Big Brother: A Road Map for Building Ubiquitous Surveillance System in Nigeria

Simon Enoch Yusuf[1] and Oluwakayode Osagbemi[2]
Department of Computer Science,
University of Ibadan,
Ibadan, Nigeria.
[1]simmypukuma@yahoo.co.uk
[2]kayodeosagbemi@yahoo.com

***Abstract*—In this paper, we propose a method to improve the security challenges in Nigeria by embedding literally hundreds of invisible computers into the environment with each computer performing its tasks without requiring human awareness or a large amount of human intervention to monitor human behaviour, natural disasters and search for stolen or lost items. Ubiquitous Dynamic Surveillance cameras embedded with Radio frequency identification (RFID) is proposed for this security system.**

Keywords-component; Ubiquitous; Surveillance; RFID; Security; Computing.

I. INTRODUCTION

The issue of security of life and property in Nigeria has taken a frightening dimension and an issue of great concern to citizens and the government.

The need to tap from the power of Information and Communication Technology (ICT) to enhance national security operations is paramount. For some time, the issue of security of life and property in Nigeria has taken a frightening dimension and an issue of great concern to citizens and the government. The problem of security spans from kidnapping in the eastern region and traverses the religious disturbances in the north, political gansterism in the west and bomb-blast becoming issues of the moment [1]. Terrorism and atrocious crimes are increasing on a world-wide scale. Moreover, natural disasters, such as earthquakes and tsunamis, have also occurred frequently in many parts of the world. Figure 1 shows the death toll reported from 2003 to 2008 in various types of natural disasters. During this five-year period, the death toll reached over 482,000 as a result of such disasters. Death toll reported in various disaster types from 2003 to 2010 is shown in the Figure 2. Several earthquakes around the world proved to be the most deadly disasters which caused 406,866 deaths in the last five years [2]. The number of people reported to be affected by these disasters (142 million) dropped by 10 per cent, while the number of people reported killed is 23833 [3]. The 2008 death toll of 235,816 was more than three times the annual average of the previous eight years [4]. In 2009 there were only 25 geophysical disasters reported compared to the 2000-2008 annual average of 37. Of these, 18 were earthquakes, four tsunamis, two volcanic eruptions and one a landslide [5]. The year 2010 was characterized by a large number of natural disasters that have claimed four times more victims than in the past thirty years for a total of 295,000 victims [6]

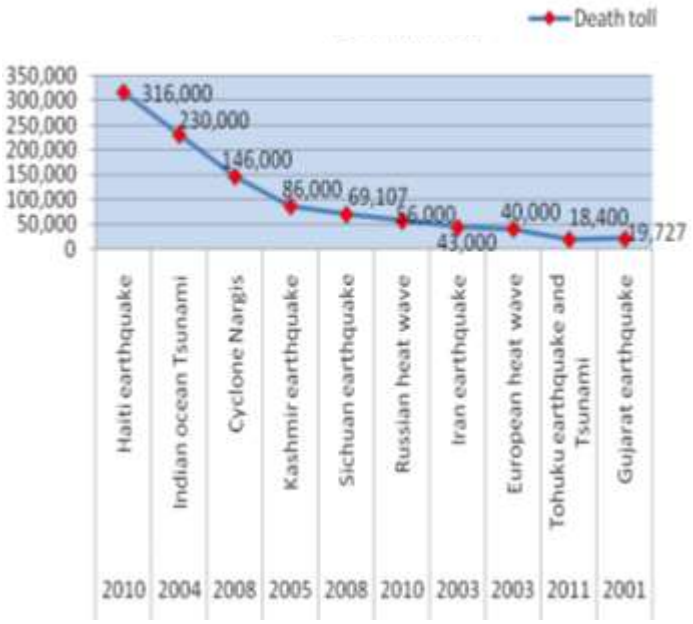

Figure 1. ten worst disaster of 21st century

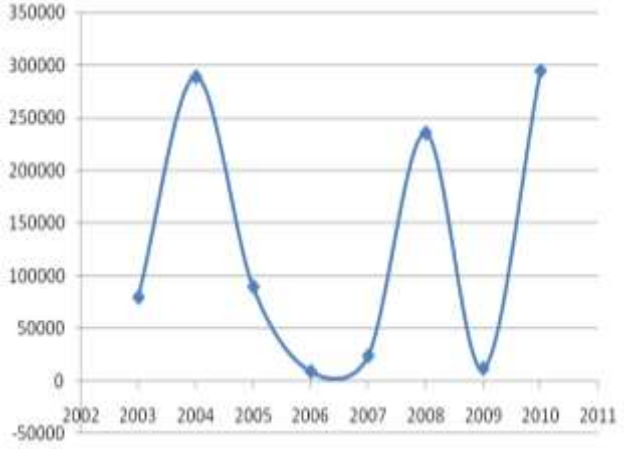

Figure 2. Average Death toll 2003 - 2010

The safety of human life is threatened by disasters caused by man and natural disasters.

In the fields of security, law enforcement, crime detection, inventory and industrial process monitoring, there is often a need to effectively identify individual subjects whether they be humans, goods or pieces of infrastructure.

II. UBIQUITOUS COMPUTING

Ubiquitous computing network is an emerging concept in computing, which integrates computation capabilities into the physical environment rather than being perceived as a visible object, so that it can provide widespread access to shared services through a variety of diverse devices irrespective of whether individuals are mobile or not.

Ubiquitous computing refers to methods of enhancing computer use by making networks of sensors and computers available and embedded in the physical environment [7]. The technologies on which ubiquitous computing applications are based span automatic identification (Auto-ID), such as Radio Frequency Identification (RFID); (wireless) communication systems, such as Global Standard for Mobile Communication (GSM); positioning services, such as Global Positioning System (GPS); and sensor networks. Together, these technologies are making new or improved security.

The term "ubiquitous computing" is a very broad term that is often overloaded to mean diverse things to different research projects. In many cases, researchers define ubiquitous computing by example, with respect to their own research. Ubiquitous computing allows us to realize additional abstractions that did not exist in traditional computing paradigms. The salient features of ubiquitous computing include the following according to [8].

- Extending Computing Boundaries. While traditional computing encompassed hardware and software entities, ubiquitous computing extends the boundaries of computing to include physical spaces, building infrastructures, and the devices contained within. This aims to transform dull, passive spaces into interactive, dynamic, and programmable spaces that are coordinated through a software infrastructure and populated with a large number of mobile users and devices.
- Invisibility and non-intrusiveness. In current computing models, computers are still the main focus of attention. In effect, people have to change some of their behaviour and the way they perform tasks so that these tasks can be computerized. To boost productivity, it is important that computing machinery disappears from the spotlight. Computers should blend in the background allowing people to perform their duties without having machines at the centre of their focus.
- Creating smart and sentient spaces. A dust of invisible embedded devices and sensors are incorporated to turn physical spaces into active, smart surroundings that can sense, "see," and "hear," effectively, making the space sentient and personalized. Ultimately, the space should become intelligent enough to understand users' intentions and become an integral part of users' everyday life.
- Context awareness. A ubiquitous computing model should be able to capture the different contexts and situational information and integrate them with users and devices. This allows the active space to take on the responsibility of locating and serving users and automatically tailoring itself to meet their expectations and preferences.
- Mobility and adaptability. To be truly omnipresent, the ubiquitous computing environment should be as mobile as its users. It should be able to adapt itself to environments with scarce resources, while being able to evolve and extend once more resources become available.

III. RADIO FREQUENCY IDENTIFICATION (RFID)

RFID is an area of automatic identification that is gaining momentum and is considered by some to emerge as one of the most pervasive computing technologies in history [9]. RFID or Radio Frequency Identification Tag Reader has revolutionized the way we live. RFID tag reader has made it possible to track any type of object by using radio frequency technology. Today RFID is a generic term for technologies that use radio waves to automatically identify people or objects (RFID Journal). There are several methods of identification, the most common of which is to associate the RFID tag unique identifier with an object or person. In most commonly touted applications of RFID, the microchip contains Electronic Product Code (EPC) with sufficient capacity to provide unique identifiers for all items produced worldwide. When an RFID reader emits a radio signal, tags in the vicinity respond by transmitting their stored data to the reader [10].

The principal advantages of RFID system are the non-contact, non-line-of-sight characteristics of the technology. Tags can be read through a variety of visually and environmentally challenging conditions such as snow, ice, fog, paint, grime, inside containers and vehicles and while in storage [11].

An RFID system consists of three main components, namely, tag, antenna, and reader. An RFID tag consists of a microchip attached to an antenna. Tags are either active or passive. Passive tags derive the power from the field generated by the reader. An RFID antenna is connected to the RFID reader. The antenna activates the RFID tag and transfers data by emitting wireless pulses.

The RFID reader handles the communication between the information system and the RFID tag. The signals transfer to the host computer and pass through to the electronic product code (EPC) network. After that, the data is stored in the database server or other business application systems. There is an important tool called RFID middleware which consists of a set of software components that act as a bridge between the RFID system components (i.e., tags and readers) and the host application software. In other words, middleware tools are used to manage RFID data by routing it between tag/readers and the systems within the businesses. Middleware solutions filter duplicate, incomplete, and erroneous data that it receives. After

digesting all data from the various sources, middleware forwards only the meaningful events to the enterprise systems. The tasks of the RFID middleware include data filtering, classification, data normalization, and aggregation of data transmitted between tags and readers for integration with the host application [12]-[21]-[28].

RFID is a type of Auto-ID technology sometimes referred to as dedicated short-range communication (DSRC), RFID is "a wireless link to identify people or objects" [13]. RFID is, in reality, a subset of the larger radio frequency (RF) market, which encompasses an array of RF technologies, including the following:

- Cellular phones
- Digital radio
- The Global Positioning System (GPS)
- High-definition television (HDTV)
- Wireless networks [14]

A. *Element of RFID*

RFID systems consist of four elements: the RFID tags, the RFID readers, the antennas and choice of radio characteristics, and the computer network that is used to connect the readers.

B. *RFID Tags*

RFID tagging is the use of very small electronic devices (called 'RFID tags') which are applied to or incorporated into a product, animal, or person for the purpose of identification and tracking using radio waves.

The tag is the basic building block of RFID. Each tag consists of an antenna and a small silicon chip that contains a radio receiver, a radio modulator for sending a response back to the reader, control logic, some amount of memory, and a power system. An active tag will be used to build this system. The reasons for the choice of this tag are because of their reading range and reliability. With the proper antenna on the reader and the tag, a 915MHz tag can be read from a distance of 100 feet or more [18]. The tags also tend to be more reliable because they do not need a continuous radio signal to power their electronics as in passive tags.

IV. RELATED WORK

One of the first applications of a radio frequency identification system was in "Identify Friend or Foe" (IFF) systems deployed by the British Royal Air Force during World War II 0. IFF allowed radar operators and pilots to automatically distinguish friendly aircraft from enemies via RF signals. IFF systems helped prevent "friendly fire" incidents and aided in intercepting enemy aircraft. Advanced IFF systems are used today in aircraft and munitions, although much of the technology remains classified [31].

Identification of people, objects and locations is an obvious application of RFID technology. Security systems that use RFID proximity cards to control access to restricted areas are perhaps the most common RFID application in use today [32].

Even in developing countries, such as Bangladesh, hospitals are using RFID-enabled staff ID cards [33]-[32]. Other hospitals have extended the use of staff ID cards to control access to computers and applications [34] - [32].

At the Georgia Veteran's Medical Centre RFID has been used for location identification [35]-[32]. Patients with visual impairments can navigate around the hospital by reading these location tags with using a cane containing an RFID reader.

RFID technology is being used to track thousands of wheelchairs, beds, IV pumps and other pieces of expensive medical equipment at several hospitals, including Bielefeld City Clinic in Germany [38], Lagos de Moreno General Hospital in Mexico [36], and the Walter Reed Army Medical Centre in the US [37]. Each item is tagged and can be located in real time via a network of RFID readers throughout the hospital. Some such systems, often referred to as Real Time Location Systems (RTLSs), also keep track of whether the equipment is available, in use, awaiting cleaning, or undergoing maintenance [32].

A. *Proposed System*

In this section we describe a framework of a surveillance system that ensures that many computers are available throughout the physical environment, but making them effectively invisible. More precisely, a proliferation of hundreds or thousands of computing devices, sensors and embedded processors that will provide new functionality, offer specialized services with the surrounding environment and available resources.

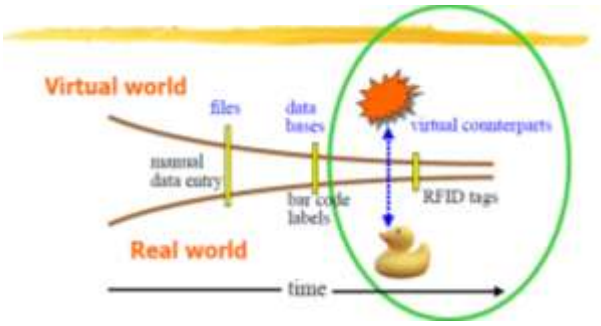

Figure 3. Tagging object from real world to the visual in a database [16]

After vigilantly studying the Camera Based Surveillance Architecture, and judged on the basis of the following parameters as provided by [17]:

i. Automation
ii. Time efficiency
iii. Ease of monitoring and administration of its operations by naive hands
iv. Impenetrable
v. Efficient for mobile and immobile objects and regions
vi. Installation cost of system

It is found that it doesn't overall fulfil the demands for ubiquitous due to technological limitations. We have come up with a roadmap using ubiquitous computing to overcome the limitations of Camera Surveillance Mechanism. The objectives of the proposed system include

- To enhance national security
- To enhance the recovery of missed and stolen items.
- To identify object and their respective location.
- To enhance policies on identifying the rightful owners of an object.

Surveillance cameras with video camera embedded with RFID is proposed in this paper to enhance national security. These surveillance cameras are connected to a recording device, IP network, and is been watched by a law enforcement officer.

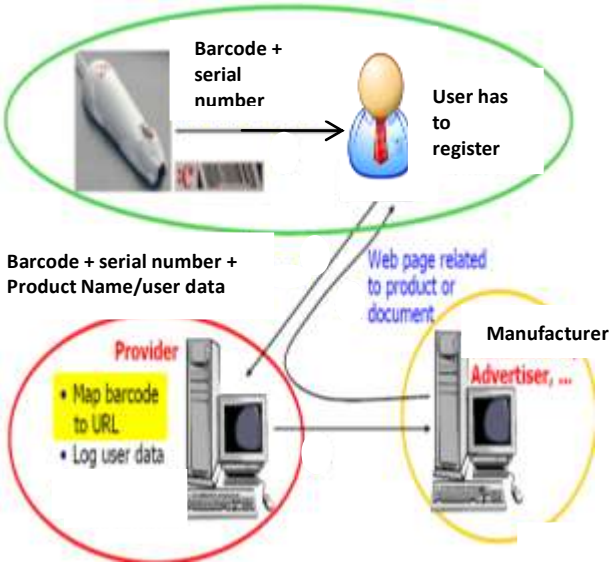

Figure 4. Mapping of barcode to Internet pages adapted from [29]

The cameras sense motion and footage. Analysis of footage is made by automated software that organizes digital video footage into a searchable database, and by automated video analysis software which can be VIRAT, HumanID [30]. The amount of footage is also drastically reduced by motion sensors which only record when motion is detected.

The surveillance cameras are embedded with RFID data server which will be communicating with both the RFID tag and RFID main data server. It is used for capturing images whether still or frames and records activities in a particular location over time. The purpose for combining both RFID and surveillance cameras is for Dynamic Surveillance which focuses over motion, location, identification and gives visual support to the system when needed. Big Brother provides a Surveillance Technique which can't be mistuned technically, manually or by any other means [17] because of RFID tag embedded with it.

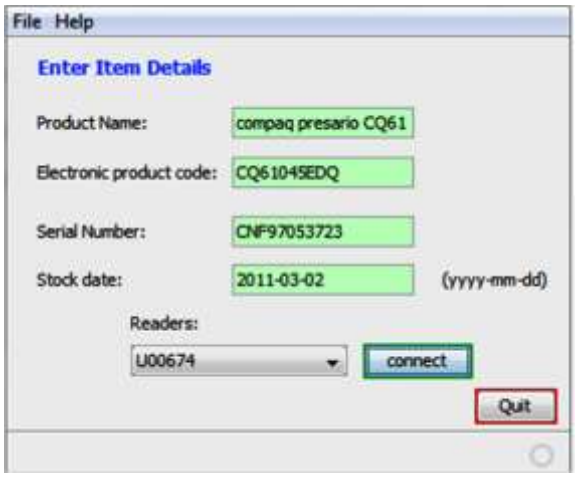

Figure 5. Taking stock of RFID tag objects

The Database consists of Product name, model number, electronic product code and readers IDs. Tags information are stored in the database and linked to the tags. The readers and tag identify objects and information about the objects, the objects are embedded with the RFID tag while in the case of humans an attachment is made to the individual cloths or in the form of any wearable device. Prototype object tag information database is shown above which provides information about the object.

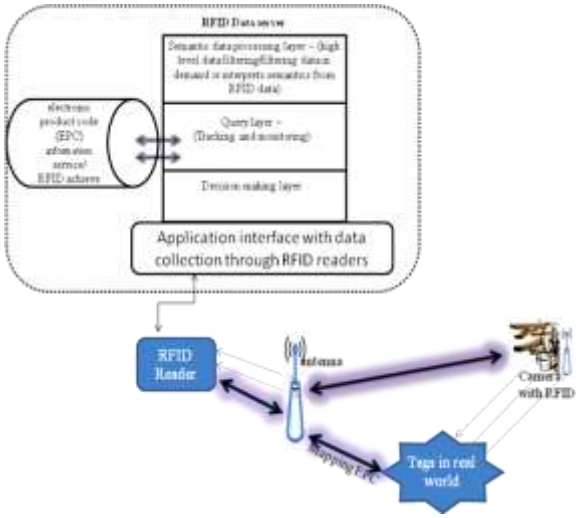

Figure 6. RFID framework

The RFID tag reader then sends an electronic signal to the embedded tag. The RFID tag responds to this signal by sending back a radio frequency signal. This signal can give the location of the object along with the product information. [15].

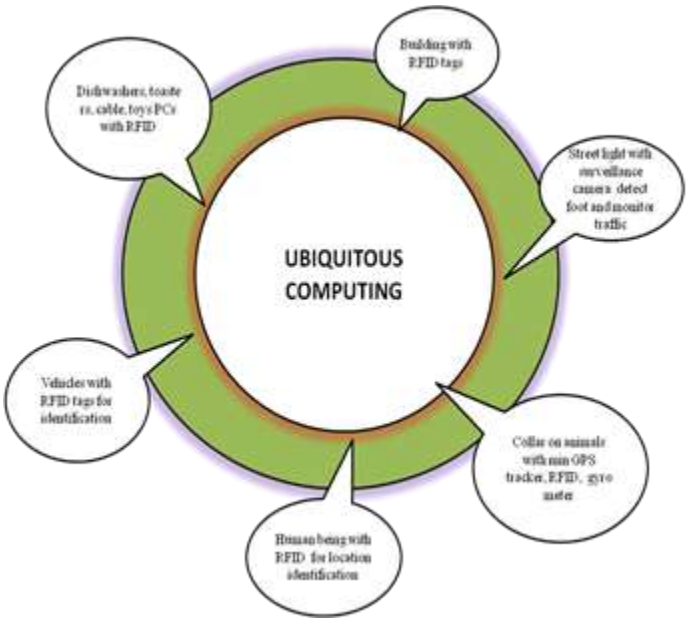

Figure 7. Ubiquitous computing Scenerio

B. RFID tags for earthquake detection

According to new research conducted by International Journal of Innovation and sustainable development, Radio frequency identification, RFID, could be used in the immediate aftermath of a major earthquake to save lives [19]. In addition, in earthquakes or tsunami, animals were the first to detect these natural disasters days before it happens and run for safety [20]. Big Brother is used to track unnatural motion in animals by combining mini GPS tracker, RFID and gyrometer chip. RFID tags are attached to a couple of hundred animals in the earthquake prone area. When these animals start to flee, the RFIDs would transmit the co-ordinates of the fleeing motion to a central computer. The GPS tracker would provide the co-ordinates where animal behaviour is abnormal to pinpoint the location of a potential earthquake. RFIDs would provide wireless transmission of the data and the gyrometer can detect uneasy motions in the animal and send warning to the connected central computer with an alarm.

C. RFID Tags for Human Identification

Big Brother can be used to identify patients in hospitals, prevent theft, and track shipments. This system provides a rapid way to read data about an individual. It can reliably identify human being and can also be used for animal identification. However, at present the most prevalent use for RFID tags is tracking merchandise. Retailers are using RFID tags to check on their merchandise to see whether they are in the premises or being transported. Big Brother (RFID) can also be incorporated into National passport just like countries like Malaysia, UK and the US now using RFID tags in passports [21].

Big Brother monitors and acts as a tracer for easy location identification. For Pupils going to school, trigger areas are set at some point in the school zone which provides alert to parent and school authority about passage of their children.

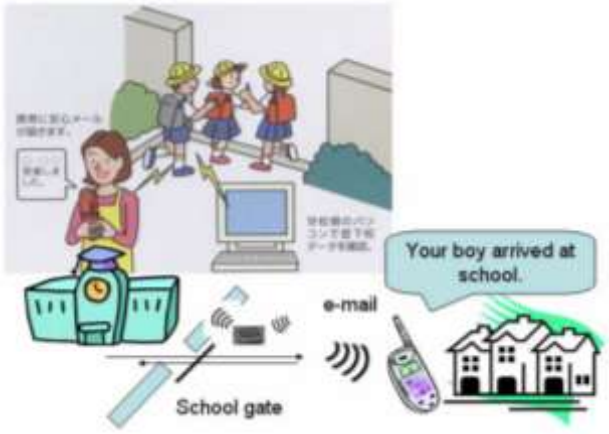

Figure 8. Checking system for prevention of kidnapping [22]

V. RECOMMNEDATIONS

Several technical problems should be considered beforehand in line with the security of the RFID system. Some of the security requirement includes [23]:

Availability: When constructing the RFID system, failure in hardware or software may occur due to deliberate action or not. Therefore, if the RFID tag cannot provide service due to attacks or physical failure during the construction of the system, the availability of the RFID system should be provided to restore the service promptly.

Forward channel security: Forward security is required to generate and provide the service through secure communication between the RFID tag and the RF reader. This is because the attacker can prey on the various information transmitted or received from the RFID tag [23].

Secure status acquisition technology: When constructing the RFID-based network, a safe service acquisition process is required to know the status of all RFID tags. This must be performed by checking the current status of all tags in the RFID system in order to ensure the availability of the service against potential physical failure that may happen during denial-of-service (DoS) attacks or during the construction of the RFID system [23].

Finally, This cost of implementation can be reduced by employing existing wireless networks.

VI. CONCLUSION

Most Surveillance agencies like National Association for the Criminal Rehabilitation of Offenders (NACRO), Home Office USA etc [27]-[17] accept the failure of Camera Surveillance due to technical, manual or any other discrepancies in the system. Thus there arises a need for better technology for Surveillance. RFID provides a Surveillance Technique which can't be mistuned technically, manually or by any other means [17]. In our work, we proposed a surveillance camera system embedded with RFID reader.

Some of the Challenges of the system include:

- Forgery: forgery is a major problem in RFID, user with illegitimate identification would devise various means to imitate legitimate tags.
- Cost: obviously, the cost of implementation is a major hurdle to consider before embarking on it. The cost of implementation can be significant, depending on the area to be covered, the number of items to be tracked, and the accuracy required.
- Denial of service attack: attackers unable to conduct forgery attack will leave the system communication channels jam preventing RFID readers from identify tags. An attacker could also seed a physical space with "chaff " tags intended to confuse legitimate readers or poison databases. Locating and removing chaff tags might be very difficult in a warehouse environment [30].
- Security and Privacy: many people consider this as in invasion of privacy because it tracks their movement and visually their activities and therefore will not allow such systems be installed around them.

REFERENCES

[1] O. E., Osuagwu, G. Nworuh, B. Asiegbu , A. Uwaleke, F. Olanapo & U. Eze, "Enhancing security of the Nigerian State through electronic roadside vehicle indentification system" 23rd National conference, Nigeria Computer Society, Conference Proceedings Volume 21, pp. 299-304, July, 2010.

[2] A. Ahmed, L. Sugianto, "RFID in Emergency Management",chap VIII Auto-Identification and Ubiquitous computing applications , RFID and smart Technologies for information converage. Infromation Science Reference. Hershey, New York 2009, pp. 39-53.

[3] Canadian Red cross articial retrieved on 2 June, 2011 from http://www.redcross.ca/article.asp?id=25285&tid=001.

[4] CBC News on World Natural disasters retrieved on 15 May, 2011 from http://www.cbc.ca/news/world/story/2009/01/23/natural-disasters.html.

[5] Alert Net News on Natural disasters in 2009 retrieved on 2nd June, 2011 from http://www.trust.org/alertnet/news/fewer-natural-disasters-in-2009-but-no-clear-trend-seen-research-group.

[6] World life Union retrieved on 23rd May, 2011 from http://www.thelivingtrees.org/forumtlt/viewtopic.php?f=12&t=6.

[7] M. Weiser "*Hot Topics: Ubiquitous Computing*", IEEE Computer, Vol. 26, No. 3, October 1993.

[8] J. F. Al-muhtadi, "An intelligent authentication infrastructure for ubiquitous computing environments". Phd dissertation, Graduate colleege of the university of illonois at urbana-champaign, 2005.

[9] R. T. Davis. "*U.S. Foreign Policy and National Security:Chronology and Index for the 20th Century"*. Praeger Security International Series (Illustrated ed.). ABC-CLIO. p. xiii=xiv. ISBN 9780313383854.

[10] "Position Statement on the use of RFID on consumer products" (2003, November). Retrieved on 23 May, 2011 from http://www.spychips.org/jointrfid_position_paper.html.

[11] C. Robert, "Radio Frequency Identification (RFID)". *Journal of Computers and Security*. Infromation Science Reference. Hershey, New York 2009.

[12] M. Bhuptani, & S. Moradpour, "RFID field guide: Deploying radio frequency identification systems". New York: Prentice Hall 2005.

[13] S. d'Hont. "*The cutting edge of RFID technology and applications for manufacturing and distribution"* Retrieved on July 10, 2003, from http://www.ti.com/tiris/docs/manuals/whtPapers/manuf_dist.pdf

[14] R. Malone, "Reconsidering the role of RFID. *Inbound Logistics"* Retrieved on September 11, 2004, from http://www.inboundlogistics.com/articles/supplychain/sct0804.shtml

[15] Horizon world wide componets co. Ltd. http://www.horizon-components.com/tag-reader-rfid-uhf-sdio.html retrived 20 june, 2011

[16] F. Mattern "Ubiquitous Computing. ETH Zurich Institute for Pervasive Computing" Copyright F. Mattern, Porquerolles, May 2003. http://www.vs.inf.ethz.ch/publ/slides/MatternPorquerolles.pdf

[17] I. Singh, H. Patil "RFID: Dynamic Surveillance Approach" IJCSI International Journal of Computer Science Issues, Vol. 7, Issue 3, No 7, May 2010.

[18] G. Simson and H. Henry, "Understanding RFID Technology" chap II, garfinkel.book Page 15 Thursday, June 2, 2005.

[19] "The use of RFID technology in earthquakes" in Int. J. Innovation and Sustainable Development, Vol 4, 253-275. Published: May 6, 2010. Inderscience Publishers. Retreved on 23 May, 2011 from http://www.sciencenewsline.com/nature/2010050612000022.html

[20] "Quora article on Technology that should be build for earthquake detection", Retrieved on 20 june, 2011 from http://www.quora.com/Earthquakes/Which-technology-should-be-built-to-predict-Earthquakes-and-warn-related-people-to-be-on-a-safety-place.

[21] S. Shah, "Semantics and Internet of things", RFID Journal White Paper.

[22] *N. Ashida, Y. Ashida, S. Sagawa, S. Suto, T. Higash., Makimoto K.and Kawahara T.* "Safety Management and Crime Prevention by IC Tags – Cases of practical use of IC tag in medical and welfare fields", 5rd APT TELEMEDICINE Workshop, Proceedings 2007.

[23] D. Seo and I. Lee, "A Study on RFID System with Secure Service Availability for Ubiquitous Computing", *International Journal of Information Processing Systems Vol.1, No.1, 2005*.

[24] D. Estrin, R. Govindan, J. Heidemann and S. Kumar, "Next Century Challenges Scalable Coordination in Sensor Networks.", Proceedings of the ACM/IEEE International Conference on Mobile Computing and Networking. Seattle, Washington, USA, 263-270.

[25] National Research Council, "Embedded, Everywhere: A Research Agenda for Networked Systems of Embedded Computers", *National Academy Press2001, Washington DC, USA.*

[26] RFID Journal (n.d.). *RFID Journal frequency asked questions*. Retrieved from http://www.rfidjournal.com.

[27] Surveillance Camera Players "ineffectiveness of surveillance cameras" updated on 17th June 2009.

[28] K. Goyal & D. Krishna, "RFID middleware integration to the entire supply chain" RFID Journal White Paper 2005.

[29] Ubiquitous Computing retrived on 2 June, 2011 from http://www.vs.inf.ethz.ch/publ/slides/MatternPorquerolles.pdf

[30] Wikipedia, retrieved June 20, 2011 from http://en.wikipedia.org/wiki/Surveillance

[31] S. A. Weis S. A. "RFID (Radio Frequency Identification): Principles and Applications" Retrived from www.eecs.harvard.edu/rfid-article.pdf on 01 August, 2011.

[32] J. Symonds, J. Ayoade, D. Parry, "Auto-Identification and ubiquitous computing applications: RFID and Smart Technologies for Information Convergence" . Chap VI . information Science reference. Hershey. New York 2009.

[33] B. Bacheldor, "RFID Take Root in Bangladesh. Retrieved February 12, 2008, from www.rfidjournal.com

[34] B. Bacheldor, "N.J. Medical Center Uses LF Tags to Protect Patient Records", Retrieved February 12, 2008, from www.rfidjournal.com

[35] D. A. Ross & B. B. Blasch, "Development of a Wearable Computer Orientation System", ACM Personal and Ubiquitous Computing 2002, 6(1), 49-63.

[36] B. Bacheldor, "Local Hospital Spearheads Mexico's Digital-Hospital Initiative", Retrieved February 12, 2008, from www.rfidjournal.com

[37] C. Broder, Hospitals Wade into Asset- Tracking Technology. Retrieved October 30, 2004, from www.ihealthbeat.com

[38] R. Wessel, "German Hospital Expands Bed-Tagging Project" 2007. Retrieved February 12, 2008, from www.rfidjournal.com

AUTHORS PROFILE

Simon Enoch Yusuf received his BSc (Hons) degree in Computer Science in 2007 from University of Adamawa State and MSc in Computer Science from University of Ibadan, Nigeria. His research Interest Includes Network security, Ubiquitous computing and ICT Diffusion in developing countries. He is a member of Nigeria Computer Society (NCS), and has published quite a number of papers in reputable Journals and conference proceedings.

Oluwakayode Osagbemi holds a BSc (Hons) degree in Computer Science (2008) and a MSc in Computer Science both from the University of Ibadan. His research interests include computer vision, content based image retrieval, and ubiquitous computing. He has published in several conference proceedings.