*Proceedings of the International Conference on Industrial Engineering and Operations Management*
*Pretoria / Johannesburg, South Africa, October 29 – November 1, 2018*

# A Review on the Security of Smart Homes in the Internet of Things

**MAZWA Khawla**
Electrical Systems and Telecommunications Engineering
National School of Applied Sciences
Kenitra, Morocco
khawla.mazwa@gmail.com

**MAZRI Tomader**
Electrical Systems and Telecommunications Engineering
National School of Applied Sciences
Kenitra, Morocco
tomader20@gmail.com

## Abstract

Today we are witnessing a new concept that is growing fast: The Internet of Things (IoT). We can see all the devices we use in any field, are transformed into a smarter version such as smart homes, smart beds, smart coffee machines and smart everything. According to the American Research Firm Gartner there will be nearly 50 billion connected devices in 2020. However, the security aspect is still at the top of the prioritized tasks in this concept.
In this paper we present a review about some categories of popular security issues in the IoT and the solutions proposed by other researchers to these issues. In addition, we investigated security attacks in smart homes and identified some possible security solutions in those environments.

## Keywords
Internet of Things (IoT), smart home, connected devices, security issues…

## 1. Introduction

Smart home is one of the applications of the Internet of Things (IoT) that continue to grow rapidly. It contains smart devices that are connected with applications and gateways like for example: smart lights, smart locks, smart TVs, smart washing-machines and alarm system. Smart home applications have gained a huge attention recently. By using IoT technology, home appliances are able to communicate with each other so the user can have access to all the devices in the home anytime and anywhere. However, the entire architecture of smart homes needs some security requirements against existing security issues. That's why, there's huge need for strong authentication mechanism to prevent from attacks.
The concept of Internet of Things (IoT) was born in 1999 in the United States and especially at the Massachusetts Institute of Technology Center thanks to Kevin Ashton. It has gained a lot of acceptance in our private life, with the access to the Internet, provided by many technologies such as Bluetooth, ZigBee, Wi-Fi...etc, aided by network gateways. The fact that the devices we use daily serves our needs and simplifies our lives as well by using our data, that impose a lot of risks for the privacy of the end user which requires confidentiality, integrity, authentication and authorization.
This paper is divided to four sections. In the first one we present the concept of the smart home, its architecture, the concept of Internet of Things (IoT) then the protocols used in the IoT succeeded by the role of the cloud in a smart home and finally some applications for it. The remainder of the paper is organized as follows, in the second section, we investigate the main security attacks in the smart home and the most important categories of these attacks then we categorize the security issues in the IoT and some cloud attacks. For the third section we describe the existing solutions proposed by other researchers for IoT as well as the security solutions for smart home. The fourth section provides a discussion. Finally, we conclude the paper.

© IEOM Society International

## 2. The smart home concept

Since the concept of IoT was introduced to the smart home implementation, this field knew some great changes and improved a lot. Smart home is designed to make houses more automated and intelligent to offer the residents a comfortable life where they can easily control and monitor all the devices inside the home. According to Satpathy [1]: "A home which is smart enough to assist the inhabitants to live independently and comfortably with the help of technology is termed as smart home. In a smart home all the mechanical and digital devices are interconnected to form a network which can communicate with each other and with the user to create an interactive space.

### 2.1 Architecture

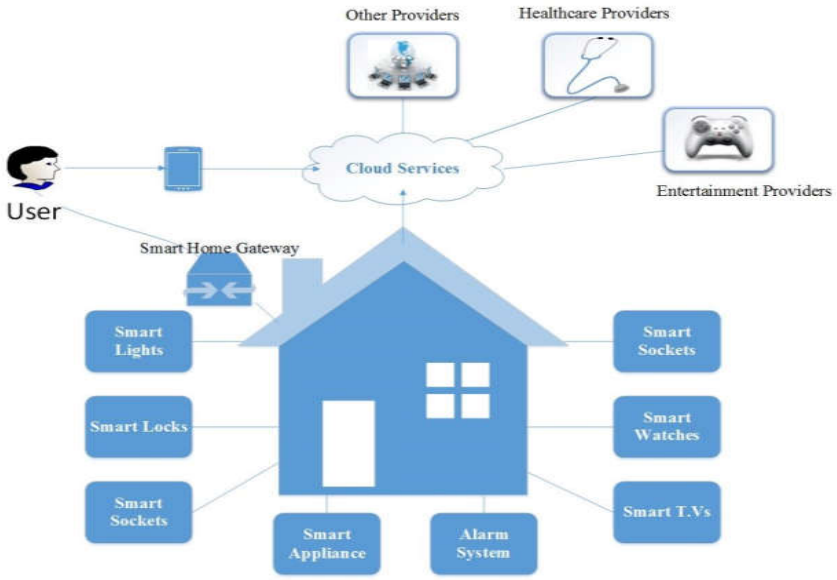


Figure 1. Architecture of a Smart Home

A smart home comprises a multitude of devices that supports different communication technologies. They are connected to applications and gateways providing connectivity to the Internet and building a tunnel between different technologies within the house. These devices form a heterogeneous network by interacting and cooperating with each other. The user connects to the smart network using mobile or tablet … etc
We can identify three elements that guarantee the success of the smart home concept:

- Connected objects (IoT)
- Cloud
- Applications

### 2.2 Internet of Things and the Smart Home

There is no standard, unified and shared definition of the Internet of Things but after several researches, a definition that we found more relevant "the Internet of Things is a network of networks which enables the identification of digital entities and physical objects – whether inanimate (including plants) or animate (animals and human beings) – directly and without ambiguity, via standardized electronic identification systems and wireless mobile devices, and thus make it possible to retrieve, store, transfer and process data relating to them, with no discontinuity between the physical and virtual worlds".
In Figure 2 we describe the main and the most important communication protocols used in a smart home based on the Internet of Things (IoT) according to the OSI model. Those protocols provide the communication between the components of a smart home and transport the information between devices.

© IEOM Society International

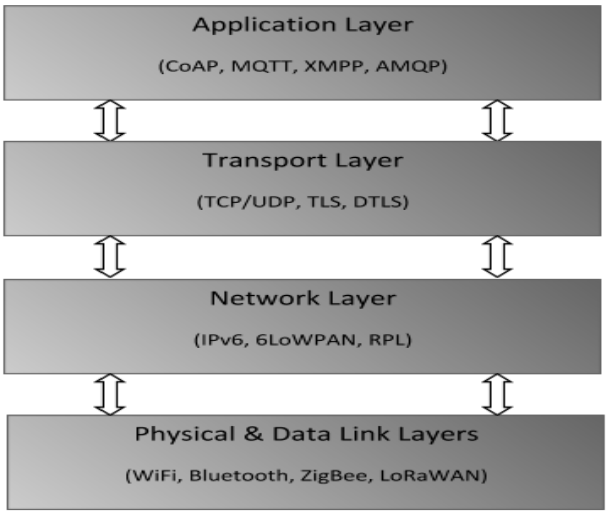


Figure 2. IoT Protocols

**Physical and Data Link Layers:** The most well known physical and data Link layers protocols used to construct the smart home are WiFi, Bluetooth, ZigBee based on the 802.15.4 standard and LoRaWAN.
**Network Layer:** Network layer protocols for the IoT and smart home applications are responsible for connecting the smart things, network devices and servers. Thanks to IPv6 functionalities (the large address space, stateless and stateful address configuration) needed by the IoT applications including smart homes to enable addressing (without using NAT Translation) of smart devices and the direct routing of packets. Other Protocols are used such as IPv6 over Low power Wireless Personal Area Networks (6LoWPAN) and Routing Protocol for Low power and Lossy Networks (RPL)
**Transport Layer:** Regarding the transport layer which ensures that the data is sent rapidly and efficiently, UDP is preferred as a simple OSI transport layer protocol for client/server network applications based on IP and Datagram Transport Layer Security (DTLS) which provides communications privacy for datagram protocols and a better security in a way to prevent eavesdropping, tampering, or message forgery.
**Application Layer:** The application layer is responsible for delivering specific application to the user. The most important application layer protocols for IoT and smart home environments are Constrained Application Protocol (CoAP), MQ Telemetry Transport (MQTT), eXtensible Messaging and Presence Protocol (XMPP) and Message Queuing Protocol (AMQP).

## 2.3 Cloud and the Smart Home

The data generated every second from smart home may contain very important and private information, but its amount can be too much to store or to be analyzed locally. To solve these problems, the cloud computing has been adopted in smart home environment.
The cloud is the most important and complex part integrated in the smart home architecture. The smart home can send data into the cloud; the user's devices will be connected to the cloud where he has the access to the shared data when he needs it.
Recently, the term Cloud computing has become more and more popular in our daily life where we can store our important files and data to prevent a computer fault from destroying it. The main task of the cloud computing is that it can adapt to user's conditions and to different circumstances such as CPU speed, memory size, storage space , etc.
The NIST organization defines: "Cloud computing is a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. This cloud model promotes availability and is composed of five essential characteristics (On-demand self-service, Broad network access, Resource pooling, Rapid elasticity, Measured Service); three service models (Cloud Software as a Service (SaaS), Cloud Platform as a Service (PaaS), Cloud Infrastructure as a Service (IaaS)); and four deployment models (Private cloud, Community cloud, Public cloud, Hybrid cloud)".
Generally, there are four deployment models for a cloud infrastructure: private, hybrid, public and community cloud.

© IEOM Society International

A private cloud is used only by the same company or by a third party and still be a private cloud for that company, this type of cloud is secure and easy to maintain but it needs a high cost to deploy it. In the public cloud different users from anywhere can easily access the public cloud via a public network like the Internet, this type of cloud has security issues and it is vulnerable to attacks. The hybrid cloud is a combination of multiple cloud computing models interconnected with each other to offer more benefits to the environment. And the community cloud is shared by different organization belong to the same community, it is usually hosted externally but it may be hosted internally by a member.
In addition, there are three types of services in use by the cloud models. Those services are Infrastructure as a Service (IaaS), Platform as a Service (PaaS) and Software as a Service (SaaS).
IaaS aims to provide access to a virtualized computer park. The consumer is capable to install an operating system or applications, for example: Openstack, OpenNebula, etc… In the PaaS the operating system and infrastructure tools are under the responsibility of the vendor. The consumer has control only on the applications but he doesn't have the control over the underlying infrastructure like Amazon Web Services. The applications in SaaS are available to consumers; they can be manipulated using a web browser, emails…from many devices like computer, mobile or tablet. Example of SaaS: Google Docs, Gmail, etc...

## 2.4 Applications in Smart Home

In smart homes, there are many kinds of applications, which provide intelligent and automated services to the user which makes his life more comfortable and even more interesting. Those applications help in the daily activities and help in maintaining a routine for individuals. Some of these applications are:
**Smart bed:** Smart bed system can be fabricated as a part of the smart home to provide a safe, sound and secured living environment for the inhabitant of smart home for example to monitor an elderly person or disabled person living alone[2].
**Smart refrigerator:** The smart refrigerator can meet the user's need with food storing function, it is equipped with a shopping and storage application that require managing and tracking the products in the refrigerator as well as sending an alert to the user if a product is about to pass its expiration date or it has not been used in a long period[3].
**Smart window:** Smart window system is a very important part of smart home. The windows are automatically controlled opened and closed by measuring environmental parameters. This system is developed to control the wind, the rain, the smoke…to make reasonable judgment to protect the user[4].
**Smart locks:** Smart lock system is very important especially because it is related to the safety of the user. The user can simply use his mobile to open and close door also he can monitor who is entering and leaving his home while he is absent[5].
**Smart light:** A lighting control system for smart homes has been developed and implemented to automatically control light in the home based on the movement of the user, it can turn off automatically when the room is unoccupied and it can turn on when the user enter the room[6].
**Smart TVs:** Smart TV provides better environment for watching TV contents due to Ultra High Definition (UHD) along with watching movies, playing games, browsing, and full support for web 2.0 features that allows viewers to satisfy their need by using the smart TV large screen. In addition, beside storage capabilities, processing and connectivity, smart TVs have full support for internal and external sensors, such as camera, face detection and recognition, voice recognition[7]…

© IEOM Society International

## 3. Smart Home security study

In this section, we studied the existing security threats in each interface of a smart home. About The security attacks in smart home, they can be categorized into two categories:

- Passive attacks
- Active attacks

The passive attacks aim to listen without modifying the data or the performance of the network. In the passive attacks, the attacker obtains information from the system, monitors the system, transmits the messages and does not modify them but he learns something from it. Generally, these types of attacks are undetectable.
The active attacks aim to modify the data or the messages, breaking into the network equipment or disrupting the performance of this network. Examples of active attacks include denial of service, message modification, and password cracking.
To be more specific there are many classic attacks such as:
**Denial of Service (DoS):** This type of attack aims to render a machine or network resource unavailable to its intended users by temporarily or indefinitely disrupting services of a host connected to the Internet. By jamming the communication between the components, the Smart Home installation will be disrupted and become unavailable.
**Eavesdropping:** In an eavesdropping attack, the attackers can choose to passively eavesdrop and spy on the network communications, overhearing information that they might not be authorized to see or they can use the active eavesdropping to disrupt the network or modify the data. The data that has been transmitted between the devices in the smart home can be eavesdropped by an adversary.
**Hijacking:** The attacker hijacks and gains control of a device. These types of attacks are difficult to detect because the attacker does not change the basic functionality of the device. Moreover, he only manipulates one device to re-infect all smart devices in the home in order to paralyze the network.

### 3.1 Audit of vulnerabilities

Nowadays, Smart homes are getting more and more attractive for consumers to be a part of their normal life but there is a huge concern about security and privacy issues in those smart homes. The main and the most important interfaces which are vulnerable to attacks are: Connected objects, Cloud, Applications.


Figure 3. Attack interfaces in a Smart Home

### 3.2 Threats on connected objects

#### 3.2.1 Attack methods

Generally the attacks on connected objects can be classified in 3 categories with regard to the existing vulnerabilities such as lack of encryption, lack of authentication and identification also the intention of the attacker:
**Attacks on connected objects themselves:** The attacker can directly attack the hardware or the software (the compromise of the connected object by a malicious code can cause its inaccessibility).
**Attacks made through connected objects:** These attacks exploit the connected devices to access to the networks such as the Internet.

**Attacks on IoT networks and communication protocols:** There are several protocols to interconnect the devices with each other. The most common attacks are the attacks based on listening to the traffic (passive attacks) and man in the middle attack (active attacks).

3.2.2 Security issues

Various audits carried on smart connected devices have estimated the existence of numerous security threats and attacks against the IoT devices. More specifically the security threats can be classified into different levels with regard to the IoT layers:

- Low-level security issues
- Intermediate-level security issues
- High-level security issues

**Low-Level Security Issues:**
In this level we are concerned with some security issues at the physical and data link layers as well as hardware level:
**Jamming attacks:** A jamming adversary in IoT can perform a variety of DoS attacks, such as transmitting wide-band noise, high-power narrow-band pulses, or interfering waveforms that can affect the sending and receiving of data.
**Insecure initialization:** In IoT the physical layer communication needs to be secured by good mechanism of initialization and configuration to secure the privacy of data and network services.
**Low-level Sybil attacks:** The Sybil attacks exist in the IoT to maliciously manipulate the systems where attackers use fake identities or abuse pseudo-identities to compromise the effectiveness of the IoT.
**Insecure physical interface:** Physical access to a device is probably the easiest way to create some kind of damage. This may be considered as one of the serious threats to exploit the network
**Sleep deprivation attack:** One of The most dangerous attacks in IoT is sleep deprivation, where the target is to maximize the power consumption of sensor nodes, so that their lifetime is minimized.
**Intermediate-Level Security Issues:**
In this level we are going to describe some security issues at network and transport layers of IoT:
**Replay or duplication attacks due to fragmentation:** To support the transmission of IPv6 packets exceeding the maximum frame size, 6LoWPAN defines a packet fragmentation mechanism. Due to the lack of authentication at the 6LoWPAN layer, malicious or misconfigured nodes may send duplicate or overlapping fragments.
**RPL routing attack:** The RPL protocol is exposed to a large variety of security attacks which affect specifically the network performance and resources.
**Authentication and secure communication:** Authentication and securing communication are essential parts in the security of the devices and users in IoT. This means using authentication mechanisms not only secure the data, the devices and users from threats but also network access and communication.
**Transport level end-to-end security:** A different types of data are stored while the communication between devices in IoT. In the transport level end-to-end security, it is recommended to use the most complex encryption level available to secure their communication.
**High-Level Security Issues:**
In this level, we are analyzing some security issues at application layer:
**CoAP security with internet:** The CoAP protocol can be maliciously exploited by various types of attacks. CoAP uses DTLS as a secure protocol and UDP is used as a transfer protocols. Therefore, the attacks on UDP or DTLS could be assigned as CoAP attack, which need to provide a secure mechanism that serves to improve the end-to-end authentication.
**Insecure interfaces:** Most devices used today in IoT may communicate with the users through some kind of web interface, cloud interface or mobile interface which poses a quite significant risk to access the data.
**Insecure software/firmware:** The connected devices in IoT always run some kind of software/firmware that might be exposed to many vulnerabilities. In addition, the software/firmware needs to be updated as soon as an exploit is discovered to protect the device against new threats.
**Middleware security:** Middleware is an important part in the IoT that is used to make the communication possible between all the components of the IoT. It needs to have certain security control from illegal access.

© IEOM Society International

### 3.3 Threats in cloud computing

Cloud attacks are increasingly targeting the smart home system, their impact can be enormous and many security attacks are proposed against the different cloud deployment models [8]such as:
**SQL Injection attacks:** these types of attacks can provide to an attacker an unauthorized access into the database using malicious code to manipulate it inserted into an SQL statement. It can also be used to add, modify and delete records in a database.
**Man in the Middle attack:** In this attack an intruder gets in the middle of communication between two targets making it appear as a normal exchange of information.
**Sniffer attacks:** It is an application or device that can read and capture network packets if the data packets are not encrypted.
**Denial of Service attacks:** A DoS attack meant to make services inaccessible to its intended users by flooding or crashing the services with traffic [9].

## 4. Proposed security solutions for Smart Home

Many researches considered home security one of the important things in the smart home system. A review of possible security solutions proposed in the literature is given in this section.
In their daily life, people use the key to open or to close the door.
This can affect the home security in many ways for example: someone can duplicate the key or they can lose it somewhere… For this reason some researchers have designed a model for face detection and face recognition for smart home security systems. In order to increase the level of security, they proposed to combine it with the password as additional authentication [10].
A solution has been proposed that identify a smart home management model for a multilevel framework and the main tasks that should be performed at each level in order to meet the system requirements. This multilevel framework covered all the IoT solutions for smart homes identified in the literature also it describes an environment of the smart home and includes its levels: cloud, utility, third party and user interface [11].
A User Privacy-enhanced Security Architecture has been proposed as a solution for smart home environment. The proposed security architecture protects the user's personal information against various security risks and provides safe services for users continuously by using some techniques such as cryptography, VPNs (Virtual Private Networks), message authentication and Anti-virus, firewall…etc [12].
Another model for Securing the authentication and message integrity for Smart Home using smart phone has been proposed. This security model uses AES256, Ephemeral Diffie-Hellman key exchange and RC4-based hash function to secure the authentication and message integrity between central hub (base station) and remote device (smart phone) [13].
Other researchers proposed a lightweight Lattice privacy-preserving aggregation scheme for Home Area Networks. The proposed scheme allows securing the consumption aggregation operation inside the home and at the same time keeping the user's confidentiality depending on homomorphic cryptosystem by encrypting and decrypting the messages [14].
An important security solution has been proposed for Smart Home Security Monitor System introducing a sensor alarm system that can send alarm messages to the user. This alarm system can guardian the home for the users when they are out and prevent them in any dangerous case (fire, theft, unauthorized entries …) [15].
Regarding the IoT, like how we classified the security issues in to many levels. We can specify three levels of security solutions to protect against security attacks and threats:
**Low-level security solutions:**
**Jamming attacks:** An approach for detection of jamming attacks by measuring the signal strength is proposed by [16]. Another approach of detecting jamming attacks via the computation of successful packet delivery ratio is proposed by [17].
**Insecure initialization:** Framework to secure initialization of IoT is proposed by [18]. Another approach aims to introduce artificial noise in signals is given by [19].
**Low-level Sybil attacks:** An approach by [20] suggests the detection of Sybil attacks through signal strength measurements.
**Insecure physical interface:** Reference [21] recommends to improve the security of the physical interface: The unnecessary hardware interfaces such as USBs providing access to the device firmware/software must be avoided.

© IEOM Society International

**Sleep deprivation attack:** In [22] A framework with 5 layers based on intrusion detection system is described.
**Intermediate-level security solutions:**
**Replay or duplication attacks due to fragmentation:** Adding timestamp and nonce options to the fragmented packets to protect against replay attack is proposed in [23].
**RPL routing attack:** A security mechanism for authentication of rank and version numbers using the hash function and digital signature is proposed by [24] to protect against attacks through RPL protocol.
**Authentication and secure communication:** The compression of Authentication Header (AH) and Encapsulating Security Payload (ESP) are proposed in [25]. Another approach by [26] called IACAC aims to generate secret keys using the Elliptic Curve Cryptography to secure the communication between devices.
**Transport level end-to-end security:** An approach for compressing DTLS is described by [27]. A lightweight implementation of Internet Key Exchange (IKE) to improve key management is proposed by [28].
**High-level security solutions:**
**CoAP security with internet:** A mapping of TLS and DTLS is proposed by [29] to provide end-to-end transport security. A prototype is suggested using a Mirror Proxy (MP) and Resource Directory by [30].
**Insecure interfaces:** A mechanisms include some configurations which discourage weak passwords, testing the interface against the vulnerabilities of software tools (SQLi and XSS), and the usage of https along with the firewalls [21].
**Insecure software/firmware:** Reference [21] recommends that the software/firmware should be updated regularly through an encrypted transmission mechanism also to use secure server to update files.
**Middleware security:** A proposition by [31] implements authentication and encryption to secure distributed applications. Another middleware supports efficient naming, addressing and profiling during communication in IoT environments is proposed by [32].

## 5. Discussion

The security of the smart home has attracted much attention recently. The existing attacks and studies reveal that today we are far away from a safe Smart Home but based on security solutions proposed by other researchers as a security measurement to smart home. We believe that all of them are reasonable and more effective, taking into account the security of the smart home network, data privacy and protecting the user.
In fact the smart home is a dream, but also a nightmare for user's privacy. There are many threats and issues with regard to the smart home applications since all the information and data in the home have to be recorded and almost everything is likely to be hacked: surveillance cameras, the refrigerator, the window, the door... In case, a criminal tries to attack the system and make it behave differently, the smart home system supposed to send an alert to the user.
As we all know the active attacks are stronger than the passive attacks and their effect is unpredictable. They have become a serious issue and their impact leads to huge losses. For example, imagine that the alarm system that supposed to protect user's home and prevent him in a dangerous situation, can send a false messages to the user which cause a misunderstanding for so many people. Another situation where the user forget to lock the door and use his mobile to lock it remotely, a man in the middle can send a notification to the user to confirm his action that the door is locked, but in reality, it's still open to the thieves which will then lead of course to a dangerous situation.
It's also important to mention that even passive attacks are dangerous in some situations, for example when an attacker gains access to the data storage area and downloads precious private user data, to be of course used in a malicious way.
To protect the smart home we have already mentioned many solutions to reduce the risk of attacks, after research and analysis and comparison between different possible solutions, we think that we have to protect all entry points of the network. The users must realize that the entire security of the network depends on the security level of the object with the lowest security. Once hackers have access to the network, they can easily manipulate other devices and infect them with malware.
Therefore, taking precautions, such as changing the default passwords on the devices and performing regular firmware updates, is a first step to mitigate the risks to fill the security gaps and secure the internet connection. So, the implementation of good practices involves questioning and evolution of the security mechanisms implemented by the designers, and by raising consumer awareness of the security of connected objects.
In a smart home, the confidentiality and the communication between devices should be maintained with effective algorithms to solve the problems within a home. A lot of work needs to be done by using data encryption, cryptography methods, authentication mechanism… etc.

© IEOM Society International

## 5. Conclusion

In conclusion, a home is a place where our private information needs to be respected. Unlike the traditional houses, smart homes can store the user's sensitive and important data and make his life better and comfortable. Even so, the user should apply effective and appropriate security measures to prevent or to secure his data from network attacks. In this paper, we have surveyed the most important security issues in a smart home and we have identified the security solutions proposed by other researchers. Additionally, we have analyzed the main elements that form the smart home and need to be secured.
In the future, we will propose a strong solution to improve the security in the smart home.

## References

[1] L. Satpathy, "SMART HOUSING: TECHNOLOGY TO AID AGING IN PLACE - NEW OPPORTUNITIES AND CHALLENGES," p. 192.
[2] A. Gaddam, K. Kaur, G. Sen Gupta, and S. C. Mukhopadhyay, "Determination of sleep quality of inhabitant in a smart home using an intelligent bed sensing system," 2010, pp. 1613–1617.
[3] A.-D. Floarea and V. Sgarciu, "Smart refrigerator: A next generation refrigerator connected to the IoT," 2016, pp. 1–6.
[4] S. Gao, Y. Qian, F. Cao, and L. Wang, "The design of smart window control system based on GSM network," 2011, pp. 1297–1299.
[5] M. Ye, N. Jiang, H. Yang, and Q. Yan, "Security analysis of Internet-of-Things: A case study of august smart lock," 2017, pp. 499–504.
[6] A. Prasetio, S. R. Akbar, and B. Priyambadha, "Implementation of semantic system in the smart home lights device based on agent," 2017, pp. 93–99.
[7] I. Alam, S. Khusro, and M. Naeem, "A review of smart TV: Past, present, and future," 2017, pp. 35–41.
[8] A. Singh and D. M. Shrivastava, "Overview of Attacks on Cloud Computing," vol. 1, no. 4, p. 3, 2012.
[9] M. Masdari and M. Jalali, "A survey and taxonomy of DoS attacks in cloud computing: DoS attacks in cloud computing," *Security and Communication Networks*, vol. 9, no. 16, pp. 3724–3751, Nov. 2016.
[10] D. A. R. Wati and D. Abadianto, "Design of face detection and recognition system for smart home security application," 2017, pp. 342–347.
[11] B. L. Risteska Stojkoska and K. V. Trivodaliev, "A review of Internet of Things for smart home: Challenges and solutions," *Journal of Cleaner Production*, vol. 140, pp. 1454–1464, Jan. 2017.
[12] S. Lee, J. Kim, and T. Shon, "User privacy-enhanced security architecture for home area network of Smartgrid," *Multimedia Tools and Applications*, vol. 75, no. 20, pp. 12749–12764, Oct. 2016.
[13] T. Mantoro, M. A. Ayu, and S. M. binti Mahmod, "Securing the authentication and message integrity for Smart Home using smart phone," 2014, pp. 985–989.
[14] "A. R. Abdallah and X. Shen, « Lightweight Lattice-based Homomorphic Privacy-Preserving Aggregation Scheme for Home Area Networks », in Proc. WCSP, 2014.pdf." .
[15] X. Hong, C. Yang, and C. Rong, "Smart Home Security Monitor System," 2016, pp. 247–251.
[16] M. Young and R. Boutaba, "Overcoming Adversaries in Sensor Networks: A Survey of Theoretical Models and Algorithmic Approaches for Tolerating Malicious Interference," *IEEE Communications Surveys & Tutorials*, vol. 13, no. 4, pp. 617–641, 2011.
[17] W. Xu, W. Trappe, Y. Zhang, and T. Wood, "The feasibility of launching and detecting jamming attacks in wireless networks," 2005, p. 46.
[18] "T. Pecorella, L. Brilli, L. Muchhi, The role of physical layer security in iot A Novel Perspective.pdf." .
[19] S. H. Chae, W. Choi, J. H. Lee, and T. Q. S. Quek, "Enhanced Secrecy in Stochastic Wireless Networks: Artificial Noise With Secrecy Protected Zone," *IEEE Transactions on Information Forensics and Security*, vol. 9, no. 10, pp. 1617–1628, Oct. 2014.
[20] M. Demirbas and Youngwhan Song, "An RSSI-based Scheme for Sybil Attack Detection in Wireless Sensor Networks," 2006, pp. 564–570.
[21] "Top IoT Vulnerabilities, Available: https://www.owasp.org/index.php/Top_IoT_Vulnerabilities, May 18, 2016." .
[22] T. Bhattasali and R. Chaki, "A Survey of Recent Intrusion Detection Systems for Wireless Sensor Network," in *Advances in Network Security and Applications*, vol. 196, D. C. Wyld, M. Wozniak, N. Chaki, N. Meghanathan, and D. Nagamalai, Eds. Berlin, Heidelberg: Springer Berlin Heidelberg, 2011, pp. 268–280.

© IEOM Society International

[23] H. Kim, "Protection Against Packet Fragmentation Attacks at 6LoWPAN Adaptation Layer," 2008, pp. 796–801.
[24] A. Dvir, T. Holczer, and L. Buttyan, "VeRA - Version Number and Rank Authentication in RPL," 2011, pp. 709–714.
[25] J. Granjal, E. Monteiro, and J. S. Silva, "Enabling Network-Layer Security on IPv6 Wireless Sensor Networks," 2010, pp. 1–6.
[26] P. N. Mahalle, B. Anggorojati, N. R. Prasad, and R. Prasad, "Identity Establishment and Capability Based Access Control (IECAC) Scheme for Internet of Things," p. 5.
[27] S. Raza, D. Trabalza, and T. Voigt, "6LoWPAN Compressed DTLS for CoAP," 2012, pp. 287–289.
[28] S. Raza, T. Voigt, and V. Jutvik, "Lightweight IKEv2: A Key Management Solution for both the Compressed IPsec and the IEEE 802.15.4 Security," p. 2.
[29] M. Brachmann, S. L. Keoh, O. G. Morchon, and S. S. Kumar, "End-to-End Transport Security in the IP-Based Internet of Things," 2012, pp. 1–5.
[30] M. Sethi, J. Arkko, and A. Keranen, "End-to-end security for sleepy smart object networks," 2012, pp. 964–972.
[31] D. Conzon, T. Bolognesi, P. Brizzi, A. Lotito, R. Tomasi, and M. A. Spirito, "The VIRTUS Middleware: An XMPP Based Architecture for Secure IoT Communications," 2012, pp. 1–6.
[32] C. H. Liu, B. Yang, T. Liu, Efficient naming, addressing and profile services in internet of things sensory environments, Ad Hoc Networks, 2014.

## Biographies

**Khawla Mazwa,** Received her Technical University Degree in Software and Network Engineering from ENSET of Rabat (Morocco) in 2014 and Bachelor's degree in Mobile Applications Engineering from EST of Sale (Morocco) in 2015. She is currently preparing a Master in Security and Information Systems at National School of Applied Sciences of Kenitra (Morocco). Her research interests include Computer Networks, Information Security and Internet of Things.

**Prof. Tomader Mazri**, HDR degree in Networks and Telecommunication from IbnTofail University, Ph.D. degree in Microelectronics and Telecommunication from SidiMohamed BenAbdellah University and INPT of Rabat, Master's degree in Microelectronics and Telecommunication Systems , Bachelor's degree in telecommunication from CadiAyyad university. She is currently a professor at National School of Applied Sciences of Kenitra and a Permanent member of Electrical and Telecommunications Engineering Laboratory. Author and co-author of twenty articles journals, forty articles in international conferences, a chapter and three books. Her major research interests are on Microwave systems for mobile and radar, Smart antennas and NG Mobile network.

© IEOM Society International