



Security Challenges in Internet of Things (IoT)

Bhaskr Mondal[#], Dilip Kumar[#], Tarni Mandal^{*}
[#]Department of Computer Science and Engineering
^{*}Department of Mathematics
National Institute of Technology Jamshedpur
Jamshedpur, Jharkhand
INDIA- 831014

Abstract: With the mounting prominence of the internet, secure transmission of information is crucial. The paper primarily focuses on recent research trends in security and privacy of Internet of Things (IoT). The benefits IoT has delivered is immense but at the cost of data security. Characteristics, architecture and limitations of IoT has been conferred for improved understanding for the readers. Security, privacy and trust has become a serious matter of concern with the increasing number of IoT. The authors have also addressed a numbers of security challenges in IoT like encryption, key distribution, PKI, trust, etc.

Keywords: Security, Internet of Things, Trust management, WSN

I. Introduction

We can see the history in short. From the year 1969 to 1995, the Internet was for boffins. From 1995 to 2000, it was available and useable only for the geeks. After 2000 it became popular on wire medium and in the year 2008, it was a trained of cyber cafes. Between the years 2007 to 2011, it became mobile and available on the mobile devices through the ISP. After 2012, it becomes available on all other devices like car, wearable devices, health care devices, smart electric grids and house-hold appliances. Originally, Moores Law described the number of transistors that can fit on an integrated circuit, which doubles approximately every 18 months. Now, a team of researchers from China has discovered that Moores Law can also describe the growth of the Internet. In a recent study, the researchers have predicted that the Internet will double in size every 5.32 years. That finding is one of several results from the study published by Guo- Qing Zhang, et al. [29], in an article of the New Journal of Physics. The researchers investigated the evolution of large-scale Internet topology, or how the Internet is structured and connected. Based on routing data of six-month intervals from December 2001 to December 2006, the researchers predicted not only the Internet's exponential growth rate which follows Moores Law, but also more specifically how the Internet evolves. Over 50 billion devices will be conned to the Internet by 2020 including vehicles, environmental sensors, and wearable sensors of BAN. All the devices must have a location by which everything going to be traceable. Smart-phones, voice-capable tablets, connected vehicles, intelligent traffic lights, smart electric grids, security systems, even thermostats of refrigerators, health monitoring devices are connected to the Internet. Most of the devices work based on location [25]. In acceleration of good governance agencies may use data fed from various sensors like grids and environmental sensors, etc. The IoT involves the broad area of embedded systems, MEMS, Cloud computing, wireless Ad-Hoc and sensor network, human computer interaction, control systems, big-data and the most important security and privacy. In other way we can define IoT as communication with anything (device) at any time and at any place. It means that things embedded with Internet connectivity can be controlled through Internet at any time regardless of day or night or during traveling at any place ubiquitously.

A. The characteristics of IoT

Event driven: The communication and action by the nodes will be event driven. An event is some signal detected by a signal like receiving data from other node or some environmental change.

Ambient Intelligence: The device should be able to resist itself from the unwanted signals or phenomena and may mobile in nature. It may save energy and recharge itself depending on the ambient condition.

Flexible Structure: It should be communicable with other nodes and the protocols should be flexible to update.

Semantic Sharing: Share information wisely with authenticated nodes. It should detect harmful nodes. Devices must communicate with each other. Device data must be shared with the server. Servers have to be share the device data.

Complex access technology: Access technologies are complex due to limited resources and low bandwidth. It uses technology like WiFi, 3G, 4G, BT, ZigBee, 6LoWPAN, NFC, DSRC etc.

B. Network architecture of IoT

The architecture of IoT is highly heterogeneous, hyper connected network. The devices (Things) on the network are of different make and configuration. Yet it needs to identify each thing uniquely. The thing connected to the network may be with IP or without IPs. A representation of IoT network architecture is shown in figure 1.

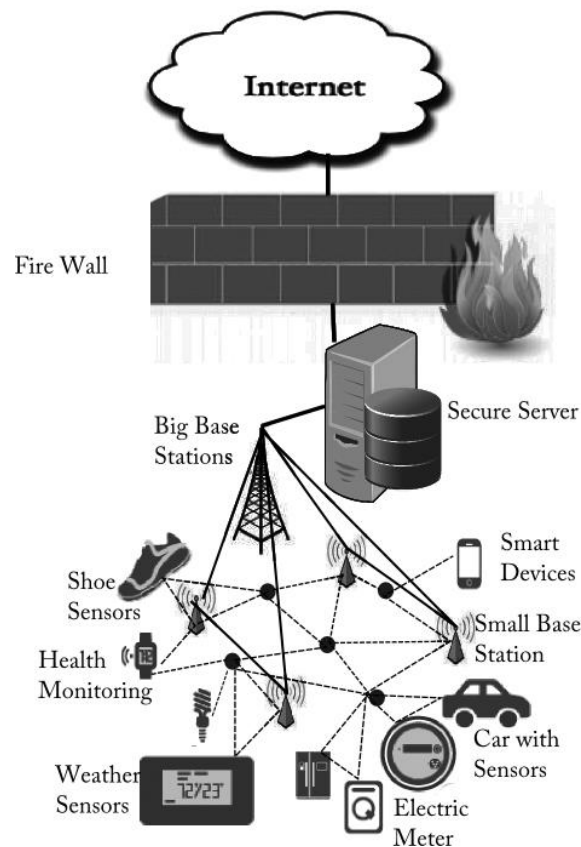


Figure 1: A representation of IoT network architecture

C. Limitations of IoT

There are lots of limitations and resource constraints of IoT devices [23]. The limitations are low processing power, less physical memory, special location, mobility, sustainability in changing weather conditions, rechargability, etc. Magno et al. 2014 discussed proposed a model for survivability of resource-intensive sensor networks through ultra-low power overlays [13].

Name	data size (e.g., RAM)	code size (e.g., Flash)
Class 0, C0	<< 10KiB	<< 100KiB
Class 1, C1	~10KiB	~100KiB
Class 2, C2	~50KiB	~250KiB

Table 1: Classes of Constrained Devices (KiB = 1024bytes)

Energy: Merlo et al. 2015 [14] has discussed in details regarding energy efficient security. Further study on optimization of energy [10, 11] consumption may be done.

Location:

Mobility: Effective Key Management in Dynamic Wireless Sensor Networks [24] [2]. Therefore, it can be observed that cryptographic [18], stenographic [19, 16] and secret sharing [17, 20, 15] algorithms designed for Internet communication will not work efficiently on the IoT. Even some light weight [9] algorithms are being proposed. In the next section the security challenges are discussed followed by comparative study of security solutions and finally the conclusion and future scopes are discussed.

II. Why Security for IoT

As the IoT nodes are of low storage, less computation power, low communication speed and heterogeneous in nature it demands light weight, smooth data access control, scalable, flexible, forward and backward secrecy, integrity and confidentiality in the security algorithms [7]. The features are discussed below:

Lightweight: Often consists of low-end sensor nodes, which rely on battery energy [12]. There self-recharging becomes a challenge and lightweight security algorithms are become a demand for IoT devices. [27]. To match the low capabilities of the IoT nodes, it is important to minimize computation, communication, and storage overhead on the IoT. Hence, cryptographic algorithms must be as fast as possible in order to satisfy these requirements and be invulnerable to DoS attacks.

Fine-grained data access control: Data access control is another issue for IoT. Due to limited resources and computing power it becomes a challenge to add extra computation load for detecting trusted and authenticated node. Data delivery and receive to authentic node must be assured.

Scalability: The system should sustain in the large network of heterogeneous nodes.

Flexibility: The system should work dynamically, such as time, location, or certain events related to patients. In IoT, the access policy should be defined by both communicating nodes.

Confidentiality: In order to prevent the disclosure of secret data, the data need to always be kept confidential at a node or local server. Data confidentiality should be resistant to device compromise attacks and controller compromised attacks). That is, compromising one node helps the adversary to gain nothing or little from the data stored at that node.

Data integrity: In IoT, the data collected by different nodes are important and secret. For e.g. a wrong location (tempered by third party) may lead a military operation to failure or make mess in smart city.

Forward and Backward secrecy: It means that even if an adversary obtains the current secrets of a node, it cannot decrypt (or forge authentication tags for) those data collected and encrypted (or authenticated) before compromise and Backward secrecy means that even an adversary has compromised (and then released) a node, it cannot decrypt (or forge authentication tags for) those data collected and encrypted (or authenticated) by the node after releasing.

Strong contextual privacy preservation: Privacy in IoT can be divided into two type i.e. content-oriented privacy and contextual privacy. Contextual privacy means an adversary has the ability to link the source and the destination of a message.

III. SECURITY CHALLENGES

A. Data Aggregation Integrity

Clustering is used where each node sends data to the cluster-head and the received raw data undergoes aggregation which is then sent to the sink. These aggregation functions involve lot of energy wastages [6]. In the aggregation process some nodes may contribute false data to attract the system. [22] proposes a lightweight verification algorithm by which the base station can determine if the computed aggregate (predicate Count or Sum) includes any false contribution.

B. Adversary model and Key Management

In dynamic environment, the efficient key updates when a node leaves or joins a cluster is most important need for IoT. Further ensuring forward and backward key secrecy and efficient key revocation for compromised nodes and minimization of impact of a compromised node on the security of other communication links are other security issues in key management in hierarchical heterogeneous. Seo2015 proposes a certificate less -effective key management protocol for secure communication in dynamic WSNs characterized by node mobility. Zho and his team proposed an efficient key management scheme for body sensor networks.

C. Trust Model

Trust is an abstract concept that can shield concrete structure, and can provide uniform decision-making for heterogeneous and multi domain IoT. Therefore, trust management is considered as a potential solution to IoT-related issues. Most important issues are uncertainty in connections as the nodes are dynamic and mobile, flexibility, efficiency in establishment of trusted connection in heterogeneous network and different security mechanism.

D. Location-based mobile attack

[25] personal privacy, privacy preservation (Centralized privacy preserving architecture, Distributed privacy-preserving architecture, Privacy preservation in road networks, Privacy preservation for snapshot location-based queries, Privacy preservation for continuous location-based queries, PIR based privacy preservation,)
Homogeneity attack: Homogeneity of sensitivity attribute in the equivalence class leads to the leakage in privacy. Suppose n tuples are present in databases that obey k anonymity. There are m numbers of sensitive attributes present with $K_1, K_2, \dots, K_m$ distinct values. The number of equivalence classes present that can have the possibility of all sensitive attributes value same in the particular equivalence class is say $(H)P$. This value of 'SE' determines the possibility of homogeneity attack [26, 30].

$$p(H) = \frac{(K_1 K_2 K_3 \dots K_m)}{(K_1^k K_2^k K_3^k \dots K_m^k)} \times \frac{n}{k}$$

Query sampling attack: To defend against this kind of attack Pan et al., 2012 [21], proposed a concept of *k*-sharing region, in which a cloaked region not only covers at least *k* nodes but is treated as the cloaked region by at least *k* nodes.

Query tracking attack: Query tracking attack (Chow and Mokbel, 2007) identifies potential query issuers by linking consecutive snapshots. To defend against this attack, Chow and Mokbel (2007) utilized the memorization property, which memorizes users in a cloaked region of a continuous query at the time when the query is initiated.

Replay attack: Wang and Liu (2009) presented the replay attack model, which estimates the likelihood of some locations being a user's actual positions by rerunning the anonymizing algorithm. It should be noted that the resilience to replay attack is correlated with the anonymizing algorithm itself.

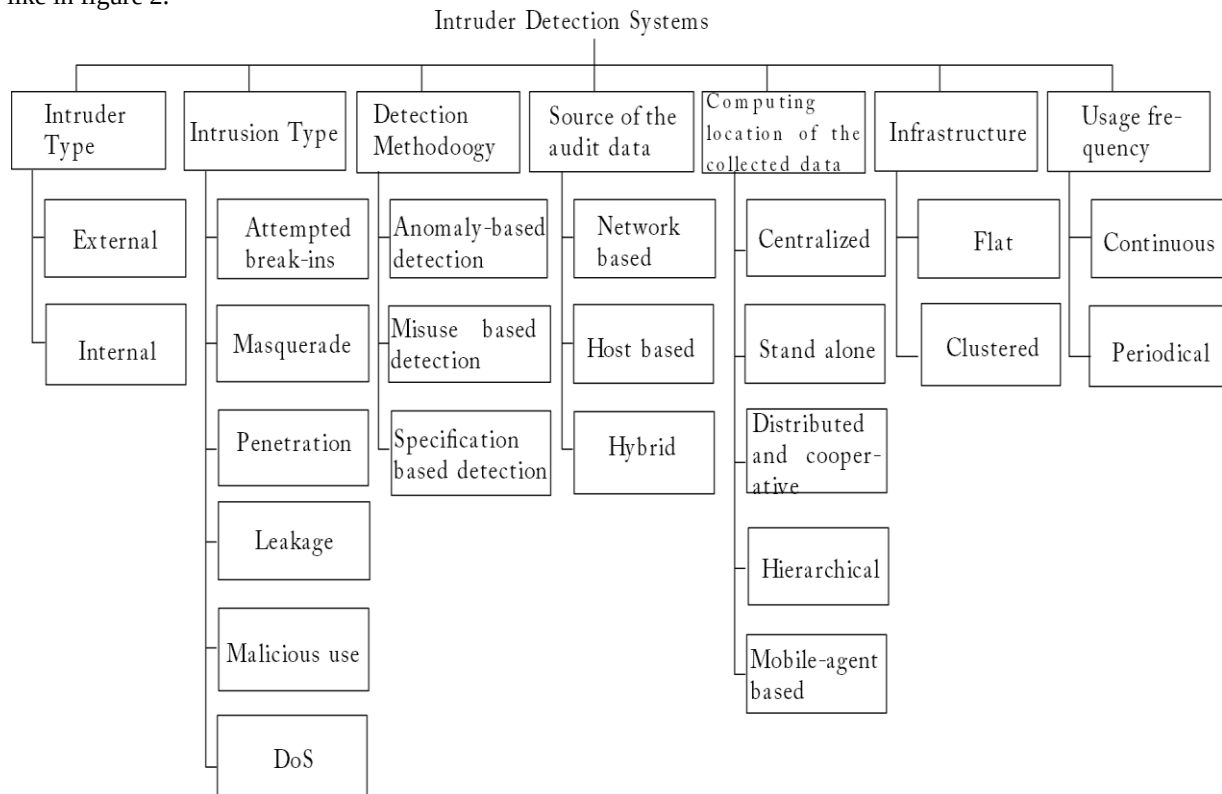
Man-At-The-End Attacks: In Man-At-The-End Attacks the attacker is intellectual human with limitless access to the target with all major protections stand up to a determined attacker till a certain period of time [1].

E. Pair wise Key Establishment

Pair wise Key Establishment basically consists of two steps first registration phase followed by an authentication phase. In registration phase one user sends its credentials generally using some one way hashing to the other user and it will be authenticated. It may be based on any biometric data [5] Zhou et al. 2013, key distribution Yang et. al. 2010.

F. Intrusion Detection

Butun et al. 2014 [4] in their paper discussed about intrusion detection in WSN and presented in classified way like in figure 2.



IV. CONCLUSION

In last three years, a large number of security algorithms and protocols have been published. Even though most of them are not much suitable for IoT due to their high computational overheads, a significant effort has been seen towards designing lightweight algorithms which may be fit for resource constrained environments. Further, research can be done in privacy preservation of location and data in dynamic mobile network and better energy efficient trust model and key distribution policy may be designed.

V. REFERENCES

- [1] Adnan Akhunzada, Mehdi Sookhak, Nor Badrul Anuar, Abdullah Gani, Ejaz Ahmed, Muhammad Shiraz, Steven Furnell, Amir Hayat, and Muhammad Khurram Khan. Man-at-the-end attacks: Analysis, taxonomy, human aspects, motivation and future directions. *Journal of Network and Computer Applications*, 48(0):44 – 57, 2015.
- [2] S. Arunkumar, M. Srivatsa, and M. Rajarajan. A review paper on preserving privacy in mobile environments. *Journal of Network and Computer Applications*, 53(0):74 – 90, 2015.

- [3] Carsten Bormann, Mehmet Ersue, and A Keranen. Terminology for constrained node networks. draft-ietf-lwigterminology- 07 (work in progress), 2014.
- [4] I. Butun, S.D. Morgera, and R. Sankar. A survey of intrusion detection systems in wireless sensor networks. *Communications Surveys Tutorials*, IEEE, 16(1):266–282, First 2014.
- [5] Ashok Kumar Das and Adrijit Goswami. A robust anonymous biometric-based remote user authentication scheme using smart cards. *Journal of King Saud University – Computer and Information Sciences*, 27(2):193 – 210, 2015.
- [6] H.R. Dhasian and P. Balasubramanian. Survey of data aggregation techniques using soft computing in wireless sensor networks. *Information Security, IET*, 7(4):336–342, December 2013.
- [7] Daojing He, S. Chan, and Shaohua Tang. A novel and lightweight system to secure wireless medical sensor networks. *Biomedical and Health Informatics, IEEE Journal of*, 18(1):316–326, Jan 2014.
- [8] Daojing He, Chun Chen, S. Chan, Jiajun Bu, and A.V. Vasilakos. Retruster: Attack-resistant and lightweight trust management for medical sensor networks. *Information Technology in Biomedicine, IEEE Transactions on*, 16(4):623–632, July 2012.
- [9] S.H. Jokhio, I.A. Jokhio, and A.H. Kemp. Light-weight framework for security-sensitive wireless sensor networks applications. *Wireless Sensor Systems, IET*, 3(4):298–306, December 2013.
- [10] Dilip Kumar and Bibhudatta Sahoo. Energy efficient heuristic resource allocation for cloud computing. *International Journal of Artificial Intelligent Systems and Machine Learning*, 6(1):32–38, 2014.
- [11] Dilip Kumar, Bibhudatta Sahoo, Bhaskar Mondal, and Tami Mandal. A genetic algorithmic approach for energy efficient task consolidation in cloud computing. *International Journal of Computer Applications*, 118(2):1–6, 2015.
- [12] Konrad Lorincz, David J. Malan, Thaddeus R. F. Fulford- Jones, Alan Nawoj, Antony Clavel, Victor Shnayder, Geoffrey Mainland, Matt Welsh, and Steve Moulton. Sensor networks for emergency response: Challenges and opportunities. *IEEE Pervasive Computing*, 3(4):16–23, October 2004.
- [13] M. Magno, D. Boyle, D. Brunelli, E. Popovici, and L. Benini. Ensuring survivability of resource-intensive sensor networks through ultra-low power overlays. *Industrial Informatics, IEEE Transactions on*, 10(2):946–956, May 2014.
- [14] Alessio Merlo, Mauro Migliardi, and Luca Caviglione. A survey on energy-aware security mechanisms. *Pervasive and Mobile Computing*, (0):–, 2015.
- [15] B. Mondal, S.S. Thakur, and S.B.L. Seksen. A novel addition based image sharing scheme for secure communication of highly secret images. In *Emerging Research Areas and 2013 International Conference on Microelectronics, Communications and Renewable Energy (AICERA/ICMiCR)*, 2013 Annual International Conference on, pages 1–5, June 2013.
- [16] Bhaskar Mondal and Tami Mandal. A multilevel security scheme using chaos based encryption and steganography for secure audio communication. *International Journal of Research in Engineering and technology*, 02(10):399–403, 2013.
- [17] Bhaskar Mondal, Tami Mandal, Sunil Kumar Singh, and Krishana Mohan Acharjee. A novel (k, n) secret key sharing scheme based on linear equations. *International Journal of Engineering Research & Technology (IJERT)*, 2(10):1679– 1682, 2013.
- [18] Bhaskar Mondal, Akash Priyadarshi, and D. Hariharan. An improved cryptography scheme for secure image communication. *International Journal of Computer Applications*, 67(18):23–27, April 2013. Published by Foundation of Computer Science, New York, USA.
- [19] Bhaskar Mondal and Sunil Kumar Singh. A highly secure steganography scheme for secure communication. In *Proceedings, International Conference of Computation and Communication Advancement (IC3A)-2013*, volume 1, pages 88–92 vol.3, Jan 2013.
- [20] Bhaskar Mondal, Deep Sinha, Navin Kumar Gupta, Nishant Kumar, and Pankaj Goyal. An optimal (n, n) secret image sharing scheme. *UACEE International Journal of Computer Science and Its Applications*, 2(3):61–66, 2012.
- [21] Xiao Pan, Jianliang Xu, and Xiaofeng Meng. Protecting location privacy against location-dependent attacks in mobile services. *IEEE Transactions on Knowledge and Data Engineering*, 24(8):1506–1519, 2012.
- [22] S. Roy, M. Conti, S. Setia, and S. Jajodia. Secure data aggregation in wireless sensor networks: Filtering out the attacker’s impact. *Information Forensics and Security, IEEE Transactions on*, 9(4):681–694, April 2014.
- [23] T. Savolainen, J. Soininen, and B. Silverajan. Ipv6 addressing strategies for iot. *Sensors Journal, IEEE*, 13(10):3511–3519, Oct 2013.
- [24] Seung-Hyun Seo, Jongho Won, S. Sultana, and E. Bertino. Effective key management in dynamic wireless sensor networks. *Information Forensics and Security, IEEE Transactions on*, 10(2):371–383, Feb 2015.
- [25] Yong Wang, Yun Xia, Jie Hou, Shi meng Gao, Xiao Nie, and QiWang. A fast privacy-preserving framework for continuous location-based queries in road networks. *Journal of Network and Computer Applications*, 53(0):57 – 73, 2015.
- [26] Zhen Xiao, Jianliang Xu, and Xiaofeng Meng. p-sensitivity: A semantic privacy-protection model for location-based services. In *Mobile Data Management Workshops, 2008. MDMW 2008. Ninth International Conference on*, pages 47– 54, April 2008.
- [27] Le Yan, Lin Zhong, and Niraj K. Jha. Energy comparison and optimization of wireless body-area network technologies. In *Proceedings of the ICST 2Nd International Conference on Body Area Networks, BodyNets ’07*, pages 8:1–8:8, ICST, Brussels, Belgium, Belgium, 2007. ICST (Institute for Computer Sciences, Social Informatics and Telecommunications Engineering).
- [28] Zheng Yan, Peng Zhang, and Athanasios V. Vasilakos. A survey on trust management for internet of things. *Journal of Network and Computer Applications*, 42(0):120 – 134, 2014.
- [29] Guo-Qiang; Yang Qing-Feng; Cheng Su-Qi Zhang, Guo- Qing; Zhang and Tao Zhou. Evolution of the internet and its cores. *New Journal of Physics*, 10:157–182, oct 2008.
- [30] Ming-Zheng Zhou, Yi Zhang, Jun Wang, and Sen-Yan Zhao. A reputation model based on behavior trust in wireless sensor networks. In *Scalable Computing and Communications; Eighth International Conference on Embedded Computing*, 2009. SCALCOM-EMBEDDED COM’09. International Conference on, pages 189–194, Sept 2009.