An Analysis of the Current State of Security in the Internet of Things

DORUK PANCAROGLU[1] and SEVIL SEN[2]

[1] STM A.S., Ankara/Turkey, dpancaroglu@stm.com.tr
[2] WISE Lab., Hacettepe University, Ankara/Turkey, ssen@cs.hacettepe.edu.tr

***Abstract* – Internet of Things (IoT), a technology in which various physical devices are interconnected with each other using a conglomeration of technologies, is one of the fastest growing sectors. This ever-increasing demand for IoT devices are satisfied by products from many different companies with varying qualities and more importantly, varying principles regarding security. The fact that unified security protocols and approaches are lacking between the manufacturers and no significant regulations or legislation concerning IoT exist in a national and international level, creates a significant security risk. Moreover, the well-known security solutions are often incompatible with IoT devices mainly because of the power and computational constraints of IoT devices. This work aims to identify the current security risks concerning IoT and present some of the solutions that address these risks. The physical, regulational and social challenges stemming from IoT security solutions will be analyzed, and future directions will be explored.**

***Keywords* – IoT, IoT Security, IoT Architecture**

I. INTRODUCTION

Internet of Things (IoT) is the name given to the network of devices embedded with software, actuators, electronics, connectivity, and sensors which enables these objects to connect with each other and establish an exchange of data. These 'things' include vehicles, smartphones, computers, wearable technologies, home electronics, home appliances, RFID tags and many other small devices.

The concept of IoT is not young, and dates back to 1982. A beverage machine in Carnegie Mellon University (CMU) was fitted with an internet connection to inform the users about the number of cokes left in the machine and whether the cokes are cold [1].

The actual term of IoT, without the specifics, is coined by Kevin Ashton, in a paper published in 1999 [2]. The first whitepaper that mentions IoT with details about its vision and capabilities is published in 2001 [3]. First publication solely focused on IoT is published in 2002 [4].

While it can be understood that IoT is a relatively new technology, it is estimated that approximately 15 billion IoT devices were connected in 2015, and this number is projected to be around 75 billion in 2020 [5].

IoT has many applications including but not limited to the following:

- Home automation (smart homes)
- Connected health
- Wearable technologies
- Smart vehicles
- Smart buildings
- Smart cities
- Smart manufacturing

The cause of the fast adoption of IoT in the numerous fields described above can be attributed to many different technologies developed concurrently in the recent years. These technologies include LTE(5G), Bluetooth Low Energy (BLE), Near Field Communication (NFC), Radio Frequency Identification (RFID), QR Codes, ZigBee [6], Power-line Communication (PLC) and Wi-Fi Direct.

The proliferation of IoT led to a boom in the industry, and the presence of various manufacturers for IoT devices and solutions has led to varying security principles and protocols, if any exists at all. This created a security deficit for a lot of IoT systems, containing different components from different manufacturers, with different levels of security.

Another concern about IoT security stems from the fact that there is a lack of international standards regarding IoT security [7]. As IoT is a relatively young field, many states and organizations lack rules and legislature, which causes a lack of standardization and coordination among manufacturers and security experts [8].

This work aims to analyze the current state of IoT security, explore the challenges it faces and the solutions developed to overcome these challenges. Additionally, some of the related works in the field of IoT security will be mentioned.

This paper is organized in five chapters: the first chapter introduces the problem. The second chapter describes the IoT architecture, detailing the layers. The third chapter explains the IoT security, detailing the principles, issues and countermeasures respectively. The fourth chapter lists some of the works related IoT security. The fifth chapter concludes the paper with an insight into future directions.

II. IOT ARCHITECTURE

IoT architecture is generally divided into three or four layers by researchers [9-11]. These layers are named Perception (also known as sensor layer), Network, Middleware (sometimes included into application) and Application. A simple representation of these layers can be observed in figure 1.

The lowermost layer, perception layer, is also called sensors layer. As its name suggests, its purpose is to gather data from

the environment with the built-in sensors [12]. In this layer, data is detected, collected, processed and transmitted to the network layer.

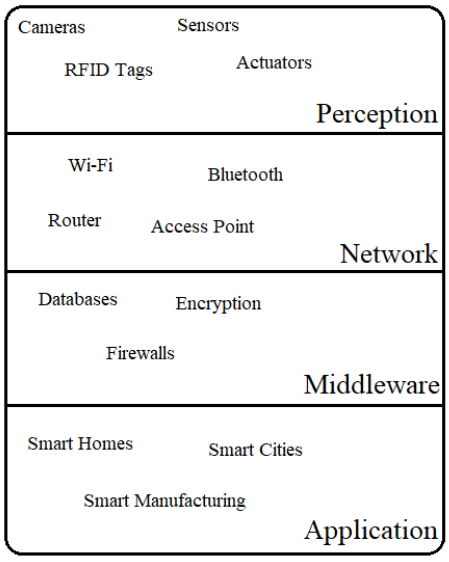

Figure 1: The four architectural layers of IoT

The middle layer, called the network layer, is tasked with the jobs of routing data and being a point of transmission between different hubs of IoT, and the devices those hubs contain. The network gateways can be described as a man-in-between, communicating with various IoT nodes via different actions such as collection, aggregation, filtering and transmission of data between sensors [11]. Technologies that are used in this layer include, but are not limited to, Wi-Fi, LTE, Bluetooth, 3G and Zigbee.

The contested layer among researchers, middleware layer, is comprised of systems for processing information, which in turn, ensure that automated actions are taken, based on the results of the information processing systems. Additionally, this layer also provides a link between the IoT systems with the database, granting the system with storage capabilities for the data that is collected [13]. Some researchers add this layer to the application layer.

The last and uppermost layer, application layer, is where the IoT meets the users. In this layer, realization of various applications of IoT, with respect to the needs and constraints of the system's objectives, happens [14]. Moreover, the guaranteeing of the data, in terms of confidentiality, authenticity and integrity is achieved in this layer.

III. IoT Security

As all connected devices, IoT needs established security solutions. But the rapid, and sometimes rushed, development in IoT devices led to reduced emphasis on security. Lack of established protocols or international agreements among manufacturers also created a disunity among the security levels of IoT devices.

While most issues are similar with conventional devices, most solutions are unsuitable for IoT devices which have different constraints such as computing and battery power. Thus, new approaches are needed to be developed urgently.

This chapter aims to explore the principles, issues and countermeasures of IoT security.

A. Principles

Considering the architectural design and the general fundamentals of IoT and the types and roles of the devices an IoT network contains, the following principles are named and elaborated upon.

- Confidentiality

  Confidentiality is a very important principle which ensures that the data is secure and available only for the authorized users and/or devices. Also, the issue of data management must be addressed as well. Collected sensor data should not be revealed to neighboring nodes [15].
- Integrity

  The integrity principle ensures that the accuracy of the data is coming from the right sender and also the data is not tampered with. Holding the integrity principle is made possible by maintaining end-to-end security for communications between the devices in an IoT network [16].
- Availability

  The availability principle dictates that the users of an IoT network should have an availability of the whole data in a system when needed. Besides data, devices and services must also be reachable and available too.
- Authentication

  The authentication principle is concerned with that fact that objects in an IoT network need to have the ability of authentication and identification of other objects clearly. This principle creates a need for a mechanism to perform mutual authentication of entities for every interaction in an IoT network [17].

The following principles are unique to IoT, and should be considered separately:

- Lightweight Solutions

  Lightweight solutions is a limitation rather than a principle, which should always be kept in mind while during the design and implementation of IoT security protocols. IoT devices have limited power and computation capabilities, and security solutions should be compatible with these devices.
- Heterogeneity

  This principle is born of the fact that IoT connects numerous devices with varying capabilities, architectures and manufacturers.

  Security protocols must be designed to work in all devices in the IoT network, as well as in different situations [18]. There is also fact that in IoT, environment is almost always dynamic, and this also has to be managed.
- Policies

  In IoT, there is a need for standards and policies for management, protection and transmission of data

efficiently. Consequentially, there must be a mechanism (such as regulations) to enforce these policies. Current policies are not suitable to the nature of the IoT.

B. Issues

Each architectural layer in IoT is vulnerable to various types of attacks and security threats. The nature of these attacks and threats can either be active or passive, and their origins can be from outside sources or from inside.

Active attacks are a type of attack, aimed at altering or outright directly stopping the service, while passive attacks function by monitoring the IoT network information without causing a hindrance to the service of IoT.

The security issues will be expanded upon by grouping them into the architectural layers, starting with the perception layer below:

- Sensor Nodes
  Sensor nodes can be intercepted physically by attackers, causing loss of property and data, and leading to other types of attacks which will be explained in the following paragraphs.
- IoT Topology
  The inherent nature of IoT topology makes it susceptible to various forms of attacks [19].
- Unauthorized Access to RFID Tags
  RIFD tags often lack well-defined mechanisms for authentication and consequently, these tags can be accessed by someone lacking any form of authorization. When an RFID tag is accessed in any way, the data stored in it can be read, modified or deleted easily [20].
- RFID Tag Cloning
  This type of attack generally occurs concurrently with the previous attack type. Captured RFID tags can be cloned to replicate or compromise sensor data in an IoT network [21].
- RFID Eavesdropping
  Due to the wireless nature of RFID communication, eavesdropping on incoming and outgoing data can be performed easily, causing crucial system data such as passwords to be gathered [22].
- Wireless and RFID Signals
  The signals can be tampered or jammed to reduce/stop communication between IoT devices [23].
- Spoofing (Replay Attack)
  Spoofing is the act of broadcasting fabricated information to the RFID sensors in an IoT, with the intent of tricking them. This type of attacks generally result in the attacked gaining full control of an IoT system [24].

For the network layer of IoT architecture, the following issues or attack types can be listed:

- Sybil Attack
  In Sybil attacks, the attacker performs a manipulation on an IoT node to create numerous identities for that node, which may cause a breach in the IoT system, causing the system to be compromised by the way of false information presence [25].
- Sinkhole Attack
  In the sinkhole type of attack, the attacker causes a node in an IoT system to become more eligible for the other nodes by various means, causing the node to become a hub to pass information from, effectively gathering all the information flowing in an IoT system.
  The attacked system believes data is passed to its original destination, or contrarily, when all flow is ceased, energy loss is caused [26].
- Sleep Deprivation Attack
  This is a type of attack which keeps the nodes awake by transmitting unneeded information constantly, causing more battery consumption and causing the shutdown of the nodes, as a consequence [27].
- Denial of Service (DoS) Attack
  In a DoS attack, the attackers flood the network with a crippling number of traffic, causing an exhaustion of resources belonging to the system targeted by the attackers, creating an unavailability of the system for the real users. [28].
- Malicious code Injection
  The attacker causes a node to be compromised, which in turn injects harmful code into an IoT system, creating a possibility to shut the whole network down [29].
- Man-in-the-Middle Attack
  This type of attack targets the communication channel of an IoT system, enabling the attacker to monitor or take control of all the communications happening among the devices in the system [30].

For the middleware layer of IoT architecture, the following issues or attack types can be listed:

- Unauthorized Access
  In this type of threat, the attacker has the potential to cause damage easily, by the means of restricting the access services of the IoT system in question, or more bluntly, by deleting the all the data in an IoT system.
- DoS Attack
  DoS attacks are similar to each other among the layers. Similar to its counterparts, DoS attacks in the middleware layer causes a shutdown of the IoT system, resulting in the services' unavailability.
- Malicious Insider
  This type of attack is almost always insider, by the way of tampering the data for personal gain or a third party. The data found in an IoT system can be easily extracted and changed for any purpose of the attacker.

For the application layer of IoT architecture, the following issues or attack types can be listed:

- Denial-of-Service (DoS) Attack
  DoS attacks occurring in the application layer are becoming more and more sophisticated, targeting the data privacy of the users in an IoT system, putting the non-encrypted personal details of the target at the hands of the attacker.
- Sniffing Attack
  This type of attack targets the IoT system by the way of a sniffer insertion. A sniffer is an application which

aims to gain control of the network information, causing a corruption of the system [31].

C. Countermeasures

Similar to the security issues explored in the previous section, the countermeasures can be grouped into the architectural layers of IoT. A simple representation of the countermeasures grouped into layers can be seen in figure 2.

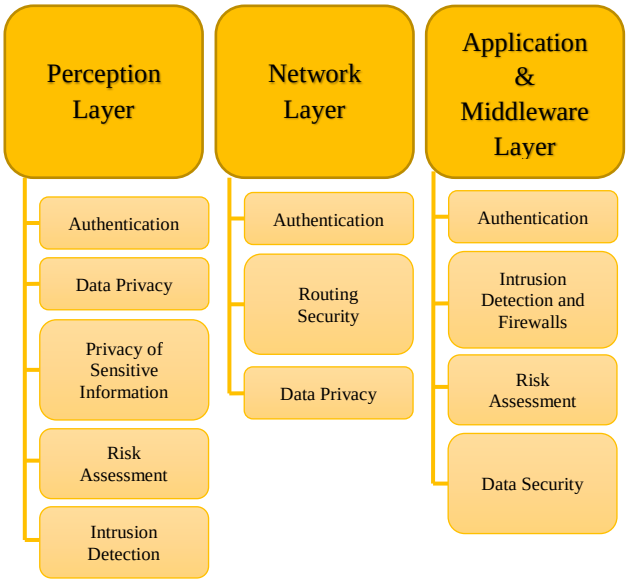

Figure 2: Countermeasures proposed for the four architectural layers of IoT

For the perception layer, the following countermeasures are proposed:

- Authentication

  Authentication in the perception layer is achieved with the help of CHA [32] (Cryptographic Hash Algorithms), which is useful in providing digital signatures for the IoT devices acting as terminals, enabling them to withstand attacks such as, brute force attack, side-channel attack and collision attack.

- Data Privacy

  Data privacy in the perception layer is guaranteed using encryption algorithms, both symmetric and asymmetric, such as DSA [33], RSA [34], DES [35] and BLOWFISH [36].

  These algorithms are used to safeguard the sensor data, preventing access by unauthorized parties, while the data is in the process of collection or transmission to the next layer of IoT architecture. Due to their low power requirements of this type of countermeasure, implementation into the sensors cannot be easily achieved.

- Privacy of Sensitive Information

  Hiding the sensitive data, and at the same time, maintaining the anonymity of the identity and location of IoT devices can be made possible with several methods. One of these is the K-Anonymity approach. This approach ensures that the identity and location of the IoT devices and the users remain protected [37].

- Risk Assessment

  Risk assessment is a fundamental part of IoT security countermeasures. Performing risk assessment enables the users to discover possible threats to the IoT system in question.

  Moreover, the process could also help in determining the best security strategies and preventing the security breaches. Dynamical Risk Assessment method for IoT is an example for this type of countermeasure [38].

- Intrusion Detection

  When an intrusion is being detected in the perception layer of the IoT system, a proper response could be initiated. For instance, a kill command is automatically sent from the RFID reader to the RFID tag, preventing unauthorized access to the data stored in the RFID tags [39].

The countermeasures in the network layer of the IoT are detailed below:

- Authentication

  Using proper authentication processes and ensuring end-to-end encryption, unauthorized access to the sensor nodes, which in turn could broadcast false information, can be prevented [40].

- Routing Security

  This type of countermeasures are implemented after the authentication phase. Routing security ensures that the data exchange between the sensors and middleware of IoT devices are handled in a private manner [41].

  Routing security is made possible by providing more than one path for routing of the data which results in an improvement for the system in detecting an error. This type of countermeasures also enable the system to keep on performing even if there is a failure in the IoT system [42].

- Data Privacy

  This type of countermeasure includes safety control mechanisms, which monitor the system for intrusions of any kind. Data privacy countermeasures also include data integrity methods, which are implemented to ensure that the received data is the same at both ends.

The countermeasures in the middleware & application layers are grouped and detailed below:

- Authentication

  The authentication countermeasures found in the middleware & application layers are similar to the other architectural layers of IoT. The authentication process forbids access to any unauthorized user using built-in identity control methods.

  This process is similar to the process of identification in the other architectural layers of IoT, but in the middleware & application layers, authentication is also encouraged by other co-operating services, meaning that users are free to choose what information should be saved by the other services

  The middleware & application layers of IoT use various technologies such as virtualization and cloud

computing, both of which are prone to attacks. Both domains require significant research to achieve a secure environment.

- Intrusion Detection & Firewalls

  The countermeasures focused on the intrusion detection in IoT provide various solutions for security threats by looking for suspicious activity and raising an alarm if said activities occur.

  Additionally, the system is monitored continuously and a log is kept for any activities of the intruders. This is managed by various techniques for intrusion detection such as anomaly detection and data mining [43-44].
- Risk Assessment

  The risk assessment countermeasures, similar to the ones in the other architectural layers, provide justification for useful security strategies, while also providing improvements in the existing structure of security.
- Data Security

  This countermeasure is made possible by various technologies of encryption, with the aim of preventing threats for stealing data from the IoT system.

IV. Related Works

This chapter will aim to present some of the works, completed or in progress, focused on the field of IoT security.

- Blockchain for IoT Security and Privacy: The Case Study of a Smart Home [45]

  This paper aims to provide security for IoT by creating a blockchain where all the devices in a particular IoT network belong, with a 'miner' device handling the communications between all the devices.
- A Novel Mutual Authentication Scheme for Internet of Things [46]

  This paper proposes a novel authentication scheme between IoT devices which is also lightweight and secure.
- Identity Authentication and Capability Based Access Control (IACAC) for the Internet of Things [18]

  This paper creates a model for access control to protect the IoT against man-in-the-middle and DoS attacks. The model is novel in the way that it provides an integrated approach of authentication and access control for IoT devices.
- Capability-based Access Control Delegation Model on the Federated IoT Network [47]

  Another work by the authors of [18], this paper enables access delegation using a capability propagation mechanism named Capability-based Context Aware Access Control (CCAAC), which is both flexible and scalable.
- A Federated Architecture Approach for Internet of Things security [48]

  A federated IoT security framework named Secure Mediation Gateway (SMGW) is proposed in this paper which provides dynamic prevention, detection, diagnosis, isolation and countermeasures against cyber-attacks.
- SIFT: Building an Internet of Safe Things [49]

  The authors propose SIFT, an IFTTT-like safety-centric programming platform for IoT devices. SIFT aims to handle the issues like security and policies and provide users with a stable platform.
- Securing the Internet of Things: A Standardization Perspective [50]

  This paper is more concerned with the network layer of the IoT architecture, and argues that existing protocols such as CoAP, DTLS and 6LoWPAN are inadequate considering the nature of IoT devices.
- Stanford Secure Internet of Things Project (SITP) [51]

  SITP is a project initiated by Stanford University. It is a cross-disciplinary research effort between computer science and electrical engineering faculty between multiple universities. The project is focused on analytics and security.
- OWASP Internet of Things Project [53]

  This is an open-source project focused on the security issues of IoT such as vulnerabilities, firmware analysis, design principles, testing and security guidelines etc.

V. Regulations About IoT Around the World

Governmental and international regulations about IoT itself, and more importantly about IoT security, is a serious issue. In particular, privacy and security concerns about data collection by IoT is a major issue for governments. Data ownership and consumer choice are the other significant factors.

A report by US Federal Trade Commission recommended some guidelines for IoT [54], the key points being:

- Data security
- Data consent
- Data minimization

As yet, no state-level or government level legislation has passed concerning IoT security. This in turn, causes a lack of security standards for manufacturers of IoT devices. China, one the leading pioneers in IoT technology and manufacturing, has recently started the process of establishing standards and regulations about IoT [55-56].

VI. future Directions & Conclusion

To sum up, IoT security is a major concern for the ever-growing number of IoT networks and applications. Research conducted in the IoT security field has only recently started and needs to develop urgently.

As explored in this paper, there are many security issues concerning IoT and most of the proposed countermeasures are not fully implemented or in progress of implementation.

As IoT devices are becoming more and more widespread, governmental control, regulations about devices and manufacturers, and lastly, legal frameworks (both national and international) will be needed immediately.

In addition, standardization in architecture and protocols would provide beneficial for the long term security and ease of production and maintenance.

Lastly, some technological changes, such as the transition from IPv4 to IPv6 and 5G, is essential for IoT to spread and reach its full potential. It should be noted that this, in turn, can bring up different security issues altogether.

REFERENCES

[1] Carnegie Mellon University. The "Only" Coke Machine on the Internet. Retrieved 22 August 2018, from https://www.cs.cmu.edu/~coke/history_long.txt

[2] Ashton, K. (2009). "That 'internet of things' thing", in. RFID journal, 22(7), 97-114.

[3] Brock, D. L. (2001). The electronic product code (epc). Auto-ID Center White Paper MIT-AUTOID-WH-002.

[4] Främling, K. (2002). "Tracking of material flow by an Internet-based product data management system", Tieke EDISTY magazine, (1).

[5] Danova, T. (2013, October 02). Morgan Stanley: 75 Billion Devices Will Be Connected To The Internet Of Things By 2020. Retrieved August 22, 2018, from https://www.businessinsider.com/75-billion-devices-will-be-connected-to-the-internet-by-2020-2013-10

[6] ZigBee, A. (2006). Zigbee-2006 specification. http://www.zigbee.org/.

[7] Hwang, I., & Kim, Y. G. (2017, February). "Analysis of Security Standardization for the Internet of Things", in Platform Technology and Service (PlatCon), 2017 International Conference on (pp. 1-6). IEEE.

[8] Weber, R. H. (2010). "Internet of Things–New security and privacy challenges", in Computer Law & Security Review, 26(1), 23-30.

[9] K. Zhao and L. Ge, "A survey on the internet of things security", in Int'l Conf. on Computational Intelligence and Security (CIS), 663-667, 2013.

[10] L. Atzori, A. Iera, G. Morabito, and M. Nitti, "The social internet of things (siot)–when social networks meet the internet of things: Concept, architecture and network characterization", Computer Networks, vol. 56, 3594-3608, 2012.

[11] M. Leo, F. Battisti, M. Carli, and A. Neri, "A federated architecture approach for Internet of Things security", in Euro Med Telco Conference (EMTC), 1-5, 2014.

[12] Xue Yang, Zhihua Li, Zhenmin Geng, Haitao Zhang, "A Multilayer Security Model for Internet of Things", in Communications in Computer and Information Science, 2012, Volume 312, pp 388-393

[13] R. Khan, S. U. Khan, R. Zaheer, S. Khan, "Future Internet: The Internet of Things Architecture, Possible Applications and Key Challenges", in 10th International Conference on Frontiers of Information Technology (FIT 2012), 2012, pp. 257-260

[14] S. Yan-Rong, H. Tao, "Internet of Things: Key Technologies and Architectures Research in Information Processing", in Proceedings of the 2nd International Conference on Computer Science and Electronics Engineering (ICCSEE), 2013

[15] M. Farooq, M. Waseem, A. Khairi, and S. Mazhar, "A Critical Analysis on the Security Concerns of Internet of Things (IoT)", Perception, vol. 111, 2015.

[16] R. Roman, P. Najera, and J. Lopez, "Securing the internet of things", Computer, vol. 44, 51-58, 2011

[17] R. Roman, J. Zhou, and J. Lopez, "On the features and challenges of security and privacy in distributed internet of things", Computer Networks, vol. 57, 2266-2279, 2013.

[18] P. N. Mahalle, B. Anggorojati, N. R. Prasad, and R. Prasad, "Identity authentication and capability based access control (iacac) for the internet of things", J. of Cyber Security and Mobility, vol. 1, 309-348, 2013.

[19] M. Abomhara and G. M. Koien, "Security and privacy in the Internet of Things: Current status and open issues", in Int'l Conference on Privacy and Security in Mobile Systems (PRISMS), 1-8, 2014.

[20] R. Uttarkar and R. Kulkarni, "Internet of Things: Architecture and Security", in International Journal of Computer Application, Volume 3, Issue 4, 2014

[21] M. Burmester and B. Medeiros, "RFID Security: Attacks, Countermeasures and Challenges."

[22] B. Khoo, "RFID as an Enabler of the Internet of Things: Issues of Security and Privacy", in IEEE International Conferences on Internet of Things, and Cyber, Physical and Social Computing, 2011

[23] L. Li, "Study on Security Architecture in the Internet of Things", in International Conference on Measurement, Information and Control (MIC), 2012

[24] A. Mitrokotsa, M. R. Rieback and Andrew S. Tanenbaum, "Classification of RFID Attacks."

[25] J. R. Douceur, "The Sybil Attack", in Peer-to-Peer Systems - IPTPS, 2002, pp. 251-260

[26] N. Ahmed, S. S. Kanhere and S. Jha, "The Holes Problem in Wireless Sensor Network: A Survey", in Mobile Computing and Communications Review, Volume 1, Number 2

[27] T. Bhattasali, R. Chaki and S. Sanyal, "Sleep Deprivation Attack Detection in Wireless Sensor Network", in International Journal of Computer Applications, Volume 40, Number 15, 2012

[28] G. Padmavathi, D. Shanmugapriya, "A Survey of Attacks, Security Mechanisms and Challenges in Wireless Sensor Networks", in International Journal of Computer Science and Information Security, Volume 4, Number 1, 2009

[29] P. S. Fulare and N. Chavhan, "False Data Detection in Wireless Sensor Network with Secure Communication", in International Journal of Smart Sensors and AdHoc Networks (IJSSAN), Volume-1, Issue-1, 201

[30] R. P. Padhy, M. R. Patra, S. C. Satapathy, "Cloud Computing: Security Issues and Research Challenges", in International Journal of Computer Science and Information Technology & Security (IJCSITS).

[31] B. S. Thakur, S. Chaudhary, "Content Sniffing Attack Detection in Client and Server Side: A Survey", in International Journal of Advanced Computer Research, Volume 3, Number 2, 2013

[32] Preneel, B. (1994). "Cryptographic hash functions", in European Transactions on Telecommunications, 5(4), 431-448.

[33] Kravitz, D. W. (1993). U.S. Patent No. 5,231,668. Washington, DC: U.S. Patent and Trademark Office.

[34] Rivest, R. L., Shamir, A., & Adleman, L. (1978). "A method for obtaining digital signatures and public-key cryptosystems", in Communications of the ACM, 21(2), 120-126.

[35] FIPS, P. (1999). 46-3: Data encryption standard (des). National Institute of Standards and Technology, 25(10), 1-22.

[36] Schneier, B. (1994). "The Blowfish encryption algorithm", in Dr. Dobb's Journal-Software Tools for the Professional Programmer, 19(4), 38-43.

[37] K.E. Emam, F.K. Dankar, "Protecting Privacy Using k-Anonymity", in Journal of the American Medical Informatics Association, Volume 15, Number 5, 2008

[38] C. Liu, Y. Zhang, J. Zeng, L. Peng, R. Chen, "Research on Dynamical Security Risk Assessment for the Internet of Things inspired by immunology", in Eighth International Conference on Natural Computation (ICNC), 2012

[39] T. Karygiannis, B. Eydt, G. Barber, L. Bunn, T. Phillips, "Guidelines for Securing Radio Frequency Identification (RFID) Systems", in Recommendations of National Institute of Standards and Technology

[40] Y. Maleh and A. Ezzati, "A Review of security attacks and Intrusion Detection Schemes in Wireless Sensor Networks", in International Journal of Wireless & Mobile Networks (IJWMN), Volume 5, Number 6, 2013

[41] Z. Xu, Y. Yin, J. Wang, "A Density-based Energy-efficient Clustering Algorithm for Wireless Sensor Networks", in International Journal of Future Generation Communication and Networking, Volume 6, Number 1, 2013

[42] C. Qiang, G. Quan, B. Yu and L. Yang, "Research on Security Issues of the Internet of Things", in International Journal of Future Generation Communication and Networking, Volume 6, Number 6, 2013, pp. 1-10

[43] A. Patcha, J. Park, "An Overview of Anomaly Detection Techniques: Existing Solutions and Latest Technological Trends", in Computer Networks, Volume 51, Issue 2, 2007

[44] J. Gubbi, R. Buyya, S. Marusic and M. Palaniswami, "Internet of Things (IoT): A Vision, Architectural Elements, and Future Directions"

[45] Dorri, A., Kanhere, S. S., Jurdak, R., & Gauravaram, P. (2017, March). Blockchain for IoT security and privacy: The case study of a smart home. In Pervasive Computing and Communications Workshops (PerCom Workshops), 2017 IEEE International Conference on (pp. 618-623). IEEE.

[46] Zhao, G., Si, X., Wang, J., Long, X., & Hu, T. (2011, June). A novel mutual authentication scheme for Internet of Things. In Modelling, Identification and Control (ICMIC), Proceedings of 2011 International Conference on (pp. 563-566). IEEE.

[47] Anggorojati, B., Mahalle, P. N., Prasad, N. R., & Prasad, R. (2012, September). Capability-based access control delegation model on the federated IoT network. In Wireless Personal Multimedia Communications (WPMC), 2012 15th International Symposium on (pp. 604-608). IEEE.

[48] , M., Battisti, F., Carli, M., & Neri, A. (2014, November). A federated architecture approach for Internet of Things security. In Euro Med Telco Conference (EMTC), 2014 (pp. 1-5). IEEE.

[49] Liang, C. J. M., Karlsson, B. F., Lane, N. D., Zhao, F., Zhang, J., Pan, Z. and Yu, Y. (2015, April). SIFT: building an internet of safe things. In Proceedings of the 14th International Conference on Information Processing in Sensor Networks (pp. 298-309). ACM.

[50] Keoh, S. L., Kumar, S. S., & Tschofenig, H. (2014). Securing the internet of things: A standardization perspective. IEEE Internet of Things Journal, 1(3), 265-275.
[51] Stanford University. Secure Internet of Things Project (SITP). Retrieved 22 August 2018, from http://iot.stanford.edu/
[52] OWASP Internet of Things Project. Retrieved 22 August 2018, from https://www.owasp.org/index.php/OWASP_Internet_of_Things_Project
[53] Internet of Things: Privacy and Security in a Connected World. Retrieved 22 August 2018, from https://www.ftc.gov/system/files/documents/reports/federal-trade-commission-staff-report-november-2013-workshop-entitled-internet-things-privacy/150127iotrpt.pdf
[54] China calls for global standard for the Internet of Things. Retrieved 22 August 2018, from https://allianzpartners-bi.com/news/china-calls-for-global-standard-for-the-internet-of-things-a947-333d4.html
[55] ISO chooses China's IoT standards. Retrieved 22 August 2018, from http://www.chinadaily.com.cn/m/jiangsu/wuxinewdistrict/2018-07/11/content_36609586.htm