

Security Challenges in IoT Platforms and Possible Solutions

Dagogo Godwin Orifama*, Hope Okoro

Department of Electronics and Electrical Engineering, University of Leeds, Leeds, United Kingdom

Email address:

dagoris2010@gmail.com (D. G. Orifama), hopeokoro@ymail.com (H. Okoro)

*Corresponding author

To cite this article:

Dagogo Godwin Orifama, Hope Okoro. Security Challenges in IoT Platforms and Possible Solutions. *Internet of Things and Cloud Computing*. Vol. 8, No. 1, 2020, pp. 1-7. doi: 10.11648/j.iotcc.20200801.11

Received: January 20, 2020; **Accepted:** February 11, 2020; **Published:** February 18, 2020

Abstract: There has been an increase in the electronic devices connected to the internet space, with at least 40 billion more devices becoming smart devices via the embedded system in 2020. The internet of things (IoT) is an emerging technology that deals with the interconnection of smart devices via the internet space, hence providing enhanced communication, interaction and service delivery. Communication between IoT devices take place over the internet, placing the internet at the heart of IoT applications, hence, extending the security challenges present in the traditional network into the IoT system. This dissertation describes the various layers of an IoT network, it made mention of the three-layer architecture and describes the functions of each of its component. Also, and more importantly, the security challenges that affects the layers of an IoT network and possible solutions for each layer were discusses. Furthermore, these items were combined in a stack to discuss on IoT platforms, which is a combination of IoT devices and services connected via a communication protocol and ensures applications are send to users in a secure system. This makes it possible for the continuity of security between different stages and data tracking between IoT devices. Issues rising from IoT platforms that make it difficult for integration with other IoT devices concludes this study.

Keywords: IoT Architecture, Security Challenges, IoT Layer Attacks, Countermeasures, IoT Platforms

1. Introduction

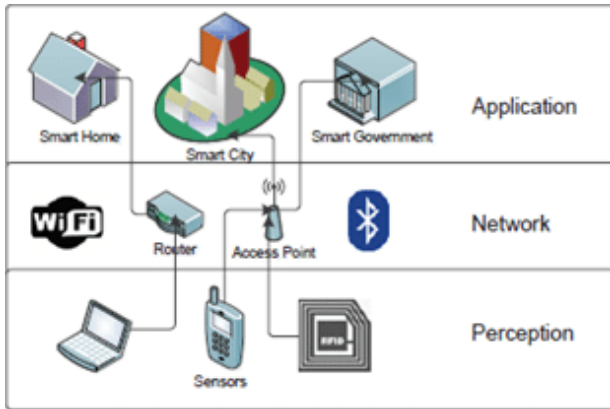
Internet of Things (IoT) is a system of interconnected computing devices, animal and people that possess a unique identifier, which can communicate with each other without intervention from humans [1, 2]. It is the natural development of machines to machine network and defined as anything from sensors to small servers. It is a paradigm made up of physical things which has an intelligent part capable of communicating with other domain sending the state of the machine or receive a control signal to be applied to the machine. The Internet of things is everything around us capable of transforming our regular actions to be recorded, processed and stored based on the current condition of the environment around the object. It is applicable in different sectors which include education, healthcare, transportation, etc. There are numerous advantages and applications of IoT, its applications are changing the way we live and perform

tasks by reducing time wastage and resources.

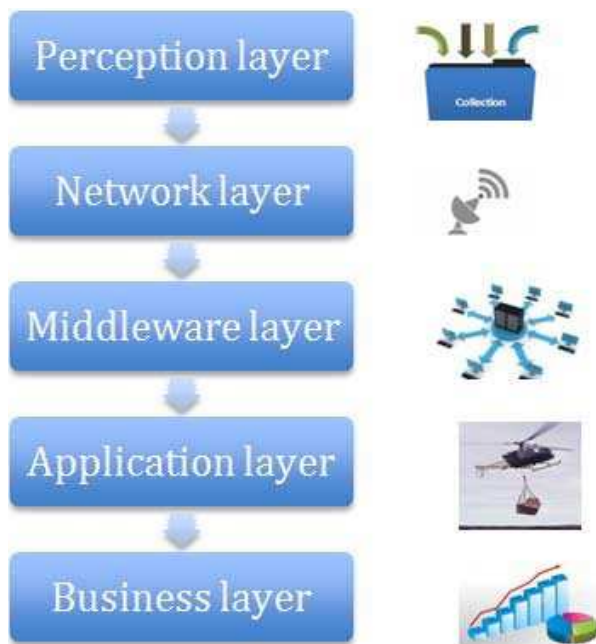
In 1999 at Procter & Gamble (P&G), Kevin Ashton introduced the phrase internet of things [3]. It has over the years evolved into a reality where objects are now connected to the internet. In recent year, IoT has drawn wide attention, one of which is the release of the 2005 annual report by the International Telecommunication Union (ITU) [4]. In this report, it was shown that RFID technologies have introduced new opportunities where objects will be interconnected. Currently, RFID has made possible the labelling and tagging of every device, hence serving as the basic identification mechanism in IoT [5].

The heart and key support for the Internet of Things is the Internet, hence most of the security challenges associated with the internet extends to IoT as well. Also, the fact that IoT nodes are assigned to position without supervision and coupled with the limited resources makes the security challenges in IoT more troublesome when compared to the traditional network. Hence, we must address these security

challenges urgently, as the rate of deployment and adoption of IoT devices is rapidly on the increase. Even though the traditional internet security threat extends into IoT, the countermeasures cannot be applied into IoT, due to the limitation of speed and processing power. This dissertation describes security challenges available in IoT Platforms and discusses possible countermeasures.



(a)



(b)

Figure 1. (a) The three-layer IoT Architecture [6] (b) The five-layer IoT Architecture [7].

2. IoT Architecture

IoT is a technology under its developmental stage and needs improvement at various level. There is no generally accepted IoT architecture [2, 8-11]. Also, different architectures have been proposed by various researchers. The three-layer architecture is the most basic architecture, it is shown in figure 1(a) with each layer explained subsequently

Physical Layer

The physical layer also known as perception layer, it is for

data acquisition. It collects data from the environment with the help of a sensor. The layer detects, collects and processes data from sensors and transmits it to the upper layer (Network layer). The perception layer includes 2-D bar codes and readers, RFID tags and reader-writers, sensors, cameras, GPS and sensor network [10].

Network or transport Layer

This layer is for connecting to other smart devices (things), network devices and servers. In other words, this network layer serves as a mediator between the internet layer and the IoT device [12]. Information obtained from the perception layers are transmitted and processed by this layer. It handles data routing and transmission to various IoT devices over the internet. At the network layer recent technologies like ZigBee, 3G, LTE, Wi-Fi etc are used for the operation of internet devices (gateway, routing and switching devices etc) to provide heterogenous network services.

Application Layer

The application layer delivers application-specific services to the user. It ensures the authenticity, integrity, and confidentiality of data. At this layer the IoT application that can be deployed, examples include: smart home, smart health, hence the purpose of IoT is achieved at this layer.

The main idea of IoT is defined by the three-layer architecture, but it is not sufficient for most IoT research. Hence, other architectures are introduced, one of which is the five-layered architecture consisting of an additional processing layer (or middleware) and business layer [7, 13-15]. The five-layer architecture is shown in figure 1(b).

3. Security Challenges in IoT

To achieve maximum security each component of the IoT system must be secured as the entire system can be exposed to threat and vulnerabilities if there is a bridge in security on a component of the system [16]. In this section, the various security challenges on each IoT layers are discussed.

3.1. Physical Layer Attacks

a) Node Tempering

An attacker with physical access to the node may alter the compromised node by changing part of the hardware or replacing it completely [17]. At this point, sensitive information can be removed.

b) RF Interference of RFIDs

The attacker through radio frequency sends noise signals which interfere with the RFID signal causing difficulty in communication. This attack is also called a denial of service attack [8, 18].

c) Physical Damage

This attack may result to a denial of service, it occurs when the attacker physically damages components of the IoT system.

d) Sleep Denial Attack

Most nodes are powered by replaceable batteries and program to sleep when not utilise, this prevents energy wastage and increases the life of the battery [19]. During the

attack the attacker prevents the node entering the sleep mode by feeding fake input to the node or supplying the node with a large amount of power which cause a shutdown of the node.

e) Injection of Malicious Node

It involves the attacker inserting a malicious node between IoT nodes. This result in the modification of data and dissemination of falsified data to other nodes. The multiple nodes are then used to carry out the attack [20].

f) Social Engineering

This attack involves physical interaction, the attacker takes advantage and manipulates IoT device users and obtaining sensitive information.

g) Node Jamming of WSN

Jamming in the context of Wireless Sensor Network, WSN is an attack done with the main purpose of interfering with the radio frequency used by sensor nodes [21]. In this attack the attacker uses a jammer to interfere with the wireless communication thus, leading to a denial of service [22].

h) Injection of Malicious code

The attacker sends malicious code into a node in the system thereby gaining access and control of the IoT system [23].

3.2. Network Layer Attacks

a) Traffic Analysis Attack

The attacker sniffs the network intercepts and examines messages using packet sniffer tools to get confidential information [24].

b) RFID Spoofing

An attacker spoofs RFID signal to obtain key information on RFID tag. The attacker uses this information to send offensive data using the same ID [18].

c) RFID Cloning

The attacker configures new RFID tags using data from valid RFID tags. In this case, the original ID of the RFID tag is not copied. With this, the attacker can transmit false data and control the data through the cloned tag [9].

d) RFID Unauthorized Access

Since the RFID system does not have a secure authentication and the tags can be accessed by anyone, this means tags can be manipulated. An attacker can observe, alter or even remove information on the node hence restricting valid access to the node [9, 25].

e) Man-in-the-Middle Attack

An attacker interferes with the communication between communicating sensor nodes via the internet to gain access and violates the privacy of the sensor node. This attack does not require the attacker to be physically present it is done through the network of the IoT system [9, 26].

f) Routing Information Attack

The attacker spoofs, modify or send routing information. This may result in dropping o packets, sending falsify data or partitioning of the network.

g) Sybil Attack

The attacker uses a single malicious node to forge multiple nodes within the network. This results in making the genuine

nodes into believing the forged nodes are many neighbours [27].

h) Sinkhole Attack

This attack sends various signals from the WSN node to a point. It compromises the safety of data since the packets are not delivered to the destination due to the attack [28, 29].

i) Denial of Service Attack

In this attack, the network is flooded by a large amount of traffic. This result in genuine users not having access to the service [30, 31].

3.3. Processing Layer Attacks

a) Data Security

The key concern when it comes to SAAS user is data security, the SAAS provider is responsible for providing such security. The major security issue occurs during data backup which is normally carried out by a third-party. The data stored in the cloud as plain text which is prone to data theft during backup [32, 33].

b) Application Security

Since the applications on cloud SAAS are accessed via the internet. An attacker can easily penetrate the IoT network. Once the attack has gained access to the network the data passing through the IoT network becomes unsafe, at this point malicious activities can be performed within the network [34].

3.4. Application Layer Attacks

a) Phishing Attacks

In this attack, an attacker obtains sensitive information such as user login details by email spoofing or using contaminated websites or applications [35].

b) Virus, Trojan Horse, Worms and Spyware Attack

The attacker gains access to a system by using malicious codes which can spread via infected software, email attachments or downloaded files and can result in tempering data or denial of service [36].

c) Software Vulnerabilities

This Vulnerability can occur due to lack of standardized code which can result in a security flaw or glitch in a software or operating system. The attacker can take advantage of such a glitch to gain access to the systems [37].

d) Data Security

In data communication user privacy is a key issue. Data can be lost or damage if perfect algorithms and mechanisms for data processing are lacking.

4. IoT Countermeasures

4.1. Physical Layer Attacks

a) physical Secure Design

To prevent an attack at the physical layer, the end nodes should be physically secured with high-quality components which is difficult to exchange. The security measure should include radio frequency circuit, chip selection and data acquisition unit design [38].

b) Anonymity

When the attacker enters the network, information about the attacker such as identity and location is hidden. This issue can be solved using the K-anonymity approach but is suitable for low processing devices [39].

c) Secure Booting

The integrity and authentication of software should be checked on various devices on the IoT network using cryptographic hash algorithm [40].

d) Authentication

To prevent false data flow into the IoT network, each device should undergo an authentication procedure before giving access to the network. This will help get rid of malicious devices from the network [41].

e) Data Integrity

To prevent data tempering IoT devices should possess an error detection mechanism such as checksum. For advanced security, the cryptographic hash algorithm should be implemented [42].

f) IPSEC Security Channel

Data transmission can be more secure by eliminating data tempering and eavesdropping. This can be achieved by providing proper authentication and encryption of data. IPsec security should provide both security features and should be utilised [43].

4.2. Network Layer Attacks

a) Data Privacy

To achieve data security at the network layer, illegal access to network nodes should be prevented. Point to point encryption security mechanism can be employed for this issue [44].

b) Sinkhole Attack

A sinkhole attack external to the network is prevented by utilising adequate data encryption and authentication as this will prevent the attacker from gaining access to the network. While sinkhole attack local to the network is prevented by using a security-aware ad hoc routing protocol (SAR) [45, 46].

c) Spoofing

Integrating a GPS location system into the IoT network can be used to prevent a spoofing attack, this technique is described and implemented in [47].

d) Routing Security

Secure routing is essential to successfully utilise a sensor system securely. To achieve this the data is routed through multiple paths to ensure an increased error detection of the network [48].

4.3. Processing Layer Attacks

a) Homomorphic Encryption

This method of encryption is used to ensure data security but requires a high level of computation [49]. It is based on full homomorphic encryption application and allows computation of ciphertexts without being decrypted [49, 50].

b) Fragmentation Redundancy Scattering (FRS)

In this method, sensitive data to be stored on the IoT cloud are broken down into fragment with each data having no significant information by itself. This data fragment is then stored on different servers to minimize data leakage [51].

c) Hyper Safe

Hyper safe is a security measure that lockdowns and prevent the modification of the write protected memory pages. This method uses a restricted pointer indexing techniques, it restricts pointing indexing which causes the conversion of controlled data into pointer indexes [52].

d) Encryption

By encrypting transmitted and stored data, data becomes more secure and this helps to overcome some potential attacks such as the side channels attack.

4.4. Application Layer Attacks

a) Risk Assessment

This method improves the security of the system by applying updates and patches of the device firmware for every detected threat to the system [54].

b) Firewalls

By using a firewall in the system unwanted packets such as unfriendly login attempts, and denial of service attack can be blocked. The packet which passes through the firewall is also authenticated hence ensuring the is from a source having access to the application [55].

c) Access Control List (ACLs)

ACL are can be applied in an IoT system, it specifies set a list of permission and policies which determine whether the incoming access request will be blocked or allowed.

d) User Authentication

This method of security provides adequate security of data by encrypting data. It prevents authorized access to data.

5. Security in IoT Platforms

IoT platform is the framework of IoT service which provides support for several operations. These operations vary from reporting, maintenance, deployment, development and the ability to provide decision making for IoT applications. However, IoT middleware deals with the heterogeneity issue of IoT systems, this is done by allowing devices and applications of different technology and contributors to safely run smoothly [56]. Basically, an IoT platform is a combination of various IoT devices and services which is connected via communication protocols. This protocol is utilized in presenting various applications to users in a secure way following the required standard. A standard IoT platforms architecture has eight layers which include: physical, Network, processing, storage, abstraction, services, application and collaboration as outlined in [57].

There have been various IoT platforms that have been introduced by companies and manufacturers such as Azure IoT (Microsoft), AWS IoT (Amazon), Jasper (Cisco). These IoT platforms have the problem of compatibility between platforms because each manufacturer has its own customized services and protocols. With each vendor using a customised

protocol, devices and architecture make it difficult to integrate with other systems.

For an increased security in IoT platforms, there is a need for a well-defined IoT framework standard which comprises of data structure, protocols and interfaces. These standards will provide the capability for various IoT platforms to be easily integrated, hence, different devices and services can be supported [58, 59].

6. Conclusions

IoT a developing area which has gathered lots of research topics in recent years just like other revolutionary technologies. Having adopted the traditional network architecture for communication has also inherited its security challenges. In this paper, the IoT architecture was discussed. Security challenges in each layer of IoT architecture were presented. Furthermore, countermeasures for providing security to an IoT network was discussed for the various security challenges. There are lots of IoT platforms which has been introduced, few of which includes Microsoft Azure and Amazon AWS. Each of these platforms has customised to have its own infrastructure, design and client needs which prevent collaborations between other platforms, this creates new security challenges. The paper further suggested a well-defined IoT framework standard as a mean to provide integration between IoT device and various IoT platform.

References

- [1] C. McClelland, "IoT Explained—How Does an IoT System Actually Work?," Medium, 20 11 2017. [Online]. Available: <https://medium.com/iotforall/iot-explained-how-does-an-iot-system-actually-work-e90e2c435fe7>. [Accessed 04 05 2018].
- [2] Yassine Chahid, Mohamed Benabdellah, Abdelmalek Azizi, "Internet of things security," *2017 International Conference on Wireless Technologies, Embedded and Intelligent Systems, WITS 2017*, 2017.
- [3] K. Ashton, "That 'Internet of Things' Thing," *RFI Journal*, no. 7, pp. 97-114, 2009.
- [4] "The Internet of Things," The international Telecommunication Union, ITU, 2005.
- [5] M. O'Halloran and M. Glavin, "RFID Patient Tagging and Database System," *International Conference on Networking, International Conference on Systems and International Conference on Mobile Communications and Learning Technologies (ICNICONSMCL'06)*, pp. 162-162, 2006.
- [6] Dhai eddine, Salhi & Tari, Abdelkamel & Kechadi, Tahar, "Forensics analysis and security challenges on Internet of Things," *Research Gate*, 2019.
- [7] Vashi, Shivangi & Ram, Jyotsnamayee & Modi, Janit & Verma, Saurav & Prakash, Chetana, "Internet of Things (IoT): A vision, architectural elements, and security issues," *Research Gate*, 2017.
- [8] L. Li, "Study on security architecture in the Internet of Things," *Measurement, Information and Control (MIC)*, 2012 *International Conference on*, vol. 1, no. Mic, pp. 374-377, 2012.
- [9] Ioannis Andre, Chrysostomos Chrysostomou, George Hadjichristofi, "Internet of Things: Security vulnerabilities and challenges," *Proceedings - IEEE Symposium on Computers and Communications*, Vols. 2016-February, pp. 180-187, 2016.
- [10] Miao Wu, Ting-lie Lu, Fei-Yang Ling, ling Sun, Hui-Ying Du, "Research on the architecture of Internet of things," *In preceeding of the 3rd International Conference on Advanced Computer Theory and Engineering (ICACTE '10)*, vol. 5, pp. V5-484-V5-487, IEEE, August 2010.
- [11] Omar Said, Mehedi Masud, "Towards internet of things: Survey and future vision," *International Journal of Computer Networks*, vol. 5, no. 1, pp. 1-17, 2013.
- [12] Marco Leo, Federica Battisti, Marco Carli, Alessandro Neri, "A federated architecture approach for Internet of Things security," *2014 Euro Med Telco Conference - From Network Infrastructures to Network Fabric: Revolution at the Edges, EMTC 2014, IEEE*, 2014.
- [13] Markus Eisenhauer, Peter Rosengren, Pablo Antolin, "A development platform for integrating wireless devices and sensors into Ambient Intelligence systems," *2009 6th IEEE Annual Communications Society Conference on Sensor, Mesh and Ad Hoc Communications and Networks Workshops, SECON Workshops 2009*, vol. 00, no. c, pp. 1-3, 2009.
- [14] Jeisa Domingues, Antonio Damaso, Rilter Nascimento, "An energy aware Middleware for integrating wireless sensor network and the internet," *International Journal of Distributed Sensor Networks*, vol. 2011, pp. 1-19, 2011.
- [15] Jollo Pero Sousa, David Garian, "Aura: an architectural framework for user mobility in ubiquitous computing enviroment," School of Computer Science Carnegie Mellon University, PA, USA, 2002.
- [16] Qi Jing, Athanasios V. Vasilakos, Jiafu Wan, Jingwei Lu, Dechao Qiu, "Security of the Internet of Things: perspectives and challenges," *Wireless Networks*, vol. 20, no. 8, pp. 2481-2501, 2014.
- [17] Daniel E. Burgner, Luay A. Wahsheh, "Security of Wireless Sensor Networks," *2011 Eighth International Conference on Information Technology: New Generations*, pp. 315-320, 2011.
- [18] Hong Li, YongHui Chen, ZhangQuing He, "The survey of RFID attacks and defenses," *2012 International Conference on IEEE Wireless Communications, Networking and Mobile Computing, WiCOM 2012*, pp. 0-3, 2012.
- [19] A. Phuphanin, W. Usaha, "Secure Coverage Control in Wireless Sensor Networks with Malicious Nodes Using Multi-agents," *2011 IFIP 9th International Conference on Embedded and Ubiquitous Computing*, pp. 390-396, 2011.
- [20] Farah Kandah, Yashaswi Singh, Weiyl Zhang, Chonggang Wang, "Mitigating colluding injected attack using monitoring verification in mobile ad-hoc networks," *Security and Communication Network*, vol. 6, no. 4, pp. 539-547, 2013.
- [21] Aristides Mpitiopoulos, Damianos Gavallas, "An effective defensive node against jamming attacks in sensor networks," *Security and Communication Networks*, vol. 2, no. 2, pp. 145-163, 2014.

- [22] Mingyan Li, Iordanis Koutsopoulos, Radha Poovendran, "Optimal Jamming Attack Strategies and Network Defense Policies in Wireless Sensor Networks," *IEEE Transactions on Mobile Computing*, vol. 9, no. 8, pp. 1119 - 1133, 2010.
- [23] Halim, Tasneem, Islam, Md, "Study on the security issues in WSN," *International Journal of Computer Applications*, vol. 53, no. 1, pp. 26-32, 2017.
- [24] Thakur Bhupendra Singh, Chaudhary, Sapna, "Content Sniffing Attack Detection in Client and Server Side: A Survey," *International Journal of Advanced Computer Research*, vol. 3, no. 2, pp. 7-10, 2013.
- [25] Ravi Uttarka, Raj Kulkarni, "Internet of Things: Architecture and Security," *International Journal of Computer Application*, vol. 3, no. 4, pp. 12-19, 2014.
- [26] Rabi Prasad Padhy, Manas Ranjan Patra, Suresh Chandra Satapathy, "Cloud Computing: Security Issues and Research Challenges," *IRACST - International Journal of Computer Science and Information Technology & Security (IJSITS)*, vol. 1, no. 2, pp. 136-146, 2011.
- [27] "Detecting Sybil attacks in Wireless Sensor Networks using neighboring information," *Computer Networks*, vol. 53, no. 18, pp. 3042-3056, 2009.
- [28] Chanatip Tumrongwittayapak, Ruttikorn Varakulsiripunth, "Detecting Sinkhole attacks in wireless sensor networks," *ICROS-SICE International Joint Conference*, pp. 1966-1971, 2009.
- [29] Ibrahim Abdullah, Mohammad Muntasir Rahman, Roy Mukul Chandra, "Detecting Sinkhole Attacks in Wireless Sensor Network using Hop Count," *International Journal of Computer Network and Information Security*, vol. 7, no. 3, pp. 50-56, 2015.
- [30] Djamel Mansouri, Lynda Mokddad, Jalel Ben-othman, Malika Ioualalen, "Preventing Denial of Service attacks in Wireless Sensor Networks," *2015 IEEE International Conference on Communications (ICC)*, pp. 3014-3019, 2015.
- [31] Abdul Wahid, Pavan Kumar, "A Survey on Security Attacks in Wireless Sensor Network," *International Journal for Innovative Research in Science and Technology*, vol. 1, no. 8, pp. 1684-1691, 2012.
- [32] D. H. Patil, Rakesh R. Bhavsar, Akshay S. Thorve, "Data Security over Cloud," *International Journal of Computer Applications*, pp. 11-14, 2012.
- [33] B. R. Kandukuri, R. P. V. and A. Rakshit, "Cloud Security Issue," *2009 IEEE International Conference on Services Computing, Bangalore*, pp. 517-520, 2009.
- [34] Ramaswamy Chandramouli, Peter Mell, "State of Security Readiness," *Crossroads*, vol. 16, no. 3, pp. 23-25, 2010.
- [35] A. K. Jain, B. B. Gupta, "Recent survey of various defense mechanisms against phishing attacks," *Journal of Information Privacy and Security*, vol. 12, no. 1, pp. 3-13, 2016.
- [36] Y. Tang and S. Chen, "Defending against Internet worms: a signature-based approach," *INFOCOM 2005. 24th Annual Joint Conference of the IEEE Computer and Communications Societies. Proceedings IEEE*, vol. 2, pp. 1384-1394, 2015.
- [37] Y. Shin, A. Meneely, "Evaluating Complexity, Code Churn, and Developer Activity Metrics as Indicators of Software Vulnerabilities," *IEEE Transactions on Software Engineering*, vol. 37, no. 6, pp. 772-787, 2011.
- [38] Yilin Mo, Tiffany Hyun-Jin Kim, Kenneth Brancik, Dona Dickinson, Heejo Lee, Adrian Perrig, and Bruno Sinopoli, "Cyber-physical security of a smart grid infrastructure," *Proceedings of the IEEE*, vol. 100, no. 1, pp. 195-09, 2012.
- [39] E. Vasilomanolakis, J. Daubert, M. Luthra, V. Gazis, A. Wiesmaier and P. Kikiras, "On the Security and Privacy of Internet of Things Architectures and Systems," *2015 International Workshop on Secure Internet of Things (SIoT)*, pp. 49-57, 2015.
- [40] G. Avoine, M. A. Bingöl, X. Carpent and S. B. O. Yalcin, "Privacy-Friendly Authentication in RFID Systems: On Sublinear Protocols Based on Symmetric-Key Cryptography," in *IEEE Transactions on Mobile Computing*, vol. 12, no. 10, pp. 2037-2049, 2013.
- [41] M. N. Babu, A. S. N. Chakravarthy and C. Ravindranath, "The design of a secure three factor authentication protocol for wireless sensor networks," *2017 International Conference on Nextgen Electronic Technologies: Silicon to Software (ICNETS2), Chennai*, pp. 184-190, 2017.
- [42] Mojtaba Alizaeh, Mazleena Salleh, Mazdak Zamani, Jafar Shayan, Sasan Karamizadeh, "Security and Performance Evaluation of Lightweight Cryptographic Algorithms in RFID," *Recent Researches in Communications and Computers*, pp. 45-50, 2015.
- [43] Daniel Migault, Daniel Palomares, Emmanuel Herbert, Wei You, Gabriel Ganne, Ghada Arfaoui, Maryline Laurent, "An Optimized IPsec Architecture for Secure and Fast Offload," *2012 Seventh International Conference on Availability, Reliability and Security, Prague*, pp. 365-374, 2012.
- [44] F. Baccelli, A. El Gamal and D. N. C. Tse, "Interference Networks With Point-to-Point Codes," in *IEEE Transactions on Information Theory*, vol. 57, no. 5, pp. 2582-2596, 2011.
- [45] S. Sharmila and G. Umamaheswari, "Detection of Sinkhole Attack in Wireless Sensor Networks Using Message Digest Algorithms," *2011 International Conference on Process Automation, Control and Computing, Coimbatore*, pp. 1-6, 2011.
- [46] S. Ahmad Salehi, M. A. Razzaque, P. Naraei and A. Farrokhtala, "Detection of sinkhole attack in wireless sensor networks," *2013 IEEE International Conference on Space Science and Communication (IconSpace), Melaka*, pp. 361-365, 2013.
- [47] S. Daneshmand, A. Jafarnia-Jahromi, Broumandan Ali, Lachapelle Gérard, "A Low-Complexity GPS Anti-Spoofing Method Using a Multi-Antenna Array," *ResearchGate*, pp. 1233-1243, 2012.
- [48] Zhanyang Xu, Yue Yin, and Jin Wang, "A Density-based Energy-efficient Clustering Algorithm for Wireless Sensor Networks," *International Journal of Future Generation Communication and Networking*, vol. 6, no. 1, pp. 75-86, 2013.
- [49] Zvika Brakerski and Vinod Vaikuntanathan, "Efficient Fully Homomorphic Encryption from (Standard)," *SIAM Journal on Computing*, vol. 43, no. 2, pp. 831-871, 2014.

- [50] G. Sun, S. Huang, W. Bao, Y. Yang and Z. Wang, "A privacy protection policy combined with privacy homomorphism in the Internet of Things," *2014 23rd International Conference on Computer Communication and Networks (ICCCN)*, Shanghai, pp. 1-6, 2014.
- [51] Y. Singh, F. Kandah and Weiyi Zhang, "A secured cost-effective multi-cloud storage in cloud computing," *2011 IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS)*, Shanghai, pp. 619-624, 2011.
- [52] Sarvesh Kumar, Suraj Pal Singh, Ashwanee Kumar Singh, Jahangir Ali, "Virtualization, The Great Thing and Issues in Cloud Computing," *International Journal of Current Engineering and Technology*, 2013, pp. 338-341, 2013.
- [53] Dongyoung Koo, Junbeom Hur, Hyunsoo Yoon, "Secure and efficient data retrieval over encrypted data using attribute-based encryption in cloud storage," *Computers and Electrical Engineering*, vol. 39, no. 1, pp. 34-46, 2013.
- [54] C. Liu, Y. Zhang, J. Zeng, L. Peng and R. Chen, "Research on Dynamical Security Risk Assessment for the Internet of Things inspired by immunology," *2012 8th International Conference on Natural Computation, Chongqing*, pp. 874-878, 2012.
- [55] Kong Shiao-tong, Application Foreign, Data Priority, "Pin-hole firewall for communicating data packets on a packet network," *U.S. Patent and Trademark Office*, vol. 2, no. 12, pp. 12-15, 2011.
- [56] Technology Theme, "Differentiating between Platform, Framework and Middleware," Technology Theme, [Online]. Available: <http://technologicalthemes.blogspot.co.uk/2009/09/differentiating-between-platform.html>. [Accessed 24 04 2018].
- [57] "H2020 – UNIFY-IoT Project: Report on IoT platform activities," [Online]. Available: <http://www.iot.gen.tr/2016/12/25/h2020-unify-iot-project-report-on-iot-platform-activities/>. [Accessed 23 04 2018].
- [58] Keiko Hashizume, David G Rosado, Eduardo Fernández-Medina, Eduardo B Fernandez, "An analysis of security issues for cloud computing," *Journal of Internet Services and Applications*, vol. 4, no. 1, pp. 1-13, 2013.
- [59] C. M. Chen, Y. H. Lin, Y. C. Lin and H. M. Sun, "RCDA: Recoverable Concealed Data Aggregation for Data Integrity in Wireless Sensor Networks," in *IEEE Transactions on Parallel and Distributed Systems*, vol. 23, no. 4, pp. 727-734, April, 2012.