Generic Architecture for Biometric and Digital Forensic Analysis

Ifeoma U. Ohaeri, Obeten O. Ekabua

Abstract*— Information Systems and Network Communications has become part of our everyday life. In recent times, there has been a massive growth in computer and electronic devices as well as network-based systems either for e-commerce, e-government or internal processes within organizations. Human beings can no longer be separated from electronic devices and the internet technology. The need for information security is increasing rapidly as a result of the amount of information made available on systems and networks which are connected on the internet. The dependence on information systems and the data that is stored, processed, and transmitted by them has recorded a tremendous increase in the rate of cyber-crimes; rise of information warfare, and threat of cyber terrorism which has even led many companies, organizations and even nations to thoroughly investigate the protection of its critical infrastructures from information, systems, and network based attacks. Therefore, it is very essential to provide an effective security measure and system that ensures the confidentiality, integrity, and availability of information systems, networks, and the services and resources made available. This can be achieved using biometric and digital forensic technology (BDFT).

***Index Terms*—About four key words or phrases in alphabetical order, separated by commas.**

I. INTRODUCTION

Security is currently a widespread and growing concern that affects all aspect of society: business, domestic, financial, government, and so on. The information society is increasingly dependent on a wide range of networks and systems whose mission is critical, such as air traffic control systems, financial systems, or public health systems [1]. Information is a critical asset of every organization due to their rapid adoption of IT (Information Technologies) into their overall business activities. This has increased the need for an effective management of the companies and institutions information. Currently, information is an asset that is as important as a company or institution's capital or work. In fact, this has born the reality of the need for information security and network management. In new generation companies and institutions, this reality is even more pressing because information one of their core business. Thus, the dependence on Information Systems (IS), and networks has skyrocketed in the last few years, hence there is need to effectively protect the information that is transmitted across these systems and networks in other to maximize their potentials [2].

Manuscript Received on December 2014.

Miss Ifeoma Ohaeri, Department of Computer Science, North-West University, Mafikeng Campus, Private Bag X2046, Mmabatho 2735, South Africa.

Prof. Obeten Ekabua, Department of Computer Science North-West University, Mafikeng Campus, Private Bag X2046, Mmabatho 2735, South Africa.

Therefore, there is no doubt that toady Information Systems and networks play a very important role in our society, economy, and also on critical infrastructures. Consequently, the potential losses that confront businesses and organizations that depend on heavily on these systems (hardware and software) have led to the argent situation of Information Security and Network Management (ISNM). The need to be properly secured inside and outside in other to harness their ever increasing dividends is the goal of this research work. We proposed Digital Forensic and Biometric Analysis for Information Security and Network Management. This is due to the current increase in the tendency of using Information Systems that are distributed over the entire internet which has resulted to the emergence of several new attacks and threats to security. This is an indication that the present-day Information Systems are very vulnerable to a host of threats and attacks such as social engineering attacks (phishing), and cyber-attacks from cyber terrorist, and hackers, including inappropriate use of the network assess by the authorized users. The tremendous growth of security in computing indicated in 2009 by ITU has led to the design and implementation of a large number of techniques, frameworks, models, and protocols by many researchers which are regularly updated by more researchers building on the platform. However, new innovations are proposed on frequent basis as the need for information security and network management cannot be over emphasized. Apparently, the current increasing complexity of Information Technology (IT) infrastructures and the permanent and global nature of security threats have made organizations and institutions all over the globe to review their approaches towards information security and network management. Suddenly, the need to improve internal security culture by establishing and maintaining proper security management process has become the concern of most organizations. Therefore, combating the emerging threats and attackers in today's dynamic. Information Communication Technology (ICT) environment requires a more effective security infrastructure designed and integrated using biometrics features. This will enable digital forensic investigations and findings. Biometric features guarantees easy identification of systems and networks hackers, and if they are identified they can be presented in court for prosecution. This will help reduce the rate at which crimes and attacks occur. Therefore, this research proposes Digital Forensic and Biometric Analysis for Information Security and Network Management. This will take a significant step in tackling information security and network management challenges [4].

II. BACKGROUND INFORMATION

Apparently, information security and network operations encompasses a lot of disciplines which can be applicable in military, political, and corporate spheres with the goal of gaining a competitive advantage. The International Standard Organization (ISO 17799) defines information as an asset that may exist in many forms and has value to an organization, industry or institution. The aim of information security is to effectively protect this asset in order to ensure business continuity, minimize business damage, and maximize return on investments. As defined by ISO 17799, information security is characterized as the preservation of: Confidentiality, Integrity methods, and Availability. Needs for information systems security and trust varies according to systems and networks but, the basic requirements include: confidentiality, integrity, and availability.

A. Confidentiality

This requirement of information system security ensures privacy and protection of data stored in a system or during transmission. It controls unauthorized profiling of users IDs. It ensures that sensitive information is not disclosed to unauthorized recipient, except the parties involved in the communication.

B. Integrity

This requirement ensures that data or information and programs are changed, altered, or modified in a specified and authorized manner. All modifications of information, data or programs are made by the explicit consent and authorization of the parties involved. This means that assets can be modified only by the authorized entities in authorized ways or to personal advantage.

C. Availability

This requirement assures that authorized users have continued and timely access to information and resources. It guarantees the proper functioning of all systems such that there is no denial of service to all authorized users. All assets are available and accessible to all authorized users at appropriate times. For instance, preventing an adversary from flooding a network with bogus traffic which delays legitimate traffic such as those containing new orders from being transmitted makes resources available. In addition, there is a requirement that cuts across these three for accountability that is - knowing who has had access to information or resources. It is apparent from this listing that security means more than protecting information from disclosure. Therefore, satisfying these security requirements requires a range of security services which includes; authentication, authorization, auditing, and non-repudiation.

i. Authentication: This is an access control measure that establishes that a message is from the source it claimed to be from and the party is indeed who he or she claimed to be. Generally it verifies both the identity and the authority of a party and prevents unauthorized access to information, system and networks. This is usually in form of password, a hardware computer-readable token, or a fingerprint.

ii. Authorization: This is a security measure that checks if a user is permitted to access the network services or perform certain tasks. This process grants a party the right of access and the privileges to granting of permission to a party to perform a given action (or set of actions). Consequently, information security can be defined as processes, and procedures to limit information access to authorized users, protect information against unauthorized modification, and ensure that information is accessible when needed. This definition stands whether that information is stored or transmitted on printed media, on computers, in network services, or on computer storage media [5]. Additionally, Information Security and Network Management (ISNM) can be described as operations, administration, maintenance, and provisioning (OAM&P) functions required to; provide, monitor, interpret, and control the network and the services it renders. Information is a data that has been processed and is being utilized with useful intensions or purposes. A user's raw detail is referred to as data, and when it is processed for useful purposes it is referred to as information. Systems are computers and electronic devices that are designed for communication. It all together forms a network when they are interconnected locally or globally to enable a wider coverage and fare sharing of information. Information systems and network security starts at the top and it is everyone's concern. Often times, security is taken to the rare of design and implementation of systems and networks. This results into systems and networks breakdown within a short time. Hence, security should be felt at all levels of systems and networks design and implementation for maximum productivity [6]. Attacks are easier, faster, and cheaper than protection and security. In fact, there are more experts in attacks than there are in protection and security because of its rewards. Developers are busy designing tools for systems and networks attacks; there are so many trainings on the use of sophisticated tools to discover systems and network vulnerabilities for exploitation. For this reason, the essence of security should not be overemphasized. It is important to adopt access control mechanisms that enhance an organization's ability to control access to assets based on several requirements. These requirements includes; business requirements and security requirements. Business requirements consist of various policy and access control mechanisms such as; policy controlling access to organizational assets based on the host and user management requirements. Host and User management consists of mechanisms to; register and deregister users, control and review access and privileges, management of authentication and authorizations profiles. System and network requirements consist of mechanism for: system and network access control, host access control, and application access control.

i. System and Network access control: This allows policy on usage of system and network services. When appropriate, the mechanism should authenticate nodes, authenticate external users, define routing, control network device security, Maintain network segregation or segmentation, Control network connections, and maintain the security of network services

ii. Host access control: The mechanisms (when appropriate) should automatically identify terminals, secure log-on, authenticate users, manage security profiles, secure system utilities, and enable terminal, user, or connection timeouts.

iii. Application access control: This mechanism limits access to applications based on user or application authorization levels. Access monitoring mechanisms monitor system

access, and system use to detect unauthorized activities. More so, mobile computing policies and standards addresses asset protection, secure access, and user responsibilities [7]. There is need for improvements on the present security methods and discoveries to implement the defined policies such that intruders and attackers can easily be identified and prosecuted in the law court. Moreover, as people and devices get interconnected globally there is need for reliable user authentication mechanism to establish that a person is who he or she claims to be. Therefore, determining identities to ensure that only authorized users of a specified facility are given access becomes a crucial issue. Also, supporting the law enforcement agents with computer-based evidences to determine who, what, where, when and how for proper representation of computer and digital crimes for legal actions. Obviously, a reliable user authentication mechanism is required to provide valid user identification because, until a suspect is proved guilty, he or she cannot be convicted. It is important to ensure that people does not commit crimes without getting the due penalties. Hence, security forms a vital aspect of information systems and networks. It is to be given the upmost priority in every system and network development cycle to ensure stability, productivity, and quality of service (QoS). Thus, Digital Forensic and Biometric Analysis for Information systems and network Management can be deployed for stronger information security and network management. [8].

III. RELATED WORKS

In the world of security, we may face a number of threats from attackers, from mis configuration of infrastructure or network- enabled devices, or even from simple unavailability or decrease in quality of service as a result of unpredicted behavior of the network. Majority of the world today has become network dependent and as such any loss of network connectivity and loss of services provided by such networks, the users are bent to suffocate and this can be potentially devastating to any business or organization [9]. It is extremely important to secure information system resources by ensuring that all the resources made available are well protected. Information security is not only a matter of usernames and passwords. It entails various regulations and data privacy and protection policies. There are some existing proposals on information security management already. All these are created by international organizations for standardization. The author in the paper titled "Aligning Security and Privacy to Support the Development of Secure Information Systems", presented a model that combines security concepts with methods for privacy requirements. The author did not provide methods that major on security and privacy of as a unified framework. It employed a typical case study that demonstrates the applicability of the work. More so, in the paper titled "Information Security Service Culture (ISSC). Information Security for End-users", the author presents a complementary part of information security, that forms the culture of information security management (managers and developers) in any company, organization, or institution. This serves as a guide to information security managers and developers to enable them formulate information security policies and controls that is best suitable for our today's technology, and end users. Furthermore, in the paper, titled "A Novel Identity-based Network Architecture for Next Generation Internet", the author designed network architecture for Next Generation Internet (NGI) that is capable of preventing operation traceability, and protects the privacy of communication parties while raising their identity to be a central element of the network. The architecture inherently supports the authentication and mobility of the parties involved in communication. The author exhibited the successful verification of the protocol security and showed its behavior in other to demonstrate its feasibility and scalability when applied on two different architectures. Moreover, another paper titled "Analyzing the Security Risks of Cloud Adoption Using the SeCA Model: A Case Study", The paper presents a single case study which describes a large Dutch utility provider in an effort to understand the facets of the Cloud and identify the risks associated with it. The SeCA model was used in an action research setting to analyze Cloud solutions and identify the risks with specific data classifications in mind. The results show how decision makers can use the SeCA model in several ways to identify the security risks associated with each Cloud solution per data classification. The research work further concludes that by using the SeCA model, a complete understanding of the security risks can be obtained on an objective and structural level. In addition, the paper, titled "The Modeling of a Digital Forensic Readiness Approach for Wireless Local Area Networks", demonstrates one of the most important challenges in WLAN digital forensics. This challenge is to intercept and preserve all the communications generated by the mobile stations and to conduct a proper digital forensic investigation. The paper attempts to address this issue by proposing a wireless digital forensic readiness model designed to monitor, log and preserve wireless network traffic for digital forensic investigations. The information needed by digital forensic experts is made readily available if it becomes necessary to conduct a digital forensic investigation. The availability of this digital information can maximize the chances of using it as digital evidence, and this reduces the cost of conducting the entire digital forensic investigation process. This is why the use of biometrics features for systems and network users is supported in this research work to enable a more easy and accurate identification. It proposes it as an effective mechanism for protecting networks, and various infrastructures of devices must be put in place to achieve an efficient quality of service, which is the reason for network security. Therefore, avenues to protect information systems and networks include digital forensic and biometric analysis. Digital forensic technology is a not a new paradigm in information technology security. It was innovated barely 40 years ago primarily for data recovery, and has relatively grown into an important part of many investigations. DF tools are readily available and are used on daily basis by the law enforcement agencies, the military, government organizations, and other private business transactions and industries. There has been rapid increase over the past decade in the developments of DF research, tools, and processes because people now rely on it on daily basis without knowing it.

The birth of DF brought a solution to crimes committed with computers such as phishing, bank fraud, money laundering, and child exploitation. Forensic tools have become such an important information assurance due to its capability to reconstruct cyber-attacks evidence for legal actions [1]. Furthermore, in 1987 Wood et al. related a story of two experts in local data recovery who worked for 70h to recover only copy of a highly fragmented database file that was unintentionally deleted by a careless researcher. In late 1980s utilities became widely advertised that could perform a variety of data recovering, including diagnoses [11]. In the early days forensic was majorly performed by computer professionals who work with the law enforcement agencies on ad hoc, case by case basis. Within the 1988 and 1990, Astronomer Clif Stoll was the most celebrated network forensic expert. The use of DF was limited because disk were small and evidences left on time sharing systems does not necessarily require recovery tools to extract them. It was only a few cases that require digital analysis media for extermination and cyber-attacks was not common. However, in 1983, the Federal Bureau Investigation (FBI) started a program called Magnetic Media Program to boast digital forensic but could only perform three (3) cases in its first year. In 1983 computer hacking was introduced as evidenced in the 1983 movie called "war games". Computer hacking was not a crime until the Computer Abuse Act of 1984 was passed in other to limit the need to subject systems and networks to forensic analysis. From 1999-2007 digital forensic exploded from being a window to see into the past via the recovery of residual data that was carelessly erased by a researcher into a criminal mind via recovery of emails and instant messages [11]. System and network forensic has brought the possibility of seeing crimes as they are being committed even several months after. Since 2008, digital forensic have gone global and it is so reliable to have left the lab into a television (TV) screen. Consequently, digital forensic is traditionally used in criminal investigations, casualty identification, medical exterminations, network intrusion detections, forensic expert testimony, repositories, consulting services, research and developments. Also it is emerging nontraditionally, in the areas of intelligence, counter intelligence, site exploitation, support to significant investigations, and others in other to overcome the full spectrum of threats and attacks that are increasing per second [12]. Furthermore, the requirements for the next generation DF were reviewed by Ricahard and Reussev in 2008. They emphasized on systems requirements. They argued that CPU cycles are wasted by inefficient system design and the inability to employ distributed computing techniques introduces significant and unnecessary delay. Generally, DF systems designers begin every new project afresh. Ayes came up with second generation computer forensic analysis at the digital forensic Research Workshop (DFRWS) in 2009. Mocas followed Ayers and proposed a framework to support theoretical underpinnings for digital Forensic research. The goal of the framework was to define a set of properties and terms that can be used as organizing principles for the developments and evaluation of digital forensic research. He emphasized that each and every digital forensic research must consider the following: context in which evidence is encountered, data integrity, authentication, reproducibility, non-interference, and the ability of proposed techniques to the approved minimization requirement [11]. More so, Pollitt reviewed fourteen (14) different models for digital forensic investigations. A large number of these models rely on the ability to make the best use of digital evidence that is collected. Moreover, Ray et al designed a proactive digital forensic system that is capable of predicting attacks and changes its collection behavior before it takes place. In addition, Brandfordt et al presented a mathematical model for deciding the content and frequency of proactive forensic event recorders. He augured that it is not wise to depend on "audit trails" and "internal logs" since the digital forensic will only be possible on future systems if the systems make proactive efforts at data collection and preservation. More so, an article on digital forensic Agenda was presented by Nancy et al. They explored research categories, topics, and problems in digital forensic and identified six (6) categories for digital forensic research as: evidence modeling, data volume, live acquisition, media types, network forensic, and control system [11]. However, this taxonomy requires thorough analysis accompanied by strategic reasoning. By this it is obvious that there is need for a better identity authentication mechanism to enable digital forensic analysis. Hence this research projects presents DFBA for Information Systems and Networks Security. DF no longer comes at a letter stage in investigation process after the evidence has been tampered with. Now it comes at the beginning of all investigations process. It is evident that DF is transiting from traditional services to an emerging and all-embracing and reliable information system and network security. Therefore, in this research we advocate the future of security by integrating digital forensic and biometric features in other to maximize systems and networks services and resources which propagate efficiency and quality of service (QoS) [1]. The term "biometrics" came from Greek and we can divide it into two aspects: "bio" which means life and "metrics" which means to measure. Biometrics is based on the anatomic uniqueness of an individual which can be used for biometric identification. These unique characteristics can be used on automated access control systems to prevent unauthorized access by checking unique physiological features or behavioral characteristics submitted with the one previously captured in the database to identify an individual. Biometrics was innovated many years ago with the first evidence when the when the cavemen signed their drawings using their fingerprints. Even the ancient Babylonians signed their business transactions which were in the form of clay tablets used the same very way. The first evidence of the use of biometric authentication recorded was in ancient Egypt. One of the administrators conducted an experiment on the systemized process of providing food to the workers during the construction of the great pyramid of Khufu. He made records of information about the workers such as; name, age, work unit, position, and occupation. He discovered later that they were cheating him, so he decided to also record the both the physical and behavioral characteristics. In the early days as far back as the 14th century the merchants in China used biometric authentication was rather popular among merchants when they simply used paper with ink to take palm prints and footprints of children to be able to recognize each and every one

of them and also differentiate one from the other. It was really interesting where and how biometric started and it is still transiting, becoming the most popular and widely accepted. Jaonnes Evangelista Purkinje, a Czech physiologist and biologist was the first who tried to categorize fingerprint patterns when he studied papillary ridges of hands and feet published and published his scientific work in 1823. Sir William James Herschel, a British officer in India, was the first European who used his fingerprints for identification in 1858. He believed that they were unique so he used them to sign documents. Also, in 1870 Alphonse Bertillon, an anthropologist who was looking for the way to identify convicted criminals not only used palm prints and footprints but also body movements and all kinds of marks on the body. This idea referred to as "Bertillonage", became very popular and was adopted in American and British police forces and this helped to minimize the circle of suspects. Apparently, Henry Fauld is considered to be the first European when he insisted on the meaning of fingerprints in the identification of criminals when he required explanations for a system to classify fingerprints, and produced very similar classification systems. Furthermore, in 1892 Sir Francis Galton published a book called "Finger Prints" where he categorized and described three main fingerprints patterns as: loops, whorls, and arches. He proposed the use of all ten (10) finger prints. The use of biometric especially the fingerprint continued to become more and more popular when a Bertillon system encountered a difficulty in identifying two identical twins, until the New York State Prison officially adopted a systematic use of finger prints in US for criminal in 1903. In 1904 it was adopted by St. Louis Police Departments in Kensas. Subsequently, the US Army adopted it in 1905 and in 1906-the U.S followed suit. Also the U.S Marine Corps used the fingerprints identification in 1908. Hence, the first automated use of fingerprint system was innovated in 1960s. It was adopted Federal Bureau Investigation (FBI) in 1969 when they tried to automate the process of fingerprint identification. In addition, Harmon and Lesk in 1965 birthed the era of face recognition where the eyes, nose, mouth, ears were located in photographs. In 1980 they used 21 specific subjective makers such as color of hair, thickness of lips to automate face recognition. More so, in 1974, the first hand geometry system came on board and Standford Research Institute and National Physical Laboratory started working on signature recognition systems. Eventually in 1980, the term "biometrics" began to be used generally to describe methods of automated human and person identification.The U.S Department of Energy started experimenting biometrics in 1983 at Sandia National Lab and the Department of Defense started the same experiments at Naval Postgraduate School and in 1985 the first retinal scanning was invented and used for secure access to the Defense Department in the Naval Postgraduate School. Gradually the middle of 80th state California adopted fingerprints for all driver license applications [13]. Consequently, as the use biometric technology was gaining ground, the first biometric association was formed in 1986 in the US called "International Biometric Association". Daugman of Cambridge University came up with the iris recognition technology in 1990. The United Kingdom formed the Biometrics Association in 1991. In 1994 the U.S. installed the boarding system which was based on hand geometry, and1997 witnessed the first Biometric Test Centre was founded which resulted in the adoption of the first biometric standards in 2002. However, till date the use of biometric has continued to increase as systems and network developers have discovered its functionalities in terms of: Universality- something that each person has; Uniqueness- something that separates this very person from others; Permanence- biometric measurement should be constant over time for each person; Measurability (collectability)- it should be easy to measure, should not demand too much time and costs; Performance- speed, accuracy and robustness; Acceptability- how well people accept biometrics; Circumvention- how easy it is to fool the system. As the value of information Systems and Networks grows rapidly the use of digital forensic and biometric technology becomes inseparable from our daily lives because it provides a means of readiness to two kinds of attacks such as: privacy attack and subversive attack. When the attacker gains access to the data to which he is not authorized it is referred to as privacy attack, and when the attacker gets the opportunity to manipulate the system files and disrupt the network it is referred to as subversive attack. Therefore, integrating biometric authentication will promote digital forensic technology by facilitating fast data analysis, easy evidence discovery, and also provide accurate identification of suspects. This will contribute in combating cyber –crimes and cyber – attacks [14].

A. Information System Security Challenges and Innovations

The term security and information systems are closely inked, and it indicates that the security of any organization or institution is as good as the security mechanism deployed. A secure information system is a sign of certainty that helps in generating value both within and outside the organization. Information Systems Security is a function whose mission is to establish security policies and their associated procedures and control elements over their information assets, with the goal of guaranteeing their authenticity, confidentiality, availability and integrity. Ensuring these four characteristics is the core function of Information Systems Security: Organizations are becoming conscious of the importance of having effective Information Systems and Networks, and managing them properly. Thus, there cannot be any useful information systems and networks without security management systems and the security controls associated with them. Therefore, it is very imperative for organizations and companies to implement security controls that will enable them detect and control any risk which they may be subjected to. However, implementing these controls is not enough, institutions and organizations should learn to manage information systems and networks over time so as to enable them react to new threats, risks and vulnerabilities in an immediate manner [15]. Information security and network management entails trust. It is very important that companies and institutions ensure that they maintain privacy when accessing and working with users' personal information or personal identifiable information (PII). In today's information society

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication Pvt. Ltd.

Privacy is a prime concern already. Privacy focus majorly on control mechanisms, but it is interrelated with, information security. There cannot be an effective privacy without a strong platform of information security. Systems and network users want to be assured that their identification profile and personal details are made private. Therefore, the challenge now is to effectively develop computing systems with privacy protection mechanisms [16]. This is why we proposed Digital Forensic and Biometric Analysis for Information Security and Network Management One of the widely accepted principles of management is that if an activity cannot be measured, it can cannot also be managed and analyzed. Therefore, metrics can be used as an effective tool for information security management (managers) to check the effectiveness of different security mechanism to confirm if they are administering the maximum security that is required of them. Many of the various security mechanisms in use today are not very efficient in ensuring that a system or network user is who he or she claims to be and is an authorized user of the facility it requests and yet they are been deployed. Though one hundred percent (100%) of security can never be achieved because of the nature of system and network vulnerability identification tools available, but improvement on current mechanisms is one of the goals of security. For this reason, we propose digital forensic and biometric analysis for Information System and network management. Also Metrics can be used to identify the level of risk associate with not deploying an effective security mechanism. This research tends to point out aspects of passwords authentication and identification which does not guarantee accurate user identification, and does not also enable digital forensic investigation. Information security is part of the overall network management principles required to; prevent the misuse, loss or inappropriate accessing, modification or disclosure of personal information, detect privacy breaches promptly, and be ready to respond to potential privacy breaches in a timely and appropriate manner. Information security and network security technologies protects systems and networks against theft and all forms of misuse of confidential business information, internet worms and viruses, all forms of systems and network violations, authorized intrusions, network downtime, service and network disruption and enables legal actions.

B. Biometric Technology

Biometric systems are directly connected to a person because they make use of an individual's unique feature for identification and authentication. Even if a biometric data of someone is altered or deleted, the main source of the data from which it was expected remains intact, and can neither be altered nor deleted. Biometric technology which includes figure 1, and figure 2, has been welcomed globally due to its potentials of easy authentication, and unique identification

It is more convenient especially, the use of finger prints readers and face recognition biometric systems. Apparently, there are no two persons in the world with the same face and same finger print. It is not possible for a person to deny the use of face and finger prints because there is no prove that someone else used your face or went out with your hands when you have them with you. Biometric data are efficient access control measures and it is a key element in digital forensic analysis. It helps to boast the level of security in information systems and networks. Also, it makes identification and authentication procedures more robust, fast, effective and convenient. The deployment of face recognition devices and finger prints readers as access control measures will help to solve the problem of individual untraced movement within a system and network. More so, it will contribute in a drastic reduction of cybercrimes and network attacks making security systems more reliable. Consequently, faces and finger prints can totally replace the numerous cards, codes, signature, and passwords which people carry around. Therefore, one of the efforts of this research is to establish a link between digital forensic and biometric features to enhance information systems and network security and provide quality of services. From forensic perspective, even more information can be extracted from the biometric access devices. The image in figure 4 shows a laptop with finger print authentication medium. The measure will find increasing application in securing laptops. The finger print sensor is the small rectangle to the bottom right of the keyboard. If the biometric data is stored in a database in a standardized way, it is possible to find statistical data, and have more information on the uniqueness of a biometric feature However, for any biometric system to be effective it must satisfy the following factors: accuracy, speed and throughput rate, acceptability to users, uniqueness, resistance to counterfeiting, reliability, data storage requirements, enrollment time, intrusiveness of data collection must be put into consideration. If the systems are implemented at banks, borders, entries of facilities, pay points, and others, identification can be more reliable because additional information is available on the location of a specific person at a specific moment. Therefore, it is expected that if biometric systems are properly implemented it will result in more reliable identification of persons to enable forensic investigations and legal actions [13].

C. Digital Forensic Technology

Digital forensics is defined as a scientifically proven method for the investigation of computers and other digital devices suspected to be involved in criminal activities and network attacks [3]. It was innovated as an avenue to suppress the increase of computer and network attacks. Proper digital forensic procedures and process model should be followed for its evidences to be admissible in a court of law for prosecution of offenders. Digital forensics applications cover several aspects which includes; the need for the law enforcements to produce the compelling and legally accepted evidences required for crime prosecution, the need for institutions and cooperation to identify and mitigate insider threats [14]. Tools for computer forensics is used to collect, analyse and extract evidence after intrusions. Demand for forensic techniques examination is already much greater than current capacity. Therefore, this research proposes digital forensic and biometric analysis for information security and network management. It aims at establishing that biometric feature authentication guarantees accurate user identification, and also enables digital forensic investigation should there be any security violation and attack. It provides legal evidences which are admissible in court for prosecution of offenders and attackers. However, it is evident that the growth in electronic transactions increases side by

side with malicious activities and network attacks. The rate of computer crimes is steadily in the increase, attackers and intruders are at liberty to exploit systems, and disrupt networks without the risk of suffering the consequences. However, combating these attacks that replicate on daily basis has become a major global concern.

Apparently, the research idea centred majorly on how to better identify users or parties to enable forensic investigations such that culprits (attackers and intruders) are identified and prosecuted in other to pay their due penalties. This research therefore, proposed Digital Forensic and Biometric Analysis (DFBA) for Information Systems and Network Security. It specifies the significance of biometric features such as face recognition and finger prints in forensic investigation. Also, it emphasizes that the use of biometric authentication will enable forensic findings and investigations [26]. However, in this research, DFBA is basically proposed to mitigate attacks and systems violation by identifying not only the attack but also who the offender is to support legal proceedings. By this, attacks are no longer rewarded but penalised [26]. Therefore, Digital forensic (DF) is referred to as a process to determine and relate extracted information and digital evidence to establish factual information for judicial review, and biometric is based on physical or behavioural uniqueness of a person [27]. Unique characteristics can be used to prevent unauthorised access to the system or network with the use of automated method of biometric control which verifies unique physiological feature or behavioural characteristics to identify a person, while analysis collects all data, evidences and findings to obtain an overview at a crime scene for the purpose of identifying and clarifying information gathered through the previous stages of investigation for further investigations and legal proceedings. Through analysis, we will justify that all data was captured accurately and common trends and patterns were identified. Apparently, this research intends to take security another step further to identify attackers and not just ward them off via access forbidden automated responses. This will go a long way in reducing the rate of attack and attack experts that are steadily in the increase [17]. The classical biometric systems that focused on face recognition and fingerprint technology are known for a long time. They are used for two different main tasks such as; access control and forensic investigation. We can refer to it as joint systems. In the description of the main concept of the Biometric Security System, the biometric features (data) must not only serve as access verification or identification, but can also be used for data protection to enable forensic investigations. We can ask, is it possible to generate some of the biometric features such as face and fingerprint or thumbprint for better forensic findings? There is enough information entropy in the fingerprint to generate suitable digital evidences. Therefore, we introduced the combination of Digital Forensic and Biometric Analysis as a more reliable security mechanism, using a thumbprint or fingerprint as a corresponding feature for identification, and extraction of digital evidence for legal proceedings. [30]. In forensic evidence analysis, the biometric devices can be important, since more information is available of the person who tries to access a building, a computer system or network. In cases with hacking this can be helpful if a suspect has been logged on with biometric data such as face and finger print [14]. Network forensic systems are concerned with capturing, recording, and analysis of network traffic for detecting intrusions and investigating them. Digital Forensic interprets and preserves all digital evidences in its most original form while proceeding further investigations, whereas, biometric systems are concerned with pattern recognition that operates by acquiring biometric data from an individual, extracting a feature set from the data acquired, and comparing this sample against an earlier registered template. Depending on the type of application the template may be stored in the system's database or on a token, such as a smart card. Biometrics techniques describe these unique distinct biological characteristics that identify a person and differentiate one from another. These biological or behavioral characteristics can be used for automated recognition [18]. Biometric verifies and confirms an individual's claimed identity by comparing the current submitted image with the previously captured image. The verification application includes both physical and logical access control while forensic is concerned with gathering and analyzing of physical evidence from crime scene to identify the culprits. Biometric is a reliable access control and authentication mechanism that can be applied in digital forensic. Advances in ICT, increased performance and availability of equipment at lower cost have paved the way for automated biometric recognition. Biometric applications may be categorized into three main groups such as: Forensic applications, Government application, and Commercial applications.

i. Forensic applications: This category can be used in criminal investigations, for corpse identification, parenthood determination, and others.
ii. Government applications: This category can be in personal documents, such as; passports, ID cards and driver's licenses; border and immigration control; social security and welfare-disbursement; voter registration and control during elections; e-Government, and others.
iii. Commercial applications: This category can be used for physical access control; network logins; e-Commerce; ATMs; credit cards; device access to computers, mobile phones, PDAs; facial recognition software; e-Health, and others.

Apparently, Biometric and Forensic can operate together to analyze human traits, and features at crime scene for proper identification of the culprits and its victims. Digital forensic and biometric over laps and support each other at crime scene to gather useful and positive identification for legal proceedings [19].

IV. INTEGRATING BIOMETRIC AND DIGITAL FORENSIC TECHNOLOGIES

Digital forensic and biometrics are tightly coupled. Forensic information can be available from biometric systems. This research intends to establish a link between digital forensic (DF) and biometric technology (BT). Also, establish a possibility of biometric based authentication enabling digital forensic investigation. It establishes that biometric features

provide a better access control, identification and authentication of any given party which helps in forensic investigation and digital evidence discovery. Digital forensic investigation involves a group of defined procedures and tasks for experimental purpose. This procedures and tasks are used to extract useful information from digital devices shown in figure 1 as evidences to commence legal proceedings in court. However, the procedures includes: preparation, data collection, examination data analysis, and reporting or presentation of findings. Preparation and data collection is the first phase in the process which is primarily to identify, label, record, and acquire relevant data from all possible sources of information. The second phase is examinations which involve forensically processing large amounts of collected data using a combination of automated and manual methods to assess and extract data of particular interest. The next phase of the process is analysis which is to analyze the results of the examination, using legally justifiable methods and techniques, to derive useful information that addresses the questions that constitutes the reason for conducting the data collection and examination. Lastly, is reporting the results of the analysis, or the presentation of findings which may include describing the actions used, explaining how tools and procedures were selected, determining what other actions need to be performed, and providing recommendations for improvement to policies, guidelines, procedures, tools, and other aspects of the forensic process [20]. However, analysis (data analysis) is one of the complex stages in digital forensic investigation. The analysis stage of forensic investigation involves; data analysis, survey, extraction and examination. Digital forensic as defined by the digital forensic research workshop (DFRWS) is the use of scientifically derived and proven methods towards the preservation, collection, validation, identification, analysis, interpretation, documentation, and presentation of digital evidence derived from digital sources for the purposes of facilitating or furthering the reconstruction of events found to be criminal or helping to anticipate unauthorized actions shown to be disruptive to planned operations. This definition embraces the broad aspects of digital forensic from data acquisition to legal actions. Analysis begins after data has been acquired or collected from the suspect system or crime scene. It basically involves critical extermination of the acquired data in other to identify evidence. Therefore, digital forensic analysis can be referred to as identifying digital evidence scientifically derived with proven methods that can be used to facilitate or further the reconstruction of events in an investigation [20][16]. Obviously, like any other investigation of events, to find the truth data must be identified in other to either verify existing data and theories or to contradict existing data and theories. Before both evidences can be extracted from a collected data, it must be thoroughly analyzed and identified. The task or challenge of digital forensic analysis is to identify the necessary evidence for legal proceedings in court [16]. On the other side, biometric identity based verification technology offers more reliable individual identification which supports digital forensic investigation. One of the questions this research tends to address is, how can biometric technology (BT) help DF perspective? It analyses a biometric situation while justifying the research objectives by providing answers to the research questions.

V. PROBLEM STATEMENT

The invention of the conventional security mechanism such as; user names and password – based authentication) mechanism emerged as a solution to mitigate authorized access to information (data) systems and networks to ensure privacy and protection. This created some level of confidence to electronic systems and device users, but the question is: can this security mechanism be trusted? Is it totally reliable? Of course, the answer is no. Over the years it has been discovered and acknowledged that password–based authentication mechanism can no longer guarantee maximum security of information, systems and networks due to the level of risk associated with it. Consequently, passwords are likened to "low-hanging fruits" due to how users choose passwords Often times users either chooses easy-to-remember PINs or passwords or they write them down for fear of forgetting them. This makes the passwords and PINs vulnerable to socially engineered attacks such as password sniffing, cracking and capturing. Sometimes the passwords are even completely forgotten, making the services inaccessible at urgent times. The interfaces between the information, systems, networks, and the users are routinely abused, as people have to remember many complex passwords and handle tokens of various types around. It is therefore difficult to ensure the confidentiality, integrity and availability of data in any communication which is the core fundamental requirement of any effective security mechanism [6] .More so; attackers commit crimes with ease without the fear of being cut because their actions are untraceable. These challenges have heightened the need to provide better individual identification and a more reliable user authentication mechanism to establish that a person is who he or she claims to be and he or she is an authorized user of a facility, information, system, or network. Therefore, this research proposes Digital Forensic and Biometric Analysis for Information, System, and Network security in other to create a reliable and secured communication domain. Digital Forensic extracts digital evidences by investigation from digital information, produced, stored, or transmitted by computers or electronic devices for legal proceedings. The use of biometric authentication will enable digital evidence discovery during a specified investigation procedures because it is easier to identify people by their features than with passwords and PINs [21].

VI. BIOMETRIC AND DIGITAL FORENSIC ANALYSIS ARCHITECTURE

This section focuses on the requirement analysis and design of biometric and digital forensic analysis architecture. It also specifies the different stages and phases that makeup the BDFA architecture. The BDFA architecture is introduced to provide a response to the problem statement and the main objectives of this research paper. However, the BDFA system architecture is used to describe the overall design, structure and behaviour of the system. It provides formal description and representation of the system in a way that supports the exact concept of the paper.

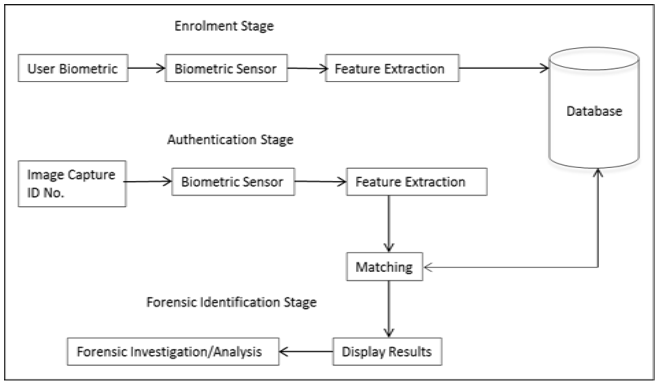

Figure 1. Biometric and Digital Forensic Analysis Architecture

The BDFA system consists of two main phases such as the biometric phase, and the digital forensic phase. The biometric phase consists of two stages which includes; the enrolment of the user biometric by the use of a biometric sensor into the database and the authentication of the user using the captured biometric. This is achieved by capturing the life fingerprint image using the biometric sensor and matching it with the minutia image stored in the database to verify and identify if the user is who he claims to be. It is basically developed for implementing fingerprint authentication and identification to impostors or any form of anomaly discovery. If any anomaly is discovered, digital forensic analysis process can then be employed in other to identify the suspect and as well the victim.

VII. Conclusions and Future Works

An important issue in designing a biometric system is the ability to determine how an individual is being recognized. This paper presents a generic architecture for biometric and digital forensic analysis. This depends largely on the context of the intended system. A biometric system can either be verification and authentication system or identification. This generic architecture is intended to be further used in developing a fingerprint authentication system that can effectively record the students' attendance using their fingerprint. This system will be introduced at lectures and laboratories. The system will take the attendance at both the beginning and at the end of the lectures to ensure that the students attend the lecture and were in class till the end of the lecture period. This will enable digital forensic analysis to discover any form of anomaly in the systems as well as identify the suspects and sometimes the victims. This will also prevent the inefficiencies encountered in the use of the traditional system where the students cheat by asking their friends to write their names or tick for them because they want to meet the required attendance that qualifies them to seat for the semester examination. This is because the lecturers are not able to monitor to ensure that they are writing their names only. Therefore, it is difficult for the lecturers to keep accurate record of the students' attendance. This makes the traditional means not efficient.

References

[1] L. Simson, and V. Garfinkel. "Digital Forensic Research: The next ten years." *Elsevier publications*, pp. 64-69, 2010.

[2] D. Mellado, E. Fernández Medina, "A Common Criteria Based Security Requirements Engineering Process for the Development of Secure Information Systems." International Journal of *Computer Standards and Interfaces*, vol. 29 (2), pp. 244 - 253, 2007.

[3] L. E Sánchez, A. S.O. Parra, "Managing Security and its Maturity in Small and Medium-sized Enterprises, "*Journal of Universal Computer Science*, vol. 15 (15), 3038 – 3058, 2009.

[4] Opdahl, A. L. and G. Sindre "Experimental comparison of attack trees and misuse cases for security threat identification." Information and Software Technology. In Press, Corrected Proof, 2008.

[5] B. Fal, A. M. "Standardization in information security management" *Journal of Cybernetics and Systems Analysis*, vol. 46, 181-184, 2010.

[6] X. Weiguan, W.Houkui, and H. Haoyi, .Donghong. "The Analysis of University Network Information Security System Based on Level Protection Model", in P*roceedings of the eight International Conference on computational Intelligence and Security*, 2012, pp.609-614.

[7] N. F. Doherty, and H. Fulford "Aligning the Information Security Policy with the Strategic Information Systems Plan." *Journal of Computers & Security*, vol. 25(2):vol. 10, pp. 55-63, 2006.

[8] R. S George Weir. "Issues and Perspectives", in *Proceedings of the first International Conference on Cybercrime, Security, and Forensics*," 2011, pp. 720-728.

[9] K. Anil, and A,Ross."Biometrics: A Tool for Information Security" *IEEE Transactions on Information Forensic, and Security*, vol. 1, June 2006.

[10] Daniel Mellado, Daniel Mellado." An Overview of Current Information Systems Security Challenges and Innovations."International Journal of Universal Computer Science, vol 18, pp.159-1608, 2012.

[11] M.F. Islam, M.I.Nasrul."A Biometrics-Based Secure Architecture for Mobile Computing*." IEEE Transaction on Biometric Authentication*, vol. 8, pp. 520-528, 2009.

[12] H. Singh Lallie. "An Overview of the Digital Forensic Investigation Infrastructure of India, *Digital Investigation - Online publication*. pp. 1742-2876, March, 2012.

[13] A. Martin, C. L. Wilson, and M. Przybocki, "An Introduction to Evaluating Biometric Systems," *IEEE publication for National Institute of Standard and Technology*, pp. 158-156, 2000.

[14] N. S. Sargur, C. Huang, S. Harish, V. Shah. "Biometric and Forensic Aspects of Digital Document Processing," 2010, pp. 720-728.

[15] W. V. Staden, and M. S. Olivier. "On Compound Purposes and Compound Reasons for Enabling Privacy." *Journal of Universal Computer Science*, vol. 17 (3), pp. 426-450, 2011.

[16] G. Pangalos, C. Linoudis, and I. Pagkalos." The Importance of Cooperate Forensic Readiness in the Information Security Framework," in *Proceedings of the IEEE Workshop on Enabling Technologies infrastructure for Collaborative Enterprise"* 2010, pp.12-18.

Ohaeri Ifeoma U, holds a BSc (Hons), and MSc, degrees in Computer Science and Information Systems in 2006, 2012, and 2013 respectively. She is currently a PhD degree candidate in Computer Science atNorth-West University, Mafikeng Campus, South Africa. Her research interest is in Information Systems and Networks Security, Software Engineering, Wireless Networks, and Routing Protocols, Cognitive Radio Networks, and Next Generation Networks.

Obeten O. Ekabua, is a Professor and Departmental Chair of the Department of Computer Science in the North West University, Mafikeng Campus, South Africa. He holds BSc (Hons), MSc and PhD degrees in Computer Science in 1995, 2003, and 2009 respectively. He started his lecturing career in 1998 at the University of Calabar, Nigeria. He is the former chair of the Department of Computer Science and Information Systems, University of Venda, South Africa. He has published several works in several International and National journals, and also in several career conferences. He has also pioneered several new research directions and made a number of landmarks contributions in his field and profession. He has received several awards to his credit. His research interest is in software measurement and maintenance, Cloud and GRID computing, Cognitive Radio Networks, Security Issues and Next Generation Networks.