A Hardware based Model for an Asset Monitoring and Tracking System: Case of Laptops

Admire Mhlaba
Department of Information Technology
Central University of Technology, Free State
Bloemfontein, South Africa
yaddly@gmail.com

Muthoni Masinde
Department of Information Technology
Central University of Technology, Free State
Bloemfontein, South Africa
muthonimasinde@yahoo.com

***Abstract*—Corporate mobility initiatives and the anytime, anywhere information workers is on the rise. This is mostly fuelled by availability of affordable and more powerful mobile computing devices, especially laptops and tablets. One direct consequence of this is a sharp increase in laptop theft; this is partly driven by the fact that laptops are portable and easy to conceal and pocket away, they fetch a good second-hand price on the informal market and availability of easy online disposal platforms such as Gumtree, where they are sold cheaply and anonymously. Despite the fact that many solutions have been developed in an attempt to annihilate this growing calamity, their cost has left many small and medium organizations preferring to do without one. In an attempt to bridge this gap, the research reported in this paper aimed at designing a generic middleware architecture for use in a hardware-based (RFIDs, wireless sensor modes, fingerprint scanners and mobile phones) affordable laptop monitoring and tracking system. The resulting system prototype was evaluated using diverse experimental cases within a university in South Africa.**

Keywords—Laptop monitoring and tracking system; Central University of Technology, Free State (CUT); Hardware based Model; Internet of Things(IoT); Wireless Sensor Networks (WSNs); in-lining middleware

I. INTRODUCTION

An asset is something that has potential or actual value to an organization. When well managed (using asset management systems), assets can among other things lead to improved financial performance and managed risk. Asset Management Systems are important that ISO has developed a standard (ISO 55001:2014) to regulate their implementation [1]. Workers throughout the world are increasingly becoming mobile; they use mobile devices such as smartphones and tablets to do their work at the office, at home, and while travelling [2]. This is resulted to the as anytime, anywhere information workers - those who use three or more devices, working from multiple locations, and use many apps [3]. Consequently, the traditional asset management and tracking systems have to be re-designed to cater for this as well as for the bring your own device (BYOD) concept. The meantime, the availability of these devices has led to an increase in their (devices) loss through theft. The main objective of this research was to prove that a real-life application built over a generic Internet of Things (IoT) architecture that innovatively and intelligently integrates wireless sensors, radio frequency identification (RFID) tags (and readers), fingerprint readers, and mobile phones, can be used to dispel laptop theft. To achieve this, a system was developed using the heterogeneous devices mentioned above and a middleware that harnessed their unique capabilities to bring out the full potential of IoT in intelligently curbing laptop theft.

The resulting system has the ability to monitor the presence of a laptop using RFID reader that pro-actively interrogates a passive tag attached to the laptop, detect unauthorized removal of a laptop under monitoring, instantly communicate security violations via cell phones, and use Windows location sensors to track the position of a laptop using Google-maps. The system also manages administrative tasks such as laptop registration, assignment and withdrawal which used to be handled manually. Experiments conducted using the resulting system prototype proved the hypothesis outlined for this research.

Applications built around the IoT paradigm are propelled by three components which expedite pervasive computing: hardware such as wireless sensors, actuators, cell phones and Radio Frequency Identifiers (RFIDs), (middleware to aid with mediation and data analysis, and applications in form of prototypes [4]. This study delivers an IoT integration architecture implementation that is tested using a laptop monitoring and tracking system. As such, the system is limited to the following elements under each of these components: Hardware – wireless sensors, RFIDs, mobile phones and fingerprint scanners; Middleware – a connection between hardware and application; Prototype – a functioning application that ties all the different hardware technologies together.

This laptop monitoring and tracking middleware was built, based on the work by Hwang and Yoe [5]. The middleware was intended to process data efficiently, consume diverse data spawned by various interconnected devices, provide event-driven services based on data generated, and allow a proficient and flexible interface to interact with heterogeneous IoT hardware. The middleware is shown in Figure 1 below; its role was to provide a standard platform to facilitate the manner in which the system interacts with different hardware by masking their heterogeneity. The rest of the paper is structured as follows: related (to this paper) literature is presented in section II, while the methodology and results are presented in sections III and IV respectively. Section V contains the discussion and further work and references are presented in the last section of the paper.

978-1-4799-7707-9/15/$31.00 ©2015 IEEE

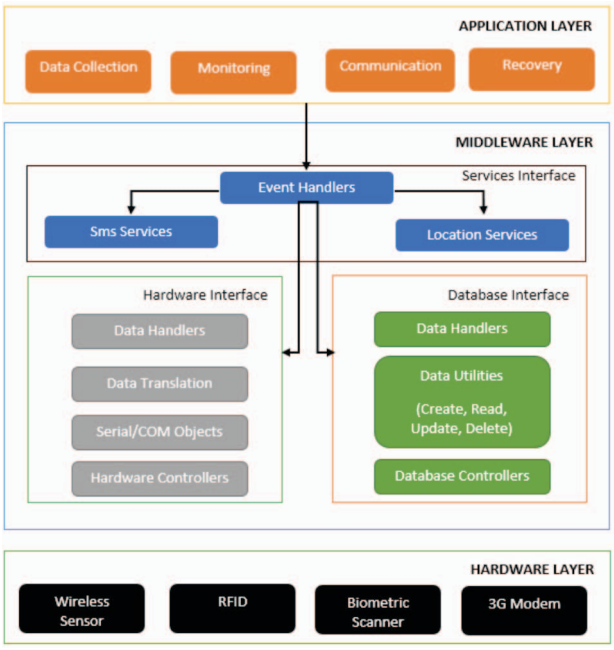

Fig 1: Proposed LMTS Middleware Architecture Adapted from [5]

II. Related Literature

A. Underling Platforms for Assest Tracking Systems

Internet of Things was developed to act as a linking platform between digital and physical worlds, with the intention to make our daily activities more manageable and affluent [6]. For this physical and digital linkage to materialize, there was a need to provide a digital identity to real-world objects. This opened up new computing avenues to be explored by researchers who are now working around the clock to deliver applications that actively participate in diverse domains with minimum human intervention, to solve real life problems. According to research commissioned by Cisco, there will be 50 billion devices connected to the internet by 2020 [7]. This explosion of connected tiny computing devices is worrisome because there are no common standards to support interoperability, privacy and integration of these heterogeneous devices.

However, the realization of this relationship between digital and real world and the development of applications is a great challenge for industry experts and individual researchers. The challenges emanate from the need to conceal the underlying complexity of the environment by shielding applications from explicit management of incompatible network protocols, miniscule heterogeneous devices, that are sometimes battery-powered and with limited computational capabilities, parallelism, data replication and network faults [8]. If poorly incorporated, it will result in applications that suffer from integration, interoperability, scalability, security and synchronized data management issues [9].

Middleware services provide a novel approach that support the implementation, maintenance, and operation of IoT-based applications through provision of a platform that shields hardware heterogeneity in sensor networks, coordinates and distributes activities to sensor nodes, performs data filtering, aggregation and storage, and significantly enhances the development of diverse applications [10]. Below is an overiew of related literature that was used in acquiring an understanding of basic and advanced concepts regarding IoT-enabling technologies, such as RFID, wireless sensors, biometric scanners and mobile phones. The last section discusses middleware architectures briefly.

1) Internet of Things

Internet of Things (IoT) is both an evolutionary and revolutionary paradigm which, since its birth in late 2008, has received considerable attention especially from researchers around the globe [7]. Internet over the years has transformed, changing from a communication medium, primarily responsible for conveying bits of data from computer to computer; and evolved into an interconnection of addressable things/objects; this has come to be known as Internet of Things (IoT) ([11]. Ashton [12] crafted the term "Internet of Things", though it had a meaning and used in a context different from what it is known today. "*IoT is an interconnection of addressable things/objects using diverse technologies such as wireless network and internet*".

2) Wireless Sensor Networks

Wireless sensor networks (WSNs) are an invaluable component of realizing IoT; they form the 'digital skin' through which to 'sense' and collect the context of the surroundings and information of the physical environment. WSNs are especially instrumental in introducing intelligence to IoT because of their ability to cooperate and collaborate in carrying out tasks. A wireless sensor network (WSN) is a digital sensory system made up of a collection of millimetre-scale, self-contained, micro-electro-mechanical devices that contain sensors, computational processing ability, wireless receiver and transmitter technology and power supply [13].

There exist a range of sensors capable of measuring physical, chemical and biological properties of objects and their environment. Prominent features of WSNs that qualify them as main candidates for 'pervasive computing' are smart integration with existing networks, multifunctional, context-awareness, self-configurability, self-sufficiency, easy of deployment [14] and indeed their support for 4As vision of the IoT paradigm [15]. Once interconnected together, sensors form a WSN. These sensors have found use in a wide range of domains including defence, science, transportation, civil engineering and security [16]. WSNs applications fall under 3 categories: detection, tracking and monitoring [15]. Examples of applications include: disaster relief operations [17], biodiversity mapping [18],; intelligent/smart buildings [19], precision agriculture [20], and (drought monitoring and prediction ([21]. WSNs also provide rich contextual information and alerting mechanisms against peculiar circumstances with continuous monitoring [22].

3) Radio Frequency Identifiers (RFIDs)

RFID is a contactless smart technology used to distantly retrieve data from or write (store) data to memory chip embedded within the integrated circuit of tags [23]. RFID is capable of remotely locating and identifying tagged objects

spontaneously using radio waves. RFIDs are microelectronic devices that comprises of a microchip and an antenna; characteristically, the microchip has data-carrying capacity of 2 kilobytes or less. RFIDs have become a common replacement of barcode technology [24]. In this case, RFID devices serve the same purpose as a barcode or a magnetic strip found at the back of debit or credit card by providing distinctive identification for tagged objects. Advancements of RFID technology instigated diverse ways to integrate the technology in a myriad applications such as healthcare, library and tracking systems.

4) Biometric Scanners

The term 'biometrics' originates from the Greek and is a derivative from the words 'bio' meaning life and 'metric' meaning standard of measurement. Biometrics therefore refers to a construct of science and technology for measuring inimitable life phenomena [25]. Biometrics in security context is a mechanism that uniquely identifies people by comparing distinctive physical characteristics; it compares distinctive physical characteristics [26]. Predominant biometric systems in place today encompass facial, iris, voice, and fingerprint recognition systems. This technology is reliable but expensive; it is one of the most applied choices of identification due to its dependability, non-intrusive interfaces, and cost-effectiveness.

5) Middleware

The feasible operation of an integrated IoT architecture that facilitates interoperability and communication between heterogeneous or homogeneous IoT objects can be realized by a lightweight software layer or a set of sub-layers interposed between the technological and the application levels known as middleware [27]. Hwang and Yoe [5] defined middleware as a software that "*supports flexible integration of hardware and application and provides services such as distributed computing environments, remote procedure calls, messaging to users, regardless of the hardware, operating system and network used*". Atzori et al. [27] pointed out that middleware has been gaining traction due to its ability to simplify development of new services and the integration of legacy technologies into new ones, while exempting programmers from knowing diverse technologies implemented at lower layers. One approach of designing middleware is called **middleware in-lining**, which is injecting the middleware code directly into the application [28].

So far, it is the WSNs and their associated technologies that play the greatest role in realizing IoT characteristics above. It is not accidental therefore that most middleware architectures in place so far are designed around WSNs. From this perspective, the middleware acts as an insulator that hides the internal workings of the system by providing homogenous and abstract environment to the highest layers (either application consumers or application developers) [29]. Tens of middleware solutions specific to WSNs have been developed; these can be categorized into three: in-network middleware that is uploaded on the nodes, server-side middleware that runs on a server, and a hybrid that combines both 1 and 2 [5]. Another categorization that is based on programming models that the architecture uses produces two broad classes: *programming support* and *programming abstractions* [9].

B. Related Applications

Object traceability is a paramount aspect that IoT is currently addressing. The proliferation of affordable wireless sensors and RFID technology triggered a great deal of interest in object tracking algorithms. Traditionally, barcode scanning was the prominent technology used in collecting data in an automatic and contactless manner [30]. Barcode scanning devices are used to perform data reading from barcodes but for this reading to work, the barcode scanner must be positioned precisely near the barcode. Compared to manual tracking processes, barcode was seen as a big break-through and a preferred faster approach to tracking objects because it was economical to install and read data from.

Despite heavy adoption worldwide, barcode technology is failing to meet up with huge business demands. RFID technology has become the leading object identification and tracking technology due to advantages such as contact-less, multi-object recognition, non-line-of-sight, long distance, large store memory, programmability and penetrability [31]. RFID has been used not only in supply chain and logistic business but in aviation industry as well. Zhang et al. [32], developed an RFID-based system to support baggage handling and baggage tracking. They suggested that baggage at the airport, may not only be assembled, as well as checked more precisely, but may also be traced across the entire world.

DHL has successfully deployed a system called DHL thermonet, which basically is an RFID-based airfreight service that allows customers to track temperatures of sensitive pharmaceuticals or biomedical products throughout the shipping process. According to DHL, if a temperature discrepancy is detected, the technology will help DHL identify the problem faster, and thus address that issue before other goods are damaged or, at least, in time to save the goods inside the carton whose tag has measured excessively warm temperatures. In addition, such an action not only saves the cost of that product, DHL explains, but also saves the customer from a potential loss in sales if goods were unable to be delivered in a satisfactory condition at the expected time [33]. Another tracking application of interest is a Child Tracking System designed by Chen [24], which accurately locates the geographical position of children playing in a park, with the intention of easily helping parents find a lost child. This system integrated three components: RFID technology, WSN and Motions detection sensors

III. METHODOLOGY

Since this research revolved around the CUT's laptop theft-deterring system, which is a real-life problem; Constructive research approach (CRA) was deemed best. In this case, a system prototype (construct) for tracking assets at CUT was developed and used to test the functionalities of the design. A novel middleware integration architecture was designed and implemented with the intention to intelligently and automatically monitor and track CUT's laptops in a flexible, secure, self-organizing and user friendly manner. Experimental design was applied in testing the practicality of a prototype system.

Constructive research implies generation of new knowledge that can be applied in solving real-world problems, using that newly acquired understanding of a phenomenon to patch up missing links in pre-existing knowledge and also entails a very close involvement and co-operation between the researcher and practitioners in a team-like manner [34]. Here, experiential learning is expected to take place. The data-gathering methods used are: document analysis of data pertaining to asset and interviews with the Head of Security and victims of laptop theft. Further, questionnaires were issued randomly to potential users of the laptop monitoring and tracking system during a case study investigation and finally, experiments were conducted during the testing and evaluation phase of the resulting system prototype.

A. CUT's Case Study

A preliminary investigation uncovered that Central University of Technology (CUT) delegated asset monitoring to security guards positioned at entry and exit points. These security personnel are not mindful of activities that take place within buildings. The institution spends a great deal of money to replace stolen laptops and data projectors. This money could have been channelled elsewhere and helped to develop the institution. Not only money is lost but valuable company and student data that may compromise the integrity of the institution, if it gets into wrong hands. Several incidents of this nature have been reported; rogue students and staff members take advantage of unavailability of security surveillance cameras or any monitoring mechanism and sneak into unattended offices, steal valuable institutional assets and get away with them.

CUT has a number of security measures in place which include the following: one, physical security personnel that are employed to ensure proper execution of access control management policies and procedures. Two, surveillance cameras, and three intrusion detection systems (IDSs) for detecting unauthorized entry into a restricted and protected regions and alerting of responsible security personnel. Others are biometrically controlled doors intended to keep unauthorized individuals out of lecture halls and laboratories and library RFID security. These security systems are disjointed; they do not talk to each other, nor do they instantaneously and intelligently send real-time security breach messages to security personnel.

B. System Prototype Design and Implementation

The middleware for this research study was implemented using a unique technique called 'middleware in-lining', which was postulated by Krakowiak [28]. Middleware in-lining entails writing middleware code in modules that are injected directly into the application. The middleware that was developed has the following characteristics: (1) uses windows operating system to hide the heterogeneity of the various hardware components, and communication protocols that are used by different parts of LMTS; (2) provides a uniform, standard, high-level interfaces to the application developers and integrators, this way the applications can easily interoperate and be refactored, ported, and recompiled; and (3) supplies a set of common services to perform various general purpose functions, in order to avoid duplicating efforts and to facilitate collaboration between top and low level-layers.

C. Hardware-based laptop tracking Model

The tracking model developed is a software-based solution that mirrors the hardware-based tracking concept depicted in Figure 2 below. This solution works as follows: (1) the laptop must be integrated with common GPS and GPRS hardware, but the GPRS module must have an irremovable SIM card. (2) The laptop serial number should not be attached on the laptop using a label, but must be printed out on a slip given to the purchasing client as a secret code known only by the buyer, along with the contact number for the embedded SIM card; and (3) if anyone steals the laptop; then the victim of the laptop theft simply sends the serial number of the laptop to the contact number given to them; (4) upon receiving the serial number, the laptop's GPRS instructs the GPS module to generate locus data and send it back to the GPRS module for transmission (this eliminates the need to have an always-on GPS, which might rapidly drain the battery of the laptop); and (5) the laptop's GPRS communicates the location of the laptop with the victim, as depicted in Figure 2. This way we can totally annihilate theft defencelessness of laptops and combat theft of assets valuable to us.

IV. RESULTS

Evaluation of the system prototype was achieved through rigorous experimental cases conducted. The aspects of the prototype that were subjected to experiments are those that help to prove or refute the success of the proposed integration architecture and middleware design in answering the research questions that instigated this study. The elements of the system that were tested include: (1) Database stress load intended to understand the ability of the system to handle scalability and its level of responsiveness to queries during operation peak times; (2) Promptness of the prototype in detecting security breach and communication of those breaches via SMS; (3) The ability to achieve laptop tracking using Google Maps and the accuracy level of windows location sensor in providing location data acquired through Wi-Fi triangulation or scrutiny of IP address data; (4) Prototype vulnerability, in terms of the detection of deceptive actions that compromise the operation of the prototype.; (5) SMS query intelligence in delivery of geographical information; (6) Fault tolerance and system flexibility; (7) Analysis of activity logs to determine prototype malfunctions; and (8) The capability of the prototype in automating functions such as Asset Registration and Asset Assignment, which are conducted manually at the problem domain.

One of the most important aspects of the system that needed to be tested was the middleware location service's ability to accurately show a laptop's location using Google maps. Figure 3 below shows the results of the experiment conducted and how the middleware is effective in generating, processing and saving asset locus data to a database. In this experiment, one subject was asked to go into any building of his choice within the campus, but without revealing the building name or building location. Here the subject was supposed to connect his/her laptop to the internet using Wi-Fi

or Ethernet cable, but was not mandated to run the LMTS, because it was configured to auto-start along with other Windows services at system start-up.

The results of the experiment are depicted in Figure 3 and the LMTS was beyond doubt able to show us the building into which the subject had gone. The building name was identified as Student Exchange house, located along Suid Street. A further experiment that was deemed paramount was to query a laptop's location using an SMS. The user simply sends a query to the system via SMS, using a specific command. The middleware then decodes the SMS query and instructs its services to trigger the respective events, which handles the user request. The results of this experiment revealed that the middleware was smart enough to translate the newly generated GPS coordinates saved on the database into a physical address. The response from the middleware comprised the following: (1) the **street name** (Suid Street); (2) **city** (Bloemfontein) in which the laptop is; and (3) the **zip code** (9301) associated with the city. This aspect of the system, proves that if hardware manufacturers can include GPRS and GPS hardware modules in laptops, laptop owners can simply query the location of the laptop from a cell phone; hence making laptop tracking easy.

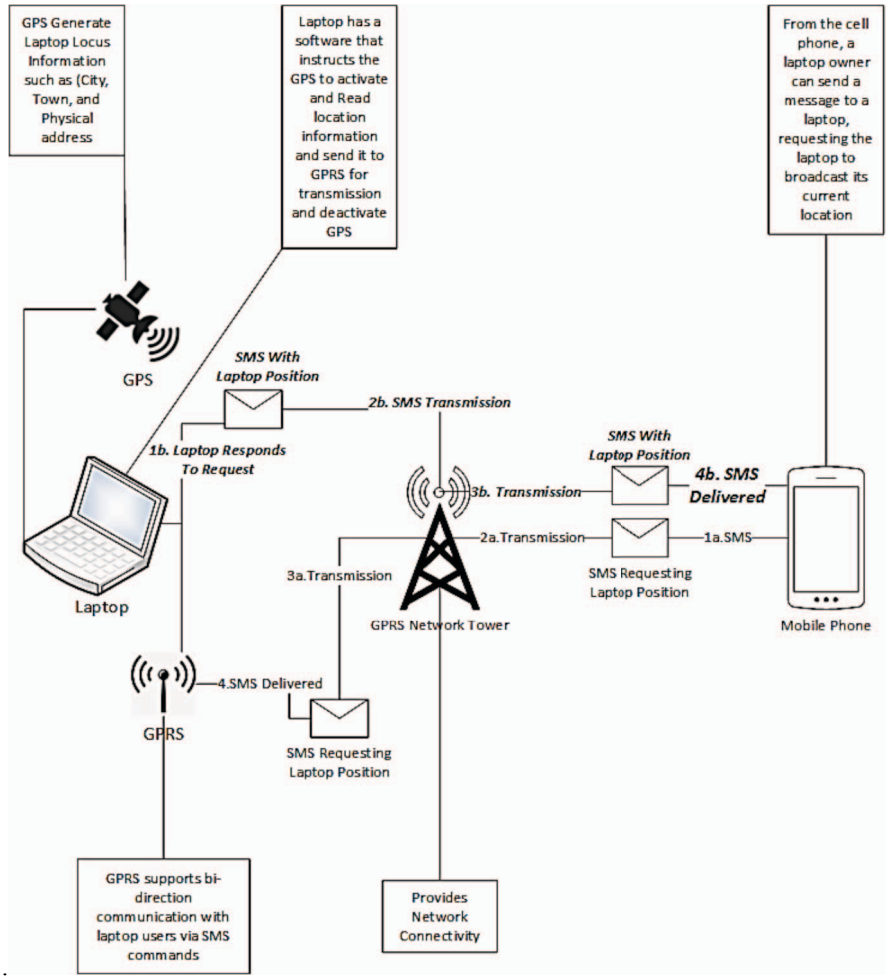

Fig. 2: Hardware based laptop tracking model

Fig. 3: Location Service

V. DISCUSSION AND FURTHER WORK

In this paper, the authors have presented both the laptop monitoring and tracking middleware and a system prototype that implements the proposed middleware architecture. The middleware supports an array of services such as: extraction of locus data from windows location sensor, laptop monitoring using RFID reader and passive tags, bi-direction SMS communication, and utilisation of database services to facilitate data management through SQL commands. The middleware can be considered as a potential hybrid middleware solution, because of its versatility and adoption of characteristics found in commonly used middleware solutions such as MiLAN [35] and Cougar [36]. The versatility of this middleware is in its ability to support parallel event handling, without compromising the delivery of services and its capacity to take advantage of resources and services offered by windows operating system environment and management of diverse hardware such as fingerprint scanner, Arduino RFID scanner, and a modem.

The good news about this hardware-based tracking system is that is can simply be integrated into other assets (smart televisions, cell phones, tablets and cars) as well, because of the minuscule nature of GPRS and GPS hardware and their maturity and reliability levels. This tracking model is advantageous in the sense that; (1) its implementation is cost effective because it uses infrastructure that has already been deployed by network service providers such as network towers and hardware such as GPRS that has proven to be reliable in achieving bi-directional communication and virtually generates accurate locus data using GPS, (2) it harnesses the strong coverage of wireless network towers and this increases reachability thus making asset recoverability more convenient, (3) it has the ability to take advantage of network roaming which means a stolen asset can be tracked anywhere around the globe, anytime by anyone, and (4) this model is not money gobbling unlike traditional subscription models, meaning once implemented, this model has high potential to be embraced by the majority and deliver unparalleled security and recovery levels.

What makes this model outstanding is the fact that it uses middleware in-lining approach; equipped with this technique, it was discovered that instructions can be programmed into hardware making it possible to achieve bi-direction machine (mobile phone) to machine (laptop) communication via SMS query commands and this can be accomplished even if the laptop is turned off. The GPRS and GPS on the laptop get their power from the battery and laptops can also be re-designed to incorporate a back-up and irremovable small battery to power-up the GPRS and GPS hardware to cater for emergency and unforeseen scenarios.

The prototype presented in this research was tested for conformance to the requirements set during a case study (of CUT) conducted. The results of this system have been briefly discussed in section IV. The prototype was developed to serve as proof of concept; the idea behind development of the prototype is twofold:

- To prove that a novel IoT-based application can be used to track laptops; despite maturity of technology in asset tracking, laptops still remain vulnerable to theft because, there are no hardware-based solutions known to the researcher that can track laptops. Most laptop tracking software are expensive due to the yearly subscription model that many cannot afford; the researcher considered them less helpful because, if a perpetrator formats (erases) the hard-drive of a stolen laptop, the laptop tracking software is permanently wiped off. This leaves us with no concrete solution to allay laptop tracking.
- The second reason was to prove that the problems identified during the CUT case study had potential to be solved using a software tool. The results of the experiments conducted substantiate this potentiality.

The presented work can be extended to provide for complete real-time integration of all security systems in a given institutions. An an over-the-air computing (OaC) functionality that allow users to extend the asset lease date further when it is about to expire can also be added to further improve the system prototype. The system prototype's ability to monitor mobile assets can also be enhanced by integrating Geo-Fencing function to allow the system prototype to report the entry or exist of a stolen asset into the organisation's premises.

References

[1] ISO, 2014. ISO 55001:2014 -Asset Management Systems: Requirements, First Edition. ISO/PC 251, *Asset management*

[2] Cisco Systems, 2012. The Expanding Role Of Mobility In The Workplace. Forrester Research Inc, 60 Acorn Park Drive, Cambridge , MA USA

[3] Schadler, Ted, 2013. 2013 Mobile Workforce Adoption Trends. In The Workplace. Forrester Research Inc, 60 Acorn Park Drive, Cambridge , MA USA

[4] Gubbi, J., Buyya, R., Marusi, S. and Palaniswami, M. (2013). Internet of Things (IoT): A vision, architectural elements, and future directions. Future Generation Computer Systems 29, 1645–1660, 16.

[5] Hwang, J. and Yoe, H. (2011). Study on the Context-Aware Middleware for Ubiquitous Greenhouses Using Wireless Sensor Networks. Sensors, 11(12), pp.4539-4561.

[6] Gershenfeld, N., Krikorian, R., & Cohen, D. (2004). The internet of things. Scientific American, 291(4), 46–51.

[7] Evans, D. (2011). The internet of things. How the Next Evolution of the Internet is Changing Everything, Whitepaper, Cisco Internet Business Solutions Group (IBSG).

[8] Han, S. W., Yoon, Y. B., Youn, H. Y., & Cho, W. D. (2004, May). A new middleware architecture for ubiquitous computing environment. In Software Technologies for Future Embedded and Ubiquitous Systems, 2004. Proceedings. Second IEEE Workshop on (pp. 117-121). IEEE.

[9] Hadim, S., & Mohamed, N. (2006). Middleware: Middleware challenges and approaches for wireless sensor networks. IEEE distributed systems online, 7(3), 1.

[10] Römer, K., Kasten, O., & Mattern, F. (2002). Middleware challenges for wireless sensor networks. ACM SIGMOBILE Mobile Computing and Communications Review, 6(4), 59-61.

[11] Du, P. and Roussos, G. (2013). Adaptive Communication Techniques for the Internet of Things. JSAN, 2(1), pp.122-155.

[12] Ashton, K. (2014). That 'Internet of Things' Thing - RFID Journal. [online] Rfidjournal.com. Available at:

http://www.rfidjournal.com/articles/view?4986 [Accessed 22 Nov. 2014].

[13] Yoneki E., & Bacon J. (2005). "A Survey of Wireless Sensor Network Technologies: Research Trends and Middleware's Role". Technical Report UCAM-CL-TR646, University of Cambridge.

[14] Blasi, D., Cacace, V., Casone, L., Rizzello, M., Rotolo, S. and Bononi, L. (2007). Ad hoc wireless sensor networking: Challenges and issues. ST Journal of Research, [online] Volume 4 - Number 1 - Wireless Sensor Networks, pp.19-25. Available at: http://www.cs.unibo.it/bononi/Publications/110930152-ST-Journal-of-Research-4-1-Wireless-Sensor-Networks.pdf [Accessed 10 Apr. 2014].

[15] ITU, (2008). Ubiquitous Sensor Networks (USN). ITU-T Technology Watch Briefing Report Series, No. 4. ITU, pp.1-7. Available at: http://www.itu.int/dms_pub/itu-t/oth/23/01/T23010000040001PDFE.pdf

[16] Priyadarshini, A. (2013). Internet of Things: Applications and Challenges In Technology And Standardization, National Institute Of Science & Technology Palur Hills, Berhampur, Orissa – 761008, India.

[17] Li Y.,↑ Huynh, D. T., Das, S. K. and Du, D. Z. (2008). Wireless Algorithms, Systems, and Applications. In: Third International Conference, WASA 2008 Dallas. Springer.

[18] Martonosi, M. (2004). The Princeton ZebraNet Project: Sensor Networks for Wildlife Tracking. Princeton University, pp.2-7.

[19] Yeh, L. W., Wang, Y. C., & Tseng, Y. C. (2009). iPower: an energy conservation system for intelligent buildings by wireless sensor networks. International Journal of Sensor Networks, 5(1), pp.1-10.

[20] Shinghal, K., Noor, A., Srivastava, N. and Singh, R. (2010). Wireless Sensor Networks In Agriculture: For Potato Farming. International Journal of Engineering Science and Technology, Vol. 2(8) ;(3955-3963), pp.1-3.

[21] Masinde, M., Bagula, A., & Muthama, N. J. (2012). The role of ICTs in downscaling and up-scaling integrated weather forecasts for farmers in sub-Saharan Africa. In Proceedings of the Fifth International Conference on Information and Communication Technologies and Development (pp. 122-129). ACM.

[22] Culler-Culler-Mayeno, E. (2006). A Technical Report: Wireless Sensor Networks and How They Work. Prepared for Ann Holms, University of California Santa Barbara. Vol. 1, pp. 01 - 08.

[23] Finkenzeller, K. (2003). RFID handbook. Chichester, England: Wiley.

[24] Chen, C. (2010). Design of a Child Localization System on RFID and Wireless Sensor Networks. Journal of Sensors, Volume 2010, 01-07.

[25] Bhargava, N., Bhargava, R., Mathuria, M. and Cotia, M. (2012). Fingerprint Matching using Ridge-End and Bifurcation Points. IJCA Proceedings on International Conference on Recent Trends in Information Technology and Computer Science 2012 ICRTITCS (6):12-1.

[26] Jain, A. K., & Kumar, A. (2010). Biometrics of next generation: An overview. Second Generation Biometrics.

[27] Atzori L, Iera A, Morabito G, 2010. The Internet of Things: A survey. Computer Networks 54 (2010) 2787–2805.

[28] Krakowiak, S. (2009). Middleware Architecture with Patterns and Frameworks. 1st ed. [ebook] pp.14-17. Available at: http://proton.inrialpes.fr/~krakowia/MW-Book/main-onebib.pdf [Accessed 11 Mar. 2014].

[29] Chatzigiannakis, I., Mylonas, G., & Nikoletseas, S. (2007). 50 ways to build your application: A Survey of Middleware and Systems for Wireless Sensor Networks. In Emerging Technologies and Factory Automation, 2007. ETFA. IEEE Conference on (pp. 466-473). IEEE.

[30] Arendarenko, E. (2009). A study of comparing RFID and 2D barcode tag technologies for pervasive mobile applications. Master's Thesis. University of Joensuu, Department of Computer Science and Statistics.

[31] Zhang, T., Ouyang, Y., & He, Y. (2008). Traceable Air Baggage Handling System Based on RFID Tags in the Airport. Applied Electronic Commerce Research (JTAER), 3(1), 106-115.

[32] Zhang, D., Liu, F., Zhao, Q., Lu, G., & Luo, N. (2011). Selecting a reference high resolution for fingerprint recognition using minutiae and pores. Instrumentation and Measurement, IEEE Transactions on, 60(3), 863-871.

[33] Swedberg, C. (2014). DHL Thermonet Tracks Drugs and Life-Sciences Goods With RFID Temperature Tag - RFID Journal. [online] Rfidjournal.com. Available at: http://www.rfidjournal.com/articles/view?10777 [Accessed 22 August. 2014].

[34] Lukka, K. (2000). The key issues of applying the constructive approach to field research. Reponen, T. (ed.), pp. 113-28.

[35] Heinzelman, W. B., Murphy, A. L., Carvalho, H. S., & Perillo, M. A. (2004). Middleware to support sensor network applications. Network, IEEE, 18(1), 6-14.

[36] Yao, Y., & Gehrke, J. (2002). The Cougar approach to in-network query processing in sensor networks. ACM Sigmod Record, 31(3), pp.9-18.