SECURITY ISSUES IN SMART HOME AND MOBILE HEALTH SYSTEM: THREAT ANALYSIS, POSSIBLE COUNTERMEASURES AND LESSONS LEARNED

Olayemi Olawumi, Antti Väänänen, Keijo Haataja, Pekka Toivanen

University of Eastern Finland, School of Computing, Kuopio Campus,
P.O. Box 1627, FI-70211 Kuopio,
E-mails: Olayemo@student.uef.fi, Antti.Vaananen@sensoftia.fi,
Keijo.Haataja@uef.fi, Pekka.Toivanen@uef.fi
Finland

Abstract: Security is an important issue in Smart Home Environments. Most especially in situations where smart homes can store and release sensitive data to third parties, which makes data collected within smart environments vulnerable to severe security and privacy abuses. Therefore, identification of these security issues is crucial to taking the appropriate steps towards mitigating them and enhancing the security of the collected data within these homes. This paper focuses its attention on the analysis of the possible security issues in smart home environments, identification of different attacks and vulnerabilities with possible recommendations, and countermeasures to mitigate these threats. Moreover, we applied threat modelling process to our Smart Environment for Assisted Living (SEAL) system identifying the assets and threats to the system and examining how our system can be designed in a more secure way that will guarantee a maximum protection of data transmitted across the system.

Key words: Bluetooth, Smart Home, SEAL, Security, Threat Analysis, Wireless Personal Area Network, ZigBee.

1. INTRODUCTION

In recent years, smart home development is on the rise and consequently faced with lot of challenges related to data and information security. Smart homes present opportunities for a comfortable and secured living, also it can help the elderly and disabled to improve their quality of life as well as prolong independent living at home. Such technologies provide an admirable infrastructure for healthcare purposes, which would allow the elderly and disabled to get some available healthcare services comfortably in their homes [1]. However, the recent rising abuses of smart environments is a major source of concern as several threats

exist to exploit the vulnerabilities found in the protocols implemented in these systems. Healthcare data collected within smart environments are vulnerable to severe security and privacy abuses, especially when smart homes can store and release data to third parties [1]. Therefore, it is crucial to identify these security issues and take necessary steps towards mitigating them and enhancing the security of the collected healthcare data in the smart environment.

SEAL (Smart Environment for Assisted Living) is developed in Computational Intelligence (CI) research group at University of Eastern Finland (UEF). SEAL is a comprehensive combination of smart home and mobile health subsystems. The subsystems provide functionalities to home residents that help them to achieve secure, healthy, and easy living and working environment even if they are suffering from chronic conditions or just want to automate equipment functionalities in their home/office or to be more aware about their health condition.

SEAL system will be used in home healthcare organizations, occupational health studies, and individual use where ambitious and challenging interdisciplinary research work can be conducted and later on companies can transfer these novel research findings into everyday use within new mobile health products. In order to achieve the ambitious goals of SEAL environment, all SEAL subsystems shall be realized as separate entities, which work seamlessly together. Seamless cooperation between subsystems requires open and common communication interfaces. High level of adaptivity will be one of the key requirements in SEAL and it can be achieved by modular planning in which subsystems can operate independently or in cooperation with other subsystems seamlessly. [2]

SEAL can be separated into two subsystem entities which are Assisted Living & Home Automation subsystem and mHealth subsystem. These two subsystems are working seamlessly together in same application and measurements can be seen in same UI (User Interface). The architectural logic behind the system is divided by the application programming interfaces (APIs), which are collecting the measurement data from different sources.

In mHealth subsystem, the use-cases can be scaled from chronic condition monitoring (with several concurrent vital signs monitoring) of a patient to active health information monitoring (e.g. weight and blood pressure) for fitness and well-being purposes. In SEAL, the vital signs and periodic measurements are collected by biosensors or measurement devices and information is transferred by wireless sensor network to SEAL Application. SEAL Application can be located either in smartphone, tablet computer, or house automation mini-PC. The data is collected by application located in a mobile device or in home gateway application depending on user location (indoor / outdoor).

In Assisted Living &Home Automation subsystem, the wireless network collects the environmental data from ambient sensors, which are located in the resident's home. The SEAL system analyzes the collected data and changes the

house automation functionality accordingly. SEAL system also monitors the indoor air quality to adjust the air flow according to measurements. Same subsystem can also include functionalities to improve quality of live, for example, by enabling video conversation with family members or friends. Security functionalities are also included, such as door control and fire/smoke detection.

SEAL Application will be designed to operate in multiple mobile platforms and provide functionalities to several end-user groups, such as healthcare professionals, healthy users who want to monitor their health status, or people who want assistance when using intelligent house technology. The SEAL system shall provide open APIs for other mobile devices, applications, and data repositories. SEAL must also provide comprehensive security measures for wireless authentication, data transmission, and data storage in mobile devices to help to achieve user needs and regulatory requirements for transferring and storing personal health data. Figure 1 illustrates our SEAL system that can be utilized in mHealth, Smart Home, and Smart Office use cases.

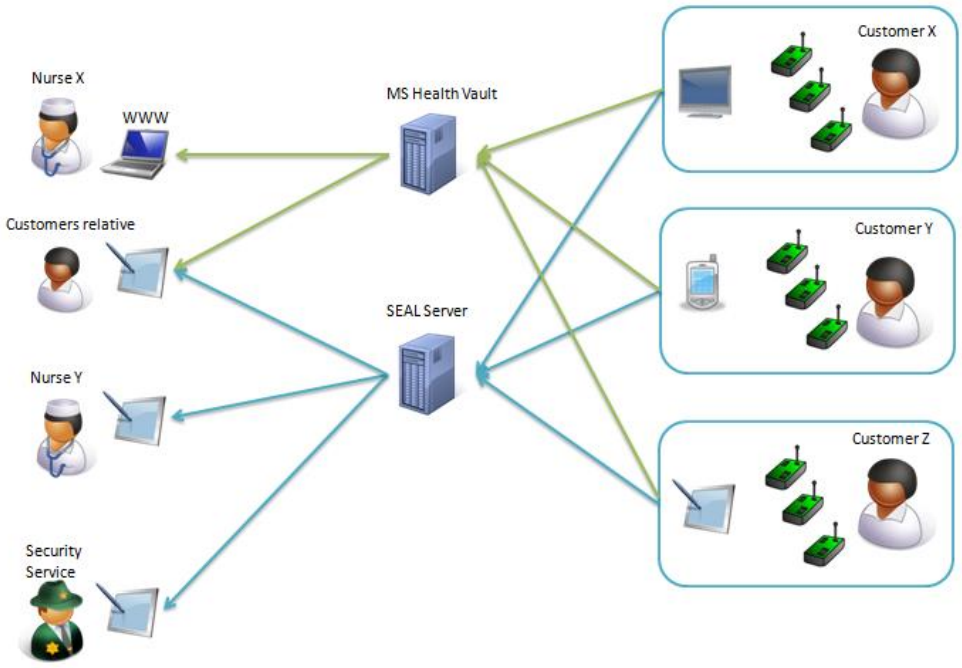

Fig. 1. SEAL System for mHealth, Smart Home and Smart Office use cases

Wireless networks are very significant and necessary for realizing Smart Home and mHealth systems. Smart environments utilize wireless interfaces, mainly Bluetooth, ZigBee, and/or WLAN (Wireless Local Area Network) for data

transmission [3]. The nature of the transmitted data varies with much being considered sensitive and important to the wellbeing of users [4]. However, each of these protocols being used in the implementation of smart environments has serious security issues that cannot be overlooked and if not recognized and attended to at the early design stage, can have severe consequences [3].

Furthermore, the recent occurrences of smart environment hacking in which attackers can take control of smart home devices from a remote location raise an alarm of the need to urgently address these challenges [13- 21].

Our results: In this paper, we provide an investigation into the possible security issues in Smart Home Systems. In addition, we analyze smart environments with an emphasis on the security challenges of the wireless network interfaces being utilized in these systems. Moreover, we apply threat modeling process to our SEAL system, identify the assets and threats to the system, and propose possible countermeasures to mitigate against these threats. Furthermore, we examine how SEAL system can be designed in a more secure way that will guarantee a maximum protection of data transmitted across the system and evaluate how the proposed countermeasures can be implemented in our SEAL environment to guarantee adequate data security. We also present some new ideas that will be used in our future research work.

The rest of the paper is organized as follows. Section 2 provides a literature review based comparative analysis of the security issues in Smart Home systems. Section 3 provides a detailed explanation into how Smart environments can be designed in a secure way using threat modeling process with SEAL system details and examples. Our proposed mitigation strategies are presented in Section 4. Finally, Section 5 concludes the paper and sketches future work.

2. POSSIBLE SECURITY THREATS IN SMART HOME AND MOBILE HEALTH SYSTEMS

This section presents the possible security threats in Smart Home Environment. As earlier presented in [7], smart homes must fulfill six main security objectives, which form the core security requirements for smart home environments; they must include Confidentiality, Integrity, Authentication, Authorization, Non-repudiation, and Availability. However, there are serious security threats that attempt to compromise one or more of these identified security requirements [7], for example, let us consider a scenario in a smart home environment in which an attacker fraudulently gains access to classified or private information, such as patient's health data, or in another scenario in which an attacker does not only gain access to the information, but can also modify it. In these cases, many of the abovementioned security objectives are being breached. [7–8]

Security threats against smart home environments can be classified mainly into two categories [7, 9]:

1) *Internal threats:* These kinds of threats originate within the smart home environment and they may be, for example, due to improper network configuration, weak password that leads to password compromise, bugs in the smart environment software, or even deficient security plan.
2) *External threats:* These are security threats to smart home internal network derived from external fraudulent nodes. There are lots of external security threats to smart home environment, which are derived from the use of various wireless protocols in the implementation of smart homes. This paper focuses its attention on external threats.

Section 2.1 explains Passive attacks, Section 2.2 discusses about Active Attacks, and Section 2.3 presents the recent news on Smart Homes hacking.

2.1 Passive Attacks

In passive attack, an attacker gains unauthorized access to private information by monitoring or listening its transmission without modifying it. In this kind of attack, the transmitted messages between the sender and receiver are not modified and thus, it is very difficult to detect. There are two types of attacks under this category: [7, 9–10]

1) *Eavesdropping Attack:* Eavesdropping is a major security threat to smart environments. It is possible for an attacker to illegally monitor home user traffic, such as email messages, Internet surfing details, and phone conversations, between the Smart Home internal network and a third party without alerting the legitimate communicating parties. Once attackers have access to any of this private information, more information about the home owner can be obtained and further attacks are inevitable. This is clearly an attack on the confidentiality of the Smart Home internal network. Let us consider a scenario in which an attacker has illegal access to the websites a home owner visited in the Smart environment. In this way, it is possible for the attacker to conduct a thorough investigation into the contents of these web pages and develop a strong knowledge about the owner's interest and objectives. All this is performed secretly without the owner being aware of any imminent danger. Eavesdropping attack on ZigBee network was demonstrated in practice in our experiment in [11].
2) *Traffic Analysis:* Traffic analysis is a passive attack in which an attacker simply observes the traffic pattern in a communication between two parties. It is possible for an attacker to observe traffic in a communication between a Smart Home owner and a third party located anywhere in the world. From this observation, the attacker can infer sensitive information (e.g., duration and frequency of messages, location of the home user, and passwords) and make a deduction about the subject matter or the results of sent messages. In traffic analysis, there is usually no evidence that an attack has taken place. Therefore, it is really hard to detect. [7,9–10]

2.2 Active Attacks

In active attacks, an unauthorized change in data or an introduction of fraudulent data into the Smart Home internal network is attempted by an attacker. This may be through modification of transmitted or stored data or the injection of new data streams into the Smart Homes internal network. There are seven sub-categories of active attacks: Masquerade Attacks, Replay Attacks, Message Modification Attacks, Denial-of-Service Attacks, Interception Attacks, Session-Stealing Attacks, and Malicious Codes: [7, 9–10]

1) *Masquerade Attacks:* In masquerading attack, an attacker can take on a false identity to gain certain unauthorized privileges. It is possible for an attacker to pretend to be an authorized home user or entity, in order to have access to the Smart Home internal network remotely and obtain private information or even modify them. Once an attacker can successfully perform a masquerade attack on a smart Home internal network, then several other attacks are possible, such as replay attack. [7,9–10]
2) *Replay Attacks:* In replay attack, an attacker captures a previously sent message between two legitimate communicating parties and re-transmits it later pretending to be an authorized entity. In Smart environments, it is possible for an attacker to capture a copy of a user's medical request or service, store it and replay later in order to make the same request or have access to the service the home user is authorized to use [7, 9]. The effect of a replay attack on a Smart Home internal network obviously depends on the content of the data being replayed: It can have only a minor effect or a severe one. We also demonstrated with experimental figures reply attack on ZigBee network in our experiment in [11].
3) *Message Modification Attacks:* Message modification means that some part of a genuine message is altered. This kind of attack may also include an attacker delaying the message or reordering it to produce illegitimate effect. For example, let us consider a scenario in which a home owner sends a message to his account officer in bank A and the content of the message is "Allow person X access to my private safe box". It is possible for an attacker to capture this kind of message and modify the content to suit his/her own purpose. The modified message may be "Allow person Y access to my private safe box". This is clearly an attack on the integrity of messages sent from the environment. [7,9–10]
4) *Denial-of-Service (DoS) Attacks:* This is when an authorized user is blocked or denied access to a service either by making the service unavailable or limiting it availability. In DoS attack, the Smart Home's internal network can be flooded with messages by an attacker in order to overload its resources with traffic. In this situation, the authorized users or Home owner will not be able to access the services of the home network. Moreover, the internal traffic transmitted via

wired or wireless networks inside the Smart Home can also be blocked by an attacker by sending numerous messages to the web servers. [7,9–10,12]

5) *Interception Attacks:* This kind of attack is also possible in Smart Homes in which an attacker intercepts all the packets destined to a remote or mobile user from the home environment. As a result of this attack, the authorized users are denied access to the services from the home network. [9–10,12]
6) *Session-Stealing Attacks:* This is an attack in which an attacker waits patiently for a legitimate user or node to authenticate itself and to start an application. After that the attacker fraudulently takes over the session by impersonating the identity of the genuine user or node. For instance, let us consider a scenario in which a Smart Home environment supports Mobile Internet Protocol. In a situation in which a home user logins to a particular service, such as Internet banking via a mobile node, and provides login name and password, smart card credential, secure ID, or a token password, it is possible for an attacker connected to a mobile node's Ethernet-based foreign link to flood the mobile node with nuisance packets in order to take over the mobile node's session. [9–10,12]
7) *Malicious Codes:* Malicious Codes are software threats that cause negative effects to the Smart Home internal network by exploiting its vulnerabilities. Malicious codes may be used to modify, destroy, or steal data as well as allow unauthorized access to the Smart home internal network. Malicious codes are classified as Viruses, Bacteria, Worms, Trapdoors, Logic bombs, and Trojan horses each posing serious threat to the security of information in Smart environment. Malicious codes can be introduced into a Smart home, for example, via software pitfalls, e-mails, web pages while surfing the web, and instant communication tools. Malicious codes are the biggest threats to Smart Home internal networks due to the fact that the home users lack the awareness of their existence or how to secure the network and protect the data. [7,9–10,12]

2.3 Recent News on Smart Homes Hacking

Recently, smart home attacks and vulnerabilities are being in the headlines of news. There are even reports of some smart environments that were successfully hacked. This trend is likely to grow because of the recent adoption of Smart Homes for Healthcare and other purposes. A brief review of some of these reports is provided in the following list:

- In July 2013, Kashmir Hill, a reporter for Forbes Magazine, published a report titled *"When 'Smart Homes' Get Hacked: I Hunted a Complete Stranger's House via the Internet".* Kashmir Hill narrated in her report how she was able to hack into Thomas Hatley's home remotely by turning on and off the lights in the master bedroom of Hatley's Oregon home. According to Kashmir, the attack was made possible, because the Smart home lack password protection by default. [13–14]

- In August 2013, Sarah Griffiths published a report titled *"Computer hackers can now hijack toilets: 'Smart Toilet' users in Japan could become victim to Bluetooth bidet attacks and stealthy seat closing"*. The report confirms that the Bluetooth controlled Satis toilet, which is popular in Japan and known to let people raise and lower the toilet set as well as triggers a bidet function and flush by using a mobile app, can be hacked, or attacked remotely due to the Bluetooth security vulnerability found in the implementation of this toilet. A warning about this vulnerability came from IT security firm Trustwave. [15]
- In August 2013, Heather Kelly, a reporter for CNN, published a report titled *"'Smart Homes' are vulnerable, say hackers"*. In this report, in addition to the Bluetooth controlled Satis toilet that was reported, she also mentioned about a cute bunny toy called Karotz, which can be controlled from a smartphone app and is outfitted with a video camera, microphone, RFID (Radio Frequency Identification) chip, and speakers. She reported how a Software engineer Jennifer Savage was able to take control of it from a computer and remotely watch live video, turning it into a malicious surveillance camera for attackers. Moreover, she reported about how Daniel Crowley demonstrated live at a Black Hat session, how it is possible for a third party to hack into a front-door lock and open it from a computer. Finally, she reported how Behrang Fouladi and Sahand Ghanoun demonstrated a hack that opened a smart lock that used the Z-Wave protocol. [16]
- In August 2013, there was a report on ABC news titled *"'Smart Homes are Convenient But May be Vulnerable to Hack-Ins"*. This report raised the issue of the growing concerns that computerized homes make it easier for thieves to get personal information. [17]
- In August 2013, there was another report on ABC news, which was titled *"'Smart Homes' could be Vulnerable to Hacking"*. This report raised the issue of the growing concerns of security experts about homes wired so everything can be controlled remotely. [18]
- In September 2014, Pierluigi Paganini published an article on Infosec institute resources webpage titled *"Risks and Cyber Threats to the Healthcare Industry"*. In this article, the author expresses worries on the risk posed by the usage of mobile devices in the healthcare industry, confirmed by a recent study by the Ponemon Institute (Under the sub-title "*Mobile device, the hidden risks*") [18]. He stated that more than half (51%) of physicians use tablets for professional purposes, and 74% use smartphones at work, and according to Transparency Market Research, the number will increase rapidly as mobile monitoring and diagnostic medical devices market will reach $8.03 billion by 2019 [19]. Moreover, the author further stated that there is going to be a significant increase in the number of patients and medical staffs that will access healthcare records and other services electronically through mobile platforms despite the

concern about lack of efficient security for mobile devices. This report raises the issue of necessity for new and unique approach to cyber security. [18–19]

- In December 28, 2015, there was also a report by Laura Hautala, published on CNET webpage titled "*Internet-connected homes open the door to hackers*". In the article, the author narrated how a security researcher at Fortinet accomplished a hack into a video stream without any coding skills [20]. The researcher simply visited a webpage Shodan.io, which is a website where varieties of internet connected devices were found, and was able to hack into the video stream just by entering the word "admin" for the camera's username and password. The author also emphasized on the need to urgently address the security of these devices, because billions of sensors will soon be designed into various appliances, security systems, health and other equipments in the future. [20]
- Finally, in May 2, 2016, there was a report by Nicole Casal M. Published on the University of Michigan webpage, which was titled "*Hacking into homes: 'Smart home' security flaws found in popular system*". She narrated how researchers at the University of Michigan were able to hack into smart home and get the PIN code to a home's front door [21]. Four successful proof-of-concept attacks were performed by them; they demonstrated how a SmartApp can eavesdrop on someone setting up a new PIN code for a door lock, and subsequently send the PIN in a text message to a potential hacker. In the second attack, they showed how an existing SmartApp could be remotely exploited to virtually make a spare door key by programming an additional PIN codes into the electronic locks. They also showed how SmartApp could be used to turn off "Vacation mode" while you are away and how fire alarm could be made to go off by injecting false message via the SmartApp. [21]

3. DESIGNING A SECURE SMART ENVIRONMENT: CASE SEAL SYSTEM

In designing a Secure Smart Environment, it is necessary to consider examining security from the perspective of the whole environment taking into consideration all elements that may need to be protected [4–6]. Data Security in Smart Environment is of paramount importance as any data breach in such system may have severe consequences.

Our SEAL system is designed to improve the user's quality of life and prolong independent living at home. Therefore, data transmitted via such a system can be categorized into two main groups: *Operational data*, which relates to day-to-day healthcare data of the smart home user and *Non-operational data*, which refers to other information that does not directly influence the user (e.g., finances and emails). [6]

A general view of the data involved in the SEAL system is given by grouping them into the categories as illustrated in Figure 2.

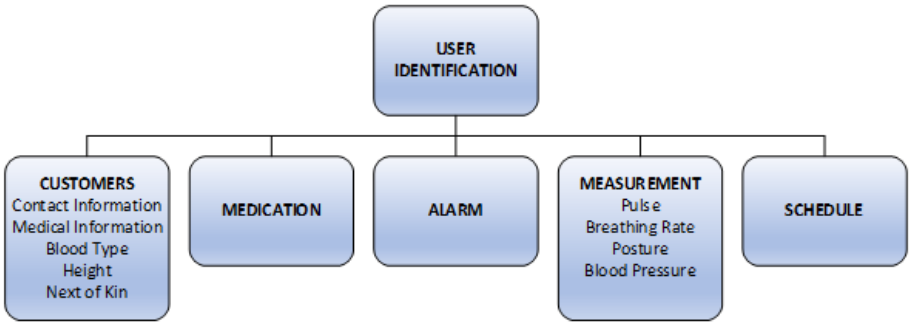

Fig. 2. General SEAL System Data Group

It is important to note that all data transmitted within the smart environment are considered equally sensitive and requires adequate protection to preserve its integrity and confidentiality. However, in designing a secure SEAL system in which data transmission is adequately protected, the first step is to determine the sensitivity of these transmitted data and their impacts if data gets compromised. Impacts are rated high, medium, or low depending on the case involved. Let us consider a scenario in which a user's medications or medical history is compromised or exposed to an intruder. The impact in this scenario could be rated as "High", because the consequences in this case may be severe [4–6].

After identifying the sensitivity of the transmitted data, then it is possible to conduct a detailed threat analysis, for example, by using Microsoft's security development lifecycle to determine the risk or potential threats that may be linked with each type of data in the smart environment taking into consideration the core elements of security, such as disclosure to an intruder (confidentiality), denial-of-access to information in the smart environment due to some attacks, and modification or destruction of data.

Threat analysis based on Microsoft's security development lifecycle was proposed in this paper, because it has proven efficient in building security into software development lifecycle from the design stage. The purpose of this analysis is to identify different potential attack paths in our system, the resulting threats, and possible mitigation strategies against them [22]. Since threat models are built on the basis of scenarios, we used data transmissions within our SEAL system and wireless communications between various users (Home & Mobile Users and Medical professionals) and the SEAL server as a case scenario in this analysis.

Conducting a detailed threat analysis in smart environment requires the following step-by-step procedure consisting of the steps explained in Sections 3.1 (Identification of Assets), 3.2 (Data Flow Diagram), 3.3 (Entry Points), 3.4 (Threat Identification & Classification), 3.5 (Threat Evaluation), and 3.6 (Threat Scenario in SEAL System Use-Case).

3.1 Identification of Assets

Analyzing threats in smart environments require the identification of all assets in the system. Assets represent the resources to be protected in the system. Since no assets means no threats [23], an attacker will always try to obtain access to the assets in the Smart home.

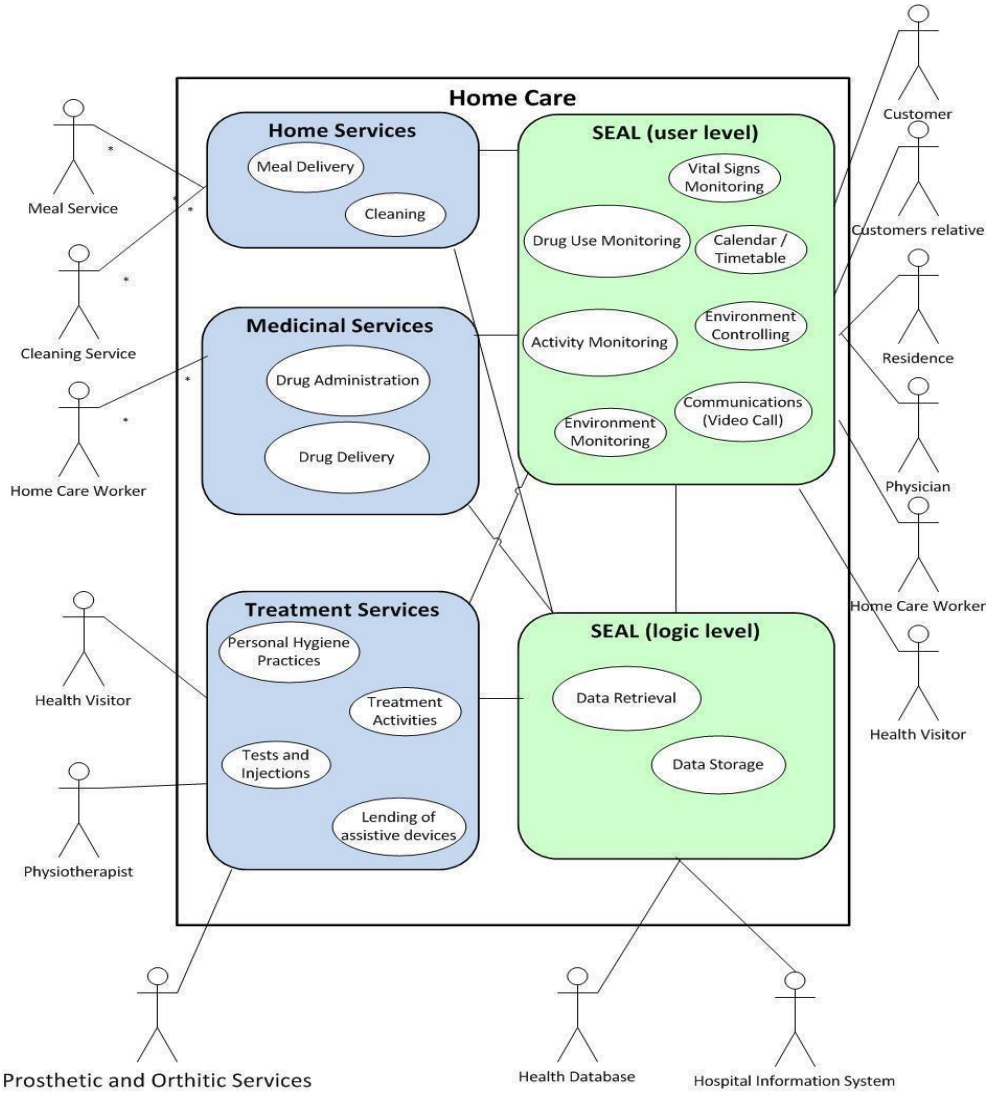

Fig. 3. SEAL System Use Case Diagram

Figure 3 illustrates a detailed diagram of the SEAL system use case and actors/assets. Identified assets in the SEAL system are the following:

- *Data assets:* This comprises of data stored on the SEAL server, data stored on the customer's device, and data transmitted over various communication mediums.
- *SEAL server:* This contains data of medical/health history for the customers and environmental data from ambient sensors.
- *Wide Area Network (WAN), Wireless Sensor Network (WSN), and Wireless Body Area Network (WBAN):* The communications of the SEAL system with the customer's devices are based on these components.
- *Users and Medical Professionals:* Users and Medical professionals are also considered as main assets of SEAL system, since they are relevant in the security perspective.

3.2 Data Flow Diagram

Once all assets in the system have been identified, then a Data Flow Diagram (DFD) can be created to investigate any aspect of the system. DFD facilitates the identification of important data flows for the definition of entry points to see where a potential attacker could interact with the system, security requirements, and possible threats [23]. The entire system can be modelled here at several levels (Level 0, Level 1, ..., Level n+1) [22]. A DFD enables diagrammatic representation of the attack paths to the Smart environments and it forms a basis for identifying various threats to the system [22].

Figure 4 presents a section of the SEAL system DFD at level 0. The rectangular blocks represent the entities (Customers and Medical professionals), the cylinder shape represents the data store, and the arrows represent data flows between the entities and the SEAL server. Some of the data flows pass through a trust level, marked by the dotted line. The SEAL server is represented by a circle, also regarded as a "black box" meaning it receives input, process it, and produces an output.

3.3 Entry Points

As mentioned earlier, all assets identified in the previous step represent valuable targets from attacker's perspective. With all assets in mind, it is possible to identify different entry points to the system. Entry points are interface through which an attacker can access the Smart home. Attacker's intention and knowledge determines if an element of a system can be used as an entry point or not. [22, 23]

The following three entry points were determined in our SEAL system:

1) Through the Wireless Body Area Network (WBAN) Central Node and User Interface, which enables communications between the mobile customers and the SEAL server.
2) Wireless Sensor Network's (WSN) Central Node and User Interface, through which the home data or health data of the home users gets into the SEAL Server.

3) Through the wireless communication link between the health professional's User Interface and the SEAL server, which enable them to have access to user's information and healthcare data on the server.

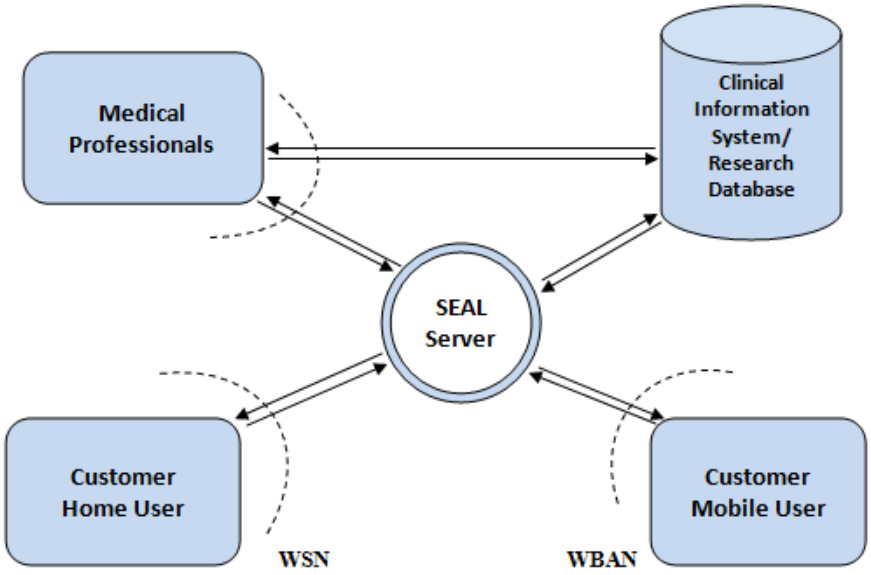

Fig. 4. Section of a Data Flow Diagram (Level 0)

3.4 Threat Identification & Classification

Once all assets and entry points are determined, vulnerabilities and possible threats to the system can be derived. Threats can be collected from the compiled information and the DFD created. It is very important to note that threats cannot be entirely removed from the system and they must be examined from the point-of-view of possible mitigation. [22, 24]

Possible threats to a system can be derived by mapping entry points to assets and classifying them according to the STRIDE taxonomy. STRIDE is a system used to identify threats and stands for the following actions carried out by an attacker: [25]

- *Spoofing Identity:* This is usually a breach of authentication process into the system. For instance, an attacker can impersonate a different person, different device, or traffic flow to gain access to the system.
- *Tampering with data (Integrity):* This is when an attacker can modify some system data either while they are at database/device or during its transit. It is

possible for an attacker to modify this data at database/device by executing malicious codes or during its transit by, for example, eavesdropping on the system, using a Man-In-The-Middle (MITM) attack, or exploiting routing protocols.

- *Repudiation:* This can also be called a breach of accountability. In this case an attacker can take some certain actions on the system, with the system unable to prove the opposite.
- *Information Disclosure (Confidentiality):* This is when an attacker can gain access to all or some system information either while they are at database/device or during its transit. An attacker can gain access to this information at database/device by remotely accessing information through successful identity spoofing or during its transit by eavesdropping or MITM attack.
- *Denial-of-Service (restriction on availability):* It is possible to loss the availability of system data while data are at database/device as a result of intentional deletion by an attacker or during its transit as a result of other attacks, such as attacks on network protocols. Mostly this kind of threat occurs simultaneously with identity spoofing and after that as a loss of confidentiality.
- *Elevation of Privilege:* This can be seen as a theft of authorization and it can be encountered in systems that grant different permission to different users. A clear scenario in this case is when an attacker or a malicious system user tries to gain higher access rights to the system than he currently legitimately has.

3.5 Threat Evaluation

After the threats has been classified using STRIDE, they can then be evaluated by determining the risk posed by these threats to the system. The SEAL system is under development and thus evaluating the possibility of the risk posed to the system is challenging at the moment. However, risk assessment is done usually with DREAD, which is based on five factors, each with a predefined weightening as follows: [22, 26]

- *Damage:* What harm is caused by the threat being exploited?
- *Reproducibility:* To what degree can the threat being exploited be reproduced?
- *Exploitability:* How much work is done to exploit the threat?
- *Affected Users:* How many users are affected by the threat?
- *Discoverability:* How easily can the threat be discovered?

After a proper evaluation of the threats, corresponding mitigations can be applied to counter them.

3.6 Threat Scenario in SEAL System Use Case

In this section, we present a detailed analysis of the potential threats to our SEAL system. Moreover, we show clearly why it is important to counter these threats, since the consequences of not taking them into account may be severe. Data transmitted via wireless communications in the SEAL system contains important healthcare information and loss of data confidentiality in such a system will always result in privacy breach. An attacker can take advantage of this to gain access to these transmitted data over the network and subsequently perform other possible attacks or even modify messages correctly sent by a communicating device. The integrity of data transmitted over wireless networks can be lost in several cases, most especially in a situation in which an attacker sends malicious instructions to the smart environment. There may also be a situation in which a legitimate user is denied access to data in the system due to interruption or attacks. This is a case in denial-of-service threat or loss of availability of data and the consequences may be a minor one or severe depending on the length of interruption.

There are also other possible potential threat cases in the SEAL system that needs to be taken into account. Data transmitted in such a system should be accurate and not tampered with in any situation. Thus, communicating devices should be authenticated in order to ensure accountability and transparency of actions performed in the system by either a legitimate user or a system administrator. Moreover, the source of all transmitted data should be confirmed or at least all transmitted data across the system should come from an authenticated device in order to base all actions on trust rather than rely on information from undependable or unidentified sources.

It is also possible for an attacker to try gain unauthorized access into the system by trying to pose as a legitimate user or even a restricted user trying to gain access to the system as an administrator. In case these threats are not taken into account, it could lead to a loss of confidentiality of the data transmitted in the system, loss of credentials, or even a situation in which a restricted user will gain more access rights as an administrator and is able to see or modify some confidential data within the system or in the worst case scenario trying to influence the system in a malicious way.

Hence, we can conclude that failure to address these various threats could result in severe cases of privacy breaches in the SEAL system.

4. POSSIBLE MITIGATION AND RECOMMENDATIONS

Deploying Smart Homes for any purpose, without considering adequate and efficient security measures makes user's privacy vulnerable. In Smart environments, security should be of high importance, especially in situations when Smart Homes will be deployed for Healthcare purposes: Security flaws in this kind of situations may have severe consequences.

The purpose of this section is to outline possible mitigation strategies against the security issues discovered in earlier Sections against Smart Homes, even though not totally eliminating their potential risk. Moreover, we present some possible recommendations to reduce the chance of security abuses in such environments.

Firstly, it is evident based on this paper and our research work that Smart Homes will always remain a target for hackers making it vulnerable to various attacks by exploiting of any found vulnerabilities in the environment. However, adequate security measures can be put in place to mitigate against these possible attacks. A possible way of countering attacks against Smart Homes is by employing the use of intrusion detection/prevention system, which will be integrated into the Smart Homes internal network for continuous monitoring of the network. Previous studies have proven the efficiency of Intrusion Detection Systems (IDS) and Intrusion Prevention Systems (IPS), which can also be utilized in Smart Homes as a second line of defence [27–31]. Such a system can efficiently monitor Smart environments internal network, detect any intrusion or attacks, and stop any malicious activities. Therefore, we recommend that the intrusion detection/prevention system would be engrossed into the design of Smart Home network as a second line of defence against attacks.

Secondly, we recommend the use of secure firewalls in Smart Home internal networks as another extra layer of defence. Firewall is becoming more significant and it has proven effective in network security; most especially Web Application Firewall (WAF) could be implemented in addition to other normal firewalls. WAF has proven efficient in stopping application attacks and data leakage and providing automated temporary patches to mitigate risks. Therefore, utilizing it in Smart Home internal network will help in continuous monitoring of the network. Firewall can be installed on the residential gateway (the access point to the Smart Home internal network) in order to examine all traffic entering or leaving the Smart Homes internal network and blocking all suspicious accesses or data.

Thirdly, we recommend the use of strong identity and message authentication scheme in Smart Homes, since this is likely to help immensely in defeating internal threats to Smart Homes. Smart Home should be designed to support robust identification and verification process as well as access rights of users should be verified, for example, via a unique ID, password, smart cards, fingerprints, or iris, before allowing access to the network resources or services.

Finally, we propose the use of digital signature scheme in Smart Homes to ensure the authenticity of sent and received messages. If a message is sent by a Smart Home user, which utilizes digital signature scheme in Smart environment, it will assure a recipient that the message was created by the known sender and that the message was not altered in transit. In addition, any change to a digitally signed message invalidates the signature. Digital Signature uses the concept of Public-Key Cryptography, which is a form of asymmetric encryption in which each

communicating party has a key pair. One of the keys is used for encryption, while the other one is use for decryption. [32]

5. CONCLUSION AND FUTURE WORK

Security is a very important issue in Smart Home Environments due to the sensitive nature of private and confidential data being transmitted via wireless communication links. These wireless technologies being used in the implementation of smart homes has serious security issues that could have serious security implications if they are not carefully taken into account. Therefore, identification of these security issues is crucial to taking the appropriate steps towards mitigating them and enhancing the security of the collected data within these homes.

In this paper, we provided a literature review based investigation into the possible security issues in Smart Home Systems. In addition, we analyzed smart environments with an emphasis on the security challenges of the wireless network interfaces being utilized in these systems. Moreover, we proposed possible countermeasures to mitigate discovered security threats. Furthermore, we applied threat modelling process to our SEAL system in order to identify the assets and threats to the system and analyze how our system can be designed in a more secure way that will guarantee a maximum protection of data transmitted across the system.

Smart homes are likely to be applicable not only in healthcare, but in various other sectors as well that affect our daily living. However, user's acceptance of these technologies will be greatly dependent on how secure they are in the future.

The problems we want to investigate in our future research work are concerned with the following issues:

1) The adoption of Smart Homes is likely to increase, not only for healthcare purposes, but in every sector that affect our daily living. Thus, new attacks against them are likely to be found. We want to further investigate more security issues in Smart environment and propose countermeasures against discovered attacks.
2) Since Smart Homes are rapidly becoming more essential for healthcare use, which is evident based on our SEAL system use case, we proposed in this paper the integration of intrusion detection/prevention systems into smart homes internal networks. We want to further research on how exactly this can be implemented to efficiently detect any intrusion or attacks and stop any malicious activities.
3) It is evident from previous studies that Steganography and watermarking techniques could be a potential solution for securing Bluetooth and ZigBee communications in the future. We want to further research novel techniques of improving security of data transmission in Smart environments using Steganography and watermarking techniques. [33–38]

REFERENCES

[1] Mouhcine G., Jonas T., Catherine W. and Khalil E., "Context-Based Access Control to Medical Data in Smart Homes," *International Conference on Computer Engineering and Applications (IPCSIT'2011),* Vol. 2, IACSIT Press, Singapore, 2011, pp. 275–279.

[2] Väänänen A., Haataja K., Asikainen M., Jantun*en I., and Toivanen P., "*Mobile Health Applications – A Comparative Analysis and a Novel Mobile Health Platform*," Proceedings of 5th Springer International Conference on Sensor Systems and Software (S-CUBE'2014),* Coventry, Great Britain, 2014.

[3] John D., Security Issues with Wi-Fi, Bluetooth, and ZigBee. TechZone, 2012. [Online]. Available: http://www.digikey.com/us/en/techzone/wireless/resources/articles/security-issues-with-wi-fi-bluetooth-zigbee.html. Accessed on November 2, 2016.

[4] Steven M., Data Security in European Healthcare Information Systems. Doctoral Dissertation, University of Plymouth, Plymouth, UK, June 1995.Available: http://pearl.plymouth.ac.uk/handle/10026.1/411.Accessed on November 2, 2016.

[5] Furnell S., Gaunt P., Pangalos G., Sanders P., and Warren M., "A Generic Methodology for Health Care Data Security," *Informatics for Health and Social Care*, Vol. 19, No. 3, pp. 229–245, 1994.

[6] Sanders P. and Furnell S., "Data Security in Medical Information Systems Using a Generic Model," *Eleventh International Congress of the European Federation for Medical Informatics (MIE'1993),* Jerusalem, Israel, April 18–22, 1993.

[7] Georgios M., Dimitrios L., and Nikos K., Security in Smart Home Environment. Wireless Technologies for Ambient Assisted Living and Healthcare – Systems and Applications (Book Chapter), IGI Global, 2011, pp. 170–191.

[8] Marti R., Delgado J., and Perramon X., "Security Specification and Implementation for Mobile e-Health Services," *IEEE International Conference on e-Technology, e-Commerce, and e-Service (EEE'2004),* Taipei, Taiwan, March 28–31, 2004, pp. 241–248.

[9] Guoyou H., Requirements for Security in Home Environments. *Seminar on Internetworking,* Helsinki University of Technology, spring 2002.

[10] William S., Cryptography and Network Security – Principles and Practice. Fifth Edition, Prentice Hall, 2011.

[11] Olawumi O., Haataja K., Asikainen M., Vidgren N., and Toivanen P., "Three Practical Attacks Against ZigBee Security – Attack Scenario Definition, Practical Experiment, Countermeasures, and Lessons Learned,"*14th IEEE International Conference on Hybrid Intelligent Systems (HIS'2014),* Kuwait, December 14–16, 2014.

[12] William S., Network Security Essentials – Applications and Standards. Fourth Edition, Prentice Hall, 2011.

[13] ABC News, 'Smart Homes' Convenient But Are They Safe? ABC News Internet Ventures, August 2, 2013. [Online]. Available: http://abcnews.go.com/blogs/lifestyle/2013/08/smart-homes-convenient-but-are-they-safe. Accessed on November 2, 2016.

[14] Kashmir H., when 'Smart Homes' Get Hacked: I Hunted a Complete Stranger's House via the Internet. Forbes, July 26, 2013. [Online]. Available:http://www.forbes.com/sites/kashmirhill/2013/07/26/smart-homes-hack. Accessed on November 2, 2016.

[15] Sarah G., Computer Hackers Can Now Hijack Toilets – 'Smart Toilet' Users in Japan Could Become Victim to Bluetooth Bidet Attacks and Stealthy Seat Closing. Associated Newspapers Ltd, August 5, 2013. [Online]. Available: http://www.dailymail.co.uk/sciencetech/article-2384826/Satis-smart-toilets-Japan-hacked-hijacked-remotely.html. Accessed on November 2, 2016.

[16] Heather K., 'Smart Homes' Are Vulnerable, Say Hackers. CNN, August 2, 2013. [Online]. Available: http://edition.cnn.com/2013/08/02/tech/innovation/hackable-homes. Accessed on November 2, 2016.

[17] ABC News, Smart Homes Are Convenient But May be Vulnerable to Hack-Ins. ABC News Internet Ventures, August 1, 2013. [Online]. Available: http://abcnews.go.com/WNT/video/smart-homes-convienient-vulnerable-hack-ins-19846474. Accessed on November 2, 2016.

[18] ABC News, 'Smart Homes' Could be Vulnerable to Hacking. ABC News Internet Ventures, August 2, 2013. [Online]. Available: http://abcnews.go.com/GMA/video/smart-homes-vulnerable-hacking-19849549. Accessed on November 2, 2016.

[19] Pierluigi P., Risks and Cyber Threats to the Healthcare Industry. InfoSec Institute, September 16, 2014. [Online]. Available: http://resources.infosecinstitute.com/risks-cyber-threats-healthcare-industry. Accessed on November 2, 2016.

[20] Hautala L., Internet-connected homes open the door to hackers. Cnet, December 28, 2015. [Online]. Available: https://www.cnet.com/news/internet-connected-homes-open-the-door-to-hackers/. Accessed on November 6, 2016.

[21] Moore N. C. Hacking into homes: 'Smart home' security flaws found in popular system. [Online]. Available: http://ns.umich.edu/new/multimedia/videos/23748-hacking-into-homes-smart-home-security-flaws-found-in-popular-system. Accessed on November 6, 2016.

[22] Lunkeit A., Voss T., and Pohl H., "Threat Modelling Smart Metering Gateways," *European Conference on Smart Objects, Systems, and Technologies (SmartSysTech'2013),* June 11–12, 2013, pp. 1–5.

[23] Swiderski F. and Snyder W., Threat Modelling. First Edition, Microsoft Press, 2004.

[24] Beckers K., Stephan F., Heisel M., and Suppan S., "Threat Analysis Methodology for Smart Home Scenarios,"*2nd Open EIT ICT Labs Workshop on Smart Grid Security (SmartGridSec'2014),* Munich, Germany, February 26–28, 2014.

[25] Microsoft, The STRIDE Threat Model. Microsoft, 2005. [Online]. Available: http://msdn.microsoft.com/en-us/library/ee823878(v=CS.20).aspx. Accessed on November 2, 2016.

[26] Leblanc D., DREADful. Microsoft, August 14, 2007. [Online]. Available: http://blogs.msdn.com/b/david_leblanc/archive/2007/08/13/dreadful.aspx. Accessed on November 2, 2016.

[27] Zhang, Yongguang, and Wenke L. "Intrusion detection in wireless ad-hoc networks." *Proceedings of the 6th annual international conference on Mobile computing and networking*. ACM, 2000.

[28] Janakiraman, Ramaprabhu, Marcel W., and Qi Z. "Indra: A peer-to-peer approach to network intrusion detection and prevention." *Enabling Technologies: Infrastructure for Collaborative Enterprises, 2003. WET ICE 2003. Proceedings. Twelfth IEEE International Workshops on*. IEEE, 2003.

[29] Zhang, X., Chengzhong L, and Wenbin Z. "Intrusion prevention system design." *Computer and Information Technology, 2004. CIT'04. The Fourth International Conference on*. IEEE, 2004.

[30] Zhang, Yongguang, Wenke L., and Yi-An H. "Intrusion detection techniques for mobile wireless networks." *Wireless Networks* 9.5 (2003): 545-556.

[31] Da S., Ana P. R., et al. "Decentralized intrusion detection in wireless sensor networks." *Proceedings of the 1st ACM international workshop on Quality of service & security in wireless and mobile networks*. ACM, 2005.

[32] Hassinen M. "Non-Repudiation and Smart Cards," *Proceedings of Miniconfrence,* University of Eastern Finland, Kuopio, November 11, 2011, pp. 77–86.

[33] Kaarna A. and Toivanen P., "Digital Watermarking of Spectral Images in PCA/Wavelet-Transform Domain," *IEEE International Geoscience and Remote Sensing Symposium,* Toulouse, France, July 21–25, 2003, Vol. 6, pp. 3564–3567.

[34] Kaarna A., Toivanen P., and Mikkonen K., "Watermarking Spectral Images Through the PCA Transform," *IS&T Image Processing, Image Quality, and Image Capture Systems Conference,* Rochester, New York, USA, May 13, 2003, Vol. 6, pp. 220–225.

[35] Podilchuk C. and Delp E., "Digital Watermarking – Algorithms and Applications," *IEEE Signal Processing Magazine,* Vol. 8, No. 4, pp. 33–46, July 2001.

[36] Artz D., "Digital Steganography – Hiding Data Within Data," *IEEE Internet Computing,* Vol. 5, No. 3, pp. 75–80, May/June 2001.

[37] Satish K., Jayakar T., Tobin C., Madhavi K., and Murali K., "Chaos Based Spread Spectrum Image Steganography," *IEEE Transactions on Consumer Electronics,* Vol. 50, No. 2, pp. 587–590, May 2004.

[38] Mokowitz I., Longdon G., and Chang L., "A New Paradigm Hidden in Steganography," *ACM New Security Paradigms Workshop,* Ballycotton, County Cork, Ireland, September 2000, pp. 41–50.

Information about the authors:

Olayemi Olawumi: Mr. Olayemi Olawumi is currently a PhD student at the School of Computing, University of Eastern Finland; he received his M.Sc in Computer Science in 2012 at the University of Eastern Finland. His primary research interests include: Computer Networks & Security, Wireless Security, Smart Homes & Computational Intelligence.

Antti Väänänen: Mr. Antti Väänänen received his M.Sc. degree in Information Technology at University of Eastern Finland. He is also a PhD student at University of Eastern Finland. He founded SenSoftia Oy with 2 partners in 2014 and since then he has been the CEO of SenSoftia Oy. He is also a partner & founder in Dikaios Oy and in Finnish Lean Solutions Oy. He has previously worked in a large ICT company (GE Healthcare) for 10 years in various positions in Hospital Information Systems design and development.

Keijo Haataja: Dr. Keijo Haataja is currently a senior researcher at the School of Computing, University of Eastern Finland. He received his Ph.D. Computer Science in 2009 from the University of Eastern Finland and his Ph.Lic. in 2007. His primary research interests include wireless communications, wireless security, mobile systems, sensor networks, data communications, computational intelligence, and intelligent autonomous robots.

Pekka Toivanen: Prof. Pekka Toivanen is a full professor in computational intelligence at the University of Eastern Finland since 2007. He received his D.Sc. (Tech.) degree in 1996 at Lappeenranta University of Technology and his M.Sc. (Tech.) degree at Helsinki University of Technology in 1989.His areas of research interest are computational intelligence, image processing, machine vision, and the compression of spectral images.

Manuscript received on 09 November 2016