Internet of Things in Biometrics Security: A survey

Asst.prof.Dr.Ekhlas Khalaf Gbashi & Maha Khamiss

University of technology/computer science department, Baghdad, Iraq

Abstract

In this study, a general survey related to Internet of Things (IoT) will be presented in addition to reviewing its benefits, drawbacks and applications. IoT is defined as a technology which operate by connecting objects as well as enabling the generation and exchanging of data, also it is a main extent of technology which a lot of studies are focused on. A lot of developments are made via the use of IoT applications. Despite its development, there are disadvantages that are beyond the control of security. The presented survey introduce security as Biometrics in IoT security.
Keywords: Internet of things; biometric; security.

1-Introduction

Widely common computing (also referred to as pervasive computing), that has been research in detail for several years, is experiencing great changes in the recent years since physical devices, like industrial devices and the home appliances, are turning into smart things to advances in computer evolvement. On the other hand, a considerable progress was recognized also in the communication field. Accessing the internet is going to be usually available to the smart things which adopt IoT [1]. IoT can be defined as a system of physical items which may be detected, monitored, manipulated, or interacted with via electronic devices communicating through different network interfaces and eventually may be connected to the wider internet [2].IoT is considered as the next great opportunity and issue to the internet, which will not be simply computer's network, yet it is going to involve multi-billions of smart things with embedded systems. The domain and size of the present internet will be increased by such system, thus novel

issues and designing prospects will be provided. Generally, internet with the smart things can be defined as constrained IP network that have high-packet loss, limited packet size, as well as intermittent connectivity, also it is defined via certain limitations related to the available power, throughput, and mainly the complexity that could be supported. A lot of studies have been reported to address such issues, from social to technological fields. Mainly, one major challenge is related to how to make full interoperability regarding the interconnected devices achievable, for the purpose of providing them with high smartness degree through permitting their adapting and autonomous behavior in addition to guaranteeing security, privacy and trust [1].

As the security is getting more and more importance, there has been an increase in the requirement for automated personal identification systems depending on biometrics. This is due to the fact that conventional identification systems depending on passwords or cards could be lost, broken, to forget passwords and stolen cards. Thus, there is a requirement for the identification systems to recognize humans without depending on what the individual remembers or possess.

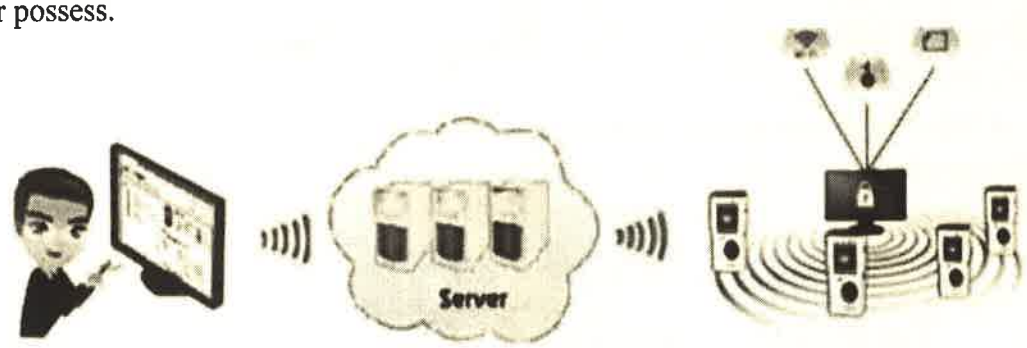

Fig 1.Iot Works in Biometrics [3]

The presented study offers general overview regarding the concerns of security and necessities in the environment of IoT.

2- Internet of things

In the last ten years, the concept of IoT was a main focus for the industrial and academic fields. The main cause of such concentration are the advantages provided via IoT [4], [5]. It has the aim of creating an environment in which all objects (smart objects [6]) will be connected to internet and these objects have the ability of communicating with each other with the least human involvement [7]. The main aim is creating 'a better world for human beings', in which the objects in this world recognize what we want and what we like and function with no precise orders [8]. In the year 1998, Kevin Ashton presented the term 'Internet of Things' [9], he indicated that "The Internet of Things has the potential to change the world, just as the Internet did. Maybe even more so".

In the year 2001, MIT Auto-ID center offered their vision regarding the IoT [10]. After that, in the year 2005, International Telecommunication Union (ITU) has presented IoT formally [11]. IoT consist of a considerable amount regarding the technologies that are adopting the concept. With regard to document, challenges and vision to realize IoT through CERP-IOT [12], whole set of technologies was indicated. IoT can be defined as extremely general concept. Researches associated to the IoT remain in their early phases. Therefore, no standard definitions exist regarding IoT. Different studies have specified these definitions.

• Definition via [13]: Things identify and virtual personality which operate in the smart spaces with the use of intelligent interface for communicating and connecting in environmental, social, and user contexts.

• Definition by [14]: Semantic origin that is related to the term consists of 2 concepts and words: Internet and Thing, the word Internet is considered as world-wide network regarding inter-connected network, according to TCP/IP, whereas the word Things can be defined as the object not exactly recognizable, Thus, semantically, IoT indicates world-wide network regarding the inter-connected objects which are specifically addressable, depending on the standard communication protocols.

- Definition of IoT: It helps things and individuals to be connected in anyplace and anytime, with anyone and anything, through the use of any service and any network/path [15].

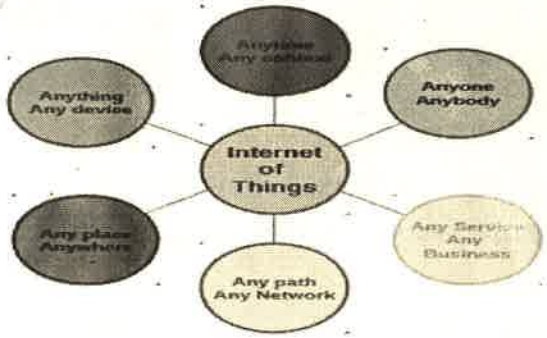

Fig 2.IOT allow s people to be connected the component environment

3-Applications of IOTs

IoT provide a suitable environment to interconnect and communicate objects, in addition to enabling various applications in various domains. Application domain could be majorly divided into 3 categories according to their aim [5], [12]: society, environment and industry.

A few of industry IoT applications in industry are the supply chain management [16], transportation and logistics [17], aviation, automotive, and aerospace. A few of the society IoT applications are the medical technology, telecommunications [18], home and office, smart buildings, healthcare, [19], ticketing, entertainment and media. A few of the IoT environment

applications are breeding and agriculture [20], [20], environmental monitoring, disaster alerting and recycling.

Gascon and Asin [22] provided fifty-four application domains under 12 categories: Electronic-health, logistics, smart water, smart animal farming, retail, smart metering, smart cities, domestic and home automation, emergencies and security, smart environment, smart agriculture and industrial control.

4-Advantages and Drawbacks of IoT

IoT utilize the data in continuous flow, it involves billions of sensors and various devices that are used for the purpose of facilitating our daily life with various areas and develop business processes. The major advantages of IoT are time (money) saving, continuous monitoring and data usability. Yet, there are some drawbacks together with the prospects that the system is providing. Even though the efficiency of IoT has been confirmed, we must tackle the IoT challenges soon [23]. The drawbacks which are being gradually removed resulting of the implementing this concept;

1-Complexity

IoT can be considered as an extremely complicated heterogeneous network that consist of connections among various networks via some communication technologies [24]. Due to the huge amount of devices connected to the internet, the data collected from IoT sensors will be extremely large. The existing sensors of systems might not have sufficient storage for keeping all the data [23]. The amount of data which is going to be taken from billions of objects connected to the system is going to increase unbelievably and such large data processing is going to be very complicated task.

2- Security and Privacy

The system operates on extremely large network system which will result in encountering certain cyber security risks. The major IoT security issues are shown in Fig. 3. Due to the increase in the connected devices, huge amounts of personal information will be gathered and stored via IoT, such data is considered as a main focus for cyber criminals and hackers [25]. There are various way for attacking an IoT system such as having access to personal information, push erroneous data in the network and to disable the availability of the network [26]. Even though that few projects were created for privacy and security of IoT, dependable security protection approach is still a requirement for data privacy, confidentiality and trust [24]. Thus, effective privacy, security and trust models appropriate for the applications of IoT must be defined, functional solutions (firewalls, intrusion prevention systems) must be developed for the purpose of ensuring the security and privacy of customers due to the fact that the acceptance and the run-up regarding IoT depends on protecting the privacy of users.

Fig 3. Security Challenges of IoT [27]

3- Convenience

This is another challenge related to IoT. Due to the fact that IoT is now in the initial stage of concept and progress, there are no convenience standards related to individual management, exchange and capture, labeling, special software, monitoring equipment, providing data definition and end-to-end security. [28][29] [30]. Recently, some standardization activities concentrated tag-based technologies were applied and such standardization activities on sensor and RFID [31].

5-Biomterics

Biometrics are indicating the authentication or identification regarding individuals depending on specific distinctive characteristics or features. Biometric identifiers can be defined as measurable and unique features which are utilized for describing and labeling individuals [32]. Biometric identifiers have 2 main categories, which are behavioral and physiological characteristics [33]. DNA, fingerprints, and Iris, belong to the physiological characteristics while rhythm of typing, voice, and gait belong to the behavioral characteristics.

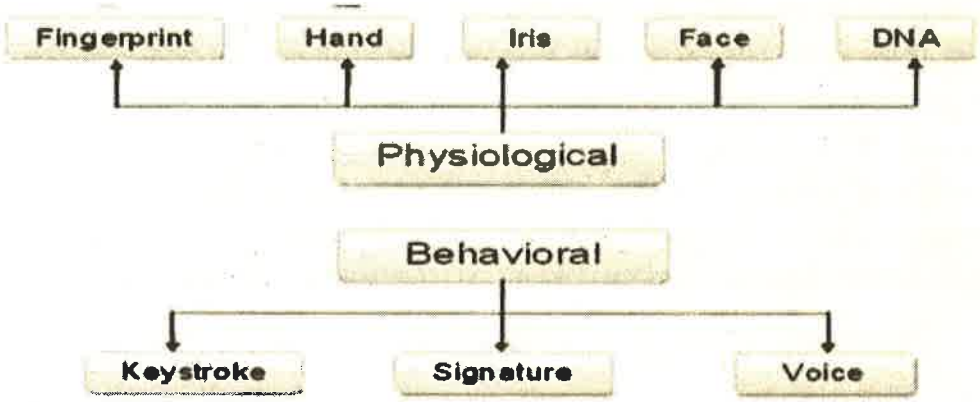

Fig 4. Types of Biometrics [3]

A. Fingerprints: Patterns related to valleys as well as the friction ridges on the fingertips of individuals are distinctive. In the past several decades, law enforcement classified and determined the identities through matching the key points which are related to bifurcations as well as ridge endings. The fingerprints are considered to be distinctive with regard to each one of the individual's fingers (even identical twins). With regard to the biometric technology, the devices which are used for finger print recognition (laptop and desktop) are majorly provided through various vendors at low costs. By using such devices, the user will not be required to type the password, yet just a touch will offer instant access.

B. Facial Image: Individual's identification through facial images could be achieved in various approaches like when capturing face's image in visible spectrum with the use of optical cameras or through the use of infrared patterns that are related to the facial heat emission. Typically, the facial recognition in the visible light will be modeling the key features from facial image's central portion. With the use of wide assortment of cameras, systems of visible light will be extracting features from the captured image which don't alter with the time, whereas keep away from the superficial features like hair or facial expression. Many methods exist to model the facial images in visible spectrum such as multi-resolution analysis, Neural Networks (NNs), Principal Component Analysis (PCA), Local Feature Analysis, and elastic graph theory. The main advantages related to facial recognition are that it is considered to be hands-free, non-intrusive, as well as accepted via a lot of users and continuous.

C. Hand recognition: Such approaches related to the personal authentications are established effectively. Hand recognition was provided for more than two decades. For achieving personal authentication, the system might be measuring the physical characteristics that are related to the hands or the fingers. Such characteristics consist of surface area, width, length, as well as the thickness of hands.

D. Iris recognition: Such approach of recognition utilizes the eye's iris that is considered to be the colored area which is surrounding pupil. The patterns of iris are distinctive. Since they are acquired via video-based image acquisition systems. The devices of iris scan were utilized in for many years in personal authentication application. The systems which depends on the iris recognition have been considerably reduced in costs and this might continue. Such approach works effectively in verification (1:1) as well as in the identification (1: N) modes (with regard to systems achieving one-to-many searches in data-base). The present systems could be applied with the existence of contact lenses and eye-glasses. Such approach isn't intrusive. It doesn't need physical contacts with scanners. This technology wad indicated for working with individuals from various nationalities and ethnic groups.

E. Retina Scan: Human retina can be specified as thin tissue which is composed of the neural cells which are found in eye's posterior. Due to the complicated structures related to capillaries which are supplying blood to retina, retina is unique for each individual. The network related to the retina's blood vessels is very complicated in a way that even the identical twins are not sharing the same pattern. Even though that the retinal patterns could be changed in the conditions of cataracts, glaucoma, diabetes, and retinal degenerative disorders, retina mainly remain unmodified through the whole life of humans. Because of its un-changing and distinctive nature, retina is defined as the major reliable and accurate biometric. Advocates regarding the retinal scanning have indicated that it is very precise that its error rate might be assessed to be just one in a million.

F. Signature recognition: The systems of biometric signature recognition might be measuring and analyzing the signing's physical activity, like speed, applied pressure, and stroke order. Also, certain systems could be comparing the signature's visual images, yet the basis regarding the system of signature biometric is considered to be behavioral, i.e. the way it is signed instead of visual, i.e. signature's image. The major advantages regarding the systems of signature biometrics: 1. Whereas there is simplicity in copying the image's signature, mimicking the signing's behavior is very complicated; 2. Low False Acceptance Rates (FAR); 3. Individuals are signing the documents; thus, the systems of signature recognition aren't seen as invasive.

G. Speech or voice recognition: Speech or voice recognition is defined as the capability of program of machine in receiving and interpreting dictations, or understanding and carrying out spoken commands. Also, voice is considered to be physiological feature due to the fact that all humans have distinctive pitch, yet the voice recognition majorly depends on studying the way of speaking, typically specified as behavioral.

5.1 Role biometrics in IOT

The biometric authentications can be defined as logical, conclusive approach for improving the identity of person, since the passwords might be replicated, while fingerprints cannot be replicated. The users are getting more contented and used to with on-device biometrics. Most recent Samsung and Apple mobile phones, in addition to various novel laptops and desktops, consist of embedded biometric sensors. In the case of authentication to smart cars or smart locks smart lock, it is essential that the authentication process occur on smart device instead of the end of user. Malwares could be utilized for spoofing the identify of authenticated users as well as unblocking smart nodes with no suitable credentials. Authentication can be majorly be splitting across the lock and the mobile device of user in the case when the validation ability has been directly embedded to smart locks. Secure locks will be stand-alone biometric validation servers, also they might not be authenticated remotely with no trusted biometric devices. The mobile

devices with the embedded biometric sensors are evolving the way that individuals are authenticating to their every-day services, such as banking, e-mails, social media, and currently physical access. IoT has advanced the way we are communicating and interacting the world. IoT is evolving with about all the security pitfalls related to life advantages and work. A lot of devices are exposed to hacking, and when securing mission critical applications, intellectual properties, financial institutions, enterprises, and agencies of governments cannot take risks. Old forms related to the authentication of users have no ability for combatting the developed and advanced security threats. Developments in the technology of biometrics allowed such authentication approach to be embedded in daily-used mobile devices. It can be considered as scalable solution which allow all types and sizes of organizations to be ahead cyber attackers. Below, a listing will be provided regarding everything about IoTs and biometric systems.

5.2 APPLICATIONS

Encryption and security standards, as well as the biometric attendance systems have been used in different fields. Creating excellent rendering regarding such "secure systems" is considered to be extremely revolutionized IoT technology which facilitate effective assurance regarding the use of maximum-security standards.

A. Electronic-Payments and Banking: Payment solutions via mobile or online modes, Electronic-Trading facilities, Block chain Systems, and so on.

B. Corporate and Enterprise levels: Facilitating the Access of authorized employees (remotely or directly).

C. Individual User Levels: The feature of IoT in the smart solutions for personal belongings, cars, home, and so on.

D. Healthcare Organizations: Simple retrieving and of corresponding data of users to have effective analysis regarding the statistics of health.

5.3 Benefits and Drawbacks of biometrics

Benefits

1- Password-less with using biometric security systems based on IoT. There is no need for typing awkward password or remembering it.
2- More effective proofing against current breaches of security breaches via the multi-layer security levels.
3- Active monitoring facilities help in implementing and improvising solutions of security for each hour.
4- Being compatible to different devices and platforms create extremely significant responses from client's end

5- Various standards of security are created for various purposes with the use of personalized biometric security features.
6- Simply validating the obtained biometric data.
7- One stop solution regarding all necessities, same biometric information could be also utilized for other security applications.
8- The modular segregation which is related to biometric systems from core operations, for distinguishing the malwares from posing possible risk to mainstream functionalities.
9- The authentication can be achieved at smart devices. Modularity smart devices and the mobile of user offer more effective de-centralization regarding the factors of security.
10- The biometric systems which are based on IoT could be utilized to authenticate the presence of a user. Therefore, extra effective approach for proving the location record of the individual.
11- More effective feasibility of implementation is provided via the full-time support assistance.
12- It is complicated to replicate the biometric data's mapping, therefore it more utilized in comparison to conventional passwords.
13- Decrease the time complexity to a moderately large extent.

Drawbacks

1- Single failure which might occur in specific module might produce deactivation's chain reaction, if in the case when suitable modularity isn't implemented.

2- Inappropriate functioning regarding the software corruptions or authenticating devices might create open path with regard to the breaches of security.

3- Improper knowledge regarding the functionality of biometric systems which are based on IoT might result in possible risks for the important data.

4-IoT is currently parcel and part of our life, also it took things to the digital levels with steps in the right direction. From the user's perspective, straightforward facilitation that is related to the security systems through IoT has efficiently decreases the possibility of threats. Furthermore, with the better manageability options on their certain devices as well as the customized authentication processes for same, things from simple to very confidential status could simply be closely monitored for improved standards of security through IoT.

6-Conclusion

In this research summary study on modern technology IOT showed a research study that pertains to IOT. IOT technology has changed dramatically in everyday life for all. In this research we have discussed many IOT applications in real life and in the future, and we have identified many of the benefits of disadvantages. IoT's Biometrics won't just be unlocking e-mail accounts, bank

apps, yet also homes, cars, and so on. This study has estimated biometric sensors that involve premise security entry consoles and work time management, is going to be at minimum five-hundred million IoT connections in the next years. As the advances in IoT and using biometrics, there is going to be infinite applications providing security and reliability in various industries like: health-care, automotive industries, smart homes, etc. that is going to be just limited through the imagination of humans. We may hope that this brief study will be useful and which helps many researchers to understand and know the many possibilities that biometric technology offers in the Internet of things and what are the basic things to be addressed.

Reference

1- Deze .Z, Song Guo, and Zixue Cheng ," The Web of Things: A Survey", Journal Of Communications, Vol. 6, No. 6, September 2011

2-Dominique D. Guinard and Vlad M. Trifa," Building the Web of Things", Manning Publications Co.,2016.

3-Subha, R. "Biometrics in Internet of Things (IoT) security." *Int. J. Eng. Res. General Sci* 5.5 (2017).

4- Carnot Institutes, "Smart networked objects and internet of things," Carnot Institutes' Information Communication Technologies and Micro Nano Technologies alliance, White Paper, January 2011, http://www.internet-of-things-research.eu/pdf/IoT Clusterbook March 2010.pdf [Accessed on:2011-11-28].

5- L. Atzori, A. Iera, and G. Morabito, "The internet of things: A survey," Comput. Netw., vol. 54, no. 15, pp. 2787–2805, Oct. 2010. [Online]. Available: http://dx.doi.org/10.1016/j.comnet.2010.05.010

6- G. Kortuem, F. Kawsar, D. Fitton, and V. Sundramoorthy, "Smart objects as building blocks for the internet of things," Internet Computing, IEEE, vol. 14, no. 1, pp. 44 –51, jan.-feb. 2010. [Online]. Available: http://dx.doi.org/10.1109/MIC.2009.143

7- D. Le-Phuoc, A. Polleres, M. Hauswirth, G. Tummarello, and C. Morbidoni, "Rapid prototyping of semantic mash-ups through semantic web pipes," in Proceedings of the 18th international conference on World wide web, ser. WWW 2009. ACM, 2009, pp. 581–590. [Online]. Available: http://dx.doi.org/10.1145/1526709. 1526788

8- A. Dohr, R. Modre-Opsrian, M. Drobics, D. Hayn, and G. Schreier, "The internet of things for ambient assisted living," in Information Technology: New Generations (ITNG), 2010 Seventh International Conference on, 2010, pp. 804–809. [Online]. Available: http: //dx.doi.org/10.1109/ITNG.2010.104

9- K. Ashton, "That 'internet of things' thing in the real world, things matter more than ideas," RFID Journal, June 2009, http://www.rfidjournal. com/article/print/4986 [Accessed on: 2012-07-30].

10- D. L. Brock, "The electronic product code (epc) a naming scheme for physical objects," Auto-ID Center, White Paper, January 2001, http: //www.autoidlabs.org/uploads/media/MIT-AUTOID-WH-002.pdf [Accessed on: 2011-08-25].

11- International Telecommunication Union, "Itu internet reports 2005: The internet of things," International Telecommunication Union, Workshop Report, November 2005, http://www.itu.int/dms pub/itu-s/opb/pol/SPOL-IR.IT-2005-SUM-PDF-E.pdf [Accessed on: 2011-12-12].

12- H. Sundmaeker, P. Guillemin, P. Friess, and S. Woelffle, "Vision and challenges for realising the internet of things," European Commission Information Society and Media, Tech. Rep., March 2010, http://www.internet-of-things-research.eu/pdf/IoT Clusterbook March 2010.pdf [Accessed on: 2011-10-10].

13- T. Lu and W. Neng, "Future internet: The internet of things," in 3rd International Conference on Advanced Computer Theory and Engineering(ICACTE), vol. 5, August 2010, pp. V5–376–V5–380. [Online]. Available: http://dx.doi.org/10.1109/ICACTE.2010.5579543

14- European Commission, "Internet of things in 2020 road map for the future," Working Group RFID of the ETP EPOSS, Tech. Rep., May 2008, http://ec.europa.eu/information society/policy/rfid/ documents/iotprague2009.pdf [Accessed on: 2011-06-12].

15- P. Guillemin and P. Friess, "Internet of things strategic research roadmap," The Cluster of European Research Projects, Tech. Rep., September 2009, http://www.internet-of-things-research.eu/pdf/IoT Cluster Strategic Research Agenda 2009.pdf [Accessed on: 2011-0815].

16- L. W. F. Chaves and C. Decker, "A survey on organic smart labels for the internet-of-things," in Networked Sensing Systems (INSS), 2010 Seventh International Conference on, 2010, pp. 161–164. [Online]. Available: http://dx.doi.org/10.1109/INSS.2010.5573467

17- Y. Chen, J. Guo, and X. Hu, "The research of internet of things' supporting technologies which face the logistics industry," in Computational Intelligence and Security (CIS), 2010 International Conference on, 2010, pp. 659–663. [Online]. Available: http: //dx.doi.org/10.1109/CIS.2010.148

18- Y.-W. Wang, H.-L. Yu, and Y. Li, "Internet of things technology applied in medical information," in Consumer Electronics, Communications and Networks (CECNet), 2011 International Conference on, april 2011, pp. 430 –433. [Online]. Available: http://dx.doi.org/10.1109/ CECNET.2011.5768647

19- G. Chong, L. Zhihao, and Y. Yifeng, "The research and implement of smart home system based on internet of things," in Electronics, Communications and Control (ICECC), 2011 International Conference on, sept. 2011, pp. 2944 –2947. [Online]. Available: http://dx.doi.org/10.1109/ICECC.2011.6066672

20- J. Burrell, T. Brooke, and R. Beckwith, "Vineyard computing: sensor networks in agricultural production," Pervasive Computing, IEEE, vol. 3, no. 1, pp. 38 – 45, jan.-march 2004. [Online]. Available: http://dx.doi.org/10.1109/MPRV.2004.1269130

21- L. Lin, "Application of the internet of thing in green agricultural products supply chain management," in Intelligent Computation Technology and Automation (ICICTA), 2011 International Conference on, vol. 1, 2011, pp. 1022–1025. [Online]. Available: http://dx.doi.org/10.1109/ICICTA.2011.256

22- A. Asin and D. Gascon, "50 sensor applications for a smarter world," Libelium Comunicaciones Distribuidas, Tech. Rep., 2012, http: //www.libelium.com/top 50 iot sensor applications ranking/pdf [Accessed on: 2012-05-02].

23- Tsai, C. W., Lai, C. F. and Vasilakos, A. V. Future Internet of Things: open issues and challenges. Wireless Networks, Vol. 20, Iss. 8, 2014, pp. 2201-2217.

24- Li, S., Da Xu, L. and Zhao, S. The internet of things: a survey. Information Systems Frontiers, Vol. 17, Iss. 2, 2015, pp. 243-259.

25- Chandrakanth, S., Venkatesh, K., Uma Mahesh, J. and Naganjaneyulu, K. V. Internet of Things. International Journal of Innovations & Advancement in Computer Science, Vol. 3, Iss. 8, 2014, pp. 16-20.

26- Gubbi, J., Buyya, R., Marusic, S. and Palaniswami, M. Internet of Things (IoT): A vision, architectural elements, and future directions. Future Generation Computer Systems, Vol. 29, Iss. 7, 2013, pp. 1645-1660.

27- Sicari, S., Rizzardi, A., Grieco, L. A. and Coen-Porisini, A. Security, privacy and trust in Internet of Things: The road ahead. Computer Networks, Vol. 76, 2015, pp. 146-164.

28- Machado, H. and Shah, K. Internet of Things (IoT) impacts on Supply Chain, [online], Available: http://apicsterragrande.org/images/articles/Machado__Internet_of_Things_impacts_on_Supply_Chain_Shah_Machado_Second_Place_Grad.pdf/

29- Yılmaz, B. Internet of Things (IoT) Nedir? [online], Available: https://burkanylmz.wordpress.com/2015/10/12/internet-ofthings-iot-nedir/

30- He, M., Ren, C., Wang, Q., Shao, B. and Dong, J. The internet of things as an enabler to supply chain innovation. In e-Business Engineering (ICEBE), 2010 IEEE 7th International Conference on, November 2010, pp. 326-331.

31- Miorandi, D., Sicari, S., De Pellegrini, F. and Chlamtac, I. Internet of things: Vision, applications and research challenges. Ad Hoc Networks, Vol. 10, Iss. 7, 2012, pp. 1497-1516.
32- Jain, A., Hong, L., & Pankanti, S. "Biometric Identification". Communications of the ACM, 43(2), p. 91-98. DOI 10.1145/328236.328110, 2000.
33- Jain, Anil K.; Ross, Arun. "Introduction to Biometrics". Jain, AK; Flynn, P; Ross, A. Handbook of Biometrics. Springer. pp. 1–22. ISBN 978-0-387-71040-2., 2008.