Computing, Information Systems, Development Informatics & Allied Research Journal
ISBN 978-2257-44-7 (Print) ISSN 2167-1710 (online)
Vol. 5 No. 1. March, 2014 – www.cisdijournal.net

www.iiste.org

A UBIQUITOUS TECHNOLOGY FRAMEWORK FOR CURBING THE BOKO HARAM MENACE IN NIGERIA

[1]Godspower O. Ekuobase
Department of Computer Science,
University of Benin,
Benin City, Edo State
Nigeria
godspower.ekuobase@uniben.edu

Ifeanyichukwu E. Anyaorah
Department of Computer Science,
University of Benin,
Benin City, Edo State
Nigeria

[1]Corresponding Author

ABSTRACT
The security threat posed by the Boko Haram sect in Nigeria has remained unabated with no hope in sight. We examined the concept and applications of ubiquitous technology and taking advantage of its potentials, proposed an architectural framework – N-tier Ubiquitous Architectural Framework (NUAF) – for curbing the Boko Haram menace in Nigeria. NUAF is a hierarchical and segregational distributed architectural framework which in its simplest form consists of the base-tier, inner-tier and top-tier. The real life implementation of NUAF is however dependent on some anticipated research sucesses in nanotechnology and wireless network security.

Keywords: Internal security, Terrorism, Boko Haram, Ubiquitous technology and Distributed architecture

1. INTRODUCTION

One of the distinguishing characteristics of nationhood is a state's ability to provide internal security for her citizens, defend her sovereignty and territorial integrity. This is obviously the minimum requirement for a nation to build a solid prosperous economy and begin the ultimate match towards social and political well-being encapsulated as national interest. To achieve national security, an enabling environment must be provided where the citizens will feel free and secured to achieve their full potentials and the state will itself be safe to achieve greatness, power, and prestige [13]. It is obvious therefore that national security is a critical issue that must be given adequate attention for the country to progress in all aspects.

Security is not the absence of threat but the ability to respond to security breaches and threats with expediency and expertise. When an entity is secured it means it is free from danger, harm or anxiety [13]. Security threats can be of two categories; natural security threats and man-made security threats. Natural security threats are in the form of natural disasters and can hardly be prevented, instead they are monitored and managed so as to reduce their effects. The man-made security threats caused by human actions and inactions, though preventable, is on the increase in Nigeria; and this calls for urgent attention. This includes terrorism, robbery, theft, arson, kidnapping, extortion, insurgency, assassination, demonstration and mob action. In recent times, terrorism happens to be more damaging to the Nigeria nation.

Consider the following terrorist activities in Nigeria as captured in her national dailies:

- Boko Haram: We did not declare ceasefire – Shekau (Vanguard: Ndahi Marama & Hugo Odiogor, Mar 03, 2013)
- Explosion in Maiduguri as APC govs hold meeting …(Nigeria Tribune: James Bwala, Mar 01, 2013)
- Plug These Security Lapses in Nigeria (The Statesman: Editorial, Feb 02, 2012)
- Security: FG must wake up (Nigeria Tribune: Godday Odidi, Feb 02, 2012)
- Boko Haram Exposing Security Lapses in Nigeria (Ngex: Tony Are, Nov 21, 2011)

Factors speculated as responsible for this menace include religious fanaticism, high youth unemployment, cultism, militia formations, widening gap between the rich and the poor, influx of illegal immigrants, political thuggery, tribalism, poor justice system, corruption, illegal drug and excessive alcohol consumption. The terrorist activities characterized by the use of heavy weapons and explosives and believed to be championed by the Boko Haram sect [1], appears to be "a torn in the flesh" of the Nigeria government and her security agencies. This was aptly captured by [8] when they said that, "Terrorism is the most alarming criminal acts and the major challenge of the government and the Nigerian people". Terrorism has of recent created a lot of panic and hopelessness among the citizens of Nigeria.

The use of bombs by these aggrieved members of the society to terrorize the citizens as a bait to get government's attention is becoming unbearable as hundreds of lives are being wasted on regular basis. Everyone is a possible victim of the Boko Haram menace because Boko Haram is known for attacking public institutions. Adagba and his colleagues [1], said "The cycle of violence being unleashed on Nigerians by the fundamentalist group, Boko Haram has heightened fears among the populace and the international community that the hostility has gone beyond religious or political colouration". A society that lives in fear and uncertainty can hardly be productive.

Prior to 2009, terrorism and bomb attacks were strange occurrences in Nigeria but had since become a common occurence. It is alarming to know that between 2009 and 2012 about 935 citizens have been killed by the Boko Haram sect according to Human Rights Watch (HRW) [1]. Few months ago (Sunday 28th Oct, 2012) a bomb blast was recorded in Kaduna one of the states in northern Nigeria, killing over 100 victims and this was not captured in the HRW record cited by [1]. Just recently (28th Feb, 2013), series of bomb blasts were reported in Maiduguri killing about six persons, security men inclusive. With the over 50 attacks since August 2011 and promises from the sect of further attacks unless their tall demand of Islamizing the nation is met further, shows that the battle is far from being over [8].

The government and the people of Nigeria have employed various measures to address the menace such as enlightenment campaigns, political solutions, legislation and state force, but tangible results are yet to be seen. Enlightenment would have been good but the members of this sect are faceless and hence can hardly be reached. Anti-terrorism laws are also a welcome development but this sect uses suicide bombers as agents and once the perpetrator is dead you can hardly trace the source. In addition, the use of dialogue and political compromise will likely encourage more of such insurgent groups to arise knowing that they can always opt for dialogue at the end of the day. We do not need to leave our national security in the hands of these enemies of national peace. A better security measure should not be beggarly; instead, it should be able to destabilize such sects and make the nation unconducive for such terrorist operations. This way other terrorist groups will not see Nigeria as a safe haven for their operations as the operations of Boko Haram has exposed the security weakness of the nation [8].

From the aforementioned discussions, it appears we have no better option to resolving bomb attacks and related terrorist activities than relying on the state security force which unfortunately in their present state is not in the position to curb such security threat in the country; probably due to their low technological consciousness. For instance, it is presently impossible for the Nigeria Police to detect explosive devices in the custody of citizens in every nook and cranny of the country for they cannot be everywhere; but this is readily possible with ubiquitous technology.

In ubiquitous computing environment, small computers and sensors are embedded in various objects and placed in our environment, and they communicate with each other and process information in a coordinated manner to offer useful services to humans such as performing environment control and offering information. It appears therefore that when bomb detection technology and ubiquitous technology are combined, explosive materials can easily be detected on transit and even at manufacturing and storage points and have the information sent to security agencies to take necessary proactive actions. When this concept is properly articulated and implemented, it can help the state force check the spate of terrorism being experienced in Nigeria. This paper lay a foundation for the realization of this concept by proposing a ubiquitous technology framework for curbing the Boko Haram menace in Nigeria.

2. BACKGROUND INFORMATION

The term Ubiquitous means ever-present, pervasive, omnipresent, all-over, everywhere or universal. As a computing term, Ubiquitous implies that computing technology is everywhere and being used at the same time unobtrusively. In Ubiquitous Computing environment, small computers and sensors are embedded in various objects and places in our surroundings, and they communicate with each other and process information in a coordinated manner to offer useful services to humans such as performing environment control and offering information [12].

Ubiquitous Computing is a post-desktop model of human-computer interaction in which information processing has been thoroughly integrated into everyday objects and activities [6]. In the course of ordinary activities, someone interacting with a ubiquitous computing environment engages many computational devices and systems simultaneously, and may not even be aware that he/she is doing so. Other terms related to ubiquitous computing include pervasive computing, ambient intelligence, and everyware. When primarily concerned with the objects involved, it is also called physical computing, the Internet of Things, haptic computing, and things that think.

2.1: History of Ubiquitous Computing (Ubicomp)

Ubicomp came as a result of Researchers' dream of pervasive computing which will enable everyday objects to recognize our needs and react to them in an intelligent manner. Technology in computing has undergone extensive changes over the years. In the early 1970s, mainframe computers dominated the computing scene based on the principle of one computer serving many people. In the 1980s, mainframe computers gave way to personal computers and notebooks, and the emphasis was one computer to one person. In the 1990s and beyond, with increased computing powers available at affordable prices, we are witnessing a new era of personal computing, that is, a phenomenon in which multiple computers are serving one person. Through the ages, technology has dramatically transformed our lives, changing the way we learn, live, work, and play. Technology shrank transistors to such microscopic sizes that they enable computer chips to be found in the things we use daily. Technology also connects computers around the world breaking down geographical boundaries as people are able to "travel" virtually everywhere, collaborate with others online, and are connected with loved ones virtually even though they may be miles away. Mark Weiser, acclaimed father of "Ubiquitous Computing" (or "Ubicomp" for short), coined the term "Ubiquitous" to refer to the trend that humans interact no longer with one computer at a time, but rather with a dynamic set of small networked computers, often invisible and embodied in everyday objects in the environment [7].

Ubicomp is seen as a technology that enables information to be accessible anytime and anywhere and uses sensors to interact with and control the environment without users' intervention. The principle guiding ubicomp is the creation of technology that brings computing to the background and not the foreground, making technology invisible. This means that people do not need to continually rationalize one's use of an ubicomp system because after learning about its use sufficiently, one ceases to be aware of it. It is literally visible and effectively invisible in the same way, for example, a skilled carpenter engaged in his work might use a hammer without consciously planning each swing. Hence, ubicomp defines a paradigm shift in which technology becomes invisible, embedded and integrated into our everyday lives, allowing people to interact with devices in the environment more naturally [3].

2.2: Features aand Components of Ubiquitous Computing

For computers to be ubiquitous, size and easy communication are two important factors that must be addressed. Computing devices must be as small as possible and capable of communicating between themselves. Technology supporting these goals is already well underway under the rubrics of nanotechnology and wireless computing.

2.2.1. Nanotechnology

The trend toward miniaturization of computer components down to an atomic scale is known as nanotechnology [14]. It involves building highly miniaturized computers from individual atoms or molecules acting as transistors, which are the heart of the computer chip. Therefore, nanotechnology's extreme miniaturization of transistors allows for impressive levels of computing power to be put into tiny packages, which can then be unobtrusively tucked away.

2.2.2: Wireless Computing

Wireless computing refers to the use of wireless technology to connect computers to a network. Wireless computing allows one to access network and communication services from anywhere within reach of a wireless network without cable medium.

2.2.1. Context awareness

Context is any information that can be used to characterize the situation of an entity. Where an entity is a person, place, or object that is considered relevant to the interaction between a user and an application, including the user and applications themselves. Context can also be defined as a combination of any information that can be sensed or received by an entity which is useful to catch events and situations. Therefore Context-awareness is the ability of an entity to usefully adapt to or react based on context. The promise of context-awareness is that computers will be able to understand enough of a user's current situation to offer services, resources, or information relevant to the particular context. The attributes of context to a particular situation vary widely, and may include the user's location, current role, past activity, and affective state. Beyond the user, context may include the current date and time, and other objects and people in the environment. The application of context may include any combination of these elements [14].

Basically, we can categories context awareness as highlighted as follows:

- Proximate Selection: Presents information, which is selected considering some context to ease a choice.
- Automatic Contextual Reconfiguration: Current context automatically leads to new information. The entity creates new bindings to context resources.
- Contextual Information and Commands: Information and commands are shown / executed manually and adapted to the current situation.
- Context-Triggered Actions: The current context leads an application to start a process automatically.

Other related terms to context awareness include adaptive, reactive, responsive, situated, context-sensitive, and environment-directed [14].

2.2.4. Natural Interaction

Learning to use the computer itself is something else to focus on, learn, or do in order to accomplish a goal presently. That is, apart from the services computer renders, which ordinarily should be the user's focus, one still have to devote time and energy to learn how to use the computer itself (examples: how to navigate, click, select, issue command, etc.). The idea behind natural interaction is for the computer to supply services, resources, or information to a user without the user having to think about the rules of how to use the computer to get them [14]. In this way, the user is not preoccupied with the dual tasks of using the computer as well as getting the services, resources, or information [14].

2.2.5: Electronic Nose

Electronic nose is a key to the use of ubiquitous technology in tackling explosive related security challenges [10]. It helps detect the presence of explosive elements in the atmosphere. Dogs have been trained to detect explosive substances but due to their fatigue and non-ubiquitous nature, there is need to build into electronic devices the sensing methodology (olfaction) of animals. This led to the drive to build electronic nose system which mimics animals' sensing system. Electronic nose systems usually consist one or more of the following technologies: Electrochemical sensors e.g. Conductance-based sensors – metal-oxide and conducting polymers, Potentiometric sensors – chemically sensitive field-effect transistors (FETs); Mass-change (piezoelectric) sensors e.g. Quartz crystal microbalance (QCM), Surface Acoustic Wave (SAW) devices; Optical sensors e.g. Fluorescent optical fibers and Colorimetric.

Many of these technologies are used in building large scale electronic noses, there is need to replicate same in nanometer-scale sensing systems that can detect traces of such substances in the air. Research on Carbon nanotude and Nanowire technologies are already under way to realize nanometer-scale sensors [11]. A breakthrough in nanometer-scale sensing systems will be a wellcomed development as most improvised explosive devices (IEDs) leave very minute trace of explosive substances in the air thereby making their detection difficult.

2.3. Applications of Ubiquitous Computing

The following subsections discuss some of the areas and fields where ubiquitous computing has been and is being applied:

2.3.1: Logistics and production

Ubiquitous computing is already well developed when it comes to Radio-Frequency Identification (RFID) systems in logistics. Practically all logistical systems today from the in-plant flow of components to the transport of consumer goods by road, air, water or rail between the producer and the market are controlled and monitored by Information Technology (IT) systems. These IT systems are based on identification systems in which a data carrier is affixed to an object which can then be recognized by a reader. Such systems allow physical streams of goods to be tracked throughout the logistics supply chain and generate tracking data for the IT systems. Unlike barcode-driven tracking systems that involves manual scanning and susceptible to defacing, RFID systems uses a transponder with a microchip as its data carrier and communicates with the reader by means of an electromagnetic field. RFID already has a long history of use in chip cards for access systems, in car keys, and in other applications [5].

2.3.2: Motor traffic

Today's cars contain a multitude of driver assistance systems that are intended to support the driver and guide the vehicle without calling attention to themselves, as a rule. The car itself thus becomes a smart object, reacting flexibly to the driving situation as well as the condition of the vehicle and the driver. The three classes of driver assistance systems are [5]:

1. Assistance systems for vehicle operation that do not directly intervene in control of the vehicle. These include rain sensors that automatically turn wipers on or off, navigation systems, and spring and shock absorber systems to improve passenger comfort.
2. Assistance systems for driving tasks that the driver can override or switch off. Adaptive cruise control is just one typical example of such systems. Other examples include four-wheel drive or warning functions for which activation is situation dependent – for instance, if seat belts are not fastened, the driver is tired, or the vehicle drifts out of its lane.
3. Assistance systems for driving tasks that independently override driver decisions. Among these are the Electronic Stability Program (ESP), which prevents skidding by intervening in the car's braking system and powertrain, or the Pre-Safe System, which reacts to full braking by automatically tightening the seatbelt or adjusting seats and headrests to their safety positions.

More ambitious approaches to driver assistance systems depend primarily on powerfully integrating information on the car's surroundings into the system (sensor fusion). Collision warning and avoidance systems use image recognition, radar, or other sensors to capture data on the car's immediate surroundings and interpret the situation. They then transmit a warning to the driver or even initiate braking or an evasive manoeuver [5]. Co-operative assistance systems exchange data between vehicles in order to give drivers information on the traffic situation in their vicinity. Any disturbance is forwarded from one vehicle system to the next within a fraction of a second. Depending on the device-specific communication, processing and visualization possibilities, communication is established with the nearest swarm object and the driver or a subordinate system is informed [5].

2.3.3: Internal and External security

On the basis of applicable law, the goal of internal and external security is to ensure the integrity of public life and to protect the state as an organizational and functional unit. The main actor in external security is the armed forces. The actors in internal security include disaster control, fire services, the police, the health sector, and the judicial system. Surveillance and networking play a key role here. In the military context, Network Centric Warfare has become an essential concept [5]. Network Centric Warfare uses comprehensive information exchange over networks that bridge the different branches of the armed forces to enable efficient communication among all elements involved in command as well as sensors and weapons. This extends down to the level of individual soldiers, who equipped with various sensors to capture their vital signs and environmental parameters themselves become part of an ad-hoc sensor network and thus supply information on conditions in individual sectors.

Monitoring systems that keep entire regions under surveillance fundamentally have the potential to monitor and collect data on people, too: Vehicles driving through thinly populated areas would be easily detectible by means of their exhaust fumes and heat generation. Used in this way, such a system would also be suitable for police and military purposes. This is particularly true if it is capable of functioning transnationally, as does the Brazilian monitoring system for the Amazon rainforest, Sistema de Vigilância da Amazônia (SIVAM). Much of the information that accrues in ubiquitous computing applications can also be used in the work of internal and external security. For example, monitoring data from telematics systems can be used in fighting crime.

2.3.4: Identification systems

Many electronic, administrative and business processes require the secure identification of persons. In the past, this has usually taken the form of state-issued identification papers. Progress in smart card and RFID technologies and improved biometric and cryptographic methods now allow digital systems to satisfy strict security requirements in personal identification. The increased need for security after the attacks on the World Trade Center on September 11, 2001in the U.S.A, and the desire for more efficient administrative processes have motivated many state institutions and some private ones to expedite projects in this area [5]. Other areas include health, entertainment and environment control [5].

2.4. Challenges of Ubiquitous Computing

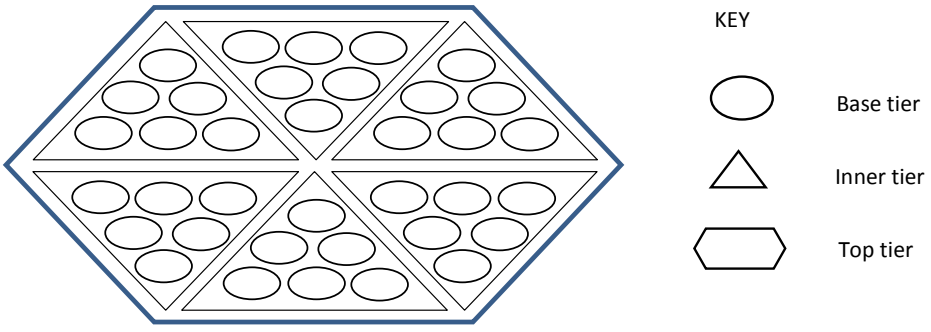

Figure 3.1: A proposed N-tier Ubiquitous Architectural Framework (NUAF)

Despite all the promises associated with ubiquitous computing it is still faced with the following challenges: Inadequate trust and lack of acceptance on the part of the user, Breaking of human privacy, security and privacy (Data protection), costs, technical obstacles (need for availability and reliability), lack of commercial concepts/business models, customer unwillingness to paying for ubiquitous computing services, negative environmental impact/high resource consumption, lack of legal regulation, lack of standardization, inadequate human-machine interface, energy supply, and shortcomings in human-to-machine interaction [5]. The research result however shows that environmental sustainability, resource consumption and legal regulation are minor challenges of ubiquitous computing's successful development. They assign a great degree of importance to standardization as the functional interplay of individual components as a key requirement of ubiquitous computing. The relevance of individual data protection and privacy varies depending on the specific application. For example, while privacy is not a primary concern in production and military applications, it is a critical challenge in security, communications and medical applications [5, 9].

3. THE PROPOSED UBIQUITOUS SECURITY SYSTEM

From the exposition of the features, potentials and applications of Ubiquitous Computing, it is easy to appreciate that the use of Ubiquitous technology can help proactively curb the menace of Boko haram. The issue then is which of the technologies or a combination of them can be used and how? To this end, we propose an n-tier Ubiquitous architectural framework (NUAF) for national policing. NUAF in its simplest form consist of the base-tier, inner-tier and top-tier as depicted in figure 3.1. NUAF is hierarchical and segregational i.e. the top-tier consist of several disjointed inner-tier which can also consist of one or more disjointed inner tiers and finally the base tier covers the smallest geographical unit of a nation or region like in the case of Nigeria, boot. We insist that no base-tier can belong to more than one inner tier and no inner tier can belong to more than one outer-inner tier and so on. The top-tier stands for nation or geographical regions (e.g. Nigeria, ECOWAS and EU).

The proposed framework is base-tier driven with ubiquitous devices mounted in strategic and unsuspecting facilities like GSM-mast, electric poles, buildings, road slabs and even trees. The ubiquitous devices which will incorporate among other ubiquitous technology, nanometer-scale electronic noses [10] and communicate in a peer-to-peer faction such that the failure of one does not cause the failure of part or the whole system. Obviously, ubiquitous systems are distributed systems and ubiquitous devices proposed are replicated computation. The segregation is to enable reliable, consistent and efficient communication of the distributed replicated computations strategies [2, 4].

As depicted in figure 3.2, on sensing an explosive element, the ubiquitous device can communicate with one or more ubiquitous devices and/or one or more Data Analysis Center (DAC), say at the police station; using group communication protocols [2]. It is the DAC that will interpret the captured data and help security agencies take appropriate intelligent decisions for necessary actions. The DAC, a distributed system is the actual security data repository that stores and manages the security data. The ubiquitous devices' data storage capability is transient though persistent. It is possible for a device to sense more than one explosive substances or explosive carriers simultaneously or in close succession.

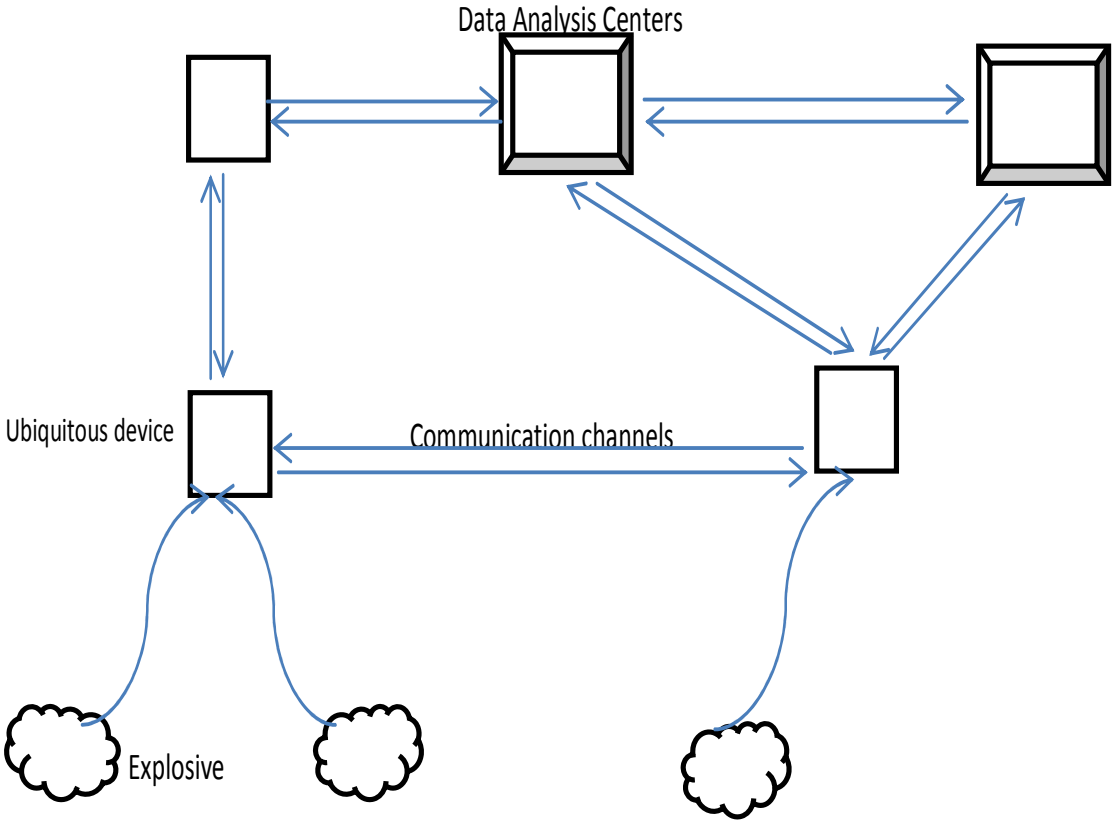

Figure 3.2: A schematic diagram of the base tier communication in NUAF

We anticipate that each ubiquitous device will consist of the following components: Intelligent nanometer-scale sensor, Network interface, Power source and Mini video camera. When the sensor senses any explosive substance, the device communicates same to nearby devices passing on to it the suspected substance and the geographic location of the carrier agent. The sensing of an explosive substance as well as a signal from a nearby device triggers the mini video camera to capture the carrier agent and its environment. It is important to note that depending on the components of the ubiquitous devices, NUAF can be applied to different security monitoring and tracking operations.

4. CONCLUSION AND RECOMMENDATIONS

Security is essential to human development and wellbeing, Nigeria in recent times has faced serious security challenges by terrorist groups (like Boko Haram) who use explosives as their major means of attack. Many measures have been put in place to curb this menace but all have proved to be ineffective. This paper explored the concepts and applications of ubiquitous computing and proposed a security framework based on ubiquitous technology - NUAF, that can help curb the menace of Boko haram sect in Nigeria. NUAF is a segmented n-tier hierarchical architectural framework for explosive monitoring and tracking.

NUAF can also be used for other security monitoring and tracking operations; depending on the component that constitute the ubiquitous device. NUAF is however a futuristic framework waiting for breakthrough in nanometer-scale electronic noses, energy generation, wireless network security, reliability and scalability. The Nigeria government should join in the research on nanotechnology and electronic noses as is presently being done by the government of United States, Canada and some European countries. A full adoption and implementation of NUAF by the Nigeria government and other regional government like the ECOWAS, EU and UN is strongly encouraged to curb terrorism in our world.

REFERENCES

[1] Adagba, O., Ugwu S. C. and Eme, O. I. (2012), "Activities of Boko Haram and Insecurity Question in Nigeria", Arabian Journal of Business and Management Review (OMAN Chapter), Vol. 1 No. 9, pp. 77 – 99.

[2] Briman, K. P. (2005), "Reliable Distributed Systems: Technology, Web Services, and Applications", USA: Springer-Media, 668pp.

[3] Chong, J., See, S., Sean, L. L., Koh, S. L., Theng, Y., and Duh, H. B. L. (2010), "Ubiquitous Computing, History, Development and Scenarios", IGI Global, retrieved online from http://www.igi-global.com/chapter/ubiquitous-computing-history-development-scenarios/37773 on 28th Dec. 2012.

[4] Coulouris, G. O., Dollimore, J. and Kindberg, T. (2005), "Distributed Systems: Concepts and Design", USA: Pearson Education, 772pp

[5] Gabriel, P., Bovenschulte, M., Hartmann, E., Grob, M. and Strese, H. (2006), "Pervasive Computing: Trends and Impacts", Germany: Federal Office for Information Security, retrieved online from https://www.bsi.bund.de on 28th Dec., 2012.

[6] Howard, M.L. (2011), "Pervasive Computing", USA: Nova Science, 244pp.

[7] Muhlhauser, M. And Gurevych, I. (2008), "Introduction to Ubiquitous Computing", USA: IGI Global, 19pp.

[8] Ogedebe, P. M. and Jacob, B. P. (2012), "The Role of Information Technology in Combating Security Challenges in Nigeria", Academic Research International, Vol. 2, No. 1, pp.124 – 130.

[9] Rocker, C. (2010), "Social and Technological Concerns Associated with the usage of Ubiquitous Technologies", Issues in Information Systems, Vol. XI, No.1, pp. 61-68.

[10] Rolfe, B. M. (2007), "Toward Nanometer-Scale Sensing Systems: Natural and Artificial Noses as Models for Utral-small, Ultra-Dense Sensing Systems", Advances in Computers, London: Elsevier Publishers, Vol.71 (Nanotechnology), 351pp.

[11] Scoutter, W. (2012), "Nanotechnology in Explosives Detection", Retrieved online from http://www.azonano.com/article.aspx?ArticleID=3089 on 28th Dec., 2012.

[12] Tronshow (2009), "Ubiquitous ID Architecture", Tronshow Project Symposium, retrieved online from www.tronshow.org/guidebook/2010/tron/e/u-05.html on 28th Dec., 2012.

[13] Udah, A. J. (2010), "Security: is Nigeria Safe", Nigerian-Swedish Chamber of Commerce, retrieved online from www.nigerian-swedish.com/pdf/SECURITY2.pdf on 27th Dec., 2012.

[14] Weiss R. J. and Craiger J. P. (2002), Ubiquitous Computing, Leading Edge, Vol. 39, No. 4, pp. 44 – 52.

ABOUT THE AUTHORS

Dr. Godspower O. Ekuobase is presently a Senior Lecturer in the Department of Computer Science, University of Benin, Benin City, Nigeria. He holds B.Sc., M.Sc. and Ph.D. in Computer Science from University of Benin, Nigeria. His research areas include Services Science, Service Oriented Computing and Web Services. Godspower is a member of ACM and IEEE Computer Society.

Mr. Ifeanyichukwu Eberechukwu Anyaorah is is presently an Assistant Lecturer in the Department of Computer Science, Auchi Polytechnic, Auchi, Nigeria. He holds ND in Computer Science from the Federal Polytechnic Nekede, Owerri, Nigeria and B.Sc. and M.Sc. in Computer Science from the University of Benin, Benin City, Nigeria. His research area is in Distributed Systems and Web Services.