Location Privacy and Internet of Things: A Comprehensive Review

[1]Yogesh Kumar, [2]Ruchika Gupta
[1]Associate Professor, Chandigarh Engineering College, Landran, Mohali, Punjab
[2]Associate Professor, Chandigarh University, Mohali, Punjab

Abstract: In recent years, Internet of things (IoT) has gained a lot of attention while describing non-traditional devices connections. The non-traditional devices can be a medical equipment, a factory machinery, or the domestic appliances linked through internet to collaboratively perform a task. Extensive review on elements of architecture, IoT features and development, their key application is given by various researchers in which it is majorly observed that the IoT vendors pay lesser importance to the security and privacy aspect that leads to the situation where IoT exists with number of security/privacy vulnerabilities. For exchanging information, Internet has been used in IoT and sensing devices are connected. In order to achieve content aware and intelligent IoT systems location information acts as one of the most crucial aspects as the breach of security and privacy of the location information eventually discloses the real-world identity of the user. A large amount of localization or positioning functions are realized, however the privacy and security threats related to IoT positioning has not been addressed much. In this paper, we present a comprehensive review on various aspects of IoT security, security challenge, describe different attacks associated to it. Major focus is given over currently affected areas by various attacks.

Keywords: Internet of Things, Location Privacy, Security Threats, Security Attacks, Sybil.

I. INTRODUCTION

Now a day's personal mobile devices data is being tracked and monitored by third party applications even without the control of data owners. There is continuous violation of data owners trust. The most desirable parameter location data is shared by the data owners through approved consent and it is continuously tracked by the third party. Therefore, it has become an important issue that the results and other important confidential data can be hacked or misuse by third party due to the disproportionate control being in favour of the third-party analysts. In recent years, Internet of things (IoT) has gained a lot of attention while describing connections among non-traditional devices. The non-traditional devices can be a medical equipment, a factory machinery, or the domestic appliances linked through internet to perform a specific task. The controllers like microprocessor-based applications from small toasters to big airlines machines has become almost omnipresent these days. In the usage of controllers' evolution, the use of IOT has taken as next step in which internet is used for connection purposes. In order to make tagged objects available for internet location, identification, and status information Radio frequency identification is used. Extensive survey on the elements of architecture, IoT features and development, and their key application is given by various researchers. Lesser importance is given to the security and privacy of the user by vendors of IoT that make it vulnerable to various security threats. The location-based services (LBS) are enabled by IoT with the increase in getting location information of the device connected. An important role is played by the location attribute within a context sensing information. Number of systems, prototypes, and solutions are proposed by various researchers by using localization and positioning modules in IoT sensor nodes and used different approaches of localization to deal with various attacks associated with IoT scenario.

This paper is divided into different sections to cover the comprehensive review about the different aspects of IoT security, its localization, and attacks. Section II describes the different security-based challenges associated to IoT while a review on different attacks in IoT is presented under section III of the paper. Section III also describes the work done by numerous researchers for protecting IoT setup from various attacks. Section IV reviews various security localization in different areas while section V overviews the security localization in IoT. Section VI describes attack mitigation techniques and finally section VII concludes the paper.

1.1 Challenges

IoT is considered as a new and relatively popular filed, however there are some issues related to different architecture layers including the security and privacy of the user information.

Following are certain challenges that are needed to be addressed while designing efficient solutions to overcome the problems:

Security Structure: There is a need to make a security structure by combining both the information and control. As present IoT is considered to remain stable-persisting as a whole over time and defence in depth of system and each logical layer security mechanism cannot be implemented. Therefore, there is a need of proper security structure to address the issue.

***Key Management*:** For an improved security mechanism, a key management is considered as important and challenging research

area. In cryptographic security it is considered as one of the most difficult aspects and in the literature no ideal solution has been found by the researchers. There are methods like higher performance of sensor node or lightweight cryptographic algorithm that are still not been applied. In case of network environment, the network security has become comparatively difficult to achieve and a key point that needs to be considered by the researchers. Moreover, law of regulations related to security and privacy has not become a major focus and no particular standard exists for IoT as of now. The personal privacy, business secretes, and national security information is also related much with IoT. Therefore, its development needs to be promoted and require a regulations and policies for it. The networking communication technology, WSNs, RFID, pervasive computing technology, and CPS development makes IoT more emerging technology. Hence, there is a need of high level of security to have good performance of system that makes security challenges as severe and creates a need to work on it.

II. DIFFERENT ATTACKS IN IOT

Here we review different attacks associated with IoT. Not all but we have tried to cover most of the recent attacks that affects the operation of the system as a whole. Now a days IoT has become very popular in different domains which makes it challenging to provide security of IoT system and a substantial loss may occur by attacking the IoT system.

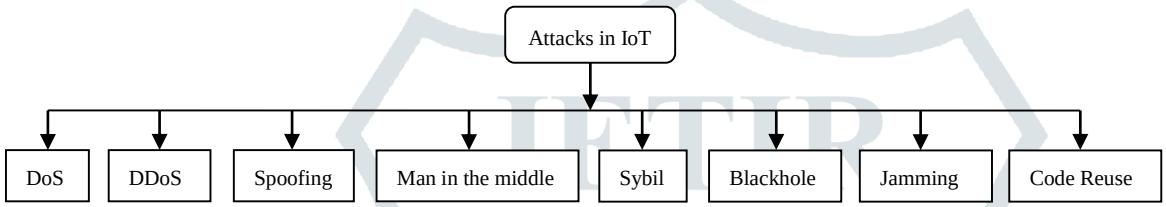

Fig. 1: Various attacks in IoT

In **2016, Lulu Liang, et.al,** consider the denial of service (DoS) attack to an IoT system. The DoS tries to disrupt the servers or network services that can be done by single attacker machine. Another form of DoS attack is Distributed Denial of Service but they are attacked by different machines to target the victim. They use Kali Linux tool for the attack and three different methods are used for launching attack and compared. The first method is DoS attack using hping3 with random source IP (1200bytes), Simple SYN flood with proofed IP is the second method while TCP connect floods used as the third method. Out of these three the first method outperforms the rest two and provide better results. In case of presence of man-in-the middle and spoofing attacks, use of quantized and unknown deterministic vector sensor data estimation are found. First, the attacked sensor is categorized and identified into different groups by using asymptotically optimum processing that helps in the distinction of various types of attacks. In **2017, Jiangfan Zhang, et.al** provide the necessary conditions using which a guaranteed attack performance is provided by spoofing attacks. The performance is taken in terms of Cramer-Rao Bound that do not consider the estimation system. The results show that by having sufficient large dimension it is possible to construct a highly desirable attack.

In **2017, Tamotsu KAWAMURA, et.al,** worked upon distributed denial of service (DDoS) attacks on IoT. The flooding and vulnerability attacks are two categories of DDoS attacks. Some malformed packets are sent by the attackers to the victim in case of vulnerability attack that confuse an application running on it. On other hand a legitimate user is disrupted by flooding attack. Tamotsu proposes an event detection module for DDoS attack that is different from existing knowledge-based filtering detection modules. The system behaviour under DDoS attacks is focused and detected by proposed module that utilizes NTP based information in synchronization service. The experimental results show that a high precision and a recall value can be achieved using proposed module. The cloud computing and IoT has gain their importance in different fields and applications. For smart cities, an IoT application assisted cloud architecture is presented in **2018, Asma Alsaidi, et.al.** The attacks and security threats occur due to unauthorized misuse and access of IoT nodes and devices collected information. The paper also describes different security attacks and their countermeasures. **Trupti Lotlikar, et.al,** focus on DoS and DDoS attacks integrating the SDN and IoT technology, given a review on OpenFlow Protocol and different SDN layered affected DoS attacks and demonstrated how it can be mitigated and weaken the impact of those attacks on the network. For simulation purpose they use Open V Switch (OVS), Floodlight SDN controller and mininet simulator.

The IoT devices become vulnerable by the occurrence of code reuse attacks by which malicious activities take place while reusing devices benign codes. This results in compromise of industrial IoT devices by the adversary and entire industrial IoT ecosystems are compromised through it. Henceforth, in industrial IoT devices detection of code reuse attacks have become very crucial and essential. Various detection schemes are proposed by different researchers for code-reuse attacks that are inefficient network level defence techniques. Therefore, in **2018, Jun-Won Ho, et.al,** used a Sequential Probability Ratio Test (SPRT) with the probabilistic inspection to detect the code reuse attacks efficiently. This is implemented on the packets coming into industrial IoT devices. The experiment results show average detection rate of 93.2 and 99 in percentage achieved using proposed scheme.

Table 1. Review on different attacks in IoT

S.No.	Author	Type of Attack	Description
1	Lulu Liang, et.al, [13] (2016)	DoS	They use Kali Linux and three different methods are used for launching attack. First, hping3 is used with 1200 bytes random source IP for DoS attack followed by simple SYN flood with proofed IP. The third method is TCP connect floods. Out of these three the first method outperforms the rest two and provide better results.
2	Jiangfan Zhang, et.al, [14] (2017)	Spoofing and Man in the Middle	Necessary conditions are provided using which a guaranteed attack performance is demonstrated by spoofing attacks. The performance is taken in terms of Cramer-Rao Bound that do not consider the estimation system.
3	Tamotsu Kawamura, et.al, [15] (2017)	DDoS	An event detection module for DDoS attack that is different from existing knowledge-based filtering detection modules. The system behaviour under DDoS attacks is focused and detected by the proposed module that utilizes NTP based information in synchronization service.
4	Asma Alsaidi, et.al, [16] (2018)	DoS, Sybil, Black hole, Jamming and wormhole	They present the architecture for smart cities through an IoT applications assisted cloud. They also described different security attacks countermeasures.
5	Trupti Lotlikar, et.al, [17] (2018)	DoS, DDoS	They integrate the SDN and IoT technology together, given a review on OpenFlow Protocol and different SDN layered affected DoS attacks and also demonstrated how the effect of these attacks can be mitigated. For simulation purpose they use Open V Switch (OVS), Floodlight SDN controller and mininet simulator. S
6	Jun-Won Ho, et.al, [18] (2018),	Code Re-use	They use Sequential Probability Ratio Test (SPRT) with the probabilistic inspection to detect the code reuse attacks efficiently. This is implemented on the packets coming into industrial IoT devices. The experiment results show that average detection rate will be 93.2 and 99.0 in percentage achieved using proposed scheme.

The availability of dimension is targeted by Denial of Service (DoS) cyber-attacks. Many defence mechanisms are proposed for protecting system, still the existing systems are not be able to give effective and efficient solutions. The potential damage has become more profound in smart grid and due to the peculiar features of the infrastructure of the DoS attacks. Further, an Intrusion detection system (IDS) based specification is proposed by author that tailored for ANSI C12.22 application layer protocol to catch specified security policy. The proprietary implementations and same or other protocols can be deployed that make use of this approach to be infeasible in all the cases. For encrypted traffic intrusion detection is done by the proposed method for one packet level inspection and tested for same protocol layer of application. After that fourth order Markov Chain is used to model a data

aggregation event logs that is made by aggregations. That makes it restricted to be used in the smart meters. Further, a hierarchical distributed IDS is proposed for the smart grid in with the main use found in assumptions of wireless mesh network technology. Author in present an IDS system on the basis of the anomaly and can be deploy on data aggregators and on headend due to its computational complexity. In authors consider the false data injection attack's timely detection against smart gird voltage phase estimation from parametric point of view.

III. SECURITY LOCALIZATION IN DIFFERENT AREAS

In WSN most of the techniques of security localization are designed for single type of attack or single step message packet transmission that is not effective in complex network environment. In 2009, a novel Double Guarantee Security Sensor Localization (DGSSL) WSN security localization algorithm is proposed by **Jingjing Gu, et.al**. The use of proposed algorithm helps in enhancing message packets security and reliability then in dynamic network environment a model of self adaptively signal attenuation is established. The experiment results show that proposed algorithm tested on different attack conditions is more accurate and gives better performance as compared to other algorithms. An automatic cyber reasoning system (CRS) is developed by **2009, Hsia-Hsiang Chen, et.al,** that meets the CGC objectives. To construct automatic defence system, they constructed the automatic defence system. Then fault localization and fuzz testing techniques are combined in the proposed technique. They have also explored two patching methods in CGC five challenges with security and availability partial successes.

Most of the WSN applications are depend on sensor nodes positions data which are not known prior to use it. A various localization approaches are proposed by different researchers; however, all have not considered if WSNs could be deployed in adversarial settings. In **2014, Nicola Basilico, et.al,** proposed a method called Verifiable Multilateration (VM) that deals with the problem by leveraging on a set of trusted landmark nodes that act as verifiers. In localization measurement, use of proposed approach is proved to be more reliable and also allow to use in undecided positions region of monitored 40 percent of the area. Then they use game theory for using VM potentialities with the aim of improving defender's strategy. A method name Verifiable multilateration (VM) is proposed in which the set of trusted landmark nodes are leveraging and act as verifiers while dealing with the problem. Still there is a need to have an effective approach that helps in ensuring secure localization and results in elimination of malicious anchor causing adverse influence. In the similar motion in **2016, Xiaofeng Xu, et.al,** proposed a novel information game based secure localization approach that proved to be more effective in achieving secure localization.

With an increase in application range identification of rogue or legitimate access point location is considered to be an important research problem. Most of the efficient access points installation uses the concept of computer simulation and mathematical modelling. In **2017, Fahed Awad, et.al,** used the concept of taking a relatively small number of the access point's received signal strength samples at known locations for proposing a new approach. The empirical results show that the proposed approach is efficient in identifying access point location efficiently and accurately. In **2018, Zhang Lieping, et.al,** proposed an WSN based RSSI-LSSVR algorithm which is a three-dimensional node security localization method. Firstly, median weighting method is used for improving the RSSI method that helps in improving the ranges precision of nodes then the three-dimensional node localization model is established to improve the localization nodes accuracy even more. In the end security localization is improved by presenting the Sybil attacks detection mechanism.

Table. 2 Review on security localization in different area

S. No.	Author	Description
1	Jingjing Gu, et.al, (2009)	Proposed a novel Double Guarantee Security Sensor Localization (DGSSL) WSN security localization algorithm.
2	Hsia-Hsiang Chen, et.al, (2009)	An automatic cyber reasoning system (CRS) is developed by authors that meets the CGC objectives and constructed the automatic defence system. The fault localization and fuzz testing techniques are combined in the proposed technique.
3	Nicola Basilico, et.al, (2014)	They propose a method called Verifiable Multilateration (VM), in which the set of trusted landmark nodes are leveraging and act as verifiers for dealing with the problem.
4	Xiaofeng Xu, et.al, (2016)	They propose novel information game based secure localization approach.
5	Fahed Awad, et.al, (2017)	In order to propose a new approach, they take a sample of received signal strength with a very less amount of access points.
6	Zhang Lieping, et.al, (2018)	They propose a WSN based RSSI-LSSVR algorithm which is a three-dimensional node security localization method.

IV. SECURITY LOCALIZATION IN IOT

For the exchange of information Internet has been used in IoT for connecting sensing devices. In order to achieve content aware

and intelligent IoT systems location information acts as one of most crucial aspects. Now a days, a large amount of localization or positioning functions has been realized, however the privacy and security threats related to IoT positioning has not been addressed much. In **2017, Liang Chen, et.al,** given a review on different solutions for improving location-based services like privacy, security, and robustness improvement in IoT systems. Firstly, Global Navigation Satellite System (GNSS) and non-GNSS based solutions for threats are given and some cryptographic privacy and security solutions of location or positioning based IoT services are then described. The detailed policy regulations regarding location data privacy legal instruments and positioning solutions of security is given. The tracking and location-based features on IoT current state of art is given in **2017, Swathi Ramnath, et. al.** In this key technical aspect's initiatives based on IoT is presented and compared with non-IoT based services. Their utilities in different application are also demonstrated and results show that the proposed approach of IoT based tracking and location gives more accurate results as compared to other existing techniques.

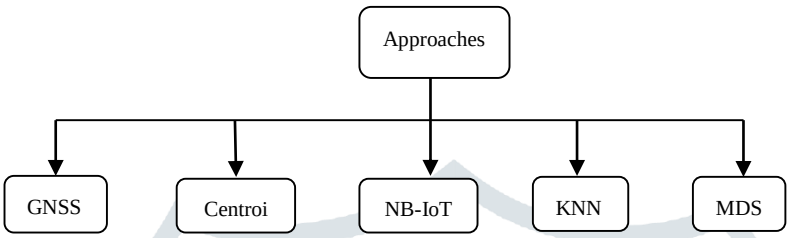

Fig. 2: Approaches used for security in Localization

The localization based on indoor fingerprinting has gained a lot of interest by proliferation of mobile devices that gives high precision. In these schemes use of channel state information (CSI) gives enhanced channel metric. In 2017, a localization-based CSI amplitude fingerprinting has been used in Narrowband Internet of Things (NB-loT) system by **Qianwen Song, et.al**. In the scheme, a CSI propagation model based centroid algorithm is optimized and a Time-Reversal Resonating Strength (TRRS) and Euclidean distance between reference and target points are calculated using multidimensional scaling (MDS). A K-Nearest Neighbor (KNN) algorithm is employed for location estimation. To get the final estimated position a positioning results are obtained after optimizing the triangular centroid algorithm location error using conjugate gradient method is combined with KNN's and MDS estimated position. The results show that the proposed approach is efficient while reducing positioning error as compared to other existing methods of localization. In medical field Localization of Health Centre Assets through an IoT Environment (LoCATE) solution is proposed by McAllister et al. that track all medical staff and patient after knowing their immediate location. Afterwards, in **2018, Cole Bradley, et.al,** analysed LoCATE, created data leaks, and security holes in the healthcare facility. In this scheme the edge node data forging is done along with launching other attacks and with the denial of service attack while gaining unauthorized access to exploit the system's weak security measures. The proposed approach is proved to be efficient to use in the future for healthcare application.

A large number of small sensors build a network that communicates with each other and consider IoT as a novel design claimed to be the innovative solution to real time problems. A WSN is made using the sensors that help in monitoring physical environment and disseminate collected data back to the base station through multiple hops. In **2018, Rathin Chandra Shit, et.al,** given a detailed analysis on different techniques of localization and hierarchical taxonomy. They also shown their applications in different context and classified these techniques on the basis of self-determining and training dependent approaches like offline training in localization. They also proposed various solutions for different issues related to localization schemes for IoT.

Table. 3 Review on security localization in IoT

S. No.	Author	Description
1	Liang Chen, et.al, (2017)	A review on different solutions for improving location-based services like privacy, security and robustness improvement in IoT systems.
2	Swathi Ramnath, et.al, (2017)	The tracking and location based IoT system and their key technical aspects are elaborated while presenting a non-IoT and IoT based initiatives for localization services with comparison.
3	Song, et.al., (2017)	A CSI propagation model based centroid algorithm is optimized and a Time-reversal Resonating Strength (TRRS) and Euclidean distance between reference and target points are calculated using multidimensional scaling (MDS). The K-Nearest Neighbour (KNN) algorithm is then employed for location estimation.
4	Cole Bradley, et.al, (2018)	They analyse the Locate, created data leaks, and security

		holes in the healthcare facility. In this work, the edge node data forging is done along with launching other attacks and with the denial of service attack gaining unauthorized access to exploit the system's weak security measures.
5	Rathin Chandra Shit, et.al, (2018)	An analysis on different techniques of localization and hierarchical taxonomy is presented. Their applications in different context and their classification on the basis of self determining and training dependent approaches like offline training in localization is elaborated.

V. SECURITY LOCALIZATION AND ATTACKS MITIGATION IN IOT

A new location spoofing security risks has been introduced in IoT by increase in the applications based on Geo-spatial location. Secure Location of Things (SLOT) framework is proposed in **2017, Pengfei Zhang, et. al.,** that helps in reducing the malicious spoofing attacks. There is different information like audibility information in SLOT that is not utilized in indicating whether the communication is possible with the node or not. Using the information, a stochastic censoring model location estimation problem is then formulated and a Maximum Likelihood Estimator (MLE) of nodes is also derived. They use two different ways namely; probabilistic mixture model (M-SLOT) and Byzantine attack distributional model knowledge, which is assumed in the first algorithm. In second algorithm the concept of Difference-Time-of-Arrival (D-SLOT) is used that not make any distributional assumptions about attack. The proposed algorithm tested and results show that a significant gain is received in well-known likelihood surface ambiguity problems as compared to currently used algorithms for the same. In future by delivering merchandise and goods a small unmanned aircraft systems (UASs) can be placed as a major role of smart cities. In broadband wireless access UASs are serve as mobile hot spots and maintain security and surveillance. It helps in giving improvement of society and malicious entities can also use it to conduct cyber and physical attacks to the people. The authors present a detailed comparison about various location privacy solutions in LBS. In **2017, Ismail Guvenc, et.al,** given a survey on various techniques that rely on acoustic sensors, ambient radio frequency signals (emitted from UASs), computer vision techniques and radars for the purpose of malicious UASs detection. They perform experiments on radar based UASs range estimation for reducing its horizon tracking.

Physical and cyber damages take place by cybersecurity attacks on smart grid in which the recent attacks on power grid in Ukraine where consumers were left without power. The IoT powered botnets get proliferated that makes recent successful Distributed Denial-of-Service (DDoS) attacks on the Internet. DDoS and other attacks affect the power services of large number of people. In **2017, Yasin Yilmaz, et.al,** proposed a scalable mitigation approach. Under the infrastructure of hierarchical data collection, they use a Minimally Invasive Attack Mitigation via Detection Isolation and Localization (MIAMI-DIL). Authors propose a distributed mechanism in order to get the results locally and server contacts are reduced while the HYB approach gives the hybrid solution to preserve the user's privacy. They perform the simulations of the proposed approach that show it more scalable and efficient. The new solutions are found for old problems in the critical areas by the advancement in technology. In medical field localization of health care solution is proposed by McAllister et al. that tracks all the medical staff and patients by knowing their immediate location. There is a need to know the location of patient or other medical staff to save the life of a patient. Various other methods are also proposed in the field of medical to protect the location information from attacks. All methods have their merits and demerits. The Locate proposed by McAllister et al. gets affected by creation of security holes in the networks of edge nodes and IoT devices that results in leak of data in the open world. In 2018, **Cole Bradley, et.al**, located the reason of security holes and data leakage created by Locate. In this, edge node data forging is done along with launching other attacks while gaining unauthorized access to exploit the systems weak security measures.

VI. CONCLUSION

Internet of Things (IoT) is a novel design paradigm, intended as a network of billions to trillions of tiny sensors communicating with each other to offer innovative solutions to the real time problems. Extensive review on the elements of architecture, IoT features and development, their key application is given by various researchers. It is observed that the IoT vendors pay lesser importance to the security and user privacy aspects that eventually lead to the situation where IoT is filled with number of security vulnerabilities. In this paper we reviewed the state of art, security challenges, privacy issues, and the major observations about the works presented by numerous researchers. This main aim of the paper is to present a comprehensive review on different aspects related to security localization. We presented with an overview on security challenges in IoT followed by elaborating various attacks that affects the IoT networks. A lot of researchers have worked upon Spoofing, Man in a middle, Sybil, DoS, and DDoS attack. The following section of the paper covers the usage of security localization in various area and the major focus is then given while emphasizing security localization in IoT. The review of various attacks in IoT and usage of security localization in IoT is given separately and well represented in the form of tables and the last section present a review on the security localization and attacks mitigation in IoT that helps other researchers to select best approach for their application while assessing existing work merits and demerits.

REFERENCE

[1] Atzori L, Iera A, Morabito G. (2010). The internet of things: A survey. Computer networks, 54, 2787–2805.
[2] Alsaidi, A., Kausar, F. (2018). Security Attacks and Countermeasures on Cloud Assisted IoT Applications. 2018 IEEE International Conference on Smart Cloud, pp. 213-217.
[3] Ali, M Q., Al-shaer, E. (2013). Configuration-based IDS for Advanced Metering Infrastructure. Proceedings of ACM SIGSAC conference on Computer & communications security, pp. 451–462.
[4] Awad, F., Omar, A., Naserllah, M., Hantash, A A., Al-Taj, A. (2017). Access Point Localization Using Autonomous Mobile Robot. 2017 IEEE Jordon conference on applied electrical engineering and computing technologies, pp. 1-5.
[5] Ali, M Q., Al-Shaer, E. (2015). Randomization-Based Intrusion Detection System for Advanced Metering Infrastructure. ACM Transactions on Information and System Security, 18, 710-730.
[6] Alseiari, F A A., Aung, Z. (2015). Real-time anomaly-based distributed intrusion detection systems for advanced Metering Infrastructure utilizing stream data mining. in 2015 International Conference on Smart Grid and Clean Energy Technologies (ICSGCE), IEEE, pp. 148–153.

[7] Bradley, C., El-Tawab, S., Heydari, M. H. (2018). Security Analysis of an IoT System Used for Indoor Localization in Healthcare Facilities. IEEE, pp. 147-252.
[8] Borgia, E. (2014) The internet of things vision: Key features, applications and open issues. Computer Communications, 54, 1–31.

[9] Berthier, R., Urbina, D I., Cardenas, A A., Guerrero, M., Herberg, U., Jetcheva, J G., Mashima, D., Huh, J H., Bobba, R B., (2014). On the practicality of detecting anomalies with encrypted traffic in AMI. in 2014 IEEE International Conference on Smart Grid Communications (SmartGridComm), IEEE, pp. 890–895.
[10] Basilico, N., Gatti, N., Monga, M., Sicari, S. (2014). Security Games for Node Localization through Verifiable Multilateration. IEEE Transactions on dependable and secure computing, pp. 72-85.
[11] Berthier, R., Sanders, W H. (2011). Specification-Based Intrusion Detection for Advanced Metering Infrastructures in 2011 IEEE 17th Pacific Rim International Symposium on Dependable Computing, IEEE, pp. 184–193.
[12] Bradley, C., El-Tawab, S., Heydari, M H. (2018). Security Analysis of an IoT System Used for Indoor Localization in Healthcare Facilities. IEEE, pp. 147-152.

[13] Chen, H H., Zheng, D Q., Huang, S K. (2016). Automatic Defense Through Fault Localization and Dynamic Patch Creation. 2016 IEEE International Conference on Software Quality, Reliability and Security Companion, pp. 408-409.
[14] Chen, L., Thombre, S., Jarvinen, K., Lohan, E S., Alen-Savikko, A., Leppakoski, H. (2017). Robustness, Security and Privacy in Location-Based Services for Future IoT: A Survey. IEEE ACCESS, pp. 1-21.
[15] Da Xu, L., He, W., Li, S. (2014). Internet of things in industries: A survey. IEEE Transactions on industrial informatics, 10, 2233–2243.
[16] Ding, C., Yang, L J., Wu, M. (2011). Security architecture and key technologies for IoT/CPS. ZTE Technology Journal, vol. 17.
[17] Gu, J., Chen, S., Zhuang, Y. (2009). Double Guarantee for Security Localization in Wireless Sensor Network. 2009 Fifth International Conference on Wireless and Mobile Communications, pp. 99-104.

[18] Gupta, R., Rao, U P. (2017). Achieving Location Privacy through CAST in Location Based Services. Journal of Communications and Networks, IEEE Comm.Soc., 19, 239-249.
[19] Gupta, R., Rao, U P. (2017). A Hybrid Location Privacy Solution for Mobile LBS. Mobile Information Systems, pp. 1-11.
[20] Gubbi J, Buyya R, Marusic S, Palaniswami M. (2013). Internet of things (IoT): A vision, architectural elements, and future directions. Future generation computer systems, 29: 1645–1660.
[21] Gupta, R., Rao, U P. (2017). An Exploration to Location Based Service and its Privacy Preserving Techniques: A Survey. Wireless Personal Communications, Springer, 96, 1-35.
[22] Guvenc, I., Ozdemir, O., Yapici, Y., Mehrpouyan, H., Matolak, D. (2017). Detection, Localization, and Tracking of Unauthorized UAS and Jammers. 2017 IEEE/AIAA 36th Digital Avionics Systems Conference (DASC), pp. 1-10.

[23] Hu, Z H. (2011). The research of several key question of internet of things. In Proc. of 2011 Int. Conf. on Intelligence Science and Information Engineering, pp. 362-365.
[24] Ho, J W. (2018). Efficient and Robust Detection of Code-Reuse Attacks through Probabilistic Packet Inspection in Industrial IoT Devices. IEEE Access, pp. 1-12.
[25] Kawamura, T., Fukushi, M., Hirano, Y., Fujita, Y., Hamamoto, Y. (2017). An NTP-based Detection Mo1dule for DDoS Attacks on IoT. 2017 IEEE International Conference on Consumer Electronics - Taiwan (ICCE-TW), pp. 15-16.

[26] Li, S., Yilmaz, Y., Wang, X. (2015). Quickest detection of false data injection attack in wide-area smart grids. IEEE Transactions on Smart Grid, 6, 2725–2735.
[27] Liang, L., Zheng, K., Sheng, Q., Huang, X. (2016). A Denial of Service Attack Method for an IoT System. 2016 8th International Conference on Information Technology in Medicine and Education, pp. 360-364.
[28] Lotlikar, T., Madhavan, S., Andrews, S., Mascarenhas, C., Mathew, J. (2018). DoShield Through SDN for IoT Enabled Attacks. Proceedings of the 2nd International conference on Electronics, Communication and Aerospace Technology (ICECA 2018), pp. 1499-1504.

[29] Polk, T., Turner, S. (2011). Security challenges for the internet of things. http://www.iab.org/wp-content/IAB-uploads/2011/03/Turner.pdf
[30] Perera, C., Zaslavsky, A., Christen, P., Georgakopoulos D (2014) Context aware computing for the internet of things: A survey. IEEE Communications Surveys & Tutorials, 16, 414–454.
[31] Ramnath, S., Javali, A., Narang, B., Mishra, P., Routray, S K. (2017). IoT Based Localization and Tracking. IEEE, pp. 1-4.
[32] Song, Q., Guo, S., Liu, X., Yang, Y. (2017). CSI Amplitude Fingerprinting Based NB-IoT Indoor Localization. IEEE Internet of Things Journal, pp. 1-11.
[33] Shit, R C., Sharma, S., Puthal, D., Zomaya, A Y. (2018). Location of Things (LoT): A Review and Taxonomy of Sensors Localization in IoT Infrastructure. IEEE Communications Surveys & Tutorials, pp. 1-34.
[34] Shi, J H., Wan, J F., Yan, H H., Suo, H. (2011). A survey of cyber-physical systems. in Proc. of the Int. Conf. on Wireless Communications and Signal Processing, Nanjing, China, November.
[35] Wan, J F., Suo, H., Yan, H H., Liu, J Q. (2011). A general test platform for cyber-physical systems: unmanned vehicle with wireless sensor network navigation. in Proc. of 2011 Int. Conf. on Advances in Engineering, Nanjing, China, December.
[36] Xu, X., Ren, Y (2016). Information Game Model for Secure Localization in Wireless Sensor Networks. 2016 IEEE International Conference on Electronic Information and Communication Technology (ICEICT 2016), pp. 195-198.
[37] Yang, G., Xu, J., Chen, W., Qi, Z H., Wang, H Y. (2010). Security characteristic and technology in the internet of things. Journal of Nanjing University of Posts and Telecommunications (Natural Science), Vol. 30.
[38] Yilmaz, Y., Uludag, S. (2017). Mitigating IoT-based Cyberattacks on the Smart Grid. 2017 16th IEEE International Conference on Machine Learning and Applications, pp. 517-522.
[39] Zhang, J., Blumt, R S., Kaplan, L. (2017). Cyber-attacks on estimation sensor networks and lots: impact, mitigation and implications to unattacked systems. ICASSP2017, pp. 3316-3320.
[40] Zargar, S T., Joshi, J., Tipper, D. (2013). A Survey of Defense Mechanisms Against Distributed Denial of Service (DDoS) Flooding Attacks. IEEE Communications Surveys & Tutorials, 15, 2046–2069.
[41] Zhang, Y., Wang, L., Sun, W., Ii, RCG., Alam, M. (2011). Distributed Intrusion Detection System in a Multi-Layer Network Architecture of Smart Grids. IEEE Transactions on Smart Grid, 2, 796–808.
[42] Zhang, P., Nagarajan, S G., Nevat, L. (2017). Secure Location of Things (SLOT): Mitigating Localization Spoofing Attacks in the Internet of Things. IEEE Internet of Things Journal, pp. 1-8.