A Review of Prospects and Challenges of Internet of Things

Osman Yakubu
Garden City University College
P.O. Box KS12775
Kumasi

Osei Adjei
Garden City University College
P.O. Box KS12775
Kumasi

Narendra Babu C.
MS Ramaiah University of Applied Sciences
Bangalore, India

ABSTRACT
The Internet of Things (IoT) connects physical objects such as baby monitors, cars, tablet computers, fridges through the internet and they are equipped with capabilities to communicate with each other. They exchange information about themselves and their surroundings and provide improved efficiencies for the benefit of users. The future Internet is an emerging world of highly networked smart items that will be able to independently communicate with each other with little or no human intervention as the world moves into the era of smart phones, smart homes, smart offices, smart vehicles, smart classrooms, smart factories to smart everything. As the Internet of Things (IoT) continues to grow security including new attack vectors, new vulnerabilities, and perhaps most concerning of all, a vastly increased ability to use remote access to cause physical destruction becomes a major concern. In this paper we seek to explain what the Internet of Things is, its future impact, challenges and how Digital Forensics Technology can be used to get evidence to prosecute offenders in the law court.

Keywords
Internet of Things, smart, forensics, tools

1. INTRODUCTION
The Internet of Things (IoT) was originally coined as a phrase by Kevin Ashton in 1990 [2] and refers to a global, distributed network (or networks) of physical objects that are capable of sensing or acting on their environment, and able to communicate with each other, other machines or computers [9]. Data is shared by these objects which are able to communicate with humans and other devices. IOTs are used in healthcare, security, transportation and the smart Home. In the (IoT) domain, objects such as baby monitors, cars and tablet computers are being equipped with the capability to communicate with each other, and they provide improved efficiencies for those who own or use them [29]. Other objects in the IoT domain include industrial refrigerators, coffee machines, TVs, microwaves, robots, wearable objects like watches and objects which come in different sizes and have sensors embedded in them. In the smart home, IoT devices may include personal Computers, kettles, cars, fridges, smart phones and washing machines.

The application of the IoT to different sectors also gives rise to specific terms such as smart homes or smart buildings which refers to IoT concepts applied to the management and control of buildings including heating, cooling, lighting, entertainment devices, security systems and household appliances [9]. Networks of sensors and computers are used in smart cities to enhance the efficiency of traffic, public transport, street lighting or other city infrastructure. Computing is made ubiquitous by the Internet of Things, a concept initially put forward by Mark Weiser in the early 1990s [39]. Using a smart phone, tablet or desktop one can manage the temperature of a home at any time of the day from a remote location. Smart fridge, one of the devices within the IoT can prompt the owner when for instance the milk is low and needs to be replenished. When they need watering, flowers embedded with sensors can send text messages to their owners. Trucks, products and animals can be geographically located and tracked anywhere they find themselves in the world. Cars are already connected to the internet and driving behaviours can be tracked. Radio Frequency Identification Device (RFID) technologies, artificial intelligence, cloud and mobile devices are part of the areas that make up the IoT

The IoT is expected to benefit society substantially, many of these benefits are being realised today as the usage of IoT devices has resulted in increased efficiency, early detection of faults, resilience and many more. Mattern and Floerkemeier [24] posit that due to their diminishing size, constantly falling price and declining energy consumption, processors, communication modules and other electronic components are being increasingly integrated into everyday objects today. By networking these devices together people can be enabled to interact with their homes and the smart things that they carry with them in ways that have never been possible [8]. Technically, the IoT architecture is based on data communication tools primarily RFID-tagged items [38]. Radio frequency identification (RFID) has been coined as the bridge that connects the physical and virtual world [10] and by adding RFID tags to everything, the RFID technology will create an IoT [19].

Through the use of technologies such as Radio Frequency Identification (RFID), sensors and other forms of embedded computing objects that are not smart are being embedded with smartness and communication capabilities [10]. Communication with such objects will be done either directly using remote methods for instance over the internet or via 'learned' control or other smart devices [29]. In the IoT devices can be uniquely identified since they have addresses that are unique and so can be contacted via the internet. Some IOTs may have a degree of server functionality and respond readily to incoming requests and queries, whereas less sophisticated devices may simply generate and transmit their output data on certain triggers [17]. Marc Benioff, Chairman and Chief Executive Officer, Salesforce.com, USA is reported to have said that the Internet of Things is ground zero for a new phase of global transformation powered by technology innovation, generating significant economic opportunities and reshaping industries [21].

2. FUTURE IMPACT OF THE IoT
BBC News [3] reports that our homes, to give one example, could soon be tracking everything we do on a daily basis, from locking and unlocking the front door, to automatically

ordering the groceries when the fridge is empty. In the second half of 2009, a number of significant public speeches were delivered on the future of the Internet of Things. Coughlin [8] reports that on August 7, 2009, Chinese Premier Wen Jiabao made a speech in the city of Wuxi calling for the rapid development of Internet of Things technologies, on that occasion, he provided the following interesting equation: Internet + Internet of Things = Wisdom of the Earth. Wen Jiabao followed up with another speech on November 3, 2009 at the Great Hall of the People in Beijing, in which he called for breakthroughs in wireless sensor networks and the Internet of Things. In the next 10 years, the Internet of Things revolution will seriously change manufacturing, energy, agriculture, transportation and other industrial sectors of the economy which, together, account for nearly two-thirds of the global gross domestic product (GDP) [21]. In April 2008, the U.S. National Intelligence Council published a report on "Disruptive Civil Technologies – Six Technologies with Potential Impacts on U.S. Interests out to 2025", these technologies included The Internet of Things [8]. The increased interaction between humans and machines will significantly change the way people work. In the estimation of Davies [9], the IT world foresees an exponential growth in the IoT in the coming years, he quotes Gartner Group as reporting that, worldwide by 2020, the IoT will connect 26 billion devices, IoT product and service suppliers will generate incremental revenues of more than US$300 billion and the IoT will result in US$1.9 trillion in added value through sales in diverse markets. Market research firm IDC is estimating that the worldwide IoT market will grow from US$1.9 trillion in 2013 to US$7.1 trillion by 2020. A 2015 Verizon report predicts the IoT will quadruple by 2020 to an estimated 5.4 billion business-to-business (B2B) connections, concentrated particularly in the automobile and health/fitness sectors. This rapid growth is based on expectations that the IoT will bring enormous benefits to European businesses and consumers. Ericsson estimates that more than 50 billion devices will be connected by 2020 and Cisco also estimated that the IoT will offer up to $14.4trillion in revenue benefits between 2013 and 2022 [5].

In terms of timing, the Internet of Things will grow all the more rapidly if favourable policies, technological progress and business collaboration prevail. This is actually the sort of "Golden Triangle" which the European Commission is seeking to harness through its regulatory (Directives, Recommendations), research (7th Research Framework Programme) and innovation (ICT Policy Support Programme) instruments [8]. The Internet of Things which is the latest wave of technological change and in its early stages will bring unprecedented opportunities to business and society [21].

3. IoT DATA STORAGE

Data in large amounts are generated as the environment is embedded unnoticeably with information and communication systems. This collection of sensors enables applications in wide range of domains, such as healthcare, social networking, transportation, environmental monitoring, business, safety etc. [22]. Data may be stored locally by an IoT device or transferred to the cloud for storage. The data obtained from the sensors can be sent over the Internet to clouds where the data storage and data processing are performed [31]. Cloud solutions offer various benefits including convenience, large capacity, scalability, and on-demand accessibility [29]. IoT devices will primarily exchange real-time sensory and control data in small but numerous messages rather than bulk data such as file sharing or multimedia streaming. Often cloud services will handle these data from a huge number of devices, and hence need to be extremely scalable to support conceivable large-scale IoT applications [43]. In the estimation of Gubbi et al. [15] the realisation of a complete IoT vision can be achieved with an efficient, secure, scalable and market oriented computing and storage resources. Cloud computing is the most recent paradigm to emerge which promises reliable services delivered through next generation data centres that are based on virtualised storage technologies [34]. Cloud platform acts as a receiver of data from the ubiquitous sensors as a computer to analyze and interpret the data, as well as providing the user with easy to understand web based visualization [15].

4. CHALLENGES IN THE IOT

The IoT could improve global health, modernize city infrastructures, and spur global economic growth, devices have grown rapidly in number and this brings with it a number of security challenges [32]. As these devices become more relevant in people's lives, security is becoming more important. These devices, due to size and power limitations, may not support the same level of security that we would expect from more traditional Internet-connected devices, the sheer scale and number of predicted devices will create new challenges and require new approaches to security [12]. Chief among the challenges confronting the IoT are security and data privacy, which are already rising in importance given increased vulnerabilities to attacks [21]. Guaranteeing the privacy of users and their data and confidentiality of business processes is also a serious challenge confronting the IoT. Technology for preserving privacy is said to be in its infancy. Also from a legal point of view, some issues remain far from clear and need legal interpretation; examples include the impact of location on privacy regulation, and the issue of data ownership in collaborative clouds of 'things' [33] since IoT data may be stored in the cloud. Fremantle and Scott [12] listed confidentiality, integrity, availability, authentication, access control, and non-repudiation as the potential attacks that are likely to occur in IoT devices.

Other identified challenges include logical threats (e.g. Denial of Service or DoS) and physical threats (e.g. tampering and theft), viruses, surveillance [4]. Data stored on cloud locations are susceptible to Structured Query Language (SQL) injection, side channel, authentication, man-in-the-middle attacks, and insecure virtual machine deletion, etc. [29] SQL injection is a code injection technique, used to attack data-driven applications, in which malicious SQL statements are inserted into an entry field for execution [26]. In cryptography, a side-channel attack is any attack based on information gained from the physical implementation of a cryptosystem, rather than brute force or theoretical weaknesses in the algorithms. For example, timing information, power consumption, electromagnetic leaks or even sound can provide an extra source of information, which can be exploited to break the system. Authentication is a process in which the credentials provided are compared to those on file in a database of authorized users' information on a local operating system or within an authentication server. If the credentials match, the process is completed and the user is granted authorization for access. When the attacker breaks into the system by proving to the application that he is a known and valid user, the attacker gains access to whatever privileges the administrator assigned that use. In cryptography and computer security, a man-in-the-middle attack (often abbreviated to MITM, MitM, MIM, MiM or MITMA) is an attack where the attacker secretly relays and possibly alters

the communication between two parties who believe they are directly communicating with each other. One example is active eavesdropping, in which the attacker makes independent connections with the victims and relays messages between them to make them believe they are talking directly to each other over a private connection, when in fact the entire conversation is controlled by the attacker.

Ensuring security in the smart home where IoT devices are prevalent for end users is very vital. IoT devices in smart home environments are also vulnerable to attacks, and a fridge for instance can be used to spread malware and the thermometer could be remote controlled to give wrong temperatures. There has even been some discussion around the possibility of large scale disruptive botnets [10] within IoT-based networks. There is also the challenge of standards and interoperability [21], standards are important in creating markets for new technologies. If devices from different manufacturers do not use the same standards, interoperability will be more difficult. The European Commission has highlighted the need to develop technological standards to support the IoT [9]. On security, security firm Kaspersky say most people barely give a second thought that a hack of a smart-connected appliance could be dangerous and a lot more threatening than a simple PC hack [2]. They further report on how unexpectedly vulnerable connected devices can be, the stunning ease in which David Jacobi managed to hack his own smart home continues to provoke bursts of laughter and awed applause during his speeches at various infosec conferences.

Drozhzhin [11] also reports how the hack of a car wash carried out by Billy Rios of Laconicly as today's car washes have smart control systems which are connected and consequently, susceptible to a remote hack. If successful, a hacker obtains full control over all aspects of the car wash's operations. There are vast opportunities to do whatever they want, including getting services free of charge, as the owner account has access to various tools, including a payment system. They can hold a car being washed inside the car wash, after obtaining control over the gates. There is even the possibility of breaking the car wash or damaging a car by a hacker, as a car wash facility is equipped with a number of moving components and powerful engines. Connected devices' users are not bothered with security, a user would never imagine that today's microwave has a means of influencing the physical world since it is a fully equipped connected computer. At the Security Analyst Summit 2015, Vasilis Hiuorios, a security expert at Kaspersky Lab reported his hack of a police surveillance system [11]. Protection of data has been an issue ever since the first computers were linked up. With the commercialization of the Internet, security concerns expanded to cover personal privacy, financial transactions, and the threat of cyber theft. In IoT, security is inseparable from safety, whether accidental or malicious, interference with the controls of a pacemaker, a car, or a nuclear reactor poses a threat to human life [40]. There is currently no agreement on how to implement security in IoT devices, data confidentiality has always been and remains a serious concern. In the Opening Remarks of FTC Chairwoman, Edith Ramirez on 'Privacy and the IoT: Navigating Policy Issues' at the International Consumer Electronics Show in Las Vegas, Nevada in January 2015, she focused on three key challenges that, in her view, the IoT poses to consumer privacy:

a) ubiquitous data collection

b) the potential for unexpected use of consumer data that could have adverse consequences and

c) heightened security risks.

She points out further that these risks to privacy and security undermine consumer trust and that trust is as important to the widespread consumer adoption of new IoT products and services as a network connection is to the functionality of an IoT device [32]. Risk to privacy is created by connected devices for health services which are collecting, transmitting and sharing large amounts of highly personal data.

In a white paper entitled "The Internet of Things Poses Cyber security Risk," Veracode researchers analyzed the security of so-called "always-on consumer IoT devices". These are Internet-enabled devices that have a significant capability to interact with the physical environment around them (e.g., hardware sensors or peer devices). Their findings were alarming, to say the least as Consumers are constantly exposed to cyber-attacks and physical intrusions due to the use of a wide range of available IoT devices, such as remote-controlled garage doors and central control devices for home automation sensors. And because these devices are naturally insecure (and their users are often unaware of any impending threats), they're easy prey for hackers. Already, broad-reaching hacks of connected devices have been recorded and will continue to happen if manufacturers do not bolster their security efforts now. In this light, Veracode's research team examined six Internet-connected consumer devices and found worrying results. They investigated a selection of always-on consumer IoT devices to understand the security posture of each product. They found that product manufacturers weren't focused enough on security and privacy, as a design priority, putting consumers at risk of an attack or physical intrusion. Their team performed a set of uniform tests across all devices and organized the findings into four different domains: user-facing cloud services, back-end cloud services, mobile application interface, and device debugging interfaces. The results showed that all but one device exhibited vulnerabilities across most categories [37]. Recognising the risks of the IoT especially the vastly increased ability to use remote access to cause physical destruction, the Executive Office of the President of the United States of America, specifically the National Security Council, tasked the President's National Security Telecommunications Advisory Committee (NSTAC) to examine the cyber security implications of the IoT within the context of national security and emergency preparedness (NS/EP). The NSTAC found that IoT adoption will increase in both speed and scope, and that it will impact virtually all sectors of our society. The Nation's challenge is ensuring that the IoT's adoption does not create undue risk. Additionally, the NSTAC determined that there is a small and rapidly closing window to ensure that IoT is adopted in a way that maximizes security and minimizes risk. If the country fails to do so, it will be coping with the consequences for generations [36].

Other threats could include Deadly Wifi Pacemaker Hack which was demonstrated by US researchers from the Medical Device Security Center which shows that with the right kit and a little know-how it is possible to hack into a pacemaker and take control. This is possible because many pacemakers contain a radio designed to allow reprogramming of the heart-control devices the radio's signal is unencrypted, allowing a malicious attacker to turn off the pacemaker completely or deliver a shock to the heart [16]. Security researcher McAfee's Barnaby Jack has also devised an attack that hijacks nearby insulin pumps, enabling him to surreptitiously deliver fatal doses to diabetic patients who rely on them [14]. The New York Times reports that with a modest amount of

expertise, computer hackers could gain remote access to someone's car just as they do to people's personal computers and take over the vehicle's basic functions, including control of its engine, according to a report by computer scientists.

from the University of California, San Diego and the University of Washington [23]. The FBI said in a cyber-

5. SOLVING SECURITY CHALLENGES IN THE IOT

The Internet of Things offers greater efficiency and opens up business prospects that entrepreneurs can take advantage of, however the growing number of security concerns have to be dealt with. These concerns include logical threats (e.g. Denial of Service or DoS) and physical threats (e.g. tampering and theft), viruses, surveillance. When the data is stored on cloud locations, it is vulnerable to Structured Query Language (SQL) injection, side channel, authentication, man-in-the-middle attacks, and insecure virtual machine deletion. In overcoming these security challenges computer forensic technology is used to identify persons who commit these security breaches for prosecution in the law court. Forensic computing is the process of identifying, preserving, analysing and presenting digital evidence in a manner that is legally acceptable in a court of law [25]. With the IoT, a key addition would be crimes perpetrated by and originating solely from technology [29].

According to McKemmish [12] computer forensics encompasses four key elements;

a) The first step in the forensic process is the identification of digital evidence, knowing what evidence is present, where it is stored and how it is stored is vital to determining which processes are to be employed to facilitate its recovery.

b) The preservation of digital evidence is very important in the forensic process, there is the likelihood of digital evidence being subjected to thorough judicial scrutiny to make sure it is admissible. There are circumstances where changes to data are unavoidable, the change must be minimal and when the change is unavoidable, the nature and reason for the change should be explained.

c) The analysis of digital evidence—the extraction, processing and interpretation of digital data—is generally regarded as the main element of forensic computing. Once extracted, digital evidence usually requires processing before it can be read by people.

d) The presentation of digital evidence involves the actual presentation in a court of law. This includes the manner of presentation, the expertise and qualifications of the presenter and the credibility of the processes employed to produce the evidence being tendered.

Well trained and experienced investigators use open source and proprietary tools such as Encase, Forensic ToolKit (FTK), Paraben forensic tools, The Forensic Recovery of Evidence Device (FRED), WiebeTech Forensic Field Kit and Logicube to carry out digital forensic investigations. To ensure that evidence obtained from these investigations is accepted in the law court, widely accepted methodologies are employed. Among the existing methodologies are the End to End Digital Investigation (2003), Extended Model of Cybercrime Investigation (2004), Framework for a Digital Forensic Investigation(2006), Common Process Model for Incident and Computer Forensics (2007) [41]. Selecting the wrong procedures will result in the rejection of evidence presenting

intelligence bulletin that series of hacks perpetrated against so-called "smart meter" installations over the past several years may have cost a single U.S. electric utility hundreds of millions of dollars annually and these attacks are set to spread [20].

in court by forensic investigators so forensic investigation must be done properly since the outcome depends on the procedures used in the investigations. Guidelines such as the Association of Chief Police Officers (ACPO) guidelines [1] are widely recognised and properly applied during investigations in addition to accepted and recognised methodologies. .

6. FORENSICS IN THE IOT

According to Oriwoh et al. [29], various major areas like Cloud, virtualisation, mobile devices, fixed computing, sensor and RFID technologies, and artificial intelligence make up the IoT, Forensics in the IoT will therefore include forensics in all these areas and more. In a typical DF, evidence is extracted from personal computers, cell phones, tablets, printers, softwares, websites, PDAs, iPods, e-mail, social networks, visited Web sites and instant messaging. In IoT-related investigations, these equipments will still be a source of evidence. Industries critical to national security and infrastructure have embraced IoT on a much more impactful scale, in the United Kingdom there is a modern flood defence systems that uses ocean sensors and satellites to collect information and communicate with each other, to offer prompt, automated early warnings and responses [7]. Someone would be required to answer what went wrong, when and how should the warning system be tampered with and it fails. A digital forensic investigator could be tasked to investigate the failure. Cloud forensics will play a key role in the IoT forensics sphere especially since the data generated from IoT are already being, or will increasingly be stored, on cloud locations [18]. The same investigative workflows and processes that have evolved to deal with big data will be increasingly applicable in the age of IoT. Investigators must be prepared to accept digital data from unfamiliar and unlikely sources as the IoT will introduce more devices resulting in gathering more data and a variety of evidence types in to every case. The same investigative workflows and processes that have evolved to deal with big data will be increasingly applicable in the age of IoT (Cassidy, 2014).

7. CHALLENGES IN IOT FORENSICS

IoT data are increasingly being stored in the cloud and according to Induruwa [18] there are many reasons that can significantly hinder the ability to conduct forensic investigations in the cloud, including the reliance on third parties to provide computing solutions. Other difficulties relate to procedural deficiencies and absence of clear contractual agreements, especially when cross border investigations have to be conducted. Forensic investigation in the IoT will suffer threats and challenges similar to forensic investigation in the cloud. Cloud forensics is made difficult by the absence of agreements between parties in the cloud which can allow for investigations within and between customer cloud-based services [29]. The identification and preservation of evidence in digital forensic investigations in emerging environments has always presented a challenge (Taylor et al. 2010). In some cloud computing systems, storage and processing of data takes place in different jurisdictions, some organisations encrypt their data before it enters the cloud and this makes forensic investigation time consuming and difficult. Oriwoh et al. [29] identified preservation as a

challenge, and suggested that devices undergoing investigation should not be turned off to preserve the modified, created and accessed times of files. Hegarty et al. [17] however argue that the claim of Oriwoh et al. [29] is likely drawn from conventional digital forensic investigations, the situation is much more complex in IoT investigations, due to the limited resources available on devices, leaving the devices running at the scene of an incident will consume power, and more importantly may result in overwriting of stored data due to constrained storage capabilities. Proprietary data formats, protocols, and physical interfaces all complicate the process of evidence extraction [27].

Hegarty et al. [17] also assert that identification of a particular data is a serious challenge as this raises the question of how to carry out "search and seizure" where one does not know where the data under investigation is coming from or is being stored. They further point out that there is also a serious challenge with preservation since it is possible that data at a crime scene will be overwritten/compressed if the devices cannot interact with a cloud service provider to store their data, and they collect more data than they can store. Where data originates must be considered to demonstrate that it is trust worthy and this is seen as a serious challenge in the IoT forensics investigation. Hegarty et al. [17] further identify presentation of the findings of IoT investigations as a another challenge as data will often have undergone aggregation and processing using analytic functions that can alter the meaning and structure of the data. The granularity and semantics of evidence from the IoT will also create challenges to digital forensic investigations, granularity of the data may be reduced due to lossy compression techniques at the device level in order to preserve limited resources such as memory, battery life, network bandwidth, etc. [17].

Evidence collection in an IoT based crime scene can be expected to focus on various sources of evidence. There are different categories of devices in the IoT domain, challenges shall be created as these different devices are investigated. There is an increase in interconnected devices, about trillions of such connected devices [4], compared to the traditional DF the number of devices are not as much. There is also the issue of large volume and type of data that will be produced by the IoT, Dlamini et al. [10] anticipate a "data deluge" within the IoT domain. In a report by International Data Corporation (IDC), Gantz and Reinsel assert that the expected growth of data that will be experienced from 2005 to 2020 will be 40,000 exabytes (where an exabyte is a trillion gigabytes) [15]. A lot of time will be spent finding evidence from this large amount of data, data format in the IoT may be different from that of the traditional digital forensics, this data will have to be put in a format by investigators so that it can be understood. One difficulty for digital forensics will be how to handle developing efficient methods of collecting all the relevant evidence from an Object of Forensic Interest that has travelled between multiple networks, leaving multiple digital fingerprints in its wake [29].

Devices in the IoT can be unreliable sources of forensic evidence, any evidence stored on them has the tendency to be changed without any human input and before digital evidence is acquired from it by investigators since the devices can learn and adjust/adapt independently depending on the situation. During investigations there is sometimes a need to contain, seize and remove physical evidence from crime scenes, removing IoT-ware (e.g. fridges) may pose challenge to DF as it currently operates - although probably not so much for physical forensics which already deals with the removal of large objects from crime scenes [28]. The internet of things revolution poses a new challenge in the never-ending pursuit for best approach to investigations [7]. There is also the issue of gaining access to confidential data such as patient's data. Hospitals may not be willing to give access to forensic investigators investigating the tampering of patient's data.

8. PROPOSED APPROACH IN IOT FORENSICS

It is evident that the Internet of Things will grow exponentially in the coming years and it will be subjected to security breaches by cyber criminals. Digital evidence will have to be gathered using digital forensic techniques to enable offenders to be prosecuted. This research recognises the fact that IoT forensics is different from other forensics and so proposes methods and tools that ensure the acquisition of evidence and a reduction of time wastage in the acquisition process while ensuring that evidence produced is legally acceptable for prosecution. Evidence Acquisition should be done simultaneously with Incident Response in all affected systems and networks at the same time and in a timely manner, without any modification of evidence. Digital forensics traditionally takes a reactive approach, evidence acquisition begins with the identification of a security incident. The evidence it is likely may no longer exist or may be modified if there is a delay especially with the IoT domain. We share in Garcia [42] proposed automated forensic response guide and believe that any solution professed should be able to identify the attack as it occurs and trigger an automated incidence response. The incident should then be verified and an automated forensics collection should be triggered and then the data should be pre-analysed, finally there should be a trigger alert to the owner. A Real-time Digital forensics for Internet of Things that investigates techniques that help to detect and analyse security attacks/incidents as soon as they occur is therefore proposed

9. CONCLUSION

The Internet of Things (IoT) is growing at a very fast pace and is occurring in critical sectors like health, transportation, home, utilities amongst others. The IoT brings substantial benefits to society. IoT devices will have increased efficiency, faults can be detected as soon as they occur and there will be improved reliability. As the Internet of Things (IoT) continues to gain popularity and more connected devices come to market, it is faced with major security concern such as the hacking of connected devices. Security breaches will have to be tracked and evidence extracted, this evidence must be reliable and must withstand rigorous cross examination in the court of law. In our estimation current digital forensics models were not designed to investigate the IoT, the few models that target IoT forensics have their own challenges which even their authors have highlighted. In this Literature Review 2, a real-time digital forensics for Internet of Things that helps to detect and analyse security attacks/incidents as soon as they occur is proposed to overcome digital evidence challenges in the IoT.

10. REFERENCES

[1] ACPO (2012) ACPO Good Practice Guide for Digital Evidence,Available at: http://www.digital-detective.net/digital-forensics-documents/ACPO_Good_Practice_Guide_for_Digital_Evidence_v5.pdf (Accessed: 20th October 2015).

[2] ASHTON, K. (2009) 'That 'Internet of Things' Thing', RFiD Journal , 22 (), pp. 97–114.

[3] BBC News (2015) How the internet of things is changing the way we live, Available at:http://www.bbc.com/future/sponsored/story/20150706-how-the-internet-of-things-is-changing-the-way-we-live (Accessed: 5th October 2015).

[4] Bos, H., Ioannidis, S., Jonsson, E., Kird, E. and Kruegel, C. (2009) 'Future Threats to Future Trust', Proceedings of the First International Conference Future of Trust in Computing Springer,(), pp. pp. 49-54.

[5] Bradley, J., Barbier, J., and Handler, D., (2013) 'Embracing the Internet of Everything To Capture Your Share of $14.4 Trillion More Relevant, Valuable Connections Will Improve Innovation, Productivity, Efficiency & Customer Experience', CISCO White Paper, (), pp. [Online]. Available at:http://www.cisco.com/web/about/ac79/docs/innov/IoE_Economy.pdf(Accessed: 29th September 2015).

[6] Buyya, R., Yeo, C.S., Venugopal, S., Broberg, J. and Brandic, I. (2009) ' Cloud computing and emerging IT platforms: Vision, hype, and reality for delivering computing as the 5th utility', Future Generation Computer Systems, Elsevier, 25(6), pp. 599-616.

[7] Cassidy, A. (2014) The "Internet of Things" Revolution and Digital Forensics, Available at:http://www.nuix.com/2014/02/19/the-internet-of-things-revolution-and-digital-forensics (Accessed: 30th October 2015).

[8] Coughlin, T (2014) Digital Storage and The Internet Of Things,Available at:http://www.forbes.com/sites/tomcoughlin/2014/11/30/digital-storage-and-the-internet-of-things/ (Accessed: 25th September 2015).

[9] Davies, R (2015) 'The Internet of Things Opportunities and challenges', European Parliamentary Research Service, PE 557.012(), pp. [Online]. Available at:http://www.europarl.europa.eu/RegData/etudes/BRIE/2015/557012/EPRS_BRI(2015)557012_EN.pdf(Accessed: 15th September 2015).

[10] Dlamini, M., Eloff, M. and Eloff, J. (2009) 'Internet of things: emerging and future scenarios from an information security perspective', Southern Africa Telecommunication Networks and Applications Conference, (), pp. 6.

[11] Drozhzhin, A. (2015) Internet of Crappy Things, Available at:https://blog.kaspersky.com/internet-of-crappy-things/7667/(Accessed: 2nd October 2015).

[12] Fremantle, P., Scott, P. (2015) 'A security survey of middleware for the Internet of Things', PeerJ PrePrints 3:e1521, PeerJ PrePrints 3:e1521(), pp. [Online]. Available at:https://dx.doi.org/10.7287/peerj.preprints.1241v1 (Accessed: 21st October 2015).

[13] Friedewald, M., Vildjiounaite, E., Punie, Y. and Wright (2007) 'Privacy, identity and security in ambient intelligence: A scenario analysis', Telematics and Informatics, 24(1), pp. 15–29.

[14] Goodin, D. (2011) Insulin pump hack delivers fatal dosage over the air, Available at:http://www.theregister.co.uk/2011/10/27/fatal_insulin_pump_attack/(Accessed: 19th October 2015).

[15] Gubbi, J., Buyya, R., Marusic, S. and Palaniswami, M (2013) 'Internet of Things (IoT): A vision, architectural elements, and future directions', Future Generation Computer Systems Elsevier,29(7), pp. 1645–1660.

[16] Halperin, D., Heydt-Benjamin, T.S., Ransford, B., Clark, S.S., Defend, B., Morgan, W., Fu, K., Kohno, T. and Maisel, W.H. (2008) 'Pacemakers and Implantable Cardiac Defibrillators: Software Radio Attacks and Zero-Power Defenses', IEEE Symposium on Security and Privacy., (), pp. 129 - 142.

[17] Hegarty, R.C. , Lamb, D.J. and Attwood, A. (2014) 'Digital Evidence Challenges in the Internet of Things ', International Workshop on Digital Forensics and Incident Analysis , (), pp. 163-172.

[18] Induruwa, A. (2011) 'Hidden in the clouds: The impact on data security and forensic investigation', IEEE International Conference on Advances in ICT for Emerging Regions, (), pp. 77.

[19] Intenational Telecommunication Union (ITU), (2005) Intenational Telecommunication Union (ITU), , Available at:http://www.itu.int/osg/spu/publications/internetofthings/InternetofThings_summary.pdf(Accessed: 5th September 2015).

[20] KrebsOnSecurity (2012) FBI: Smart Meter Hacks Likely to Spread,Available at: http://krebsonsecurity.com/2012/04/fbi-smart-meter-hacks-likely-to-spread/ (Accessed: 17th October 2015).

[21] Kvochko, E., O'Halloran (2015) Industrial Internet of Things: unleashing the potential of connected products and services, Geneva: World Economic Forum.

[22] Lane, N.D., Miluzzo, E., Lu, H., Peebles, D., Choudhury, T. and Campbell, A.T. (2010) 'A survey of mobile phone sensing',Communications Magazine, IEEE , 48(9), pp. 140 - 150.

[23] Markoff, J. (2011) Researchers Show How a Car's Electronics Can Be Taken Over Remotely, Available at:http://www.nytimes.com/2011/03/10/business/10hack.html?_r=0(Accessed: 11th October 2015).

[24] Mattern, F., Floerkemeier, C. (2010) 'From the internet of computers to the internet of things', Springer-Verlag, (), pp. 242-259.

[25] McKemmish, R. (1999) 'What is Forensic Computing?', Australian Institute of Criminology, Trends and Issues in Crime and Criminal Justice, (118), pp. .

[26] Microsoft (2011) SQL Injection, Available at:https://technet.microsoft.com/en-us/library/ms161953(v=SQL.105).aspx (Accessed: 15th September 2015).

[27] Miorandi, D., Sicari, S., De Pellegrini, F., and Chlamtac, I. (2012) 'Internet of Things: Vision, Applications and Research Challenges',Elsevier Ad Hoc Networks, 10(7), pp. 1497–1516. doi:10.1016/j.adhoc.2012.02.016.

[28] Oriwoh, E., & Williams, G. (2015) ' Internet of Things: The Argument for Smart Forensics', Handbook of Research on Digital Crime, Cyberspace Security and Information Assurance, (), pp. 407-423. doi:10.4018/978-1-4666-6324-4.ch026.

[29] Oriwoh, E., Jazani, D., Epiphaniou, G. (2013) 'Internet of Things Forensics: Challenges and Approaches', Proceedings of the 9th IEEE International Conference on Collaborative Computing: Networking, Applications and

Worksharing, DOI 10.4108/icst.collaboratecom.2013.254159(), pp. .

[30] Osborne, G., and Slay, J. (2011) 'Digital Forensics Infovis: An Implementation of a Process for Visualisation of Digital Evidence',IEEE 2011 Sixth International Conference on Availability, Reliability and Security, (), pp. 196–201. doi:10.1109/ARES.2011.36.

[31] Pereira, P., P. ,Eliasson, J., Kyusakov, R., Delsing, J., Raayatinezhad, A. and Johansson, M. (2013) 'Enabling Cloud Connectivity for Mobile Internet of Things Applications',Proceedings of the 2013 IEEE Seventh International Symposium on Service-Oriented System Engineering, (), pp. 518-526.

[32] Ramirez, E. (2015) 'Opening Remarks of FTC Chairwoman Edith Ramirez, Privacy and the IoT: Navigating Policy Issues',International Consumer Electronics Show Las Vegas, Nevada, (), pp. [Online]. Available at:https://www.ftc.gov/system/files/documents/public_statements/617191/150106cesspeech.pdf(Accessed: 15th October 2015).

[33] Sen, J. (2013) 'Security and privacy issues in cloud computing',Architectures and Protocols for Secure Information Technology Infrastructures, (), pp. 1-45.

[34] Shawish, A. and Salama, M. (2014) 'Cloud Computing: Paradigms and Technologies', Inter-cooperative Collective Intelligence: Techniques and Applications, Studies in Computational Intelligence, Springer, 495(), pp. 39-67, DOI: 10.1007/978-3-642-35016-0_2,.

[35] Taylor, M., Haggerty, J., Gresty, D. and Hegarty, R. (2010) 'Digital evidence in Cloud Computing Systems', Elsevier Computer Law & Security Review, 26(3), pp. 304–308 doi:10.1016/j.clsr.2010.03.002.

[36] The President's National Security Telecommunications Advisory Committee (n.d.) 'NSTAC Report to the President on the Internet of Things', , (), pp. [Online]. Available at:http://www.dhs.gov/sites/default/files/publications/IoT%20Final%20Draft%20Report%2011-2014.pdf (Accessed: 19th October 2015).

[37] Veracode (n.d.) 'The Internet of Things: Security Research Study',Veracode White Paper , (), pp. [Online]. Available at:https://www.veracode.com/sites/default/files/Resources/Whitepapers/internet-of-things-whitepaper.pdf (Accessed: 18th October 2015).

[38] Weber, R.H. and Weber, R. (2010) Internet of Things: Legal Perspectives, Zurich: Springer.

[39] Weiser, M (1991) 'The Computer for the 21st Century', Scientific American , 265(), pp. [Online]. Available at:https://www.ics.uci.edu/~corps/phaseii/Weiser-Computer21stCentury-SciAm.pdf (Accessed: 30th September 2015).

[40] Wind River Systems, Inc. (2015) 'Security in the Internet of Things, Lessons from the Past for the Connected Future', Wind White Paper, (), pp. [Online]. Available at:http://www.windriver.com/whitepapers/security-in-the-internet-of-things/wr_security-in-the-internet-of-things.pdf (Accessed: 21st October 2015).

[41] Yusoff, Y., Ismail, R. and Hassan, Z. (2011) 'Common Phases of Computer Forensics Investigation Models', International Journal of Computer Science and Information Technology, 3(3), pp. 17-31. DOI : 10.5121/ijcsit.2011.3302 .

[42] Garcia, J. (2005) *Proactive & Reactive Proactive & Reactive Forensics Forensics*, Available at:*https://www.rediris.es/cert/doc/reuniones/af05/proactive_n_reactive_forensics.pdf*(Accessed: 9th November 2015).

[43] Kovatsch, M., Lanter, M. and Shelby, Z., 2014, October. Californium: Scalable cloud services for the internet of things with coap. In Internet of Things (IOT), 2014 International Conference on the (pp. 1-6). IEEE.