Scientific Research Publishing

Advances in Internet of Things, 2023, 13, 1-11
https://www.scirp.org/journal/ait
ISSN Online: 2161-6825
ISSN Print: 2161-6817

Internet of Things for Digital Forensics Application in Saudi Arabia

Faihan B. Bindrwish[1], Amer Nizar Abu Ali[1], Wed H. Ghabban[2], Alaaldin Alrowwad[3], Najmah Adel Fallatah[1], Omair Ameerbakhsh[1], Ibrahim M. Alfadli[1]

[1]Information System Department, College of Computer Science and Engineering, Taibah University, Madina, Saudi Arabia
[2]Applied College, University of Tabuk, Tabuk, Saudi Arabia
[3]Department of Business School, The University of Jordan, Aqaba Branch, Aqaba, Jordan
Email: Nfallatah@taibahu.edu.sa

How to cite this paper: Bindrwish, F.B., Ali, A.N.A., Ghabban, W.H., Alrowwad, A., Fallatah, N.A., Ameerbakhsh, O. and Alfadli, I.M. (2023) Internet of Things for Digital Forensics Application in Saudi Arabia. *Advances in Internet of Things*, **13**, 1-11.
https://doi.org/10.4236/ait.2023.131001

Received: October 18, 2022
Accepted: January 1, 2023
Published: January 4, 2023

Abstract

Despite the extensive empirical literature relating to the Internet of Things (IoT), surprisingly few attempts have sought to establish the ways in which digital forensics can be applied to undertake detailed examinations regarding IoT frameworks. The existing digital forensic applications have effectively held back efforts to align the IoT with digital forensic strategies. This is because the forensic applications are ill-suited to the highly complex IoT frameworks and would, therefore, struggle to amass, analyze and test the necessary evidence that would be required by a court. As such, there is a need to develop a suitable forensic framework to facilitate forensic investigations in IoT settings. Nor has considerable progress been made in terms of collecting and saving network and server logs from IoT settings to enable examinations. Consequently, this study sets out to develop and test the FB system which is a lightweight forensic framework capable of improving the scope of investigations in IoT environments. The FB system can organize the management of various IoT devices found in a smart apartment, all of which is controlled by the owner's smart watch. This will help to perform useful functions, automate the decision-making process, and ensure that the system remains secure. A Java app is utilized to simulate the FB system, learning the user's requirements and security expectations when installed and employing the MySQL server as a means of logging the communications of the various IoT devices.

Keywords

Smart Home, Internet of Things, Digital Forensic, FB Framework

1. Introduction

Technology is most influential when it seamlessly integrates itself into people's

everyday lives [1]. Since the latter-half of the twentieth century, people's lives have been transformed in terms of how they work, how companies function and how people enjoy their free time. Much of this is attributable to advances in information technology. The next iteration in this process is the IoT which is rapidly becoming incorporated into various aspects of people's lives, work and the wider society. Clearly, the IoT is a very recent innovation but the possibility of machines communicating with each other was first discussed during the first half of the nineteenth century and when the telephone was invented during the 1830s, this helped to demonstrate that machines could indeed offer a means of direct communication [2]. Among the first applications of the IoT was when a dispenser of Coca-Cola was sited on campus at the Carnegie Mellon University. Connecting this device to the Internet enabled the students to remotely confirm that there was a cold beverage available to dispense prior to placing an order [2].

IoT comprises two elements: the Internet and various other "things". The Internet is a network of computers spanning the globe, enabling a means of communication and access to a wealth of data and information. Networks connect to each other by means of standard Internet protocol (IP), offering services to people irrespective of the country they are in. In effect, the Internet connects the separate networks of companies, governments, educational institutions and private parties. The scope of some of these networks is local whereas other are international but all are connected using a range of electronic, optical and wireless networking technology [3].

Meanwhile, the "things" include people and objects that exist around the globe. Among the objects are electronic and technical devices as well as items that are not conventionally computerized including clothing, furnishings, and food among other items [4]. Numerous definitions have been suggested by the likes of businessmen, academics and technologists but these definitions tend to be quite specifically focused on their respective fields of interest. For instance, Sivaraman *et al.* in their study of smart home security define the IoT as a series of Internet-connected devices such as smart homes that enable people to monitor from remote locations [5]. Examples include using a smart phone whilst away from the home to turn lights on and off or control alarm systems. The IoT is defined as interconnected devices that are able to observe developments in their surroundings such as utilities and vehicles [5].

Whilst the IoT is rapidly becoming indispensable to those with access to the technology, it also presents a series of risks and particularly for forensic investigators. Forensic analysis involving conventional computer technology is grounded on well-established processes and the intention is to ensure that the integrity of the digital evidence is carefully preserved. Numerous models have been developed which specify the approach that forensic investigators should take but no such methods have yet been agreed for the diverse and evolving setting of the IoT [5].

The objectives of the current study are as follows: Developing the FB Framework which will serve as a digital forensic investigation model capable of man-

aging a range of IoT-enabled objects as well as a range of sensors in the setting of a smart home, thereby enhancing security and making life both easier and more enjoyable for the inhabitants, Utilizing the FB Framework to amass all relevant forensic evidence that may be of use when undertaking a forensic investigation and Operating the FB Framework as part of a simulation exercise to prove its capabilities and reliability when performing its range of tasks.

2. Literature Review

Zawoad and Hassan considered the possibility that the pace at which IoT devices are being developed and adopted has created an environment that is ripe for cyberattacks [6]. For this reason, they recommend that further research is required into the known issues with forensic investigations of IoT scenes to achieve a better understanding of the nature of the problem. Meanwhile, Perumal *et al.* developed a model for use by digital forensic investigators offering a series of organised levels to assist with analysing digital evidence such as planning, authorisation and the chain of custody [7].

Zawoad and Hassan's [6] research served as a springboard for forensic investigations in IoT settings and the proposal was undertaken at a high level. In addition, while Perumal *et al.* [7] demonstrate a thorough grasp of the topic and suggest an organized process, their research was not truly appropriate for the realm of digital forensics. Kebande and Ray considered the inadequacies of existing digital forensics methods for use when conducting digital forensic investigations in IoT settings [8]. In particular, Kebande and Ray note that the currently available digital forensic techniques and methods are unable to handle the heterogeneous and decentralized aspects of IoT settings. Kebande and Ray also state that work is required to agree standard frameworks for the application of digital forensics in IoT settings so as to help ensure the effectiveness of investigations [8]. Towards this goal, Kebande and Ray develop a generic framework for conducting digital forensic investigations involving the IoT to help improve the accuracy of the process. This framework incorporates security features, incident processes, rules when investigating and international information technology standards. They claim that by adopting such a comprehensive approach, this framework enables digital forensic investigations to be conducted in IoT settings in an effective manner [8]. However, Nieto *et al.* argue that while Kebande and Ray's framework offers a degree of certainty regarding the development of IoT infrastructure, it fails to adequately incorporate ethics and privacy [9].

There is also the distinct possibility that a user could refuse to cooperate with the investigation process. Recognizing this possibility, Nieto *et al.* develop the PRoFIT model to assist with forensic digital investigations in IoT settings [9]. As such, the model incorporates the potential for users to demand that their privacy be respected, noting that collaboration in forensic digital investigations should be encouraged. Similarly, Willers *et al.* assert that while the merits of automated smart home systems are apparent, surprisingly little research has been conducted to establish the most effective approach when identifying and collecting

digital evidence from such settings [10]. Consequently, Willers *et al.* advocate those future researchers should examine the forensic acquisition of data and the best ways in which to analyze home automation systems.

Willers *et al.* suggest a forensic investigation model for use in smart homes based on three distinct scenarios to gauge how useful the framework is [10]. This entails collecting data on site, employing a third party to preserve the necessary evidence, appreciating the peculiarities of the smart home setting, and verifying the degree of security [10]. Cyber attackers are currently able to exploit most of the available auto-unlocking methods to gain access to domestic systems without permission. Ho *et al.* suggest a way in which unlocking attacks can be effectively prevented by ensuring that the user is in the vicinity of the door when it is allowed to open [11]. One way in which this could be achieved is for the smart lock to utilize wireless methods to confirm that the wearable device and smart key are both in the vicinity. Ho *et al.*'s method requires the user to use touch to indicate the door should be opened by means of body-area networking (BAN) that can generate a touch-limited channel [11]. As the user approaches the smart lock, a secure Wi-Fi signal is transmitted between the wearable device and the smart lock. As a result, when the user touches the door, this is detected by the smart lock and the BAN channel is used to convey an intent signal to the wearable device. Upon receiving the signal, the wearable device transmits a secure wireless signal that the smart lock should be unlocked. Upon receiving the instruction to unlock from the wearable device, the smart lock verifies that it has recently issued an intent signal and only then is the door allowed to open [11].

Tian *et al.* conducted research in which it was asserted that those using IoT apps are confronted by critical issues that are not limited to the possibility of deceit [12]. Tian *et al.* believed that most smart apps make too many requests for permission from users, and this is not necessary. It is the descriptions that determine the number of requests that will be made [12]; e.g. an app may be responsible for managing the heating in a room but it may also request permission to control the lighting. According to Tian *et al.*, this constitutes a serious overreach and the users of these apps do not appreciate why these requests for permission are made. Responding to the identified problem, Tian *et al.* developed Smart Auth to help mitigate the adverse effects of overreach [12]. SmartAuth offers protection to users by analyzing their various IoT apps, examining in detail their source codes and activity with the results being compared to the claims made about what the apps are intended to do. It is claimed that this innovation will not only benefit current users of IoT platforms but also assist users in future. It has the ability to efficiently apply highly complex twelve context-sensitive policies and outperforms the existing means of policy enforcement. Permissions can only be granted by the human user and, therefore, this innovation helps users to understand precisely what IoT apps do, thereby making them better able to understand whether granting permission is in their own interest [12]. Tian *et al.* claim that SmartAuth amasses all relevant data from the IoT apps and via a user-friendly interface conveys information in an understandable way so that the

user is made aware of what granting permission will mean in practical terms.

3. Proposal System

3.1. FB Framework Overview

The intention is to devise a system whereby each of the agencies depicted in Figure 1 are incorporated into the automatic FB Framework smart system. At the heart of the FB Framework in a central unit that serves a s a hub. Java software is utilized in the FB Framework so that the system is able to communicate with the user's smart watch, thereby enabling all of the features of the smart home to be controlled as desired.

Once operational, the FB Framework will continuously monitor any security issues (e.g. detecting water or gas leaks) whilst also enabling the user to select from a range of services provided by the system via their smart watch. It would have been possible to control the system using a smart phone or a dedicated tablet computer but for the purpose of the current study, the decision was taken to utilise a smart watch. In addition, any users of the system who may be untrustworthy are monitored by cameras (power and memory limitations permitting). Importantly, all data passing between the smart watch, the IoT devices and the server are stored because this could be useful to criminal profilers at a later date.

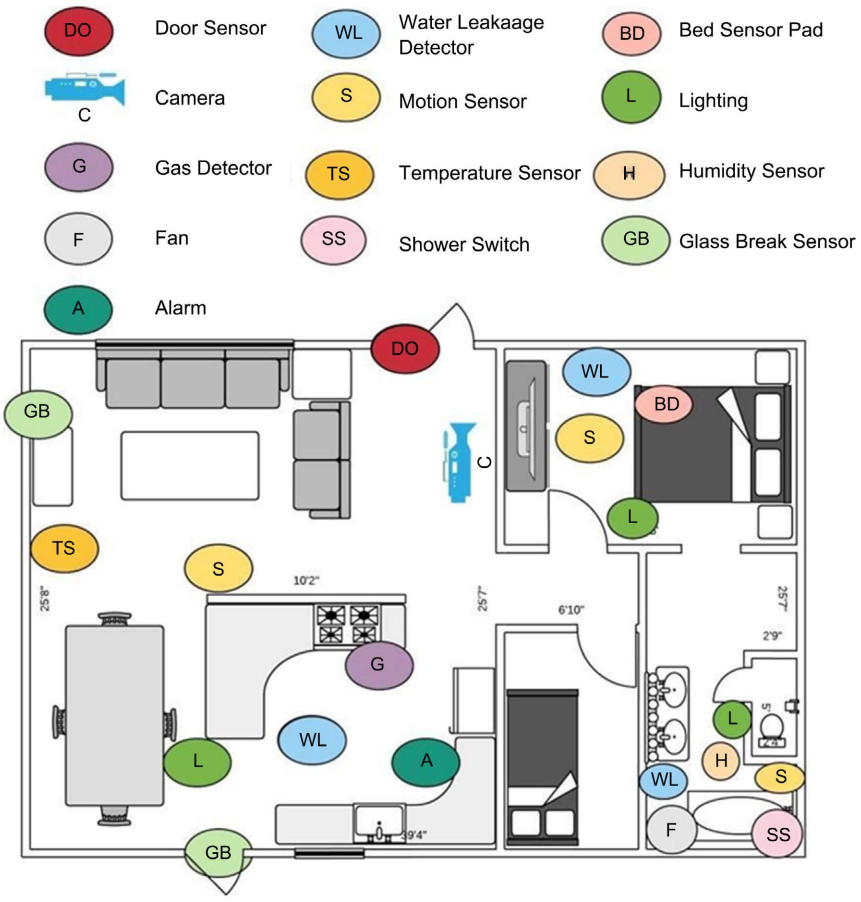

Figure 1. Distribution of the FB Framework technology throughout the apartment.

The system is also able to monitor the health of those suffering with cardiac problems and epilepsy. The ability of an automated system to continuously monitor vulnerable people and contact the emergency services could save lives. Similarly, action will be taken if no signal is received from the user's smart watch, even if this is just because the battery needs charging. In effect, the FB Framework offers users a simple and customizable means of managing a range of IoT devices, all of which can be controlled using a smart watch. The added security aspect is based on the ability of the user to make decisions about how IoT devices are to function with automatic action being taken in the event that the user is unable to offer a response when contacted.

3.2. Apartment Setup

The system is also able to monitor the health of those suffering with cardiac problems and epilepsy. The ability of an automated system to continuously monitor vulnerable people and contact the emergency services could save lives. Similarly, action will be taken if no signal is received from the user's smart watch, even if this is just because the battery needs charging. In effect, the FB Framework offers users a simple and customizable means of managing a range of IoT devices, all of which can be controlled using a smart watch. The added security aspect is based on the ability of the user to make decisions about how IoT devices are to function with automatic action being taken in the event that the user is unable to offer a response when contacted.

In the bedroom there are BD (bed), S (Motion), WL (water leakage) and L (lighting) sensors and controls. Located in the kitchen are the S1 (motion), G gas detection), WL (water leakage), A (alarm), GB (broken glass), and L (lighting) sensors and controls. Meanwhile, in the bathroom are the S1 (motion), F (fan), SS (shower), H (humidity) and L (lighting) sensors and controls. As such, a separate sensor is required for each of the tasks that the system offers, some of which offer security benefits whilst others offer the user greater convenience. The following section sets out the system architecture.

3.3. Architecture of the System

Figure 2 illustrates how the FB Framework comprises a convenience agent as well as a security agent, and a communication server which manages every interaction among the information and instructions received from the watch and the check cases of the additional servers. Depending on the response received, the various IoT devices are controlled by the system accordingly. Furthermore, it is demonstrated that if no response is received from the user, the FB Framework will automatically take appropriate action. It is the communications server that is responsible for collecting all communications between the smart watch and the various devices as well as the data generated by the sensors positioned around the apartment. These communications and data are encrypted and stored on a remote server so that they are safe and secure. Network communication

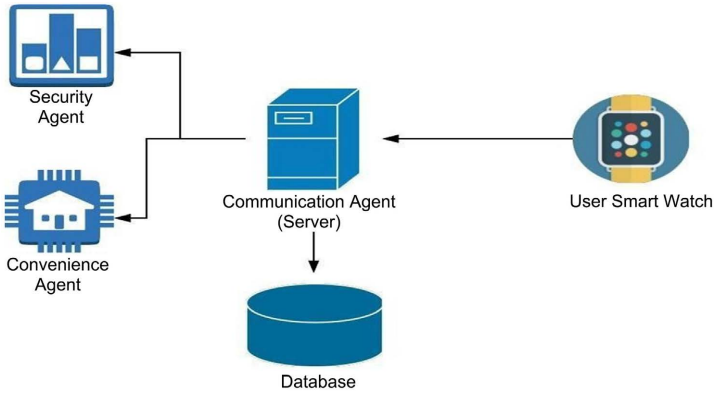

Figure 2. Architecture of the system for the FB Framework.

data remain secure by means of encryption and it is only possible to add a new IoT device to the system once the user has confirmed it is safe.

3.4. Configurations for the User

The section providing an overview of the FB Framework explained that when setting up the system, it is necessary for the user to specify their convenience and security preferences so that the system can then work on an automated basis.

The following is a list of the preferences that need to be specified when setting up the system:

- Between which hours of the day should the motion sensors trigger the lighting system to function using soft lighting, so as to avoid the user being dazzled by bright lights?
- Between which hours of the day should the FB Framework ask the user if they are ready for the coffee machine to be activated?
- Within which range of temperatures would the user like the interior of the apartment to be maintained at?
- What is the maximum humidity for the bathroom, beyond which the fan will be activated?
- How many times should the shower be turned on before the FB Framework sends the user a reminder to activate the laundry equipment?
- Once in bed, after what period of time should the FB Framework switch off the lights and television?
- After what period of time should the FB Framework send a message to alert a third party that an IoT security device has been activated.

3.5. Configurations for the User

The FB Framework acts as a hub to which information is sent from the IoT devices and smart watch and all communication is stored and tracked. It may appear unnecessary to record all of the data twice, but this approach ensures that there is a reliable flow of information between the smart watch and the sensors, thereby avoiding the possibility of system failure that could trigger false investigations. In addition, this approach helps to ensure that the data have not been

manipulated because the system verifies that the data obtained from the communication agent tallies with that received by the smart watch. As such, the communication agent stores the relevant data such as the event date and time, the name of the sensor, the user's response, whether the response was automatic or initiated by the user, and the data flow (issued by the smart watch or the communication agent). Such information would be useful for forensic investigators in the event that it is necessary to analyse the data and gain a true and accurate appreciation of how events played out.

4. Methodology

4.1. Typical Daily Events

The following example plays out over various time intervals throughout the day.

Table 1 provides description and a summary of what may happen on a typical day when everything goes to plan. However, the table also shows that not every day of a person's life is exactly the same and they will not always do the same things at an identical time day-in, day-out. For instance, the occupant may not wish to be woken at 7am on a weekday if they have taken a holiday from work or they are ill. Similarly, at the weekend they are likely to have a different routine or no routine at all.

Table 1. Typical daily activities.

Time	Activities
7:00AM	The alarm function of the smart watch sounds to wake the user.
7:15AM	The ideal temperature is achieved, so the air conditioning system is instructed to switch off. As the user walks to the bathroom, the lights are switched on.
7:20AM	Upon entering the bathroom, motion sensors instruct the lighting system that soft lighting is required in the lounge.
8:00AM	A signal is sent to activate the coffee machine.
8:30AM	When the user leaves the apartment to go to work, all of the IoT devices are placed into hibernation/safe mode.
5:00PM	Upon returning from work, the lighting is activated and a temperature of 70˚ Fahrenheit is maintained in the lounge.
6:00PM	Upon entering the bathroom, motion sensors turn on the lights and the increase in humidity is detected by the humidity sensors, thereby triggering the fan to be activated.
6:20PM	The laundry equipment starts to wash the user's clothes and the television asks if the user wishes to watch a film.
10:00PM	Movement in the bed is detected and the air conditioning system responds by lowering the temperature to 65 ˚Fahrenheit whilst the lights are switched off.

Maybe the user is late returning from work or has other matters to attend to, thereby preventing them from taking a shower. Alternatively, the user may decide to sleep at a friend's home. Given the wide range of scenarios that could play out, it would be impractical and extremely inconvenient if the schedule had to be continually reprogrammed. If the system continued to stick rigidly to the planned schedule, this would soon prove to be annoying and of little practical use.

Recognizing these potential problems, the following section considers a number of unusual events and the need for the system to be sufficiently flexible to accommodate such changes. As such, this enables the user to change their routine. For instance, instead of the coffee machine being activated at a specific time, the user's smart watch will receive a prompt asking whether they are ready for drink to be prepared for them. Similarly, the lights and television will not be switched off at a specific time, rather the various sensors in the bed and bedroom will anticipate when the user is likely to be asleep and only then turn the lights and television off. This enables the user to continue watching television or read in bed until a later time on certain nights (e.g. at the weekend).

4.2. Unusual Evens

In order to ensure that the system is of practical use, all of the associated data are stored externally and encrypted to ensure that it remains secure.

4.3. Accidents and Intrusion

Sensors on the windows of the apartment are able to detect if the glass breaks. When a breakage is detected, the user is notified via their smart watch. If no response is received from the user, the system will inform the police after a certain period of time has elapsed (specified by the user during the process of setting up the system). If the user believes it possible that a burglary could be occurring, the call to the police would be approved. Alternatively, if the user believes the broken glass has been caused by a storm, they will instruct the system not to contact the police. However, if the user fails to respond to the message sent to their smart watch within the specified timeframe, the FB Framework system would automatically call the police to inform them of the incident.

The protocol for calling the fire brigade or police is specified by the user when setting up the FB Framework system. **Figure 3** illustrates that irrespective of whether or not contact is made with the emergency services, all relevant communication data are stored by the FB Framework system along with the dates and times of those communications between the communication agent, sensors and smart watch. As such, it is possible for forensic investigators to obtain this data along with details relating to the specific sensors involved, from where data came, where data were transferred to, how users responded to event notifications, whether the actions taken were instructed by the user or occurred automatically, and the time when the glass broke.

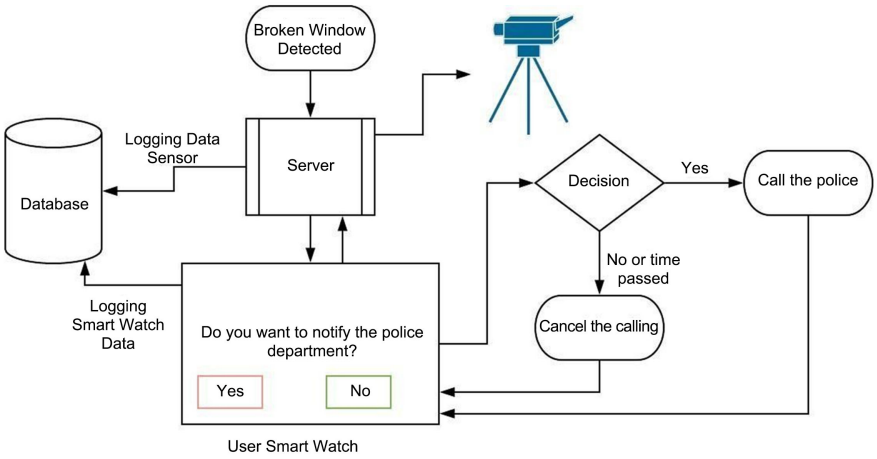

Figure 3. The breaking of glass.

Therefore, the forensic investigators will be able to identify the sensors that identified the issue and if there was any unusual movement then they will be able to view the video footage. This would be especially useful if the user was away from their home when the incident occurred. Furthermore, the process illustrated in **Figure 3** is similar to the second question regarding whether the alarm should be activated. The message on the smart watch could be altered to ask about setting off the alarm rather than calling the police.

5. Conclusions

Deploying IoT technologies in residential settings benefits the inhabitants by affording them greater usability and flexibility. The FB Framework system is advanced because it can accommodate a range of different scenarios that could play out in a smart home. Be that as it may, there remain several problems that must be overcome to enable the full benefits of the IoT to be realized. For instance, at present there is not an approved digital forensic framework for when conducting forensic investigations using IoT devices. What is more, previous research on such matters has overlooked critical elements that could enhance IoT security such as storing server and network logs ad observing what occurs within the home by viewing video footage.

Consequently, this study advocates the use of the FB Framework system which is capable of monitoring and tracking the data generated by smart homes. In addition, this system affords users considerable flexibility by enabling them to control IoT devices via their smart watch. The FB Framework has the capacity to make automatic decisions, thereby offering improved security. The current study has also simulated a Java application server coupled alongside a database server utilizing SQL to simulate the FB Framework.

Conflicts of Interest

The authors declare no conflicts of interest regarding the publication of this paper.

References

[1] Say, M. (2014) How the Internet of Everything Transforms Traditional Industries, Forbes. https://www.forbes.com/sites/groupthink/2014/07/29/how-the-internet-of-everything-transforms-traditional-industries/?sh=7ceae99d2a1c

[2] Foote, K.D. A Brief History of the Internet of Things, DATAVERSITY. http://www.dataversity.net/brief-history-internet-things/

[3] Madakam, S., Ramaswamy, R. and Tripathi, S. (2015) Internet of Things (IoT): A Literature Review. *Journal of Computer and Communications*, **3**, Article ID: 164173. https://doi.org/10.4236/jcc.2015.35021

[4] Kosmatos, E.A., Tselikas, N.D. and Boucouvalas, A.C. (2011) Integrating RFIDs and Smart Objects into a Unified Internet of Things Architecture. *Advances in Internet of Things*: *Scientific Research*, **1**, 5-12. https://doi.org/10.4236/ait.2011.11002

[5] Sivaraman, V., Gharakheili, H.H., Vishwanath, A., Boreli, R. and Mehani, O. (2015) Network-Level Security and Privacy Control for Smart-Home IoT Devices. 2015 *IEEE* 11*th International Conference on Wireless and Mobile Computing*, *Networking and Communications* (*WiMob*), Abu Dhabi, 19-21 October 2015, 163-167. https://doi.org/10.1109/WiMOB.2015.7347956

[6] Zawoad, S. and Hasan, R. (2015) FAIoT: Towards Building a Forensics Aware Eco System for the Internet of Things. 2015 *IEEE International Conference on Services Computing* (*SCC*), New York, 27 June-2 July 2015, 279-284. https://doi.org/10.1109/SCC.2015.46

[7] Perumal, N., Norwawi, M. and Raman, V. (2015) Internet of Things (IoT) Digital Forensic Investigation Model: Top-Down Forensic Approach Methodology. 2015 *Fifth International Conference on Digital Information Processing and Communications* (*ICDIPC*), Sierre, 7-9 October 2015, 19-23. https://doi.org/10.1109/ICDIPC.2015.7323000

[8] Kebande, V.R. and Ray, I. (2016) A Generic Digital Forensic Investigation Framework for Internet of Things (IoT). 2016 *IEEE* 4*th International Conference on Future Internet of Things and Cloud* (*Fi-Cloud*), Vienna, 22-24 August 2016, 356-362. https://doi.org/10.1109/FiCloud.2016.57

[9] Nieto, A., Rios, R. and Lopez, J. (2017) A Methodology for Privacy-Aware IoT-Forensics. 2017 *IEEE Trustcom/BigDataSE/ICESS*, Sydney, 1-4 August 2017, 626-633. https://doi.org/10.1109/Trustcom/BigDataSE/ICESS.2017.293

[10] Willers, O., Guajardo, J. and Seidel, H. (2016) MEMS Gyroscopes as Physical Unclonable Functions. *ACM Conference on Computer and Communications Security* (*CCS*), 591-602. https://doi.org/10.1145/2976749.2978295

[11] Ho, G., Leung, D., Mishra, P., Hosseini, A., Song, D. and Wagner, D. (2015) Smart Locks: Lessons for Securing Commodity Internet of Things Devices. *ACM ASIA Conference on Information*, *Computer and Communications Security* (*ASIA CCS*), 461-472. https://doi.org/10.1145/2897845.2897886

[12] Tian, Y., Zhang, N., Lin, Y.-H., Wang, X.F., Ur, B., Guo, X.Z. and Tague, P. (2017) SmartAuth: User-Centered Authorization for the Internet of Things. *USENIX Security* (*USENIX*), 361-378.