e-ISSN: 2250-0758 | p-ISSN: 2394-6962
Volume-10, Issue-1 (February 2020)
https://doi.org/10.31033/ijemr.10.1.13

IoT: Effective Authentication System (EAS) using Hash based Encryption on RFID Attacks

Dr. Janaki Sivakumar[1], Ms. Smitha Nayak[2] and Dr. Amala Nirmal Doss[3]
[1]Assistant Professor, Department of Computing, Muscat College, Sultanate of OMAN
[2]Assistant Professor, Department of Computing, Muscat College, Sultanate of OMAN
[3]Assistant Professor, Department of Computing, Muscat College, Sultanate of OMAN

[1]Corresponding Author: pjanaki78@gmail.com

ABSTRACT

Internet of Things (IoT) is undoubtedly a well-known research area. Security on IoT communication services is the major challenge with advanced technology and devices. This paper mainly focusing on Perceptron layer based attacks and counter measures based on Effective Authentication System (EAS). This paper is ordered as outlining IoT Architecture, Types of Threats ,Perceptron Layer based attacks, sensor based communication services ,RFID mechanism ,Tag identify and verification by back end server and Hash based Effective Authentication System (EAS) to avoid pseudonym attacks .This paper proposes EAS as security measure by preventing privacy attack, pseudonym attack, location tracking and asynchronous attack.

Keywords**--** EAS, RFID, IOT, Network

I. INTRODUCTION

Internet of Things when it was introduced by Kevin Ashton in 1999(Daniele Miorandi et al., 2012), his dream is that in 2020, there will be 50,000,000 smart devices ,so that each person will have approximately 7 devices .now in 2018, IOT 's rapid growth is developing smart cities , smart solutions and smart people as given in Figure 1.

IoT allows different devices can be integrated flawlessly for transforming, collecting data and providing information data. Physical devices like fridges, heaters, televisions, and so on, could be easily accessible and manageable. The IoT allows devices. But Still, threat related to security, privacy and Identity are still unanswered.

IoT enabled Smart devices have sensors attached to it, which can be controlled remotely from anywhere in the globe. Either Devices of personal use or devices used for community needs , are collecting data and processing it in real time to supply effective results in order to improve the effectiveness of the system(M. Rouse et al.,2016).

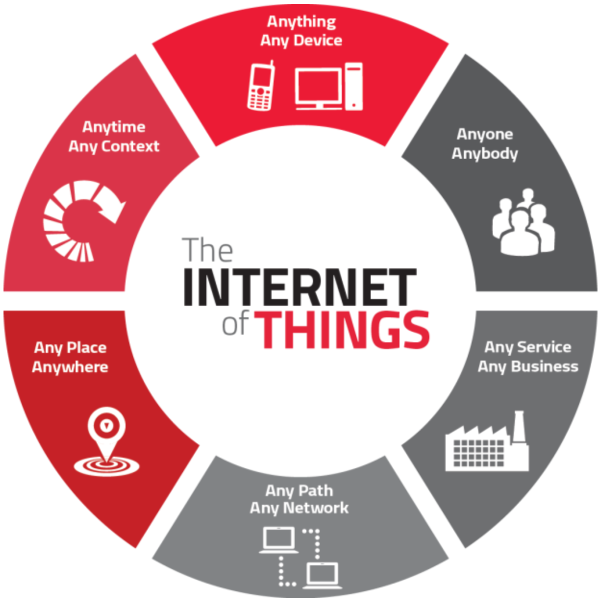

Figure 1: IoT -Connecting Smartly

e-ISSN: 2250-0758 | p-ISSN: 2394-6962
Volume-10, Issue-1 (February 2020)
https://doi.org/10.31033/ijemr.10.1.13

II. LAYERED ARCHITECTURE OF IOT ENVIRONMENT

As per Rafiullah Khan (Rafiullah Khan et al., 2012), layered architecture of IoT has been derived as given in Figure 2.In this Five Layer Architecture, Low level Layer named as Perceptron Layer is perceiving data from the outside system.Sending ,receiving data is taking palce in this perceptron layer.Perceiving data from environment includes reading data from Sensor,Camera,Maps and Barcode readers. Next level layer which is known as Network Layer leads the role of Network and Transport layer of traditional OSI architecture. Network Layer includes Gateway and Network management center in some special cases. Middleware layer's responsibilities are service management and storage of data. Middleware layer process the information from Network layer and takes decision automatically. Next, Application Layer as usual presents the data according to the need of the user in smart way. Presenting data to smart devices to smart usage such as smart cities, smart farming, smart homes and smart travel are the responsibilities of Application Layer. Business layer at the last, makes knowledge out of the smart data presented by application layer. This knowledge gained by business layer is used to make money to the service provider.

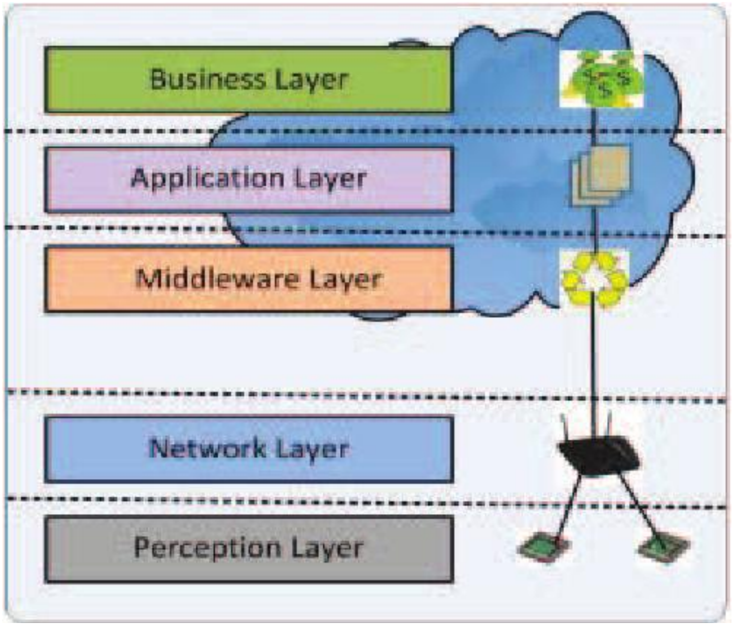

Figure 2: IoT Layered Architecture

III. IOT ATTACKS

In this paper, IoT attacks have been classified into three major categories such as Physical-attacks, Cyber-attacks and Network Attacks. Physical attack includes attacks in smart devices(Janaki Sivakumar et al.,2013). Cyber-attacks include software attacks and Encryption attacks. Network attacks involved network devices and network services.

Physical-Attacks

The use of sensors in IoT devices unsurprisingly helps to improve the functionality of the devices. At the same time, these sensors also used for counter attacks on the devices or system. Research works (A. K. Sikder et al., 2017), (Y. Son et al., 2017)(A. Nahapetian et al., 2016) lists all the recent attacks on IoT environment that have been made through sensors. Attacks based on these sensors highly risky on Devices, Applications and Cloud. Sensor related attacks are increasing in time, since attackers do not need any high cost /complicated tools (R. Schlegel et al., 2011) (R. Templeman et al., 2013). Manufacturing defects with limited security measures also one of the major roots for these physical attacks.

Cyber Attacks

Software and encryption attacks are known as Cyber-attacks in any IoT systems. Security weakness in IoT applications makes hackers work easier .Hackers apply code injections for DoS, false positives approach, Breaking Encryption key(Janaki Sivakumar et al., 2017), Active-X script, spoofing and man in the middle attacks are very common cyber-attacks.

Network Attacks

Adversaries try to attack the security of IoT network through various sources. Node Tempering allows

e-ISSN: 2250-0758 | p-ISSN: 2394-6962
Volume-10, Issue-1 (February 2020)
https://doi.org/10.31033/ijemr.10.1.13

sensor damage by altering sensitive data. Traffic jamming blocks the communication channel by sending unwanted messages as interference (Ammar Yassir et al., 2012). A code injection interrupts data transmission over network. Sleep deprivation allows node to shut down or sleep mode .destruction of routing loops to gain routing and access control (Wahab et al., 2017).

IV. PERCEPTRON LAYER BASED SECURITY CHALLENGES

Equipment's such as RFID readers, GPS, gateways, sensors and other devices require to be secured efficiently. In the top 10 IoT vulnerabilities poor physical security has identified by OWASP. First of all we have to ensure that only the authorized people can access the sensitive data produced by devices or physical objects. In order to do that, we need to define the policies for physical identity and access management. Perceptron layer contains various sensor modules, which are useful for data collection and data control. Perception layer technologies include Wireless Sensor Networks (WSN), implantable medical devices (IMDs), radio-frequency identification (RFID) and global positioning system (GPS).

In Perceptron Layer various sensor technologies such as Bluetooth, Wi-Fi and GPS which are easy for hackers to impose various kinds of attacks (Pan et al., 2017). Hackers' first target is hardware parts of the IoT network and the adversary needs to be close to the IoT systems.

Perceptron Layer Attacks

a) Node Tempering: destroying the node with sensors by transmitting signals, examine the signal to get Access rights and update accordingly (Kaushal et al., 2015).

b) Node Jamming: find the radio frequencies of wireless nodes, blocks the signals which stop the communication of nodes and stop IoT services. Denial of Service attack sends huge amount of Noisy signals which will support the hacker to jam the Radio frequencies (Sonar et al., 2014).

c) Node Injection: Middle Man attack, actually set up a new forge node between the sender and receiver node to get control over IoT Communication System and its services(Kaushal et al., 2015).

d) Social Engineering: adversary gets access to useful and secret information on IoT system .This type of attack is categorized into physical attack because the attacker physically communicates with the network of IoT to serve his task(Peris-Lopez et al.,2016).

e) Sleep Deprivation Attack: Attack over sensor node batteries by making the sensor node busy. So sleep activation process will not be so effective, which will lead to more battery consumption. As a result of it sensor node will become dead due to power and in due, IoT services will get interrupted.(Nia et al., 2016)

f) Code Injection: In this attack the adversary can physically insert a malicious program into a node and by implementing this attack into a node it would get access of the whole IoT system (Doinea et al., 2015). For Example: An attacker inserts any plug and play device into a node with harmful virus then it would gain full access of that node and control all the IoT system(Farooq et al., 2015).

g) Tag Cloning: In IoT system, tags are deployed on various physical objects which are visible and thus data can be read and also modified by some hacking techniques. So the crucial data can be easily accessed by any cybercriminal that can discover duplicate tag and hence the user cannot distinguish between duplicate and original data (Doinea et al., 2015).

h) Spoofing: Intruders spreads false information on the Radio Frequency Identification System as pseudonymity and collects information on IoT communication system and gets control over the network (Jeyanthi et al., 2017).

i) Eavesdropping: Hacking identity information such as password or RFID, and acting as original node is the way of attack and this happen since RFID has wireless characteristics(Doinea et al., 2015).

V. ROLE OF RADIO FREQUENCY IDENTIFICATION (RFID)

Radio frequency identification technology (Figure 3) is the mechanism to identify devices, recognize data related to these devices on IoT environment automatically, which is the non-contract recognition technique (Ahuja et al., 2010). Because of this, the recognition of radio frequency identification (RFID) works well in the any environment.

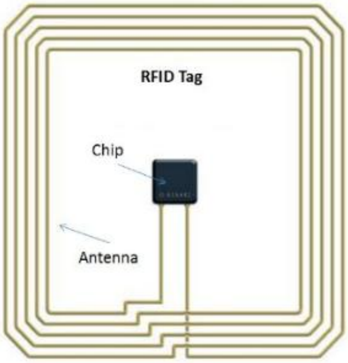

Figure 3: RFID

Attaching a RFID tag on IoT devices (Figure 4), which involves the information of device, the dedicated

e-ISSN: 2250-0758 | p-ISSN: 2394-6962
Volume-10, Issue-1 (February 2020)
https://doi.org/10.31033/ijemr.10.1.13

recognition terminal can recognize this attached device through reading the tag. RFID enabled device does not depend light source and can pass data through external material unlike bar code (Domdouzis et al., 2007).

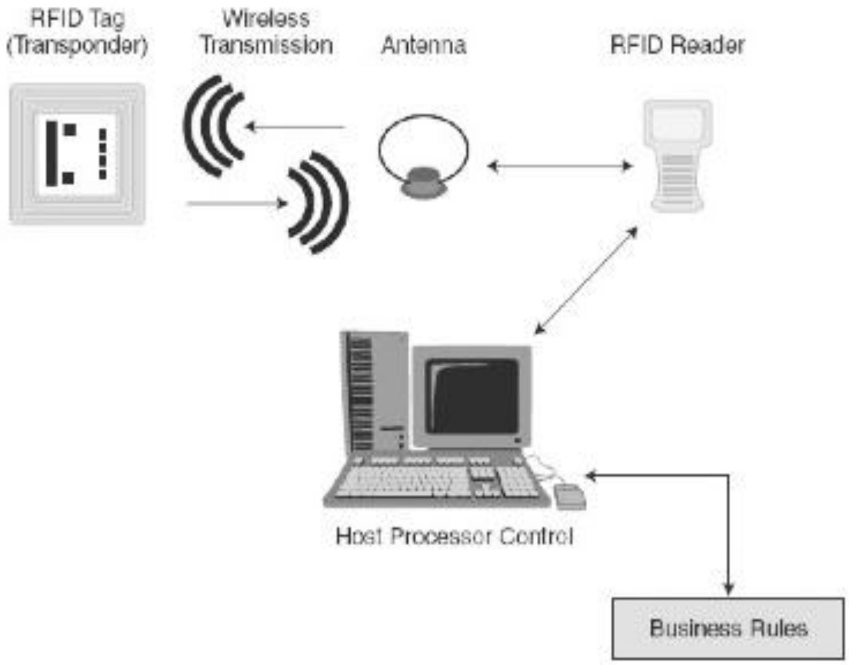

Figure 4: How Does RFID Work

RFID has been used into many environments such as smart car parking, smart cards, smart guard gate and smart health systems. Some retailers have invested RFID technology, and also authorized RFID producers to attach tag on their goods, so that the low-budget RFID tags are pervasively produced. Wal-Mart passed a resolution, which producers must sufficiently take advantage of the RFID, attaching RFID tags on all products to reduce manpower and material resources (Coltman T et al., 2008). Generally, a typical RFID framework is composed of a reader, tag and a database (Shen Y et al., 2008), which is shown in Figure 5.

- ***Reader***: The main function is read data of tag or writes data to tag by transferring energy via radio frequency (Ferrero R et al., 2015). RFID reader needs to communicate with database.
- ***Tag***: Tag is classified into active tag, semi-passive tag and passive tag; based on the frequency, tag is classified into low-frequency tag, high-frequency tag and ultrahigh frequency tag (Want R et al., 2006). By various applications, the proper tags are needed to be chosen.
- ***Database***: It stores all information of tags which indicate all objects.

Mechanism of RFID systems:

Step 1: Reader sends signals via antenna, and tag receives signal and sends internal tag data.

Step 2: Reader receives and verifies the tag data.

Step 3: Reader sends verification result to the host computer which is connected to a database.

e-ISSN: 2250-0758 | p-ISSN: 2394-6962
Volume-10, Issue-1 (February 2020)
https://doi.org/10.31033/ijemr.10.1.13

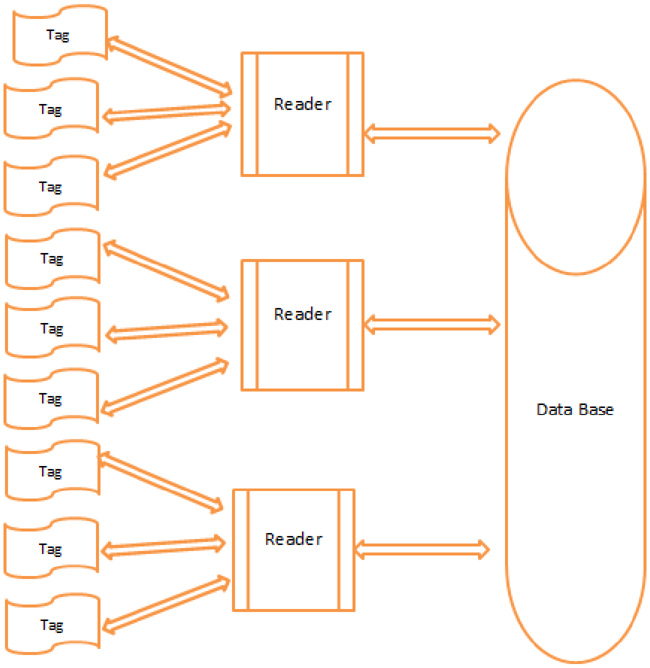

Figure 5: RFID System

VI. EFFECTIVE AUTHENTICATION SYSTEM (EAS) FOR RFID ATTACKS

Cryptographic processing is one among the main tasks in securing the sensor data on IoT. These operations include encryption - decryption, key - hash generation, and sign - verify hashes that are commonly used in order to guarantee privacy of data. An effective key management (EKM) supports efficient key updates for dynamic wireless sensor networks and ensures forward and backward key secrecy (Seo S et al., 2015). Similar to CL-EKM, a Hash Graph (HaG) scheme for key pre-distribution among a large set of sensor nodes in a sustainable and secure way was proposed (Levi A et al., 2017). This scheme is no limit on the total number of generations providing flexible network lifetime. A hierarchical key assignment scheme is provably secure with respect to key in distinguishability and relies on perfect secret sharing (Castiglione A et al., 2014). Whatever the key distribution system, Effective Authentication System (EAS) provides secure communication.

The major security risk is the leakage of the tag ID Value, when the tag sends response to pseudo reader. Since TagID (TID) is easy to trap, more concentration is need on response to the request by the reader. This proposed Tag based Effective Authentication system uses 2 parts of Response value of Tag. First part of response value is used to identify the Reader and another part is used for response to reader after verification.

EAS –Working Principle

Initialization

Tags store their own identifiers and the secret value (T_{ID}, $K_{n,\, i}$)

Readers store their own identifiers R_{ID}

Backend server store all readers data R_{ID} and tags data (T_{ID}, $K_{n,\, i}$, $K_{o,\, i}$)

Step 1: Authentication Request

The reader generates a random number R_r and it sends query to the tag

Step 2: Response Message

The tag generates a random number R_t using its own identification T_{ID}.

The tag calculates M = H (R_r (**OR**) R_t (**OR**) T_{ID}) and α = H ($K_{n,\, i}$,(**Ex-OR**) R_t

M value is divided into two parts M_L and $M_{R.}$

The tag sends data M_L, R_t and α to the reader.

Step 3: Passing to Server

The reader calculates β = H (R_{ID} (**Ex-OR**) R_r).

The reader sends M_L, R_t, R_r, α and β to the backend server.

Step 4: Backend server process

Server verifies the legitimacy of the identity of the reader and tag.

If the reader and tag identity are legitimate, the server will update the secret value shared by tag and the server.

Otherwise the server finishes the authentication process.

Server Process :

a. Calculates β (**Ex-OR**) R_r .if H (R_{ID})= β (**Ex-OR**) R_r, continue, else abort . The hash function SHA3-224 is recommended.

b. Calculates α (**Ex-OR**) R_t .if H ($K_{n,i}$)= α (**Ex-OR**) R_t , continue,

Else if H ($K_{o,i}$) = α (**Ex-OR**) R_t ,continue, else abort

c. Calculates M_L' = H (R_r (**OR**) R_t (**OR**) T_{ID}) according to the tag's data pair stored by it. If M_L' = M_L, the tag is authenticated, otherwise abort the process.

d. The tag's secret value M_R' is updated as $K_{n,i}$ = H ($K_{o,i}$ (**Ex-OR**) T_{ID}).

e. Calculates

N = H (R_{ID} (**Ex-OR**) R_r) (**Ex-OR**) T_{ID} and

γ = $K_{n,i}$ (**Ex-OR**) $K_{o,i}$

Step 5: Response from Server to Reader

Server sends the value N, γ , M_R' to the reader.

Step 5: Response from Reader to Tag

Reader calculates T_{ID} = N (**Ex-OR**) H (R_{ID} (**Ex-OR**) R_r and sends (γ, M_R'$)$ to Tag

Step 5: Response from Tag

If M_R' = M_R and updates T_{ID} as $K_{o,i}$ (**Ex-OR**) γ, then authentication success.

Otherwise the authentication process is terminated.

By updating the tag's secret key value and random number, EAS helps for secure communication in RFID systems by preventing privacy attack, pseudonym attack, location tracking and asynchronous attack. Because of the nature of hash function, it is difficult for attackers to obtain confidential information such as T_{ID} and R_{ID}. The random number of each communication is different, and the transmitted information of the label is different each time, which can effectively prevent the fixed output caused by the location tracking problem.

VII. CONCLUSION

IoT is a new and rising technology that has all over world's attention. Despite of many hacking cases, encrypted communications or proper authentication methods are not proposed effectively. In this paper, the major three common security attacks have been reviewed. Security threats based on IoT layered architecture also reviewed. Perceptron layer is more adequate to get affected with attacks. RFID mechanism is dealt in detail with mechanism of RFID sensor. Strong security properties are achievable within simple security protocol designs that are suitable for implementation in RFID systems. This paper proposes an improved scheme based on hash function to overcome the shortcomings of existing protocols. With a properly selected key distribution scheme, Reader identity and authentication by Tag using EAS-Effective authentication system has been proposed as a solution to location tracking, cloning, and replay attacks.

REFERENCES

[1] Daniele Miorandi, Sabrina Sicarib, & Francesco De Pellegrini. (2012). Internet of things: Vision, applications and research challenges. *Survey Paper*, pp. 1497–1516.

[2] M. Rouse & I. Wigmore. (2016). *Internet of things*. Available at: http://internetofthingsagenda.techtarget.com/definition/Internet-of-Things-IoT.

[3] Rafiullah Khan, Sarmad Ullah Khan, Rifaqat Zaheer, & Shahid Khan. (2012). *Future internet: The internet of things architecture, possible applications and key challenges*. Available at: https://pure.qub.ac.uk/en/publications/future-internet-the-internet-of-things-architecture-possible-appl.

[4] Janaki Sivakumar, Ammar Yasser,et al. (2013). Intent based security challenges in android-An analysis & recommendation. *International Journal of Computer Science and Network Security, 13*(1).

[5] A. K. Sikder, H. Aksu, & A. S. Uluagac. (2017). 6th sense: A context aware sensor-based attack detector for smart devices. *In 26th USENIX Security Symposium (USENIX Security 2017), Vancouver, BC*, pp. 397–414.

[6] Y. Son, H. Shin, D. Kim, Y.-S. Park, J. Noh, K. Choi, J. Choi, & Y. Kim et al. (2015). Rocking drones with intentional sound noise on gyroscopic sensors. *In USENIX Security*, pp. 881–896.

[7] A. Nahapetian. (2016). Side-channel attacks on mobile and wearable systems. *In Consumer Communications & Networking Conference*, pp. 243–247.

[8] R. Schlegel, K. Zhang, X.-y. Zhou, M. Intwala, A. Kapadia, & X. Wang. (2011). Soundcomber: A stealthy and context-aware sound trojan for smartphones. *NDSS, 11*, 17–33.

[9] Janaki Sivakumar & Hameetha Begum. (2017). Integer factorization in RSA encryption: Challenge for cloud attackers. *International Journal of Computer Science Trends and Technology, 5*(2), 405-408.

[10] Ammar Yassir, Dr. Priyanka Roy, & Janaki Sivakumar. (2012). Designing a security network for the information technology risk management. *International Journal of Advanced Research in Computer and Communication Engineering, 1*(9).

[11] Wahab, A., Ahmad, O., Muhammad, M., & Ali, M. (2017). A comprehensive analysis on the security threats and their countermeasures of IoT. *International Journal of Advanced Computer Science and Applications, 8*(7), 489-501.

[12] Pan, Yao, et al. (2017). Taxonomies for reasoning about cyber-physical attacks in IoT-based manufacturing systems. *International Journal of Interactive Multimedia & Artificial Intelligence*, 45-54.

[13] Kaushal, Kanchan & Varsha Sahni. (2015). DoS attacks on different layers of WSN: A review. *International Journal of Computer Applications 130*(17), 8-11.

[14] Sonar, Krushang & Hardik Upadhyay. (2014). A survey: DDOS attack on internet of things. *International Journal of Engineering Research and Development, 10*(11), 58-63.

[15] Peris-Lopez, Pedro, et al. (2016). *Attacking RFID systems*. Available at: https://www.researchgate.net/publication/257298033_Attacking_RFID_Systems.

[16] Nia, Arsalan Mohsen & Niraj K. Jha. (2016). A comprehensive study of security of internet-of-things. *IEEE Transactions on Emerging Topics in Computing, 5*(4), 586-602.

[17] Farooq, M. U., et al. (2015). A critical analysis on the security concerns of internet of things (IoT). *International Journal of Computer Applications, 111*(7), 1-6.

[18] Doinea, Mihai, et al. (2015). Internet of things based systems for food safety management. *Informatica Economica, 19*(1), 87.

[19] Jeyanthi, N., Shreyansh Banthia, & Akhil Sharma. (2017). Security in IoT devices. Security breaches and threat prevention in the internet of things. *IGI Global*, 96-116.

[20] Ahuja, S. & Potti, P. (2010). An introduction to RFID technology. *Communication Networks, 2*, 183–186.

[21] Domdouzis, K., Kumar, B., & Anumba, C. (2007). Radio-Frequency Identification (RFID) applications: A brief introduction. *Advanced Engineering Informatics, 21*, 350–355.

[22] Coltman, T., Gadh, R., & Michael, K. (2008). RFID and supply chain management: Introduction to the special issue. *Journal of Theoretical and Applied Electronic Commerce, 3*, 3–6.

[23] Shen, Y., Wang, Z., & Zhou, C. (2008). RFID principle and its application in vehicle. *Storage, Transportation & Preservation of Commodities, 30*, 44–46.

[24] Ferrero, R., Gandino, F., Montrucchio, B., Rebaudengo, M., & Zhang, L. (2015). A novel simulator for RFID reader-to-reader anti-collision protocols. *In Proceedings of the International EURASIP Workshop on RFID Technology*, pp. 59–64.

[25] Seo, S., Won J., Sultana, S., & Bertino, E. (2015). Effective key management in dynamicwireless sensor networks. *IEEE Transactions on Information Forensics and Security, 10*, 371–383.

[26] Levi, A. & Sarimurat, S. (2017). Utilizing hash graphs for key distribution for mobile and replaceable interconnected sensors in the IoT context. *Ad Hoc Network, 57*, 3–18.

[27] Castiglione, A., Santis, A., & Masucci, B. (2014). Hierarchical and shared key assignment. *In Proceedings of the International Conference on Network-Based Information Systems, Salerno*, pp. 263–270.