Global Journal on Application of Data Science and Internet of Things
Vol. 3, Issue 1 - 2019

SECURITY AND PRIVACY ASPECTS IN SMART IoT ENVIRONMENT

PRAVIN WARARKAR[*], SHASHIKANT PATIL[*], CHINMAYA VYAS[*]

ABSTRACT

Internet of Things (IoT) has undergone a sea change in the last few years. Quite potent development has shaped up the common perception of Internet towards a unified vision of smart objects communicating with each other. As we observe the recent trends a lot of issues have been addressed by the available wireless technologies but the issue of security and privacy still remains a vulnerable one and Internet of things technology is no exception to it. In today's world particularly sensitive data is managed and any sort of leakage of data can breach the privacy of any user. Due to this fact sometimes the efficacy of the IoT system as whole has been put under serious doubts by several organisations. With the fact still remains that a lot of systems are particularly connected with each other unsupervised increases the complexity of the system as whole. This is one of the main reasons behind less penetration of the IoT technology in the Indian market. This Chapter deals with the brief description of the challenges pertaining to the area which we need to overcome in the coming years so as to make the technology effective and efficient. This Chapter also discusses various economic and cultural reasons which led to severe privacy related issues in the IoT technology as whole. This Chapter also focuses of the impacts of some of the attacks on the IoT technology and discuss the possible prevention methodologies. A proper review regarding the advances in security and privacy is also done which also discusses appropriate solutions after identifying challenges and future aspects in the given area.

KEYWORDS: Internet of Things, Privacy, Security, Safety, Attacks.

INTRODUCTION

The interconnection of plethora of devices via internet with the usage of simple protocols can be stated as a best definition of Internet of Things (IOT). IOT can be termed as a great technological revolution providing economic benefits, enhancing quality of life, providing security and privacy aspects. IoT covers a wide range of applications traffic control, smart homes, congestion control, smart city framework etc. [1]. Recent trends and developments have seen quite of surge of IoT technology in the field of medical science with health monitoring and lifestyle monitoring systems being integrated to it [2].

[*]SVKM's NMIMS University, Mumbai, MPSTME, Shirpur Campus, Maharashtra, India.
Correspondence E-mail Id: editor@eurekajournals.com

 ISSN: 2581-4370

Since due to obvious transmission of data from one side to another cloud technology used for this open sharing. With so much to offer and have wide applications in various fields, IOT enabled devices are made with an objective of single application and are made with little security issue consideration. The IoT devices may also encounter security issue within the device. IoT applications may encounter security issue when the devices are connected with the physical world. Like Leverett discusses a system which was assumed to be in a safer network but was eventually assessable via internet technology [3]. With the no. of interconnected devices increasing day by day the security and privacy aspects involved with the network will also increase. Privacy is also another aspect where personal data can be collected from various sources. The classification of data is though one of the aspect i. e., categorisation whether it is benign or classified data in terms when the security of the system is breached or if the data is leaked then the privacy of the user is affected or not is to be examined. Though in a general case the privacy of the system should be maintained [4]. Finally it is important to consider encryption algorithms providing safety of data. The Intelligent data management is one of the fundamental privacy mechanism since it involves the collection of required data only. The redundant data should be discarded because it acts as a liability which needs to be taken care of. Secure cryptographic algorithms have already been developed for resource constraint environments but overall security and privacy requirements must be addressed with basic and appropriate mechanisms. Personal health Plans are confined to the available data from the patient, which is incomplete. Thus pose a challenge in terms of data mining and analysis of the data. Now since IoT connects everything to the internet. Thus the smart wearable devices and objects are providing enormous amounts of data. Smart Objects have enormous potentials to transfer the data from mobile health and ambient assisted living environments. IoT has nowadays enabled patients to switch to personalized health care systems wherein they can monitor their own ambience. The sending of alerts at the time of emergency, prediction of anomalies in the health and the transfer of collected data to a secure information system has been made possible by the advent of IoT.

LITERATURE SURVEY

There are many evolving technologies which have a close association with IoT:

RFID: The issues associated with have been identified [5, 6]. The potent threats are automatic identification and tracking through hidden tags [7]. The security measures such as encryption, destroying tags etc. have been suggested. It uses the automatic Identification and data capture technology (AIDC) [8].

Wireless Sensor Networks: The integration of different functionalities like sensing, processing and communication to from a network forms a base of wireless sensor networks which in turn becomes a sort of extension for Internet of things. The issues associated with the technology are data collected via sensor [9], disturbances in the network [10], changing network topology, anomaly associated with the base stations [11]. The sensor deployments have been carried out in large scale as well small scale networks and typically managed by wireless standards like Bluetooth [12], Zigbee [13], Z Wave [14], and ANT [15]. The other challenges include environmental effects, characteristics of network and resource scarcity.

Smart Phones: It is another technology which has brought a revolution in the actual visualisation of the vision of IoT. Since a plethora of mobile devices are actually connected via internet connection. The mobile phones actually have a quite sensitive amount of information about the user like its location, personal data, accounts

 ISSN: 2581-4370

information etc. [16]. The detection of privacy breach [17], the architectures have been created which keep privacy aspect via sensing intact [18], another aspect is secured location based services have also been dealt with caution [19].

Cloud services: The large amount of data has been effectively managed by cloud services. The sudden expansion in the information has been handled by the cloud computing paradigm. The research in the field of cloud has been primarily focussed on the data protection and prevention of leaks of data or information [20]. The store, processing and information of IOT application carried out by COSM [21] and Arrayent [22].

SECURITY ASPECTS IN IOT

IoT is one of the most trending technology in current generation and its advantages in various sector and applications are well known. But despite of enormous benefits, there are few drawbacks also exist. One of them is Security and Privacy concern in IoT. The communication sector of Internet of things is highly distorted from the security point of view and is vulnerable to loss of privacy for the end users. The information transfer from one host to another has led to several security breaches in IoT and is a major concern in terms of security aspects.

SECURITY PROBLEMS DUE TO WIRELESS SENSOR NETWORK

The issues prevailing in the Wireless networks can be classified as:

i. Attacks on confidentiality and verification
ii. Silent attacks on service unification and coherence
iii. Attacks on approachability of network: The denial of service (DoS) ([24], [25]) attack comes in this category. This restraint of availability of information to authorized users can take place on different layers of a network [26], [27], [28]. This resistance is done by unknown third party violator:

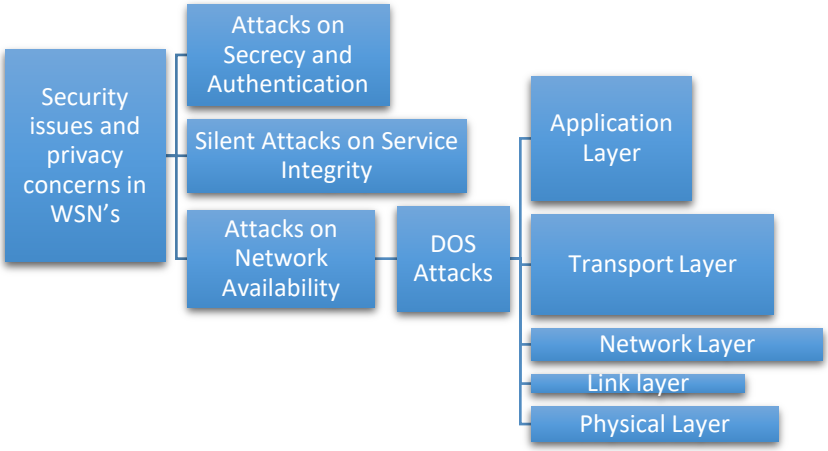

Figure 1.Security and privacy concerns in WSN's [35]

ATTACK OF DoS ON PHYSICAL LAYER

Several functions has been performed by physical layer in a wireless sensor network such as modulation and demodulation, transmission and reception of data, encryption at transmitter side and decryption at receiver side, generation and selection of suitable carrier frequency,[29]. Physical layer of WSN is mainly strike through.

1. Node Interference: Physical alteration of node position to obtain sensitive information is known as node tampering or node Interference.
2. Jamming: In this DOS attack it keeps hold of the communication channel and then the transfer of information is prohibited or blocked between each other due to the control over the communication channel.

 ISSN: 2581-4370

ATTACK OF DoS ON LINK LAYER

Function of Data link layer in Wireless Sensor Network includes merging of several data streams from various correction. In addition to this, the data link layer ensures the reliability between point-to-point or point-to-multipoint connection [38]. The DoS attacks occurs in this layer are:

1. Battery Consumption: Unexpected high traffic in a channel is caused by this type of DoS attack, which results in limiting the accessibility of that channel to a very few number of nodes. This kind of disturbance in the channel occur due to large number of "sending requests" (Request to send) and transmissions over the channel.
2. Collision: This kind of DoS attack can be seen when two nodes concurrently transmit information/ data in the form of packets on the channel of same frequency at the same time. The crashing affect causes minute changes in the packet and then eventually leads to mismatch of the packet at the receiver side. This causes the re-transmission of the disposed packet [39].
3. Biased: As described in [39], unfairness is an attack based on repeated collision. It is also referred as exhaustion based attacks

ATTACK OF DoS ON NETWORK LAYER

Routing is the primary function of network layer in Wireless Sensor Network. The particular DoS attacks takes place in this layer are:

1. Homing: It involves the search of cluster heads and key managers which can actually cause the whole network breakdown.
2. Sybil: In this attack, a single node is replicated by the attacker which represents it with multiple identities to other nodes.
3. Replaying, Spoofing and misdirection of traffic.
4. Hello flood attack: It is mainly involves the overcrowding by the useless messages. In this attack a single node transmits a useless message which is then further broadcasted or retransmitted by the attacker to create congestion in the network.

ATTACK OF DoS ON TRANSPORT LAYER

Main function of transport layer in the WSN architecture is to provide reliability of data transmission between source and destination and to avoid congestion resulting from large volume of traffic in the routers. The DoS attacks in this layer includes:

1. Flooding: The undesirable or useless data causes excessive traffic in the network which is termed as intentional traffic.
2. De-synchronization: In this the fake messages are generated at one side of the host or at both sides requesting retransmission of the data for certain correction to be made caused due to errors. These faulty instructions cause the dropping of energy levels at both sides or at a single side.

ATTACK OF DoS ON APPLICATION LAYER

Main responsibility of application layer in the Wireless Sensor Network is to manage the traffic. It also behaves as the presenter of software program for various applications which performs the translation of information into a user friendly and accessible form or helps in assembling data by transmitting queries. In this layer, stimulating the sensor nodes initiates a trail-based DoS attack to generate a large amount of traffic in the path towards the base station [40], [39].

Some secondary DoS attacks are as follows [23], [27], and [28]:

Black Hole, Node Subversion, Neglect and Greed Attack, Interrogation, Message Corruption, False Node, Passive Information Gathering, Node Outage, Node malfunction.

 ISSN: 2581-4370

Other security and privacy aspects in the sector of Internet of Things are:-

The entire IoT framework is susceptible to worm and virus attack. Unauthorized access to sensitive information like bank passwords, personal details like contact number and address.

Attack on any one device may risk the integrity of whole network and all devices connected in that particular network. Thus a single security failure can shut down the entire network of devices due to interconnectivity between them. It may lead to easy access of confidential information like financial status of an organization, bank details.

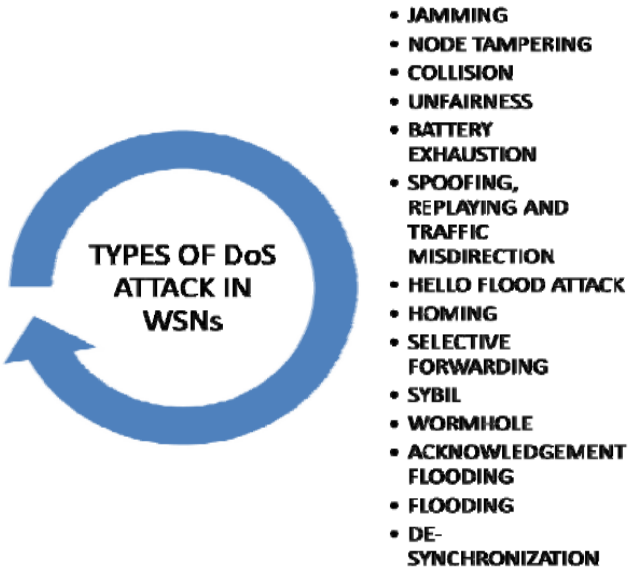

Figure 2.Types of Denial Attacks in wireless Sensor Network [23]

PRIVACY THREATS AND CHALLENGES IN IoT

The ever changing characteristics of IoT led to many security breaches and concerns. This section presents the classification of these challenges and threats.

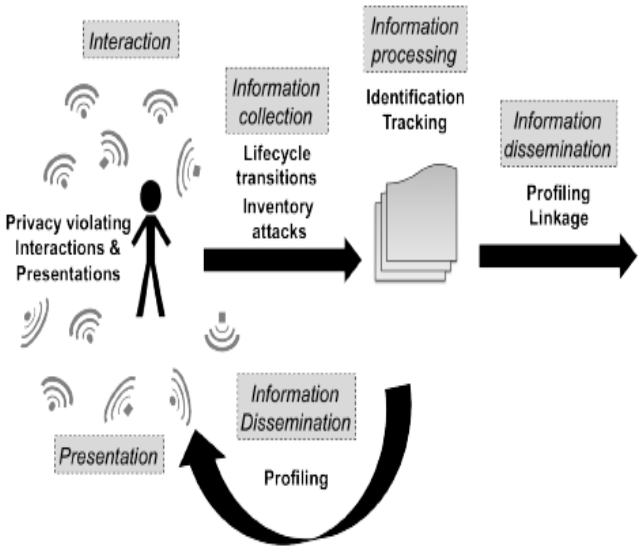

Figure 3.Attacks in different phases [32]

The above figure gives the division of various attacks in phases. There are 4 steps to this division. In the first method the threat is defined and subdivided into some particular division with

 ISSN: 2581-4370

surety of privacy breech. The second method the analysis is done on the IOT progressions and it measures the intensity of threats and tries to neutralise it with maximum effectivity. In the last method we look for remedies to counter these attacks from related field of work. And finally we present the most probable solution to eradicate the particular known threat.

IDENTIFICATION

IDENTIFICATION is the process by which a name or an address can be related with a specific being and all particulars about him. This threat of identification is currently the most ongoing one in our service model where information manifold is kept in places outside the user`s control. Firstly the use of camera for digital snooping is being integrated at a mind boggling rate and purposefully used in non-security means [30, 31]. Since the physiological features database from social media platforms (e. g. Instagram) is readily available to private agencies, the accurate prediction of an identity just by the pictures is a real time on going application [32]. Previous researches showed that an individual can be recognised by his Radio Frequency usage or identification [29]. Thirdly voice modification and recognition is vehemently used worldwide in day to day mobile applications and their subsequent databases are already available easily. They can be used to identify an individual anywhere and anytime just by a simple request by the Government [33]. Since speech recognition is fast and easily available and also interacts perfectly with IOT systems the security can be easily compromised with a valid question on defence mechanisms of present day security. Identity protection has already gained news in spheres of data anonymization [34] and identity management [35].

LOCALIZATION AND TRACKING

It is the threat where the target can be tracked and his location can be pin pointed accurately. It can easily done via GPS or cell phone location applications. Examples are GPS stalking [36]. This shows that users take it as privacy concerns when that can`t control their private information like location etc. The ongoing research in this area has proposed three main approaches a) client server b) trusted third party and c) peer to peer/distributed. Although these findings are on right path and fairly accurate yet they are not full proof and require additional research to be fully secure.

PROFILING

Profiling is the means by which the information of a particular target is obtained and co related with the database to predict the interests. This method is generally used by E-Commerce industries in offer validation and advertisements. The examples which justify breech of privacy is shown in [37]. Also accumulating data and selling this volatile information to marketing giants is prevalent today. This greatly impacts IOT as it has led to data explosion and a data boom. This has created more number of access points for the attackers to compromise the security of an individual.

LIFECYCLE TRANSITIONS

Privacy of users is also put at risk when smart devices accidently disclose sensitive information during their transitions. Most commonly the photos and videos are targeted. As these violations are mainly due to stored data in background, it gives an insight into our faulty collection phase of our model. This issue is amplified due to two features in IOT A) growth in number of intractable identities for e. g. financial data collected by credit card companies or heath related data collected by insurance companies. B) When items of everyday use become smart, then handling of this huge amount of data becomes difficult leaving personal space vulnerable to attacks.

 ISSN: 2581-4370

CHALLENGES FACED BY THE IOT HEALTH SYSTEMS

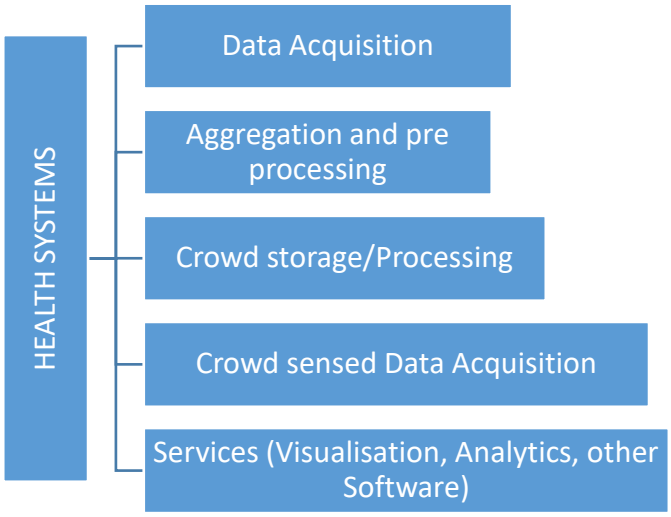

Figure 4.Process involved in processing of an information Via IOT based Health systems

The above mentioned are the components of an IOT based health system. IOT finds a major application in the health industry. The following section discusses the challenges faced by the health systems. At first let us have a brief look at the working of the same then analysing the challenges faced by them in the subsequent sections.

- **DATA ACQUISITION:** It involves collection of data from the various Wireless body area networks (WBAN's) or from the light weight sensors deployed [41].
- **DATA AGGREGATION AND PRE-PROCESSING:** The aggregation and pre-processing of the collected data is necessary in order to curtail the amount of data being handled and transmitted. The following process is carried out with the assistance of cloudlets and concentrators [42, 43].
- **CROWD SENSED DATA ACQUISITION:** It is quite an emerging phenomenon. It has simultaneous acquisition and aggregation of the data available. For e. g. , from a wearable sensor any two physical quantities like temperature and humidity.
- **CROWD STORAGE/PROCESSING:** Its services includes multiple services on one or more racks. The government regulations must be complied with.
- **SERVICES:** Various algorithms and decision sensing analytics services being provided here.

TECHNICAL CHALLENGES FACED BY THE HEALTH SYSTEM

1. **WIRELESS STANDARDS AND INTEROPERABILITY:** The wireless standards used in a system should be often pose a challenge since their interoperability is a big issue reason being they have to communicate and set links between two different devices which pose a challenge.
2. **PROTOCOL DESIGN CHALLENGES:** They deal with the path loss and low power gain in the WSN. The emergency resource allocation for message packets. Thermal aware routings to avoid tissue damage is one of the main challenges.
3. **DATA PRIVACY CHALLENGES**: Protecting the data from unauthorized access as always been a major concern. The primary crypto level challenges are part and parcel. The several encryption schemes which prevent these have been developed.

 ISSN: 2581-4370

4. **SYSTEM LEVEL SECURITY:** The attempts are made to procure the secret keys of the system.
5. **DATA TRUSTWORTHINESS CHALLENGES:** It deals with the distinction of sensor malfunction and the intentional sensor tampering.
6. **DATABASE CHALLENGES:** The health records data tampering pose a serious challenge to the IOT based health system. The database deals with the health records of the individuals any sort of tampering or mishandling may breach the privacy of the patient. Thus several statistical and machine learning tasks have been deployed.
7. **VISUALIZATION:** The data burden is reduced drastically on the doctor and handling the patient data has been made easy. Now multiple patients can be serviced which makes the whole process less time consuming.

CONCLUSION AND FUTURE SCOPE

The chapter showcases a Comprehensive analysis of the privacy and security threat and challenges in the Internet of things. A brief review is done regarding the evolution of the Internet of Things technology and then how the technologies related to it like WSN, RFID etc. were affected when then need for a secured and private network was essential. Then we studied various types of attacks on the layers such as physical, data link, network layer, transport and application layer. Then after possible explanation of the attacks and studying the securing breaches in the network we go on to analyse the possible ways to tackle the security and privacy aspects in the networks.

Finally our focus is on two main thoughts: Firstly IOT is a booming technology and it has several privacy concerns and hence must handle with a possible foresight and preparedness regarding the attacks. Secondly a useful consequence is a collective action backed by a legal framework to provide technical solutions. The possible future scope has a main focus on improving privacy aspects in distributed networks of the IOT technology. Additional ways to enhance the privacy like attribute based encryption (ABE) technologies are deeply studied in order to improve system characteristics.

REFERENCES

[1]. A. Zanella, “Internet of Things for smart cities,” *IEEE Internet Things J.* , vol. 1, no. 1, pp. 22-32, Feb. 2014.

[2]. Tadapaneni, N. R. (2019). Role of Fog Computing in the Internet of Things. International Journal of Scientific Research and Engineering Trends.

[3]. E. P. Leverett, “Quantitatively assessing and visualising industrial system attack surfaces,” M. S. thesis, Dept. Computer Lab. , Univ. Cambridge, Cambridge, U. K. , 2011.

[4]. P. Ohm, “Broken promises of privacy: Responding to the surprising failure of anonymization,” *UCLA Law Rev.* , vol. 57, no. 6, pp. 1701-1777, Aug. 2010.

[5]. Juels A. RFID security and privacy: a research survey. Selected Areas in Communications, IEEE Journal on 2006; 24(2):381-394, doi: 10. 1109/ JSAC. 2005. 861395.

[6]. Langheinrich M. A survey of RFID privacy approaches. Personal Ubiquitous Computer 2009; 13(6):413-421, doi: 10. 1007/s00779-008-0213-4.

[7]. Van Deursen T. 50 Ways to Break RFID Privacy. Privacy and Identity Management for Life, IFIP Advances in Information and Communication Technology, vol. 352. Springer Boston, 2011; 192-205, doi: 10. 1007/978-3-642 20769-3 16.

[8]. Khoo, Benjamin. "RFID as an enabler of the internet of things: issues of security and privacy." Internet of Things (iThings/ CPSCom), 2011 International Conference

 ISSN: 2581-4370

on and 4th International Conference on Cyber, Physical and Social Computing. IEEE, 2011.

[9]. Zhang W, Wang C, Feng T. GPˆ2S: Generic Privacy- Preservation Solutions for Approximate Aggregation of Sensor Data (concise contribution). Pervasive Computing and Communications, 2008. PerCom 2008. Sixth Annual IEEE International Conference on, 2008; 179 - 184, doi:10. 1109/PERCOM. 2008. 60.

[10]. Zhang R, Zhang Y, Ren K. Distributed privacy preserving access control in sensor networks. Parallel and Distributed Systems, IEEE Transactions on 2012; 23(8):1427 - 1438, doi: 10. 1109/TPDS. 2011. 299.

[11]. Internet of Things European Research Cluster (IERC). The Internet of Things 2012 - New Horizons. 3rd edn. , Halifax, UK, 2012.

[12]. Bluetooth SIG. Specification of the Bluetooth system. http://www. bluetooth. com [Online. Last accessed: 2012-10-12], 2001.

[13]. ZigBee Alliance. ZigBee specification 2006.

[14]. Z-Wave Alliance. The Z-Wave Alliance. [Online. Last accessed: 2012-10-12], 2012.

[15]. ANT wireless-Dynastream Innovations Inc. http://www.thisisant.com/ [Online. Last accessed: 2012-10-12].

[16]. Privacy Rights Clearinghouse. Privacy in the Age of the Smartphone. [Online. Last accessed: 2012-10-12], 2005.

[17]. Enck W, Gilbert P, Chun BG, Cox LP, Jung J, McDaniel P, Sheth AN. Taint Droid: an information flow tracking system for real time privacy monitoring on smart phones. Proceedings of the 9th USENIX conference on Operating systems design and implementation, OSDI'10, USENIX Association, 2010; 1-6.

[18]. Lane ND, Miluzzo E, Lu H, Peebles D, Choudhury T, Campbell AT. A survey of mobile phone sensing. IEEE Communications Magazine 2010; 48(9): 140-150. 58.

[19]. Krumm J. A survey of computational location privacy. Personal Ubiquitous Computing 2009; 13(6):391-399, doi: 10. 1007/s00779-008-0212-5.

[20]. Squicciarini A, Sundareswaran S, Lin D. Preventing Information Leakage from Indexing in the Cloud. Cloud Computing (CLOUD), 2010 IEEE 3rd International Conference on, 2010; 188 -195, doi: 10. 1109/ CLOUD. 2010. 82.

[21]. COSM - connect to your world [Online. Last accessed: 2013-01-30], 2013.

[22]. ARRAYENT - the platform for connected products [Online. Last accessed: 2013-01-30], 2013.

[23]. Aashima Singla, Ratika Sachdeva, "Review on Security Issues and Attacks in Wireless Sensor Networks International Journal of Advanced Research in Computer Science and Software Engineering <www. ijarcsse. com>. Volume 3, Issue 4, April 2013 ISSN: 2277 128X

[24]. M. Sharifnejad, M. Shari, M. Ghiasabadi and S. Beheshti, "A Survey on Wireless Sensor Networks Security", SETIT, (2007).

[25]. B. T. Wang and H. Schulzrinne, "An IP traceback mechanism for reflective DoS attacks", *Canadian Conference on Electrical and Computer Engineering*, *vol. 2*, (2004)May 2-5, pp. 901-904.

[26]. Sen, Jaydip. "Security and privacy challenges in cognitive wireless sensor networks." *arXiv preprintarXiv: 1302. 2253* (2013).

[27]. M. Saxena, "Security in Wireless Sensor Networks-A Layer based classification", Technical Report, Center for Education and Research in Information Assurance &Security-CERIAS, Purdue University. pages. cs. wisc. edu/~msaxena/papers/ 2007-04- cerias. pdf, **(**2007).

[28]. J. Sen, "A Survey on Wireless Sensor network Security", *International Journal of Communications Network and Information*

 ISSN: 2581-4370

Security, *vol. 1*, *no. 2*, (2009)August, pp. 59-82.

[29]. http://sensors-and-networks.blogspot. in/2011/08/physical-layer-for-wireless-sensor. html

[30]. Liu X, Krahnstoever N, Yu T, Tu P. What are customers looking at? Advanced Video and Signal Based Surveillance, 2007. AVSS 2007. IEEE Conference on, 2007; 405 -410, doi: 10. 1109/AVSS. 2007. 4425345.

[31]. Senior A, Brown L, Hampapur A, Shu CF, Zhai Y, Feris R, Tian YL, Borger S, Carlson C. Video analytics for retail. Advanced Video and Signal Based Surveillance, 2007. AVSS 2007. IEEE Conference on, 2007; 423-428, doi:10. 1109/AVSS. 2007. 4425348.

[32]. Solon O. Facedeals lets you check in to venues with your face. WIRED Magazine. http://bit. ly/Pdgsry [Online. Last accessed: 2012-10-12], 2012.

[33]. Talbot D. Siris großer Bruder. Technology Review. http://bit. ly/RUyLBS [Online. Last accessed: 2012-10-12], 2012.

[34]. Sweeney L. k-anonymity: a model for protecting privacy. Int. J. Uncertain. Fuzziness Knowl. -Based Syst. 2002; 10(5): 557-570, doi: 10. 1142/ S021848850200 1648.

[35]. Uzuner O, Luo Y, Szolovits P. Evaluating the State of- the-Art in Automatic De-identification. Journal of the American Medical Informatics Association 2007; 14(5):550-563, doi:10. 1197/jamia. M2444.

[36]. Voelcker J. Stalked by satellite - an alarming rise in GPS-enabled harassment. Spectrum, IEEE 2006; 43(7):15-16, doi:10. 1109/MSPEC. 2006. 1652998.

[37]. Odlyzko A. Privacy, economics, and price discrimination on the internet. Proceedings of the 5th international conference on Electronic commerce, ICEC'03, ACM, 2003; 355-366, doi:10. 1145/948005. 948051.

[38]. Ahmad Abed Alhameed Alkhatib, and Gurvinder Singh Baicher. "Wireless sensor network architecture." *International conference on computer networks and communication systems (CNCS 2012) IPCSIT*. *Vol. 35*. 2012, pp. 11-15.

[39]. Sunil Ghildiyal, Amit Kumar Mishra, Ashish Gupta, Neha Garg, "Analysis of Denial of Service (DoS) Attacks in Wireless Sensor Networks" IJRET: International Journal of Research in Engineering and Technology; eISSN: 2319-1163 | p ISSN: 2321-7308

[40]. Al-Sakib Khan Pathan, "Denial of Service in Wireless Sensor Networks: Issues and Challenges", Advances in Communications and Media Research, Vol. 6 (Edited by Anthony V. Stavros), ISBN: 978-1-60876-576-8, Nova Science Publishers, Inc. , USA, 2010.

[41]. A. Benharref and M. Serhani, "Novel cloud and SOA-based framework for E-Health monitoring using wireless biosensors," IEEE Journal of Biomed. and Health Inf. , vol. 18, no. 1, pp. 46-55, Jan 2014.

[42]. F. Hu, D. Xie, and S. Shen, "On the application of the internet of things in the field of medical and health care," in IEEE Int. Conf. on and IEEE Cyber, Physical and Social Computing Green Computing and Communications (GreenCom), (iThings/ CPSCom), Aug 2013, pp. 2053-2058.

[43]. N. Powers, A. Alling, K. Osolinsky, T. Soyata, M. Zhu, H. Wang, H. Ba, W. Heinzelman, J. Shi, and M. Kwon, "The Cloudlet Accelerator: Bringing Mobile-Cloud Face Recognition into Real-Time," in Globecom Workshops (GC Wkshps), San Diego, CA, Dec 2015.

 ISSN: 2581-4370