SENSOR NETWORKS (WSN)*

As described in [12], WSN comprise of independent nodes whose wireless communication takesplace over a limited range of frequency and bandwidth. The following are parts of communicating nodes of a typical wireless sensor network:

i. Microcontroller
ii. Memory
iii. Sensor
iv. Battery
v. Radio Transceiver

As the communication range of each sensor node of WSN is limited, multi-hop relay of information is seen between the source and the base station. The wireless sensors collect the required data with the help of collaborationamongst the various nodes, and then this collected information is sent to the sinknode from where it is directed to routing towards the base station. Thecommunication network which is formed dynamically by the use ofwireless radio transceivers allows data transmission between nodes. Multi-hop transmission of data requires different nodes to take diverse traffic loads [13].

B. *RADIO FREQUENCY IDENTIFICATION (RFID)*

RFID technology is used in information tags interactingwith each other automatically. In RFID radiofrequency waves are used for interacting and exchanging information between one another. It does not require alignment inthe same line of sight or physical contact. Thewireless technology of Automatic Identification and Data Capture (AIDC) [14] is used. A RFID is made up of the following two components [13]:

i. RFID tags (Transponders)

An antenna is embedded in a microchip which is seen a RFID tag. The RFID tag consists of memory units, these units houses aunique identifier known as Electronic Product Code (EPC).The main function of the EPC in each tag is providing a universalnumerical data. By this data a particular tag is recognizeduniversally.As per the classification in [13], the following are the types of RFID tags:

i. Active tag: An internal battery is housed in this type of tag,which facilitates the interaction among unique EPC with itssurrounding EPCs remotely from a limited distance.
ii. Passive tag: This tag consists of the information relayof its EPC which occurs only by its activation by a transceiver which should come under a pre-defined range of the tag. Due to the lack of an internalbattery in the passive tags, it is substituted by its utilization ofthe electromagnetic signal emitted by a tag reader throughinductive coupling as a source of energy.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 9, September 2016

A RFID tag and tag reader operate in conjunction with each other, the EPC of the RFID tag is the identifying signature of aparticular tag under the scan of the latter.

ii. RFID readers (Transceivers)

When the EPC of the tag under its scan, the RFID reader functions as the identification detector of each tag by its interaction with EPC of the tag.

IV. PRIVACY AND SECURITY CONCERNS IN IOTS

A. *SECURITY CONCERNS SEEN IN IOTS*

Internet of Things actually is a virtual network of real world systems and real-time interactions amongst them. The M2M (Machine to Machine) is the initial stage in development of IoT. It has unique characteristics, deployment contexts and subscription. In IoT unattended operation without human intervention is possible by the wireless area network (WAN) or WLAN. However by providing improvements in social efficiency it creates an array of new problems which are concerned with the breach of privacy and that information security [15].

i. *Front-end Sensors and Equipment*

The data is received by the front-end sensors and equipment via the built-in sensors. Then they transmit the data using modules or M2M device, which helps in achieving networking services of multiple sensors. This methodology comprises of the security of machines along with business implementation and node connectivity [15].

The Perception Nodes or machines are mostly distributed in the absence of monitoring scenarios. An intruder can have easy access to these devices which lead to damage or illegal actions on these nodes. Possible threats are analysed and threats are categorized as unauthorized access to data, or threats to the Internet and denial of service attack.

ii. *Network*

In IoT, network plays an important role in providing a comprehensive interconnection capability, effectualness and thriftiness of connection. It also provides authentic quality of service. Since a large number of machines sending data leads to network congestion, as large number of nodes and groups exist in IoTsthis may be resulted in denial of service attacks.

iii. *Back-end of it systems*

Back-end IT systems are the gateway, middleware, they have high security requirements and gathering, examining sensor data in real time or pseudo real-time which helps in increasing business intelligence. The security of IoT system has seven major standards they are as follows; privacy protection, access control, user authentication, communication layer security, data integrity, data confidentiality and availability at any time.

B. *PRIVACY CONCERNS SEEN IN IOTS*

Privacy is the right of entity acting in its own behalf, to determine the degree to which it will interact with its environment, comprising of the degree to which the entity is willing to share information about itself and with others, as defined in the Internet security glossary [16].

The environment is sensed by connected devices in IoTs. Then the gathered information and particular events are broadcasted to the server which carries out the application logic. This is performed by Mobile or/and fixed communication.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 9, September 2016

Privacy should be protected in the device, in storage during communication and also at processing which discloses the sensitive information [17].The privacy of end users and their data protection are the important challenges which need to be addressed in the IoTs.

i. Privacy in Device

While working with devices the sensitive information may be leaked out in case of unauthorized manipulation or handling of hardware and software in these devices. For example, an intruder can re-program a surveillance camera and it could send data not only to the legitimate server, but also to the intruder. Therefore, data robustness and tamper-resistance is essential in the devices that gather sensitive data. TheIoTs security can be ensured by trusted computing technologies like device integrity validations, tamper-resistant modules and trusted execution environments.

In order to provide the privacy in the devices, there exist numerous problems which are needed to be addressed. The problem may include the location privacy of the device holder, non-identifiability means protecting the identification of the exact nature of the device, protecting the personal information in case of the device theft or loss and resilience to side channel attacks. Location Privacy in Wireless Sensor Networks is achieved by using the algorithm Multi-Routing Random walk [18] in the wireless sensors, in the case of the Protecting of display privacy and Protection of personal Identifiable Information(PII) in case of device loss, theft could be achieved by having QR codes(Quick Response Code) technique [19] were selected.

ii. Privacy during Communication

During the transmission of the data to assure data confidentiality, the most common approach is encryption. In encryption data to packets are added which provides a way for tracing, e.g. sequence number, IPsec-SecurityParameterIndex, etc. These data can be used for linking packets to the analysis of same flow traffic. Secure Communication Protocol can be the suitable approach [20].

During the communication if in case it is not feasible to the device's identity or user's identity in order to decrease the vulnerability then Pseudonyms can be replaced in this case. One of the examples is Temporary Mobile Subscriber Identity (TMSI). Devices should communicate if and only if when there is a need, to deviate from the privacy disclosure induced by communication. In 3GPP machine type communicationsafter a certain period of inactivity in the devices will detach them from the network. This helps to avoid unnecessary collection of location information by the network.

iii. Privacy in Storage

Following principals should be considered while protecting privacy of information storage:

- Only the least possible amount of information should be stored that is needed.
- In case of mandatory then only personal information retained.
- Information is brought out on the basis of "need-to-know".

Pseudonymization and Anonymization could be used to conceal the real identity tied with the stored data. It makes possible that without disclosing any specific record, a database could allow access only to statistical data (sum, average, count, etc.). To ensure the output typically aggregate queries, it is independent of the absence or presence of a particular record which adds noise called as differential privacy [21] could be the appropriate technique.

iv. Privacy at Processing

It is consisting mainly of two folds. Firstly, personal data must be treated in a way that it should be compatible with the intended purpose. Secondly, without the explicit acceptance and the knowledge of the data owner, their personal data should not be disclosed to third parties or retained by third parties.

By considering the above two points, Digital Rights Management (DRM) systems [22] is most compatible. It controls the consumption of commercial media and defends against re-distribution illegally. One can define privacy

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 9, September 2016

policies for personal data in a rights object or license instead of exercising principles for commercial media which must be obeyed during the data processing. DRM requires trusted devices, secure devices to work efficiently and effectively.

User's permission and their awareness are requirements for distribution of personal data. User notification aids to avoids abuse

V. CONCLUSION

The IoT technology draws huge changes in everyone's everyday life. In the IoTs era, the short-range mobile transceivers will be implanted in variety of daily requirements. The connections between people and communications of people will grow and between objects to objects at any time, in any location. The efficiency of information management and communications will arise to a new high level. The dynamic environment of IoTs introduces unseen opportunities for communication, which are going to change the perception of computing and networking. The privacy and security implications of such an evolution should be carefully considered to the promising technology. The protection of data and privacy of users is identified as one of the key challenges in the IoT.

This survey presented Internet of Things with various security and privacy concerns. This paperalso surveyed security and privacy concerns at different layers in IoTs. In addition, identification of several open issues related to the security and privacy that need to be addressed by research community to make a secure and trusted platform for the delivery of future Internet of Things is the need.

REFERENCES

1. Siragelidin, B. Baharudin, L. T. Jung, "Hybrid scheme for trust management in pervasive computing," Information Retrieval & Knowledge Management (CAMP), 2012 International Conference on, pp. 45-49, March 2012.
2. W. Itani, A. Kayssim, A. Chehab, "Privacy as a Service: Privacy-Aware Data Storage and Processing in Cloud Computing Architectures," DASC '09 Proceedings of the 2009 Eighth IEEE International Conference on Dependable, Autonomic and Secure Computing, pp. 711-716, 2009.
3. S. S. Yau, Y. Yin, H. G. An, "An Adaptive Approach to Optimizing Tradeoff between Service Performance and Security in Service-based Systems," International Journal of Web Services Research, vol. 8, no. 2, pp. 74-91, 2011.
4. Ponemon Institute, Microsoft, "Achieving Data Privacy in the Cloud: United States," Microsoft – Trustworthy Computing: Cloud Privacy, pp. 1-16, 2012.
5. H. Lin, J. Shao, C. Zhang, Y. Fang, "CAM: Cloud-Assisted Privacy Preserving Mobile Health Monitoring," Information Forensics and Security, IEEE Transactions on, vol. 8, no. 6, pp. 985-997, June 2013.
6. N. Liampotis, I. Roussaki, E. Papadopoulou, Y. Abu-Shaaban, M. H. Williams, N. K. Taylor, S. M. McBurney, K. Dolinar, "A Privacy Framework for Personal Self-Improving Smart Spaces," Computational Science and Engineering, 2009. International Conference, vol. 3, pp. 444-449, 29-31, 2009.
7. K. Maekawa, Y. Okabe, "An Enhanced Location Privacy Framework with Mobility Using Host Identity Protocol," Applications and the Internet, SAINT '09. Ninth Annual International Symposium on, pp. 23-29, 20-24, 2009.
8. G. O. Yee, "A Privacy Controller Approach for Privacy Protection in Web Services," In Proceedings of the ACM Workshop on Secure Web Services, pages 44-51, 2007.
9. G. Zhao, Z. Li, W. Li, H. Zhang, Y. Tang, "Privacy Enhancing Framework on PaaS," Cloud and Service Computing (CSC), 2012 International Conference on, pp.131-137, 22-24, Nov. 2012.
10. National Institute of Standards and Technology, "NIST Cloud Computing Standards Roadmap," NIST - US Department of Commerce, 2013.
11. M. Langheinrich, "Privacy in Ubiquitous Computing," Chapman & Hall / CRC Press, pp. 1-44, 2009.
12. Akyildiz, I.F. ; Georgia Inst. of Technol., Atlanta, GA,USA ; Weilian Su ; Sankarasubramaniam, Y. ; Cayirci,E "A survey on sensor networks." Communicationsmagazine, IEEE 40.8 (2002): 102-114.
13. Shen, Guicheng, and Bingwu Liu. "The visions,technologies, applications and security issues ofInternet of Things." E-Business and E Government(ICEE), 2011 International Conference on. IEEE,2011.
14. Khoo, Benjamin. "RFID as an enabler of the internet ofthings: issues of security and privacy." Internet ofThings (iThings/CPSCom), 2011 InternationalConference on and 4th International Conference onCyber, Physical and Social Computing. IEEE, 2011.
15. D. Jiang, and C. ShiWei, "A Study of Information Security for M2M of IoT," 3rd International Conference on Advanced Computer Theory and Engineering (ICACTE), 2010, pp. 576-579.
16. RFC 2828, "Internet Security Glossary," May 2000.
17. Y. Cheng, M. Naslund, G. Selander, and E. Fogelström, "Privacy in Machine-to-Machine Communications: A state-of-the-art survey," International Conference onCommunication Systems (ICCS),Proceedings of IEEE, 2012, pp. 75-79.
18. L. Zhou, Q. Wen, and H. Zhang. "Preserving Sensor Location Privacy in Internet of Things." In Computational and Information Sciences (ICCIS), proceedings of IEEE, 2012, pp. 856-859.
19. Tepekule, U. Yavuz, and A. E. Pusane, "Modern KodlamaTekniklerinin QR KodUygulamalarınaYatkınlıg, " On the Use of Modern Coding Techniques in QR Applications.", Proceedings of IEEE, 2013. pp.1-4.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 9, September 2016

20. M.Giannikos, K. Korina, N. Fotiou, G. F. Marias and G. C. Polyzos, "Towards secure and context-aware information lookup for the Internet of Things." In Computing, Networking and Communications (ICNC,) Proceedings of IEEE , 2013, pp. 632-636.
21. R. Hall, A. Rinaldo, and L. Wasserman, "Differential Privacy for Functions and Functional Data," Journal of Machine Learning Research, 2013, pp.703-727.
22. E. Liu, Z. Liu, and F. Shao, "Digital Rights Management and Access Control in Multimedia Social Networks" In Genetic and Evolutionary Computing, Springer International Publishing, 2014,pp.257-266.

BIOGRAPHY

Samiksha Ravindra Suryawanshi is Assistant Professor in Department of Information Technology, Karmaveer Bhaurao Patil College of Arts, Science and Commerce, Vashi, Mumbai, MS, India. She received M.Sc. (Information Technology) degree in 2011 from University of Mumbai, Mumbai, MS, India.She has qualified National Eligibility Test (NET) for lectureship conducted by University Grants Commission, India. Her research interests are Artificial Intelligence, Computer Networks, Pattern Recognition, Cloud Computing, and Internet Technologies.