Advances in Science and Technology, Vol. 4, No. 1, March / April 2010, pp 11 - 31

Design and Implementation of an Automatic Examination Screening System (AESS)

Chukwuemeka Etus[1] and Felix K. Opara[2]
[1]Department of Information Management Technology [2]Department of Electrical and Electronic Engineering
Federal University of Technology, Owerri, Nigeria.
(Submitted: September 14, 2009; Accepted: January 6, 2010)

Abstract

Automatic Examination Screening System (AESS) is a computer – based database management information system designed and implemented for higher institutions in Nigeria to assist lecturers and security personnel in the prompt detection of the presence of unqualified students and impersonators in the examination halls. The AESS system is an automatic software – based system having two major parts: the hardware and the software, respectively. The hardware includes the PC computer, fingerprint scanner and the web camera (webcam) biometric devices. The later two devices serve as input and data capture devices to the former, which is a fast data processing computer and multimedia system. Again, structured programming method of software development was adopted as the software design technique for AESS Systems. The software designed and developed includes; the visual basic input and output program forms with their flowcharts, and then the Microsoft access database. The AESS system designed and implemented is a veritable, flexible, reliable and effective registration, screening and information management solution for the combat of examination malpractices on campus in a more organized and coordinated manner.

Keywords: Automatic Examination Screening System, Management Information System, biometric devices, software–based system, stand-alone system, distributed wireless system.

1.0 Introduction

Conducting examinations in Nigeria universities has become a very stressful process due to the fact that the number of students in the institutions exceeds the staff available to manage them. The lecturers barely know the number of students in their classes let alone their names. This has led to conducting examinations being bedeviled by such malpractice as impersonation and their likes. It is hard for one to effectively identify by sight students (identical twins, triplets and their likes), who come to take examinations since they are too many. Again, students are in the habit of avoiding school and departmental fees payments. These debts run into huge amounts which would have been used for administrative and infrastructural bills. Most times, it may be difficult to, at a glance, identify those that have completed all their necessary payments and those that have not.

Known methods of authentication like the use of identification (ID) cards have failed since the identification cards can be faked. Furthermore, with the advent of Integrated Circuit (IC) technology and various levels of integrations, especially the Very Large Scale Integration (VLSI), automatic microprocessor based screening systems were designed and implemented [Paul, Alane, and Ari, 2004]. These have tremendous screening and control capabilities due to their high reliability and flexibility at the design and implementation stages, but without database. These systems operated with punched cards, codes and voice sensors with limited securities, capabilities and efficiencies. Therefore, it is now pertinent to put in place an automated database system which would effectively manage the students' information, authenticate and identify them before they enter the examination halls. And since the students' information includes their payment status, it is ensured that not only genuine students, but also students who are up-to-date in their payments, take examinations. Hence, the Automatic Examination Screening System (AESS) Machine is hereby proposed as a possible solution to handle students' examination screening exercises with its attendant challenges and problems.

2.0 Literature Review on AESS Considerations and Applications

This section gives concise literature review on AESS

predecessor systems, and AESS system technology, hardware, software, network, and human-computer interface / interaction considerations.

2.1 Ouick Review of AESS Predecessor Systems

Prior to the advent of computerized access control system, authorized personnel in establishments and high security facilities had to present identity cards to security personnel at the entrance to these establishments or facilities before they were granted access into the establishment or facility**.** This system of authentication had its pitfalls, the major one being the issue of identity theft. Identity theft is a situation where a person assumes the identity of authorized personnel to gain access to a secured facility, information or an establishment (Hornby, 2000). The identity cards can be stolen or faked by identity thieves and used to illegally gain access into restricted areas. Hence, this was a much unsecured method of preventing unauthorized access. Alternatively, systems involved entering a combination of numbers and characters known as personnel identification number (PIN) known to the authorized personnel on a computerized interface. But the use of PIN has password guessing as its short coming. Generally, the methods of granting access to a restricted area can be classified into three(3) namely (Fingerprint Basics, 2009): (a) What you have – where tokens are used such as identity card with a magnetic strip, passport or access card, typical of the first systems mentioned above. (b) What you know – where it is required to enter a password, as seen in the second system described above. (c) Who you are – where physical (biometric) attributes such as fingerprints, retina patterns, voice identification, are used to grant access to users. Of all the three, the biometric systems offer a more reliable system with less susceptibility to intrusion by unwanted persons.

Since September 11, 2001 tragic event in the United States of America, there has been a great deal of interest in using biometrics for identity verification (US GAO release, 2002), particularly acute in the areas of visa and immigration documentation and government-issued identification card programs (STGISC release, 2001). Soon after the attack, Larry Ellison, head of California-based software company Oracle Corporation, advocated the deployment of mandatory national ID cards with fingerprint information to be matched against a national database of digital fingerprints to confirm the identity of the ID card carriers [Bowman, 2000]. There has been a recent discussion between the United States and the European Union concerning the creation of biometric passports. Biometrics is so closely bound to a person, more reliable and not easily forgotten, lost, stolen, falsified, or guessed. Hence, biometric systems is been introduced to forestall the discrepancies inherent in the previous systems. This is because biometric identifiers rely on unique biological information about a person, for example, a 3-D image of the individual's hand, a scan of the person's iris, a fingerprint, a voice print or a facial image, used to recognize individuals by the sound of their voice, color of their eyes, shape of their faces, and so on. Devices using biometric identifiers attempt to automate this process by comparing the information scanned in real time against an "authentic" sample stored digitally in a database. The technology had several teething problems, but now appears poised to become common features in the technological landscape.

2.2 AESS Technology Considerations and Applications

AESS majorly implements biometric technology. Biometric is defined as the "measure of an individual's unique physical or behavioral characteristics to recognize or authenticate identity" (Halstead and Bornby, 2001). Biometric technologies are therefore defined as "automated methods of identifying or authenticating a living person based on his physiological or behavioral characteristics" (Fingerprint Basics, 2009). It is necessary to "automate" because without it, we also would be desirable of a variety of very common but significantly less reliable identification such as inked fingerprint on an ID card (badge) (Fingerprint Basics, 2009]). The term in any biometric access control implies that three major components are present: (a) A mechanism to scan and capture a digital or analog of a living personal characteristics; (b) Compression, processing and comparison of the image; and (c) Interface with the application systems. These pieces can be configured in a variety of ways for different situations.

Again, the most important aspect of biometric technology is the identification and authentication aspect. In the effort to clarify the difference between identification and authentication, Dr George Tomko (a leading Canadian researcher in the field of biometric phonics), describes identification as "a process of matching physiological or behavioral characteristics of a person to an established pre–confirmed record" (Halstead and Bornby, 2001). He further describes it as a "one–to-many" (or "1:N") search process. The question answered by the machine is "Do I know you?" The search algorithm searches a database and returns a likely list of candidates that has been previously entered in the system. On the other hand, the submitted identification characteristics are used to authenticate the individual by matching them with those existing in the database. This he called a "one–to–one" (1:1) search process, where the question answered by the machine is "Are you who you claim to be?"

Considering the term "living person", the question being answered is "what if the intruder uses a latex finger, digital audio tape, prosthetic eye, etc?" Many, but not all systems include methods of determining whether the characteristics presented are alive, thus separating the field of biometrics from the forensic identification field; though basic principles transcend both fields. A final point about the definition is the examination of physiological and behavioral characteristics. A physiological characteristic is a relatively stable physical characteristic, such as fingerprint, iris pattern, and blood vessel patterns on the retina. This type of measurement is basically unchanging and unalterable without significant duress. A behavioral characteristic is more like a reflection of an individual's physiological makeup majorly influenced by physical traits such as sex and size, which includes signature, keystroke patterns (how one types on a keyboard) and voice. Because of the variability over time of references (database) each time they are used, generally, behavioral biometrics work best with regular use.

The differences between physiological and behavioral methods are important for several reasons. Apart from injury, the fingerprint of an individual is the same day in and day out. The voice however, is influenced both by controllable actions and psychological factors. Developers of behavior based systems, therefore, have a tougher job adjusting for intrapersonal variations. For instance, it is easier to build a machine where you place your hand every time for identification than it is to build algorithms that take emotional states and little variations into consideration. Also, physiological systems tend to be larger, more expensive and may be threatening to user. Because of these differences, no biometric technology can serve all security needs. Given the accuracy of current technology, a number of scientists have pointed out that biometric systems based solely on a single biometric system may not always meet performance requirements" (Fingerprint Basics, 2009). The easiest solution to this is the use of multi-biometrics from which "data from multiple and independent biometric identifiers are fused; reinforcing the identity of a subject." (Halstead and Bornby, 2001).

The most widely used biometric is the fingerprint, which is a tiny specific adaptation form of patterns of "ridges" and "valleys" on our fingers. These patterns also make it easier for the hands to grip things, in the same way a rubber tread pattern helps a tire on the road.. This is because each person has a unique, easily accessible identity design, which represents him/her alone on his/her finger tips. The genetic code in DNA gives general orders on the way

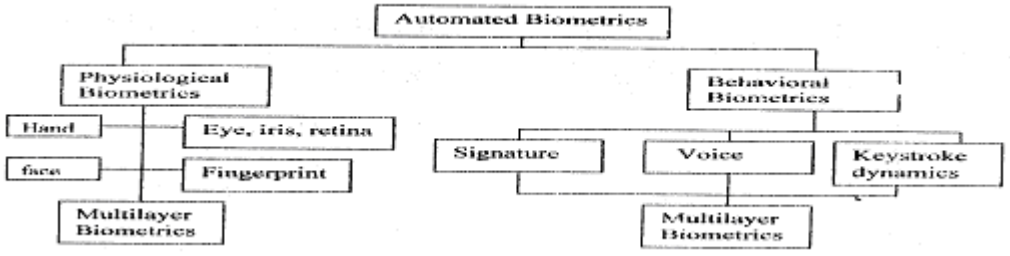


Figure 1: Biometric technologies

skin should form in a developing fetus, but the specific way it forms is a result of random events. The exact position of the fetus in the womb at a particular moment and the exact composition and density of the surrounding amniotic fluid decides how every individual's ridge and valley would form (STGISC release, 2001). So, in addition to the countless things that go into deciding our genetic make-up in the first place, there are innumerable genetic and environmental factors influencing the formation of the fingers. Just like the weather conditions that form clouds in the coastline of a beach, the entire development process is so chaotic that, in the entire course of human history, there is virtually no chance of the same exact pattern forming twice. Consequently, fingerprints are a unique marker for any person.

A typical fingerprint (Figure 2) comprises of ridges and valleys as earlier mentioned. The ridges are the dark areas of the fingerprint while the valleys are the white areas that exist between the ridges. Many classifications are given to patterns that can arise in the ridges and some examples are given in Figure 2 above. These points are also known as the minutiae of the fingerprint with some type of orientation - arch, right loop, left loop, and whorl - to help determine the core. The most commonly used minutiae in current fingerprint recognition technologies are ridge endings and bifurcations because they can be easily detected by only looking at points that surround them. Extensive research has been done on fingerprints in humans. Two of the fundamentally important conclusions that have risen from the research are that fingerprints of individuals are unique, and also that a person's fingerprint will not naturally change structure after about one year of birth. In practice two humans with the same fingerprint have never been found - even the fingerprints in twins are not the same. However, while two fingerprints may look basically the same at a glance, a trained investigator or an advanced piece of software can pick out clear, defined differences. These are the basic ideas of fingerprint analysis, for both crime investigation and security. A fingerprint scanner's job is to take the place of a human analyst by collecting a fingerprint sample and with the aid of an application program, detect those unique features that combine to make a unique print (Jain *et al.*, 2004), and use them to identify the person by comparing them to other samples on record. Let's find out how fingerprint sensors / scanners do this.

2.3 AESS Biometric Hardware Considerations and Applications

Biometric devices employed in AESS include fingerprint identifier and web camera. Fingerprint identifiers (sensors device or scanners) were used due to their ease of data capture and accuracy rate when compared to others biometric identifiers. Fingerprint identifiers are used for scanning fingerprints, and most of its techniques fall under the categories of optical, capacitive, ultrasonic, temperature, and pressure sensing and scanning (STGISC release, 2001). Fingerprint scanning (image acquisition) involves many of the algorithms that require a linear scan of the fingerprint image by moving a fixed size window across the picture in a grid-like pattern (see Figure 9b). Bank of Gabor filters (Klein and Beutter, 19992) oriented to different angles are applied to the fingerprint image to clean (preprocess) it from noises that can result to false alarm or authentication mistakes. The preprocessed fingerprint become enhanced, giving stronger assurance that using such data could lead to faster and stronger certainty of matching (see Figure 9a for the matching algorithm flowchart). A June 2004 report (Jain, Ross and Prabhakar, 2001) by National

Figure 2: A typical fingerprint

Institute of Standards and Technology (NIST) showed that fingerprint identification systems have an accuracy rate of 98.6 percent when one fingerprint is used, while the accuracy rises to 99.6 when two fingerprints are used and then to 99.9 percent when four, eight and ten fingerprints are used. However, the report also showed that the accuracy rate for fingerprint identification drops as people's age increase, especially for those more than 50 years old, yet it has remained the most reliable till date.

Another biometric hardware used is the web camera (webcam), which is a web-based continuous adaptive monitoring, video and picture capturing device, connected to computer or computer network, often using USB or, if they connect to networks, use Ethernet or Wi-Fi (Wikipedia, 2009). The term monitoring is used explicitly to depict the task of fetching new information relevant to one query resulting in a still image, or to several related queries, resulting in a video stream. Recently, Apple and other computer hardware manufacturers began building webcams directly into laptop and desktop screens (Linux release, 2009), hence reducing the need to use external Universal Serial Bus (USB) or Firewire webcams. Webcams are well known for their low manufacturing costs, flexible and user-controlled applications and games, which includes tracking of video and picture features (including faces, shapes, models and colors observation and tracking), still image / Picture capture, videoconferencing, video security, and aggregators applications (Wikipedia, 2009).

2.4 AESS Software Considerations and Applications

AESS consist of a Database Management System (DBMS) – a software program that typically operates on a database server or mainframe system to manage the creation, maintenance and reporting of data by accepting and responding to queries from users, and are used to provide users with simultaneous access to a database (Opara, 2003). It accepts data input, stores that data for later retrieval and provides query languages for searching, sorting, reporting, and other "decision support" activities that help users correlate and make sense out of collated data. DBMS have a number of common features which include data dictionary, utilities, security, query languages. Relationally organized databases (Samuelson, 2006) can be created with DBMS applications such as Microsoft Access, mySQL, Oracle, dBASE, or Paradox, which have the necessary tools to organize, manipulate, and locate structured information (records, tables or objects). DBMS may be configured in many ways: (i) a stand alone system with a single user (e.g. a single user PC based application); (ii) many users working at dumb terminals connected to a central machine (e.g. a traditional terminal - mainframe environment); (iii) a network of intelligent workstations communicating with a central server (a "client - server" architecture); or (iv) a network of intelligent client workstations communicating with an application server, which in turn is communicating with the DMBS.

In each of the above configurations, the database itself may reside on one server machine, or be distributed amongst many independent servers, with a collection of "persistent" data organized in multiple related files dependent on one another and from one another in the sense that they keep occurring in every record concerned with the particular program, hence making data maintenance easier and also saving auxiliary space. Also, AESS application software design considerations follows software development life cycle initially proposed by (Gorshie, 1986), in top-down design approach, best illustrated and explained using system flowcharts (as used in AESS design in section 3 of this work) (Pratt and Adamski, 1987).

The software security issues considered in the cause of this work includes defensive programming password policy, and authentication. Defensive programming is a form of defensive design in software intended to ensure the continued function of a piece of software in spite of unforeseeable usage of the said software (Wikipedia, 2009). In defensive programming, the programmer never assumes a particular function call or library will work as advertised, and so attempts to handle all possible error states in the code without allowing any bug-looking aspect of an application, because if the application contains a known bug, Murphy's Law dictates that the bug will occur in use (Wikipedia, 2009). The technique is used especially when a piece of software could be misused mischievously or

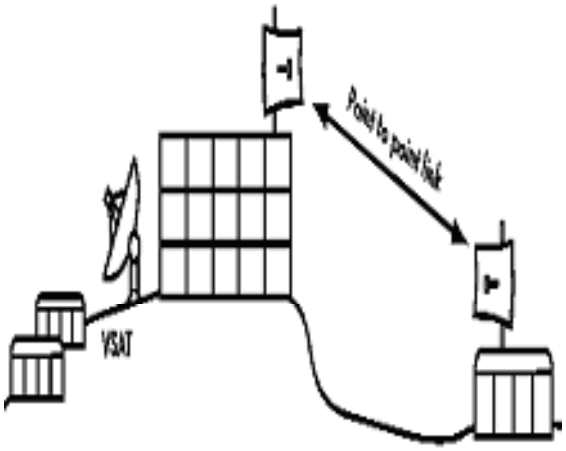
inadvertently to catastrophic effect; hence, defensive programming approach improves software HCI and source code, in terms of: (a) General quality – by reducing the number of software bugs and problems; (b) Comprehensible source code – by making the source code readable and understandable enough to be approved in a code audit; and (c) Predictability - by making the software behave in a predictable manner despite unexpected inputs or user actions.

On the other hand, some networks may require users to provide a password or a random number from a security token, by employing password policy. Password policy, as part of an organization's official regulations, is a set of rules (advisory or mandated by technical means) designed to enhance computer security by encouraging users to employ strong passwords and use them properly; often taught as part of security awareness training. The level of password strength depends, in part, on how easy it is for an attacker to submit multiple guesses, such that while some systems limit the number of times a user can enter an incorrect password before some delay is imposed or the account is frozen, some other systems make available a specially hashed version of the password for validity check (Microsoft, 2002). Enforcing password policies (usually by security administrators delegating a set of rules to end-users) either done by mouth approach or by creating your own custom passfilt (Egbe, 2003), can be a real issue of many headaches in any network setting, for which care must be taken to ensure complete authentication.

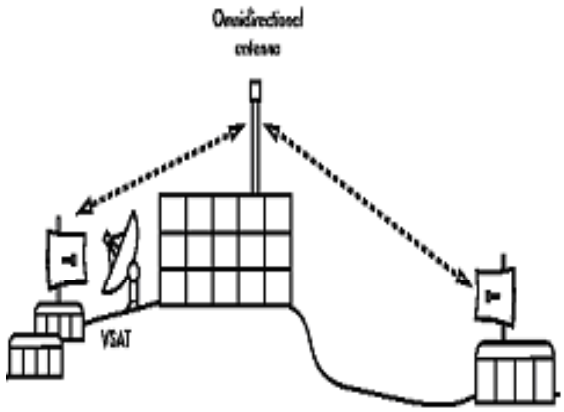
Again, the U.S. Government's National Information Assurance Glossary (Wikipedia, 2009), defined authentication as the act of establishing or confirming something (or someone) as authentic, real or genuine; that is, that claims made by or about the subject are true. This might involve confirming the identity of a person, the origins of an artifact, assuring that a computer program is a trusted one, or establishing the identity of an originator or receiver of information. Authentication can be weak when it relies on one authenticator, or strong when relying on two or more authenticators based on layered authentication approach where a combination of methods is used, e.g., a bankcard and a PIN, which is a two-factor authentication. Authentication can be location-based - such as that employed by credit card companies to ensure that a card is not being used in two places at once, or time-based - such that it only allows access during normal working hours or certain periods of time. Basically, human authentication factors (a piece of information used to **authenticate** or verify a person's identity on appearance or in a procedure for security purposes and with respect to individually granted access rights) are generally classified into three (3) in the order of strength of allocation (Wikipedia, 2009). They are as follows: (a) ownership factors - something the user has (e.g., wrist band, ID card, security token, software token, or phone); (b) knowledge factors - something the user knows (e.g., personal identification number (PIN), password, or pass phrase); (c) inherent factors - something the user is or does (e.g., fingerprint or retinal pattern, DNA sequence, signature or voice recognition, unique bio-electric signals, or any other biometric identifier).

2.5 AESS Network Considerations and Applications

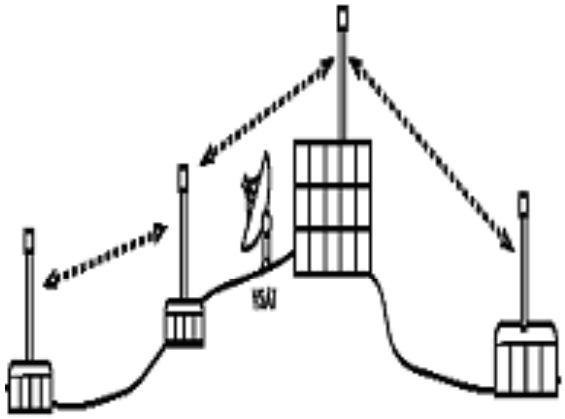
AESS is deployable over electromagnetic wave (EMW) networks (also called wireless or radio communication networks), which are the prime means of information broadcast and information exchange in several applications nowadays. These include radio, cell phones, infrared networks, wireless LANs, and Internet, among others. In general, wireless technique needs no physical connecting wires, hence, suitable for remote and mobile locations and personal services. During transmission, antenna radiates EMW energy (forces) into the medium (air), and for reception another antenna picks up EMW from surrounding medium in particular frequencies (wave swings or beats), carrying information [Bantz and Bauchot, 1994]. The frequency bands are chosen according to the distance and geographical conditions, while the waves are modulated for bearing coded information and demodulated to extract the information. As seen in Figures 3(a), (b) and (c); there are two categories of wireless communication: Directional (point to point) and Omni-directional (all directions). Directional wireless communication has frequencies range of 2GHz to 40GHz, commonly referred to as the microwave frequencies. The antenna used here are parabolic disc-shaped, the waves are directional and best suitable for point-to-point transmissions in



a. Central VSAT sent by point-to-point link to remote site (The VSAT is a broadband wireless connection that connects to the internet).



b. Central VSAT now shared by multiple remote sites (All three sites can also communicate directly at speeds much faster than VSAT).



c. multipoint-to-multipoint mesh (Every point reach each other at very high speed, & use the central VSAT to reach the Internet.

Figure 3: Wireless communication facilities illustrated

terrestrial and satellite communication. Omni-directional broadcast uses frequencies in the range of 30MHz to 1GHz, also called the broadcast radio range for area transmission.

The wireless data networks can be classified according to their coverage areas. The smallest coverage area is termed Wireless Personal Area Network (WPAN), where the network is limited to an office. The next class is Wireless Local Area Network (WLAN) which connects users in and out of a building, and even connects within a community (i.e. a wireless community area network roams and serves an industrial or university campus community). A wireless metropolitan area network (WMAN) connects the residents and visitors to a city, and finally, the most extensive network is a Wireless Wide Area Network (WWAN), which connects an entire country.

In 1990, the IEEE 802.11 was formed with a charter to develop a MAC protocol and physical medium specification for wireless LANs [Bantz and Bauchot, 1994; Pahlavan, Probert and Chase, 1995; Crow et al, 1997]. There are many protocols in the 802.11 family, and not all are directly related to the radio protocol itself. The IEEE 802.11 wireless LAN sometimes called Wi-Fi, is composed of a series of specifications as shown in figure 5(a), to provide wireless LAN services that are consistent with 802.3 Ethernet network. The three IEEE802.11 wireless standards currently implemented in most readily available gear are: (i) **802.11a:** ratified by IEEE on September 16, 1999, uses ***Orthogonal Frequency Division Multiplexing*** (***OFDM***) modulation scheme, has a maximum data rate of 54Mbps (with actual throughput of up to 27Mbps), and operates in the band between 5.745 to 5.805GHz and between 5.150 to 5.320GHz. The high frequency means shorter range compared to 802.11b/g at the same power thereby making it incompatible with them. 802.11a is not nearly as popular as 802.11b/g with relatively unused spectrum when compared to others, legal for use in a few parts of the world, and its equipments quite inexpensive [Bantz and Bauchot, 1994]. (ii) **802.11b –** also ratified by the IEEE on September 16, 1999, uses ***Direct Sequence Spread Spectrum*** (***DSSS***) modulation in a portion of the ISM band from 2.400 to 2.495GHz, with a maximum rate of 11Mbps (and

actual usable data speed of about 5Mbps), and is probably the most popular wireless networking protocol in use today with millions of supporting devices shipped since 1999. (iii) **802.11g -** finalized in June 2003 but now the de facto standard wireless networking protocol (despite its late arrival as it now ships as a standard feature on virtually all laptops and most handheld devices), uses the same ISM range as 802.11b, but uses ***Orthogonal Frequency Division Multiplexing*** (***OFDM***) modulation scheme, has a maximum data rate of 54Mbps (with usable throughput of about 22Mbps), and can fall back to 11Mbps DSSS or slower for backwards compatibility with the hugely popular 802.11b.

Until recently, wireless LANs was in little use due to its high price, low date rates, occupational safety concerns and licensing requirements (Bantz and Bauchot, 1994). Having addressed these problems, the popularity of wireless LANs have grown rapidly into four application areas: LAN extension, cross building interconnects nomadic access and adhoc networks (Pahlavan, Probert and Chase, 1995; Crow *et al.*, 1997; Keshav, and Sharma, 1998). These use network protocol data unit treated independently and routed from source End System (ES) to destination ES through the networks using typically two protocols operating in each ES and router at the network layer (an upper sub-layer providing inter-networking function and a lower sub-layer providing network access). The protocol source and destination address fields in the address headers contain a 32-bit address which consists of a network identifier and a host identifier. The address is coded to allow a variable allocation of bits to specify network and host as shown in figure 6. This encoding provides flexibility in assigning addresses to hosts, allowing a mix of network sizes even on the Internet (Lammle, 1999). The three (3) principal network classes are best suited to the following conditions: (a) Class A - Few networks, each with many

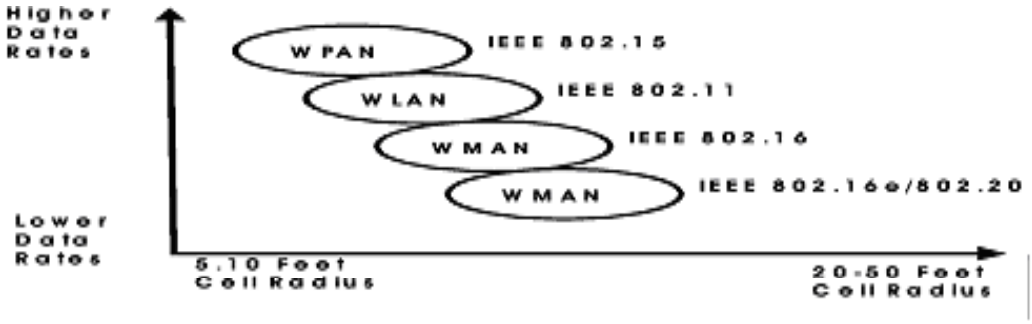
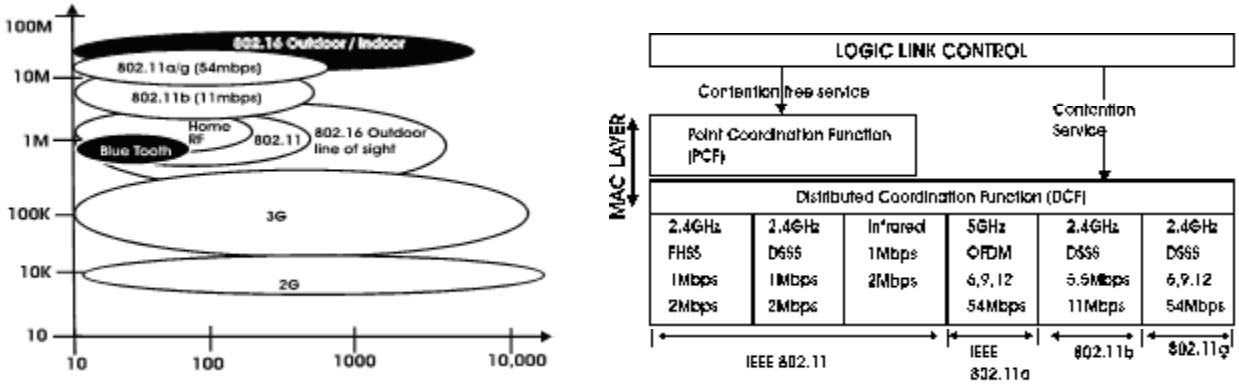


Figure 4: The IEEE Wireless Standards



a. IEEE 802.11 standards Comparison **b.** IEEE 802.11 Protocol architectures

Figure 5: IEEE 802.11 Networks

hosts. (b) Class B- Medium number of networks, each with a medium number of hosts. (c) Class C - Many networks, each with a few hosts.

The 32-bit address (known as IPv4 address) is usually written in dotted decimal notation, with the decimal numbers representing each of the octets of the address. All class A network addresses begin with a binary 0 with reservation of network addresses with a first octet of 0 (binary 00000000) and 127 (binary 01111111), so there are 126 potential class A network numbers, which have a first dotted decimal number in the range 1 to 126. Class B network addresses begin with a binary 10 so that the range of the first decimal number in a class B address is 128 to 191 (binary 10000000 to 10111111), so that there are 2^{14} = 16,384 class B addresses. For class C addresses, the first decimal number ranges from 192 to 223 (11000000 to 11011111), and the total number of class C addresses is 2^{21} = 2,097, 152. Class D and E addresses, have the range 224 to 255 reserved for their networks and are used for special functions only and are not commonly assigned to individual hosts. Class D addresses are used for multicast addressing, which is a single address that points to more than one device which are defined on the network with the range of the first byte 224 and 239 defined by turning on the first three bits and turning off the fourth bit (11100000 = 224 and 1110 1111 = 239). Class E addresses are used for scientific or experimental purposes with the range of the first byte 240 and 255 defined by turning on all the first four bits, thus; 11110000 = 240 and 11111111 = 255. In particular environments, it may be best to use addresses all from one class. For example, a corporate internetwork that consists of a large number of departmental LANs may need to use class C addresses exclusively whereas singular LAN like AESS LAN can use class D addresses exclusively. Therefore, AESS network implements distributed computing with parts that run and communicate simultaneously on multiple computers over the network containing more than one hardware and software systems, processing elements, storage elements, concurrent processes, or multiple programs running under a loosely or tightly controlled regime (Leslie, 1987). Hence, distributed computing can implement Concurrency, Multiprocessor systems, Multicore systems, Multicomputer systems, Computing taxonomies, Computer clusters, Grid computing, and programming Languages (Wikipedia, 2009). Hence, distributed programming typically falls into one of several basic architectures or categories: client-server (where smart client code contacts the server for data, then formats and displays it to the user and inputs at the client is committed back to the server when it represents a permanent change), 3-tier architecture (where three tier systems move the client intelligence to a middle tier so that stateless clients can be used), N-tier architecture (where web applications further forward their requests to other enterprise services), tightly coupled or clustered (where a cluster of machines closely work together, running a shared process in parallel), peer-to-peer architecture (where there responsibilities are uniformly divided among all machines, and peers can serve both as clients and servers with no special machine or machines providing a service or managing the network resources), and space based (where an infrastructure creates illusion (virtualization) of one single address-space, data are transparently replicated according to application needs, and decoupling in time, space and reference is achieved). Alternatively, a "database-centric" architecture can enable distributed computing to be done without any form of direct inter-process communication, by utilizing a shared database (Opara and Etus, 2007), as in AESS.

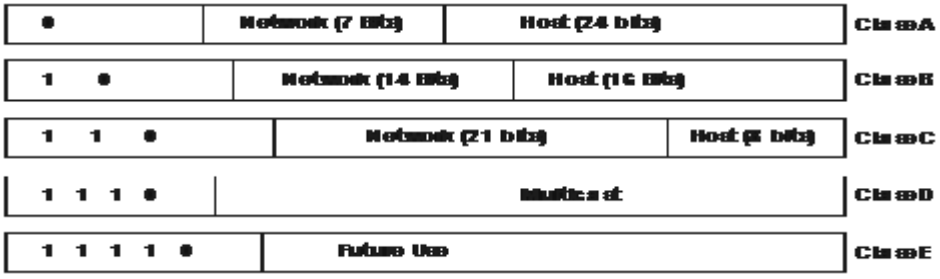


Figure 6: 32-bit Protocol Address Formats.

2.6 AESS Human – Computer Interfacing / Interaction Considerations and Applications

The importance of a focus on human-computer interaction (HCI) has been recognized by industries, academia and governments. User Interfaces is one of the six "core subfields" of Computer Science. HCI is very important or central to a number of important application areas such as global change research, computational biology, commercial computing, and electronic libraries (Hartmanis, 1992). Two surveys of Information Services practitioners and managers listed Human Interface technologies as the most critical area for organizational impact (Grover and Goslar, 1993). New regulations, such as Directive 90/270 from the Council of European Communities, are being passed that require interfaces to be "easy to use and adaptable to the operator" (Pat, 1993). Everyone knows that designing and implementing human-computer interfaces is difficult and time-consuming. In software generally, there is no "silver bullet'' (Fredericks, 1985) to making user interface design and implementation easier. Furthermore, as new styles of human-computer interaction evolve, such as 3-D visualization, the amount of effort directed to the design and implementation of the user interface can only increase. Hence, user interfaces are especially hard to design and implement because of these (Brad, 1993): (a) iteration of design and implementation, (b) reactiveness of interfaces, (c) multiprocessing, (d) real-time requirements for handling input events, (e) software robustness while supporting, aborting and undoing actions / activities, (f) difficult of testing user interface software, (g) diminishing support for user interfaces, (h) extremely complex interface tools, and (i) difficulty of modularization of user interface software.

AESS network management, in general, provides a means to configure the system while still meeting or exceeding design specifications, and it involves monitoring and controlling the network system so that it operates as intended. This means that network management may be performed by human, by an automated component or both. However, AESS Network Management System (NMS) is software designed to improve the overall performance, reliability of the system and ensure interoperability of devices based on IEEE 802.3 and IEEE 802.11 standards. Again, in the design of any NMS, there is the need to recognize management framework of Internet Activity Board on TCP/IP protocol implementation. The framework consists of these components (Alberto and Indra, 2000): A conceptual framework that defines the rules for describing management information (known as the structure of management information (SMI)), a virtual database containing information about the managed device (known as the Management Information Base (MIB)), and a protocol for communication between manager and an agent of managed device (known as Simple Network Management Protocol (SNMP)). The network management system performs the functions of fault management (mainly for the detection, isolation and resolution of network problems), configuration management (process of initially configuring a network and then adjusting it in response to changing network requirements), accounting management (tracking the usage of network resources), performance management (monitoring network utilization, end-to-end response time, and other performance measures at various points), and security management (managing the security services that pertain to access control, authentication, confidentiality, integrity and non-repudiation).

3.0 AESS System Design and Analysis

This section presents the complete AESS system design and analysis, which is the main crux of this work. Here, various elements of the design were analyzed and shown, which includes AESS component sub-systems, parameter definitions / specifications, algorithms / flowcharts (highlighted in line with structured programming design principles and standard symbolic representations of step-by-step events in top-down design method), control programs, input processing programs, output processing programs, and user interface forms.

3.1 AESS Complete System

The block diagram of the complete system design is presented in Figure 7 below, as consisting of five major blocks: The fingerprint scanner, web camera and PC computer blocks make up the hardware components, while the Visual Basic Application and

Microsoft Access Database blocks make up the software components. Each block details have been thoroughly investigated and their functional analysis given.

3.2 AESS Hardware Analysis

AESS hardware includes the fingerprint sensor / scanner device, the webcam device, and the PC computer. The first two devices are computer interfaced peripherals that are configured on the PC computer on installation of their device drivers, which operate as input devices to the AESS programs. The workings of the AESS hardware devices have been quickly analyzed below.

3.2.1 Fingerprint Scanner Device

The fingerprint scanner hardware component used is the capacitance type. As an optional device used in detecting fingerprint patterns measures alterations in the voltage output due to changes in the capacitance between the ridge and valley of the finger. The scanner senses and scans the finger, extracts the features from the captured fingerprint image; then the matcher program compares the extracted features with a template of stored features in the computer. Here is a typical capacitance fingerprint scanner device as used in the design.

The first phase of the fingerprint verification process is the fingerprint enrollment phase as shown in Figure 8. It is very important to know the size and quality of the image that the fingerprint sensor takes so as to have an idea of how to preprocess it. From this image, minutiae for matching are extracted. This process repeats, resulting in the generation of a 'live template', which is then stored in the database. The fingerprint scanner device is connected to the computer through the Universal Serial Bus (USB) port. The port detects, installs and configures the scanner when plugged in. This provides with it the scanner port interface program through which the fingerprint scanner is accessed and fingerprints extracted. The extraction success is measured by: (i) taking several images of the same fingerprint to cover various aspects of the image, which includes Position, dryness, humidity, dust, brightness, darkness, etc.; (ii) a threshold set for the acceptance or rejection of a specific fingerprint for recognition, verification and matching. Figure 9 gives the fingerprint scanner enrollment flowchart and extraction interface.

Fingerprint scanning (image acquisition) involves many of the algorithms that require a linear scan of the fingerprint image, and is achieved by moving a fixed size window across the picture in a grid-like pattern. But, fingerprint matching (verification) is the process used to determine whether two sets of fin-

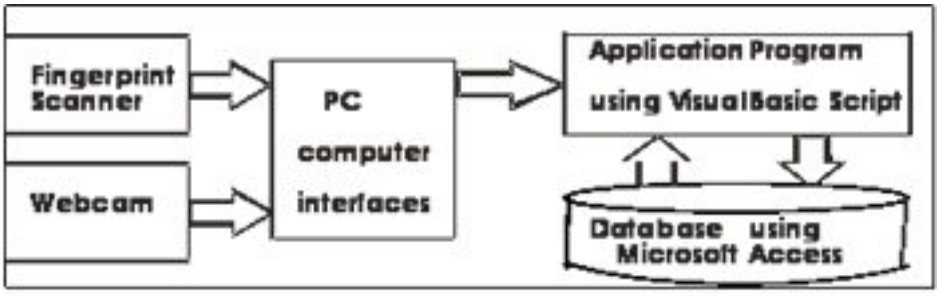
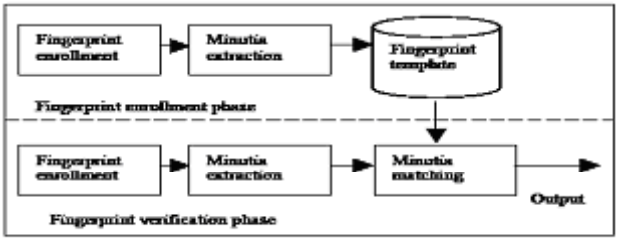


Figure 7: Block diagram of AESS complete system

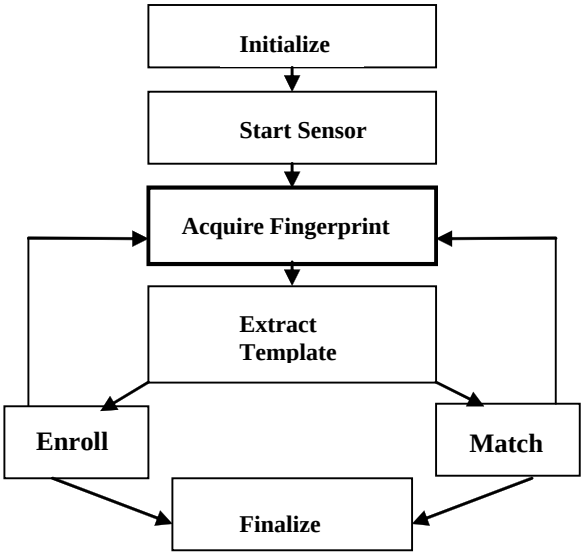
a. Capacitance fingerprint scanner



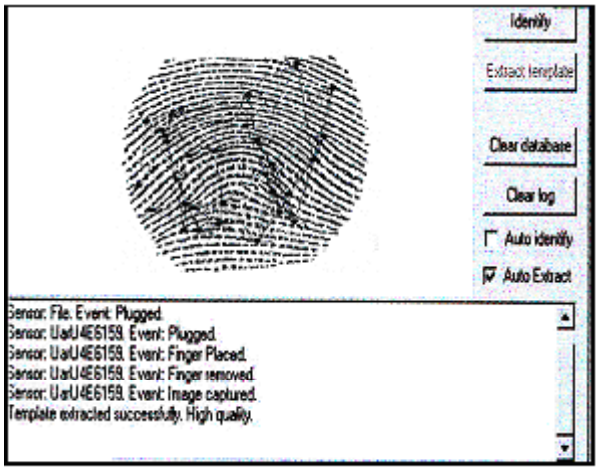
b. Fingerprint verification external procedures

Figure 8: Fingerprint scanner device and procedures

gerprint ridge detail come from the same finger. Most modern fingerprint matching technologies use minutiae matching (Karu and Jain, 1996; Senior, 2001; Jain and Hong, 1997; Jain *et al.*, 2000; Mehtre and Murthy, 1986; Daugman, 1985). Minutiae are usually matched together by their distance relative to other minutiae around it such that if multiple points in one image have similar distances between them and multiple points in another image then the points are said to match up and are most likely from the same fingerprint. It is the idea of this paper to add that the minutiae algorithm is fast and also that the region constraints between minutiae edges should be approximately the same as well.



a. Fingerprint Enrolment and verification program flowchart



b. Fingerprint acquisition window

Figure 9: Fingerprint scanner USB port interfacing

3.2.2 The Webcam Device

The webcam image extraction flowchart and interface in Figure 10(a) are used to obtain pictures of students for storage in the database. Image features like faces, shapes, models and colors can be observed and tracked to produce a corresponding form of control, but in AESS each student's picture is just displayed on authentication of the student's fingerprint, for a more complete identification. The Lightwave detachable webcam used is mounted on the computer monitor as in figure 10(c), to allow for hands-free computing, improve computer accessibility, provide higher degree of freedom (DOF) and ensure interactivity.

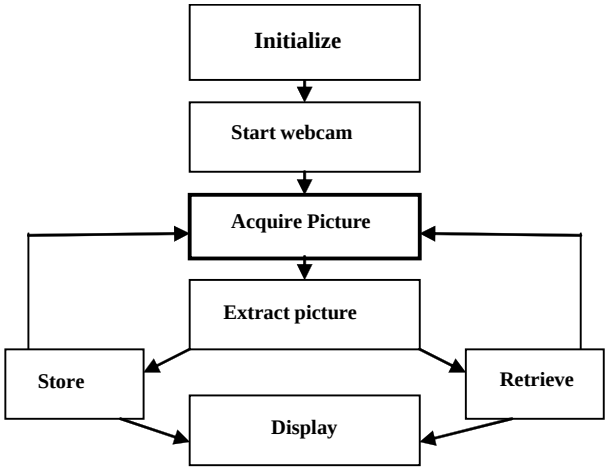
3.3 AESS Software Design Platforms

The AESS software is developed as a client-server application. Its software includes the back-end database program designed using a static DBMS - the Microsoft Access application software and the front-end interface program designed using Visual Basic 6.0 enterprise edition application software, a member of the Visual Studio family - programming language family that can manipulate hardware operations and manage dynamic link libraries for hardware components (Egbe, 2003). The Visual Basic front-end program is designed as an input/output program, to initialize the devices, access them, extract data from them, store the data in the database, retrieve the stored data, compare and display the data as appropriate. The platforms, designs and functions of the AESS programs have been subsequently shown and analyzed below.

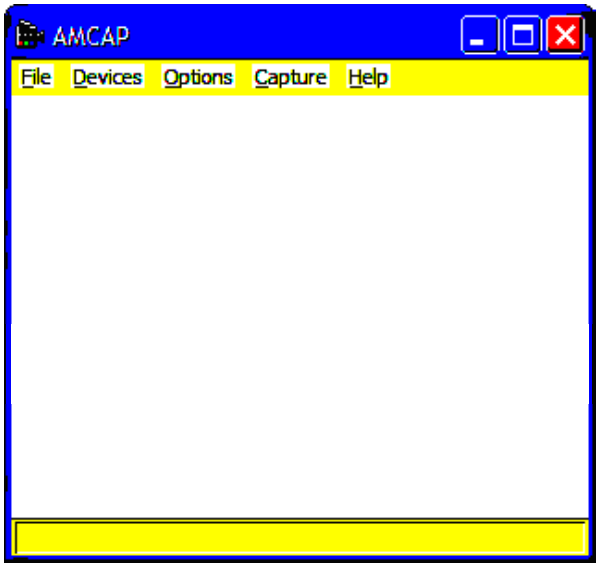
The Microsoft Access database is a single, static database (Microsoft, 2002). It is a static database because when deployed in a large scale in a distributed system, the database has to be stored in a server (e.g. computer in the department) while the users access the data in the database with client systems (e.g. computers at the examination centers). Another reason for using static database is the security considerations. Microsoft Access allows the administrator to create security policies to ensure that the data in the database is not easily compromised. Using Microsoft Access, one can manage a variety of information from a single database file. Within the file, these are used:

(a) Tables - to store data; (b) Queries - to find and retrieve just the data you want; (c) Forms - to view, add, and update data in tables; (d) Reports - to analyze or print data in a specific layout; (e) Data access pages - to view, update, or analyze the database from the Internet or from an intranet. Microsoft Access provides these three methods to create an access database: (i) Create a database by using a Database wizard (ii) Create a database by using a template (iii) Create a database without using a Database Wizard. The designed students' academic database information system software houses data collection of the following particulars: (i) Student personal and family profile (ii) Student academic profile (iii) Student payment status. The design specifications are reflected in the database table fields created as shown below.

The visual basic programming mimics object - oriented pattern of programming. It uses subroutines and modules on forms. AESS subroutines simply comprise set codes in which all the variables and syntax applied are all aimed at accomplishing a common goal. Subroutines are visible to the forms in which it is called. Modules however have a wider scope than the subroutines; they can be used to define universal variables which are always visible to the forms used in the project. Forms are the foundations you generally use to build Programs. A form is where all the things that people interact with as they use your program are put or kept. The objects put on the forms are controls, which enable the users to use the program. These include text objects, command buttons, image objects, amongst many others. A project is the group of all the files that make up your VB program and includes forms, modules, classes, graphics and active controls (Egbe, 2003). The AESS application program was developed using seven(7) VB forms. It however consists of the **administrator program** (used for registration of students' data and updating the database) and the **screening program** (used for the authentication and identification of students). A good look at AESS subroutines and forms as they are used in the component programs algorithm and design, will suffice.



a. AESS Picture capture, storage and retrieval program flowchart

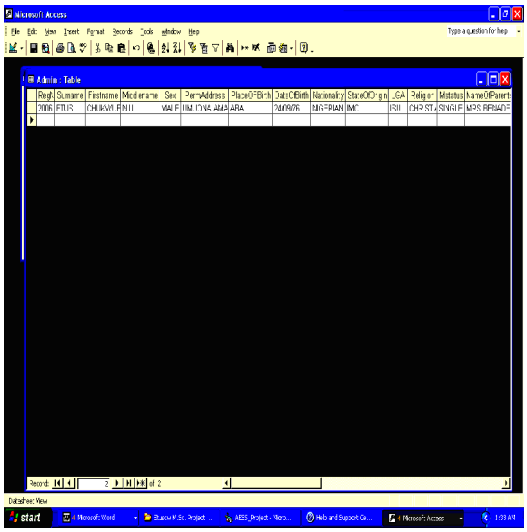


b. AESS Picture capture window

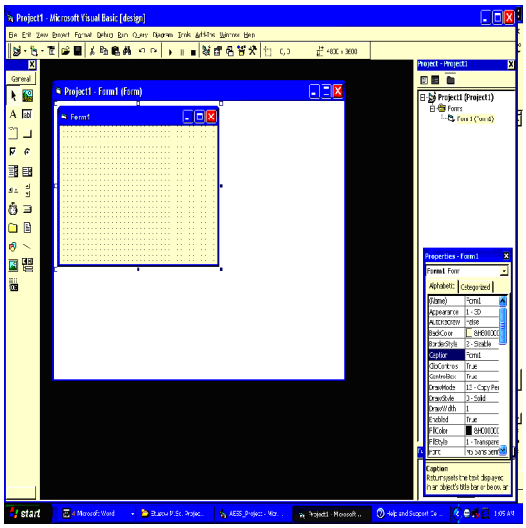
c. Webcam device mounted on PC

Figure 10(a) and (b): Fingerprint scanner USB port interfacing

a. MS Access design platform



b. Database specifications



c. VB 6.0 design platform

Figure 11: AESS software design platforms

3.4 AESS Program Modules Design and Analysis

The AESS program design and analysis tools include algorithms and flowcharts, and these are given in the sub-sections below. The design algorithms show how controls work together in regular relations to achieve the design phase of AESS system modules development. These depend upon the information obtained and contained in the system specification phase of the system development process. AESS main and subroutine program algorithms and codes are not given in this paper for space, but only the program flowcharts and forms. AESS system program was designed and developed following the program module algorithms and flowcharts. These gave rise to the system interface forms. The interface forms designed were source-coded (source codes not included here for space) to run the AESS application software. The VB compiler translated the source codes into computer machine codes during packaging to run the application in every computer that meets its minimum requirements. The design is to achieve the goals and objectives of this work and thereby overcoming the shortcomings and limitations of the existing manual system.

3.4.1 AESS Control Form Module

No system development effort can succeed without control. The controls needed in AESS are in the areas of: (i) Function (ii) Budget (iii) Schedule, and (iv) Quality. In order to make sure that AESS system is developed with proper and necessary functions, within budget, on schedule and to a good quality expectation, a number checkpoint are needed. These checkpoints are important for ensuring quick reviews, and timely decisions in organized basis. AESS data processing is done by the input and output programs under the supervision of the control program. The types of control considered in the design of AESS include: (i) Input / access Control (ii) Data entry control (iii) Processing control (iv) Output control (v) Data Organization and file storage controls.

3.4.2 AESS Input Program Module Design

To establish the input requirement of the new system, the content of the actual data records needed to

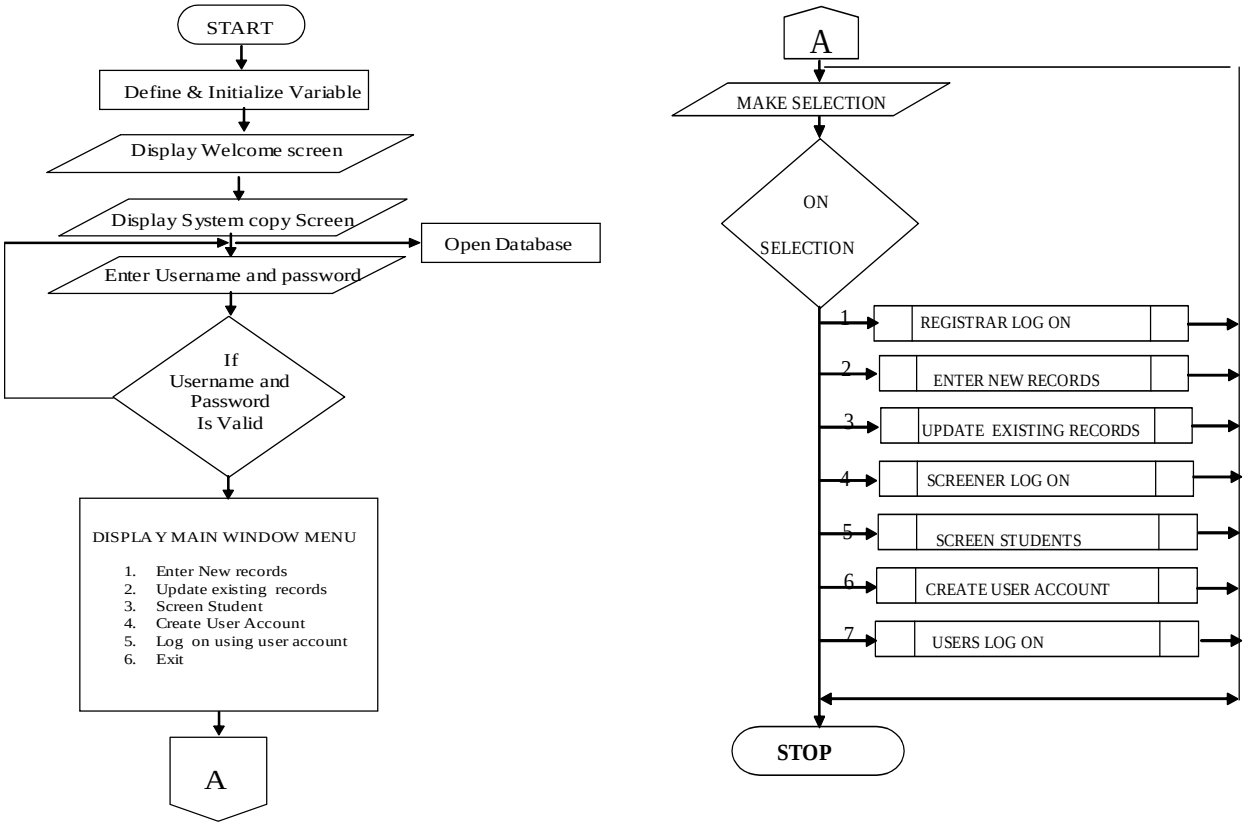


Figure 12: AESS Main program module flowchart

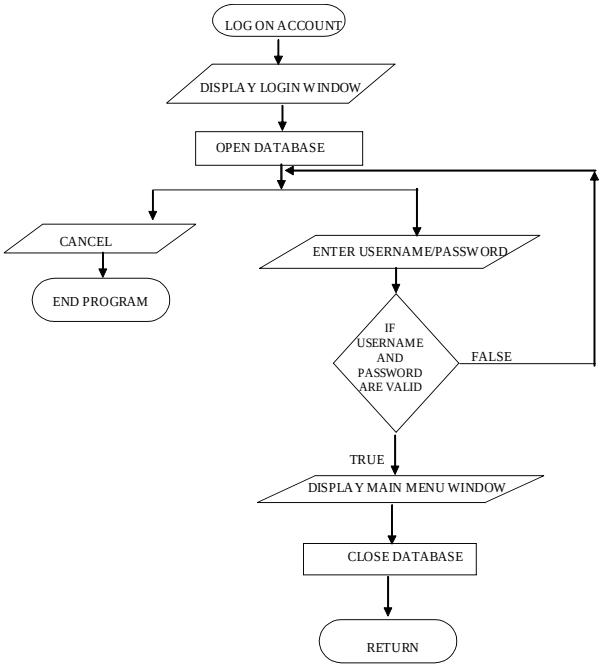
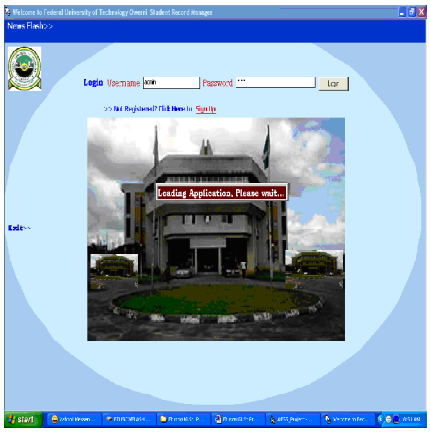


Figure 13: AESS Log on/off account module flow-chart

a. The splash screen form



b. The Welcome / Administration form

Figure 14: AESS control forms

produce the output are determined first. Given the volume and content of records available input methods are evaluated. At this stage of system development; input documents and formats are

designed. The design is developed to reflect Completeness, Accuracy, and Control.

3.4.3 AESS Output Design

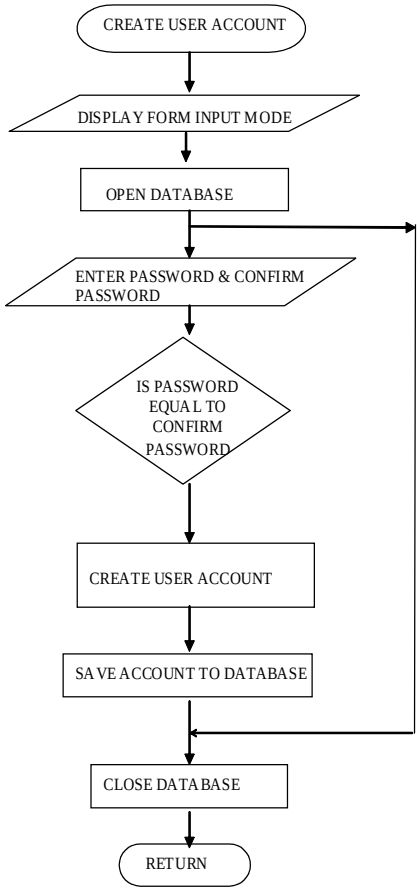
For an effective design of this system output the following evaluation for a number of trade-off are involved. These criteria include: (i) Use (ii) Volume (iii) Quality and (iv) Cost. Work begins by establishing data content, for design of either out document of display. The developer working with the result obtained builds a list of data elements to be included in each of the system.

4.0 AESS Implementation and Evaluation

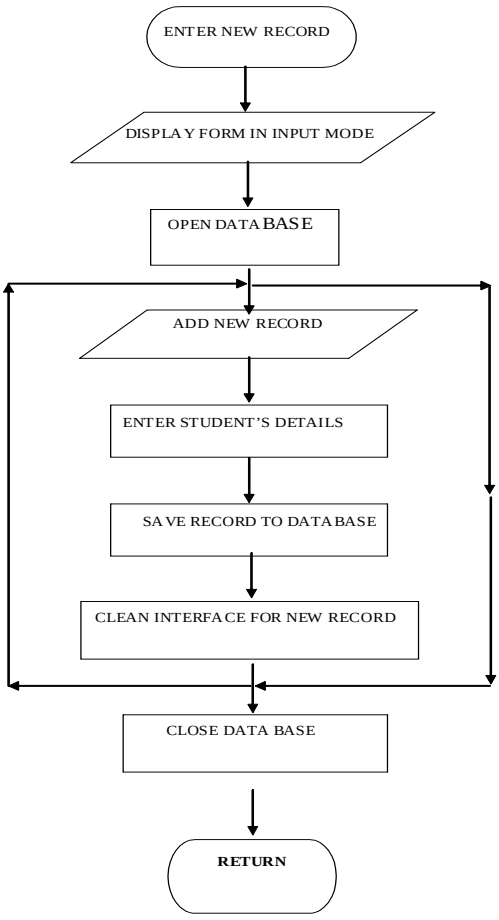
This section presents the system implementation and evaluation in terms of packaging, installation, running, function testing, results obtained, operations guide, deployment, and cost evaluation of the stand-alone and distributed AESS system.

4.1 AESS Packaging

The AESS software may be packaged for deployment using the Microsoft Visual Studio 6.0 Package and Deployment wizard as shown in Figure 19 below. This wizard enables one to add crucial files needed for the proper running of the software including the database into a distributable package and send this package to a distribution environment such as a server. It also contains Object Linking and Embedding (OLE) - a technology that allows a programmer of windows based application to create an application that can display data from different applications and also allows the user to edit the data from within the application in which it was created. There are three options on the wizard. You can either package the software or deploy it or, in case of any administration or management modifications, manage the scripts.

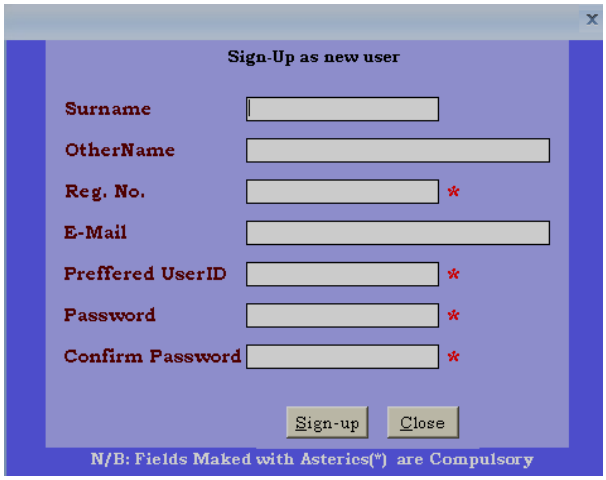


a. Create user account module

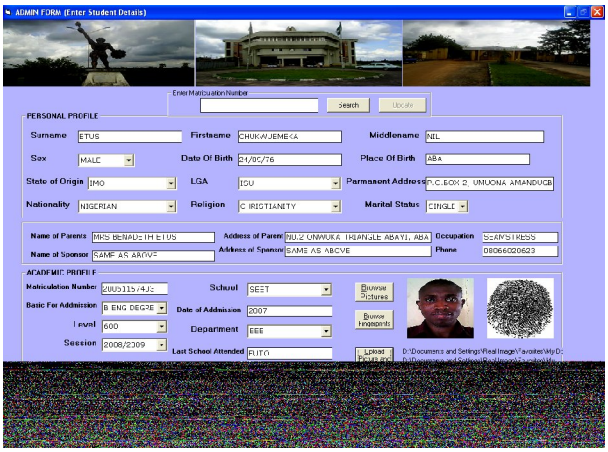


b. Enter new record module

Figure 15: AESS input module flowcharts

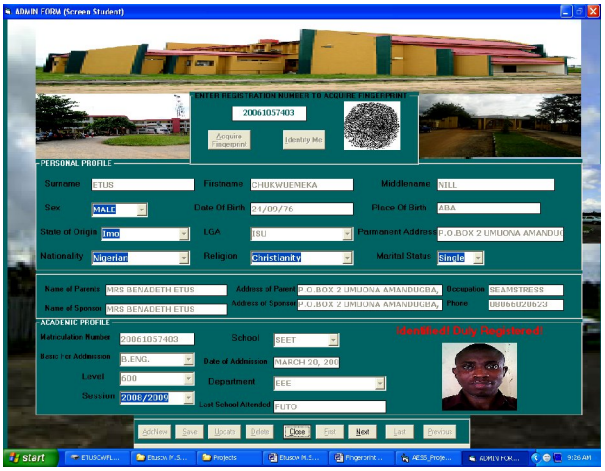


a. The sign-up form

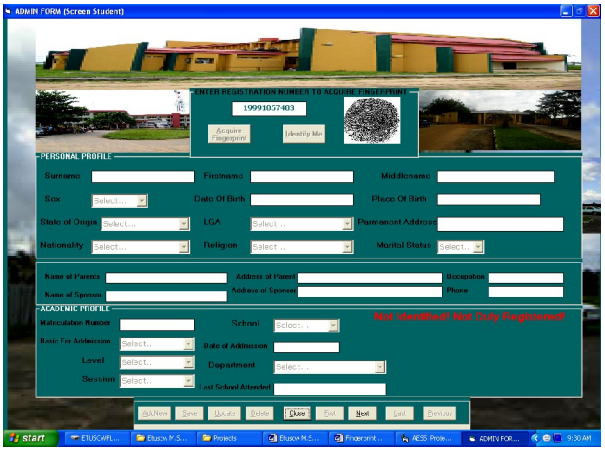


b. The registration form

Figure 16: AESS Input forms



a. Screen form (student Identified)



b. Screen form (student unidentified)

Figure 18: AESS Output forms

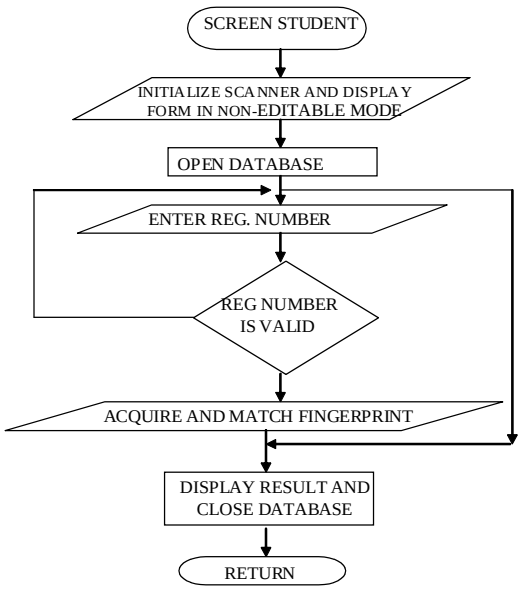


Figure 17: Student screening module flowchart

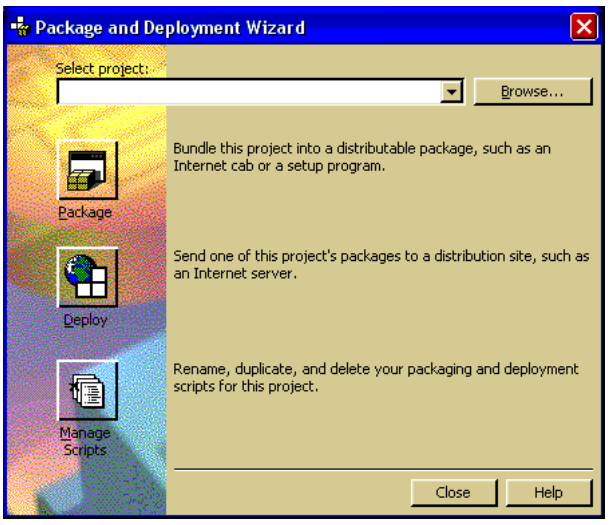


Figure 19: VB package and deployment wizard

4.2 AESS Software Installation and Running

There are minimum system requirements for all software, and this software is no different. For adequate deployment and running of AESS software for optimum performance, the following requirements must be met: (a) CPU: Intel Pentium 1 compatible systems and above (b) RAM: at least 32MB (c) Operating system: Windows 95/98/NT/2000/XP/ Vista (d) USB ports for connecting the fingerprint scanner and webcam.

4.3 AESS Functional Testing and Results

AESS functional testing and result shows that after installing the software, the location folder should, by default, be C:/Documents and Settings/User/Start/ Menu/Progams/Etuscw AESS Project. When the software runs, the splash screen form appears and later loads the AESS homepage form. On entering "admin" or "ADMIN" as the username and password, the "enter new records" and "update existing records" labels becomes highlighted. On clicking any of the two labels, the new records form or records update form, as appropriate appears and initializes the fingerprint scanner and webcam interfaces ready for data capture. After entering the necessary information, uploading and saving the information, each student new record registration or record update is confirmed and stored in the database.

The "screen student" label becomes highlighted on entering "screen" or "SCREEN" as the username and password, and clicking on the label, the screening form appears and the fingerprint scanner interface and form are initialized and loaded respectively. On placing the index finger on the fingerprint reader, the scanner program automatically starts running. The fingerprint finally obtained is compared with the ones in the database. If a match is found, the student's information, photograph and an appropriate confirmatory (identity and fees payment status) messages are displayed. The confirmatory message displayed may read "IDENTIFIED BUT FEES NOT PAID-UP!" or "IDENTIFIED AND FEES PAID-UP!" depending on whether the student has paid-up the school and/or departmental fees or not. But if no match is found, then no student information is displayed but only a non-authorization message which reads "NOT IDENTIFIED AND PAYMENTS UNVERIFIABLE!" is displayed.

4.4 AESS Operation Guide

The test result information above form the operation guides of AESS system. This is in addition with the following: (a) If you have the software in a CD, allow the CD to open (b) Copy the AESS software entire folder the hard disk (c) Send the AESS icon to the desktop (d) Click on the AESS icon to run and interact with the database in the AESS folder in the computer hard disk. Operate AESS as described in operations guide above (see section 4.3 above).

4.5 AESS Deployment

The AESS as designed can be quickly deployed as a stand-alone system (see Figure 20a). The database software is stored, accessed and managed together with the application software in the same computer. Registration of students is done during matriculation or thereabout using any of the stand-alone systems and the updated database copied into others before examinations with the master copy preserved at the department for security purposes, while and the authentication of the students is done at the examination centers. This is such that students' record updates are done only at the master stand alone system at the department and no updates allowed at the examination halls, each student's information in the database is accessed and displayed by fingerprint matching on the stand-alone system. Also, AESS is ultimately designed to operate in a client-server environment (see Figure 20b). The database software is accessed, managed and stored in the server using application program, while the application software is also installed in the client systems from where the database is also always accessed. Registration of students is done during matriculation or thereabout using the server or any of the client systems that are wirelessly linked and connected with the server, while authentication of the students is done at the examination centers using only the client systems while the server remains at the department to secure and preserve the database. This is such that each student's information in the database should be accessed, displayed and updated from the clients at the examination centers by

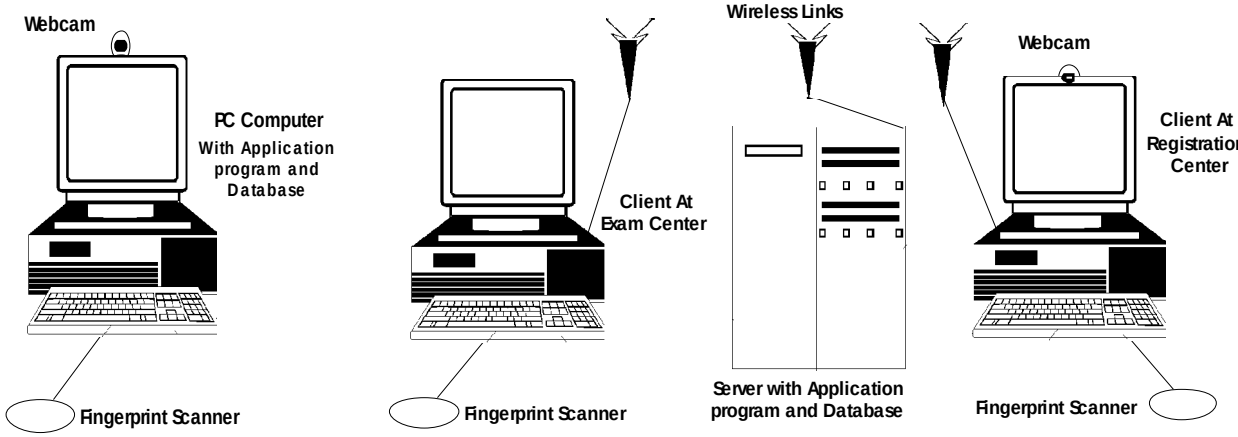
fingerprint matching.

If any student's fingerprint is matched (whether on the stand-alone or over the distributed system), the student's information (student's photograph, personal, family, matriculation, school fees and departmental dues payment-status details) are displayed and permission into the examination hall is granted, but if the fingerprint could not be matched with any in the database then the student is not identified nor allowed into the hall. With the displayed information, each student's claims can be verified.

encountered, limitations, and recommendations both for AESS deployment and use in higher institutions but especially in Federal University of Technology Owerri (FUTO), and for further work peculiar to AESS system in order to enhance its robustness, security, and reliability so that it can reflect 21st century systems.

5.1 Conclusion

AESS as proposed was designed, the software developed (using software tools packages like Visual Basic 6.0 enterprise version and Microsoft Office



a. Stand-alone AESS Model **b.** Distributed Client-server AESS system Model

Figure 20: AESS System deployment Models

4.6 AESS Cost Evaluation and Analysis

This is the estimation of the stand-alone and distributed wireless AESS system costs of implementation and deployment. The prices of the system components were obtained during the feasibility study and market survey phases of the system design for both the hardware and the software, with the most expensive component being the fingerprint reader which costs about $192. From the cost analysis, about two hundred and eighty thousand naira (₦280,000) is required to implement the stand-alone AESS; and about a minimum of two million five hundred thousand naira (N2,500,000.00) is required to execute the wirelessly distributed AESS fully and successfully.

5.0 Conclusion and Recommendation

This section finally presents the conclusion, problems

2007 version software development tools respectively were used to realize the goals of the AESS system) and integrated with the hardware. The entire system as fully implemented as a stand alone was successfully tested and results ascertained. Also, its implementation design strategy as a client-server based (distributed) system over wireless LAN network was equally made to ensure that the system is deployed to cover all examination halls on campus, using database situated in the various departments of the university, just to protect the database against all odds. Therefore, the Automatic Examination Screening System (AESS) machine reliably helps in its little way to ensure a good check on the menace of impersonation at examination centers by unqualified entities, and also ensures better compliance of fees payment by students. It is easy to use and somewhat cheap to implement, hence it is cost effective. Also, its database can be easily managed by any administrator, and does not need

any special training for one to be able to do so. In general, the AESS system designed, developed and deployed has students' registration and screening applications (the primary functions). It is also provisioned for course registration, result computation, result retrieval and transcript preparation secondary applications.

5.2 Problems Encountered and Limitations

Implementing the project had its pitfalls. One major issue encountered was compatibility issues. The software had compatibility problems with the newer version of the windows operating system, Windows Vista, especially with the dynamic link library files. So is it advised that, for optimum operation, it should be installed in systems with windows XP operating system. Also, acquiring the fingerprint scanner and webcam was not an easy task, since obviously they could not be built around.

5.3 Recommendations

Having carried out this work thus far, some recommendations are necessary to ensure its deployment and use, and also for further research around this work. They include:

1. AESS administrators' passwords should be reviewed and changed regularly to avoid unauthorized access and use of the system.
2. An enabling environment should be provided to accommodate the AESS solution and also facilitate its full deployment on campus.
3. This work can be expanded to incorporate course registrations, result computation, transcript preparation and result / transcript retrieval on-line functions.
4. Development and installation of information technology infrastructures like wireless network and other rugged advances in database and information technology. Only then can this solution and its likes be utilized to their full potentials. Some of these likes may be developed with modifications at AESS input processing forms and devices, output processing forms and devices, and its program codes, to becoming either a database-driven security system, communication system, or an observation and monitoring system (for wide variety of ambient and climatic conditions of temperature, lightening, and other weather conditions and forecasts).

References

Alberto Leon-Garcia and Indra Widjaja 2000, "Communication Networks; Fundamental Concepts and Key Architectures", McGraw-Hill series in Electrical and Computer Engineering, Boston, U.S.A, 2000.

Bantz, D. and Bauchot, F. 1994, "Wireless LAN Design Alternatives", IEEE Network, March / April, 1994.

Bowman, E. 2000, "Everything You Need to Know About Biometrics," Second Edition. Identix Corporation, January, 2000.

Brad A. Myers 1993, "Why are Human-Computer Interfaces Difficult to Design and Implement?", Computer Science Department, Carnegie Mellon University Pittsburgh, sponsored by the Avionics Lab, Wright Research and Development Center, Aeronautical Systems Division (AFSC), U. S. Air Force, Wright-Patterson AFB, OH 45433-6543 under Contract F33615-90-C-1465, Arpa Order No. 7597, PA 15213, CMU-CS-93-183.

Crow, B. 1997, "IEEE 802.11 Wireless Local Area Networks", IEEE Communications Magazine, September, 1997.

Daugman, J. 1985, "Uncertainty relation for resolution in space, spatial frequency, and orientation optimized by two-dimensional visual cortical filters, J. Opt. Soc. Am. **2,** 1160–1169.

Egbe T. 2003, "Visual Basic 6.0 for Engineers and Scientists," Joint Heirs publications, Benin City.

Fingerprint Basics, http://www.wikipedia.com/fingerprint (Accessed May 22, 2009).

Frederick P. Brooks 1985, "Silver Bullet: Essence and Accidents of Software Engineering," PhD thesis, Computer Science Department, Carnegie Mellon University, Technical Report CMU-CS-85-151, (April, 1985).

Gorshie W.G. 1986, "Computer Organization; Hardware and Software," 2nd Edition, Prentice Hall international Inc.

Grover, Varun, and Goslar, Martin 1993, "Information Technologies for the 1990s, The Executives' View", Communications of the ACM **36**(3), 17-19,102-103.

Halstead, B. D. and Bornby, S. U. 2001, "Biometric

Authentication and Identification Systems for Border Controls: A look at U.S. and Canadian Programs", New York, Hilltop Publishers.

Hartmanis, Juris et.al. (November, 1992); "Computing the Future," Communications of the ACM **35**(11), 30-40.

Hornby, A. S. 2000, "Oxford Advanced Learners' Dictionary of current English", Sixth Edition, London, Oxford University Press.

http://biometrics.ese.msu.edu/biometricsgrandchallenge.pdf Accessed May 19, 2009.

http://en.wikipedia.org/wiki/Authentication.

http://en.wikipedia.org/wiki/Defensive_programming.

http://en.wikipedia.org/wiki/distributed_computing

http://en.wikipedia.org/wiki/webcam

http://www.biometrics.ese.msu.edu/EverythingyouneedtoknewaboutBiometrics2000.pdf. Accessed May 03, 2009.

http://www.nhmrc.cv.nctu.edu.tw/biometricsinU.S/2001.pdf. Accessed May 16, 2009.

Jain, A. K., and Hong, L., and Bolle, R. 1997, "On-line Fingerprint verification, IEEE Trans. Pattern Anal. Mach. Intell. **19** (4), 302–314.

Jain, A.K., Prabhakar, S., and Hong, L., Pankanti, S. 2000, "Filter bank based fingerprint matching," IEEE Trans. Image Process, **9** (5) 846–859.

Jain, A.K., Prabhakar, S., Hong, L., and Pankanti, S., 2004, "Biometrics: A Grand Challenge," Proceedings of International Conference on Pattern Recognition, Cambridge, U.K., pp.2-6.

Jain, A.K., Ross, A., Prabhakar, S. 2001, "Fingerprint matching using minutiae and texture features", in: Proceedings of the International Conference on Image Processing (ICIP), Thessaloniki, Greece, pp. 282–285.

Karu, K. and Jain, A.K. 1996, "Fingerprint classification", Pattern Recognition **29**(3), 389– 404.

Keshav, S. and Sharma, R. 1998, "Issues and Trends in Router Design", IEEE Communications Magazine, May 1998.

Klein, S. and Beutter, B. 1992, "Minimizing and maximizing the joint space-spatial frequency uncertainty of gabor like functions: comment," J. Opt. Soc. Am. **9**(2), 337–340.

Lammle, T. 1999, "CISCO Certified Network Associate Study Guide", Sybex Inc., Alameda, USA. 1999.

Leslie Lamport 1987, (28 May, 1987); "Subject: distribution (Email message sent to a DEC SRC bulletin board at 12:23:29 PDT)". http://research.microsoft.com/users/lamport/pubs/distributed-system.txt. Retrieved on 28-05-2009.

Linux release (May, 2009); Linux 2 6 26 - Linux Kernel Newbies

Mehtre, B., and Murthy, M. 1986, "A minutiae-based fingerprint identification system," in: Proceedings of the Second International Conference on Advances in Pattern Recognition and Digital Techniques, Calcutta, India.

Microsoft Front Page 2002, "User guide for Microsoft FrontPage," Microsoft Corporation, Texas, pp 209-211.

Opara, F. K. 2003, "Computer and Data Management with Systems Maintenance Guide. Springfield Publishers ltd., Port Harcourt.

Opara, F.K. and Etus, C. 2007, "Determination of IPV6 Protocol, its Deployment and Efficiency in Computer System Networks in Nigeria", Journal of Engineering Research and Development, Duncan Science Publication, C/River, Nigeria, 2007.

Pahlavan, K., Probert, T. and Chase, M. 1995, "Trends in Local Wireless Networks", EEE Communications Magazine.

Pat Billingsley 1993, "1990 EC Directive May Become Driving Force", SIGCHI Bulletin **25**(1), 14-18.

Paul, Rosenzweig, Alane, Kochems and Ari Schwartz 2004, "Biometric Technologies: Security, Legal, and Policy Implications", Published by heritage foundation.

Pratt P.J. and Adamski J.J. 1987, "Database Systems Management and Design", Boyd and Fraser, Boston, pp 16, 27.

Samuelson, O. S. 2006, "Introduction to Database Management and Administration", London, Prentice and Hall.

Senior, A. 2001, "A combination fingerprint classifier", IEEE Trans. Pattern Anal. Mach. Intell. **23**(10), 1165–1174.

STGISC release 2001, "Biometric Identifiers and the Modern Face of Terror: New Technologies in the Global War on Terrorism," Hearing before the Subcommittee on Technology, Terrorism and Government Information of the Senate Committee on the Judiciary, 107th Cong. 1st Session.

U.S. GAO 2002, "Technology Assessment: Using Biometrics for Border Security", U.S. General Accounting Office (GAO), GAO-03-174.