CENTRE FOR ICT & YOUTH DEVELOPMENT
CICTYD
VOLUME 2
OCTOBER, 2012

THE DON BOSCO INTERNATIONAL JOURNAL OF INFORMATION COMMUNICATION TECHNOLOGY & YOUTH DEVELOPMENT

Olaniyi, O.M, Adewumi, D.O., Oluwatosin E.A, Adeyiga J.A, & Sanusi A **(2012)**,"Implementation of Voice Over Internet Protocol(VOIP) Communication Service for Campus Environment", **Don Bosco International Journal of ICT and Youth Development, (DIJYD),Nigeria,2(1),11-16.**

J51

Olaniyi, O.M, Omotosho, A, Oluwatosin E.A., Adegoke M.A. & Akinmukomi, T **(2012),** "Student's Exeat Monitoring System Using Fingerprint Authentication and Mobile Short Message Service", **Don Bosco International Journal of ICT and Youth Development (DIJYD),Nigeria, 2(1),76-85.**

J50

TABLE OF CONTENT

The Don Bosco International Journal of ICT & Youth Development Vol 2. Oct 2012

Students Exeat Monitoring System Using Fingerprint Biometric Authentication and Mobile Short Message Service

[1]Olaniyi, O.M, [2] Omotosho. A, [3]Oluwatosin E.A, [4]Adegoke M.A, & [5]Akinmukomi, T.
[1]Department of Computer Engineering
[1]Federal University of Technology, Minna ,Niger-state, Nigeria.
[2,3,4,5]Department of Computer Science and Technology
[2,3,4,5]Bells University of Technology, Ota , Ogun-state, Nigeria.
E-mail: [1]engrolaniyi09@yahoo.com, [2]bayosite2000@yahoo.com ,

Abstract
Exeat is a generic term commonly used to describe a period of absence from a centre of learning either for entire day, or parts of a day for appointments, interviews, open days and other fixtures in privately owned academic environment. The current method of monitoring student's movement is inefficient and brings difficulty to the University Halls management checking student's exit/entry into the halls of residence as well as impersonation. By using nexus combination of Ubiquitous Mobile Computing Technology through Mobile Short Message Service and biometric fingerprint approach exeat management and monitoring is quick and easy. Result after testing of the designed and simulated system shows that exeat monitoring systems is less prone to forgery as stakeholders are carried along, capable of preventing impersonation among students, and provide absolute electronic compliance to the policy of issuing exeat to students in the University Halls of Residence.

Keywords: Exeat, biometrics, SMS, ICT.

1. INTRODUCTION

The increasing use of technology in all aspects of society makes confident, creative and productive use of Information and Communication Technology (ICT) an essential skill for life. ICT capability encompasses not only the mastery of technical skills and techniques, it also facilitates the understanding of these skills in learning, everyday life and employment. ICT capabilities are fundamental to participation and engagement in modern society (The Global Information Technology Report, 2008).

In Information Technology (IT), biometrics refers to technologies for measuring and analyzing human physiological characteristics such as fingerprints, eye retinas and irises, voice patterns, facial patterns, and hand measurements, especially for authentication purposes. Examples of behavioural measureable characteristics include signature recognition, gait recognition, speaker recognition and typing recognition. Biometrics authentication is by measuring a person's physiological or behavioral features. In the past, the common perception of biometrics was that they were limited to use by government facilities and high security areas. However, biometrics is becoming more prevalent in day-to-day applications. It is a type of verification that can be used for authentication when using computers for a variety of purposes.

The concept of exeat is most commonly used to describe a period of absence from a centre of learning. It is also used at certain colleges to define a required note to take absence from school either for entire days, or parts of a day for appointments, interviews, open days and other fixtures (Frischolz 2000). Access control is concerned with determining allowed activities of legitimate users, mediating every attempt by a user to access a resource in the system. Several means and technique have been adopted to restrict access to various domains of human endeavors(Omidiora 2009), but not much has been done with regards to biometrics exeat monitoring system in the privately owned academic domain such as in the Bells University of Technology Ota, Nigeria. The current paper tally approach to exeat has been found to be inadequate because it can be forged or duplicated and does not provide a reliable student monitoring.

The combination of biometric and mobile SMS technology would improve the existing protocol of issuing and managing exeat to students. In literature, different biometric technologies have been applied for verifying users for access to different sensitive places according to the level of security required. These include: Level one Access: ID cards, card keys; Level two Access: PIN, passwords, secret questions.; Level three Access: finger, facial, iris, gait, voice, handprint.; Level four Access: level one + level three.

The technologies help in restricting access to the system, allowing access to only those who own a gate card or id card(level 1), know a specific code(level 2), have determined physical mark(level 4), or have a combination on of both card keys and have a determined physical mark (level 4 mainly for advance systems (Matyas and Riha 2000) .

This work proposed exeat system on the level three for absolute solution to the required security measure for the problem domain. This proposed exeat system would assists the university administrator to utilize existing student information for managing and monitoring the students in the hall of residence through electronic administration and monitoring of exeat, the parents / guardian to be mobile SMS alerted and prevention of impersonation at the School gate. The paper is organized into five sections: Section one Introduced the problem and justification of the proposed solution, Section two review related works in the problem domain, Section three provides materials method used to provide the solution, Section four describe how the method and materials were implemented and tested while the Section five concludes the paper.

2. RELATED WORKS

A number of works has been done in the area of biometric technology and mobile communications over the years to the problem of entity entry/exit control. In Abdul Kadir et al (2009) proposed an RFID matrix card based auto identity system to the manual problem of monitoring student in boarding schools. Upon initial study of the three Boarding school in Malaysia, current process of maintaining students records in and out was not only tedious, misinformation always happen as students tend to provide inaccurate information. In Matjaz and Tusar (2007), a flexible modular system based on integration of arbitrary access sensors and an arbitrary number of stand-alone modules were applied to solve the problem of entity exit/entry.

The system was tested with four sensors: a door sensor, an identity card reader, a fingerprint reader and a camera. However, identity cards can be lost, stolen and misused. Bochkov et al (2007) examined the security problem of identity theft where he specifically addressed the following issue: Why should we care about identity theft?; What options are available to solve this problem? What the solutions are?, and why some are more effective than others?.

The authors discussed other biometric technologies that are emerging including vein patterns, facial thermographs, DNA typing, sweat pores, hand grip, fingernail bed, body odor, ear shape, gait pattern, skin luminescence, brain wave pattern, footprint recognition and foot dynamics. Also in relation to the identity theft, Vijay and Dattatray(2010) discussed the issue of using multimodal biometrics in systems. Biometric systems based on single source of information are called unimodal systems (i.e. using one source to access necessary information.

Of all the emerging biometric technologies, fingerprint identification is one of the most well-known and publicized biometrics because of their uniqueness and consistency over time, fingerprints have been used for identification for over a century, more recently becoming automated (i.e. a biometric) due to advancements in computing capabilities. It became popular as a means of identification and verification because of the inherent ease in acquisition, the numerous sources (ten fingers) available for collection, and their established use. According to Maltoni et al. (2003), fingerprint is one of the most mature biometric traits and considered legitimate proof of evidence in courts of law all over worldwide.

Fingerprints are, therefore, used in forensic divisions worldwide for criminal investigations. More recently, an increasing number of civilian and commercial applications are either using or actively considering using fingerprint-based identification because of a better understanding of fingerprints as well as demonstrated matching performance than any other existing biometric technology. The discovery of uniqueness of fingerprints caused an immediate decline in the prevalent use of anthropometric methods of identification and led to the adoption of fingerprints as a more efficient method of identification(Lee et al., 1991).

With recent advances in internet and mobile technology, electronic service is becoming an important factor because different people can provide and obtain services without the limitation of location. The excellent e-service provides service via different channels and uses internet technology to provide customers with service in a cost effective manner. Customer communities are managed through e-mail, SMS messages, faxes etc. (Hua et al 2004). SMS Alert combines and integrates the benefits of cell phone technology and alarm and monitor systems, as it enables an individual to control and keep in contact with home, business or machinery and equipment. It instantly sends an SMS or missed call the moment the alarm is triggered.

It can also be used to control and monitor machinery and equipment. Khiyal et al (2009) presented a method that focuses mainly on controlling home appliances remotely and providing security when the user is away from the place. The system is SMS based and uses wireless technology to revolutionize the standards of living and provides ideal solution to the problems faced by home owners in daily life. An attempt has been made to review existing works on biometric implementation with a view of knowing the current tools used in its various application. Fingerprint technology is so far the most suitable and reliable approach for the system development as it basically takes care of security and prevents impersonation among students. It is less prone to forgery compared to the existing method on ground and hence can be deployed to solve the problem of student exeat at Bells University of Technology, Ota hall of residence.

3. MATERIALS AND METHODS

The following scientific approaches were used to achieve the central idea of this work. They are: Requirement definition and infrastructural modeling

3.1 Requirement Definition of the Proposed Service Infrastructure

(i). **Mobile Students Exeat Monitoring and Management System Requirement**

This requirement follows from the assumption that in order to automate the exeat management system, the system should provide:

a) **Eligibility and Authentication:** The system should be designed in a way that only allows access to authorized personnel.

b) **Uniqueness:** A student has only one exeat and it cannot be used by another person.

c) **Accuracy:** The administrator should be able to compute records and generate exeat reports with lesser errors.

d) **Integrity:** students' exeat records can only be modified, updated or deleted by the assigned administrator.

e) **Reliability:** The system should work robustly without any loss of records due to good and reliable database and also should be able to notify parents/guardians in lesser time.

f) **Flexibility:** More modules expected of exeat operations can be integrated into the system to increase functionality. g) **Convenience:** students should be able to enter/exit the university with minimal sign in/out time.

(ii) Service Provision Requirement

The infrastructure should allow the administrators to monitor registration of staff/supervisors and students, allow supervisors to grant exeat to students, record time of exeat granted, check student exeat number, monitor whether a particular student has returned after the exeat duration expired or not etc.

3.2 Infrastructural Model and Architect

(i) **Overall System Architecture**

The Students Exeat Monitoring Automated Systems involves two important technologies namely: i) Biometric Fingerprint Technology (Scans the fingerprints of users)

ii) SMS technology (automatically sends alert to parents or guardian). The hardware phase integrated into the system is the biometrics fingerprint scanner.

The software phase is divided into two sub-phases:
i) Front End (application interfaces the users would interact with)

ii) Back End (database where the information is stored). In designing the front and back end of the system, some development tools required are: i) **Microsoft Visual Studio (.Net Framework):** The programming language used is C# which is an elegant and type-safe object-oriented language that enables developers to build a variety of secure and robust applications that run on the .NET Framework. C# can be used to create traditional Windows client applications, XML Web services, distributed components, client-server applications, database applications etc. ii) **Microsoft SQL Server 2005:** It is a fast, stable and true multi-user, multi-threaded SQL database server; SQL (Structured Query Language). This serves as the database at the back end because it is fast, robust and easy to use. Access to the database will be limited to the administrator in order to prevent unauthorized individual from having access to sensitive information. The designed system is a client-server system that describes a network in which processing is divided between a client program running on a user machine and a network server program. The system architecture of the designed system is shown in figure 1. The system components include fingerprint scanner, exeat management system, the system database and an SMS gateway.

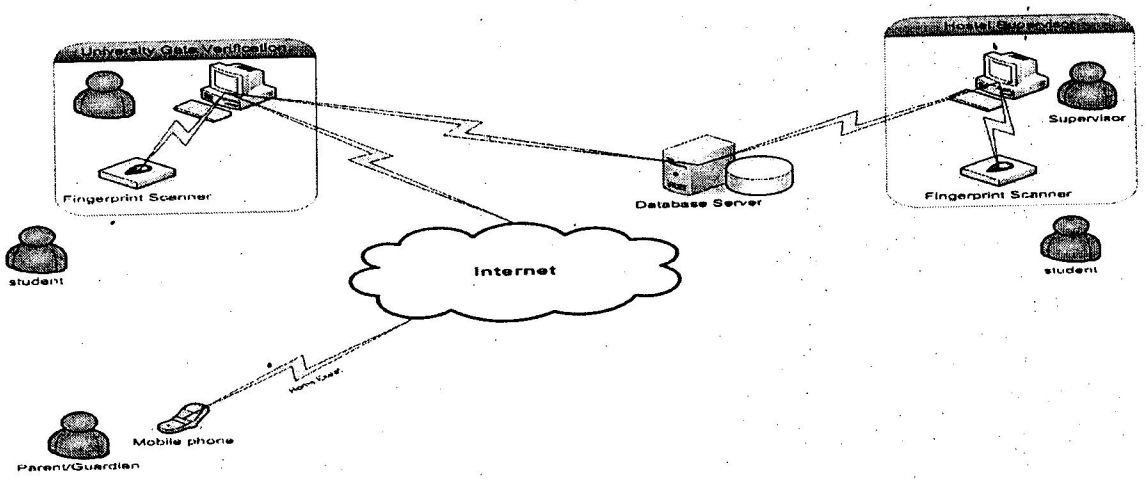

Figure 1: System Architecture of the Mobile Students Exeat Monitoring Systems

Major System Components

The Fingerprint Scanner

The Fingerprint scanner enrolls and verifies the identity of every person based on the marks on his or hers fingers and these marks have a pattern that cannot be changed or removed. The print is made up of ridges and furrows as well as characteristics that occur at minutiae points. Standard systems are comprised of a sensor for scanning a fingerprint and a processor which stores the fingerprint database and software which compares and matches the fingerprint to the predefined database. Within the database a fingerprint is usually matched to a reference number or Pin number which is then matched to a person's name. In instance of security, the match is generally used to allow or disallow access. (Thorton, 2000).

Database Server: In other to make comparison possible, the fingerprint representation and students matric number have to reside in a data repository. In this paper, a centralized database was used for storing each student's data. There will also be a link between the biometric data stored in the database to some information about the student's identity. When the database is queried, the feedback will not just include the biometric data, it also includes the personal information relating to the corresponding student and the database was implemented using Microsoft SQL Server 2005.

SMS Gateway

Message Alert format that is used is the Express Bulk SMS, with an SMS account opened. This will enable parents/ guardians get alerts when their ward takes home exeat. The exeat system is implemented as a server system. It enrolls, verifiers by granting exeat, and for the home exeat it sends an SMS over the internet to a number that has been specified in the database.

ii. Biometric Authentication Framework

Biometric authentication requires comparing a registered or enrolled biometric sample (biometric template or identifier) against a newly captured biometric sample. The biometric authentication system is used in two phases: The Enrolment phase and The Verification phase.

Enrolment Phase Design

In the enrolment phase, a sample of the biometric trait is captured, processed by the computer and then stored in the system database for comparison at a later date. During this phase, the biometric characteristic of an individual is first scanned by a biometric reader to produce a raw digital representation of the characteristics. A quality checker is performed in to ensure that the required sample can be reliably compared during the verification stage. In order to facilitate matching, the raw digital representation is usually further processed by a feature extractor to generate a compact but expressive representation called a template. The template is then stored in the central database of the biometric system.

L_m is the minutiae list; L_l is topological vectors list for lines; L_r is ridge count vectors list for lines.

Minutiae list

Let M_i – is minutiae which is indexed to number i .

The minutiae list L_m is in the following form

$$L_m = \{M_i = \{(x_i, y_i), \alpha_i, t_i, v_i, \theta_i, p_i, h_i\} \mid i \in 1..n_1\}, \quad (2)$$

$| L_m | = n_1$ – cardinal number; $(x_i, y_i), \alpha_i, t_i, v_i, \theta_i, p_i, h_i$ – coordinates, direction and type of minutiae as well as value and direction of curvature, probability and density of lines about minutiae.

Topological vectors list

Topological vectors list for lines is synthesized on the basis of all the nodes of skeleton, excluding minutiae nodes, and written in the form of

$$L_l = \{V_i = \{(e_j, n_j, l_j)\} \mid i \in 1..n_2, j \in 1..m_l\}, \quad (3)$$

Where V_i – topological vector for skeleton nodes cluster; $| L_l | = n_2$ – cardinal number and $n_2 > n_1; i$ – index like the number of topological vector; j – number of link in topological vector; e_j – event, and l_j – length of link, formed with minutiae with number n_j; m_l – quality of links taking into account central line in the form of

$$m_l = 4m + 2 \quad (4)$$

Ridge count vectors list

Ridge count is calculated as the quantity of lines, placed on the straight line between two minutiae. In electron systems for one minutia Mi , as a rule, some similar values are determined.

$$L_r = \{R_i = \{(r_j, n_j)\} \mid i \in 1..n_3, j \in 1..n_4\}, \quad (5)$$

where R_i – is a vector of ridge count for the nodes group of the skeleton as ordered by index j set of ordered pairs (r_j, n_j); $| L_r | = n_3$ – cardinal number and $n_3 > n_1; i$ – index as a number of vector and $n_4 < n_1; r_j$ – ridge count value, and n_j – minutiae number on a link j.

(iv) **Model Analysis**

The structure of the proposed system model can be analyzed using the use-case diagram, class diagrams sequence diagram and flowchart diagram. The use-case scenario of the infrastructure is shown in Figure 4 showing the interactions of the porters, guardians/parents and students on each tier of the model. The use case diagram has three actors. The registered porter login into the desired Mobile Students Exeat Monitoring and Management System Service, identified the student requesting exeat in the system, grant exeat to student. If the student desired to go home, an SMS alert is automatically sent to the guardian/parent to notify them. All information here is stored in the database and can be used for future reference. Figure 5 shows the Class diagram of the Mobile Students Exeat Monitoring System, Figure 6 shows the Sequence diagram of the Mobile Students Exeat Monitoring System and Figure 7 shows the Class diagram of the Students Exeat Monitoring System.

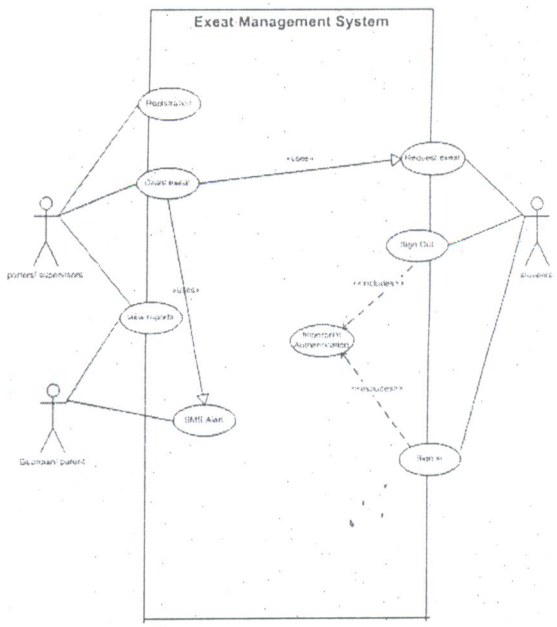

Figure 4: Use case diagram of the Mobile Students Exeat Monitoring Systems Using Fingerprint Biometric Authentication

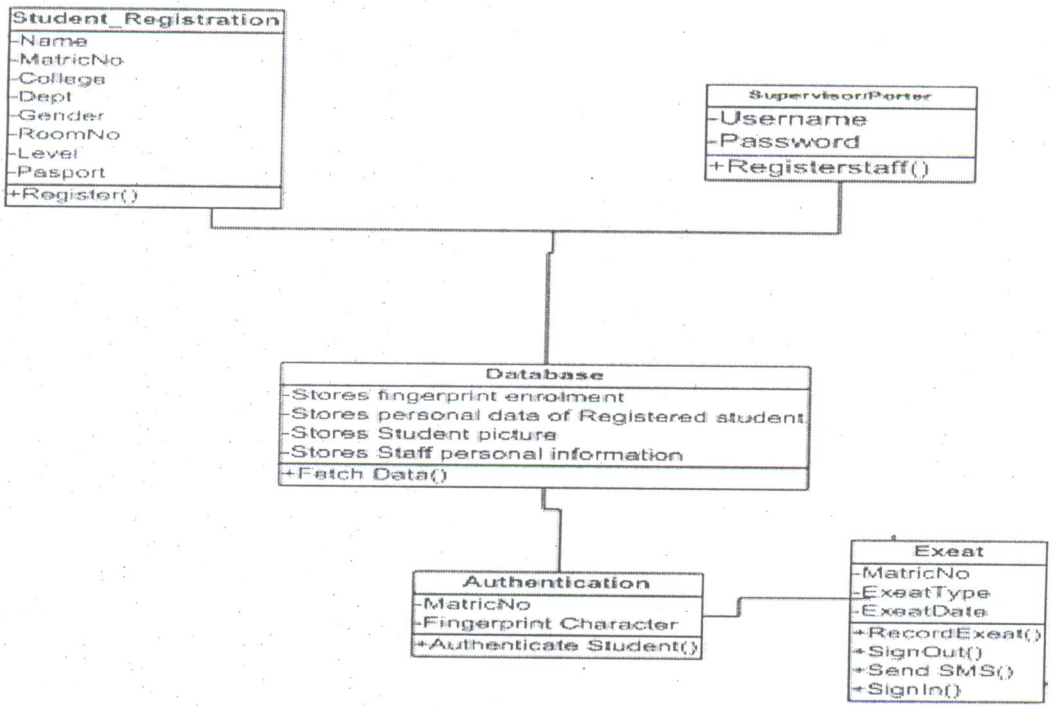

Figure 5: Class diagram of the Mobile Students Exeat Monitoring Systems Using Fingerprint Biometric Authentication

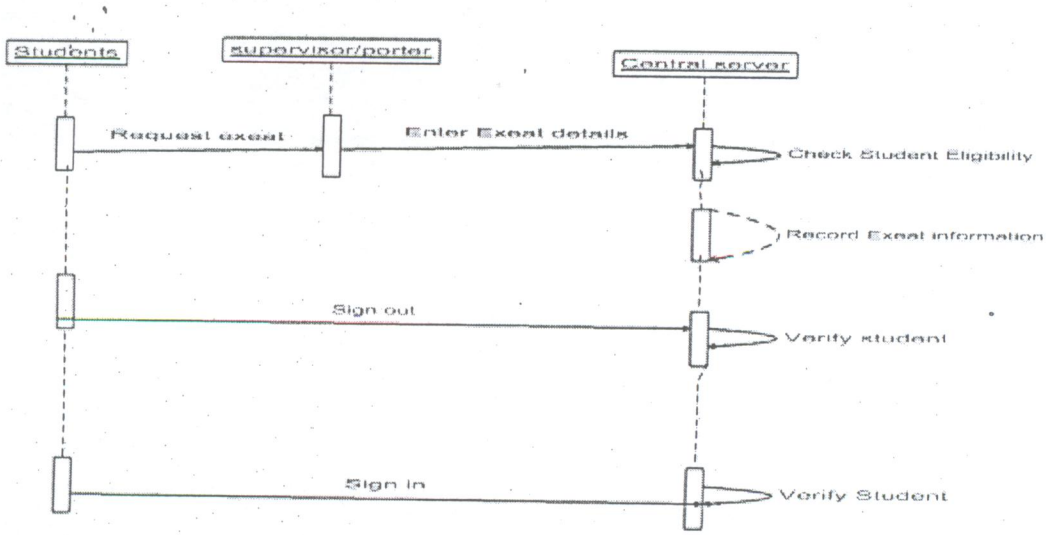

Figure 6: Sequence diagram of the Mobile Students Exeat Monitoring Systems Using Fingerprint Biometric Authentication

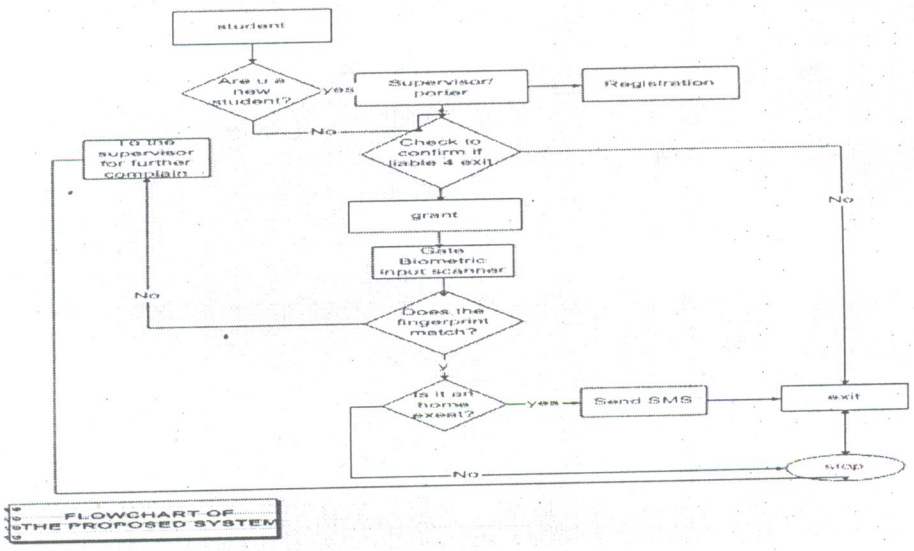

Figure 7: Class diagram of the Mobile Students Exeat Monitoring Systems Using Fingerprint Biometric Authentication

4. IMPLEMENTATION AND RESULT

The implemented system was tested using actual students' data in a typical university setting. During testing the staff logs in using his or user name and password and is allowed to grant day and home exeat, manage student records, enroll new students and then monitor if the student has returned at the expected time or not. The system grant the day exeat by verifying the fingerprint of the student and then it notifies the supervisor in charge the number of exeat that has been granted. For the home exeat it grants the exeat and then sends an SMS to the guardians phone number via the SMS gateway; stating that the student or ward has left school, and then when that student returns it verifies that the person has returned.

The exeat grant page is in two forms: the home and day exeat. This page is used to manage the type of exeat that the student has been granted. It keeps a record of the entire student and their information. The student that requires the exeat is selected from the list and granted the exeat either day or home, when this is done the status of the student changes to: "student name" has not signed in.
For a successful request granted, in the case of the day exeat as shown in figure 8 the system displays the message "exeat granted" while for home exeat request it grants the system shows the message "now sending SMS" as shown in figure 9, once this is done, it shows the message "an SMS has been sent" to confirm the SMS delivery.

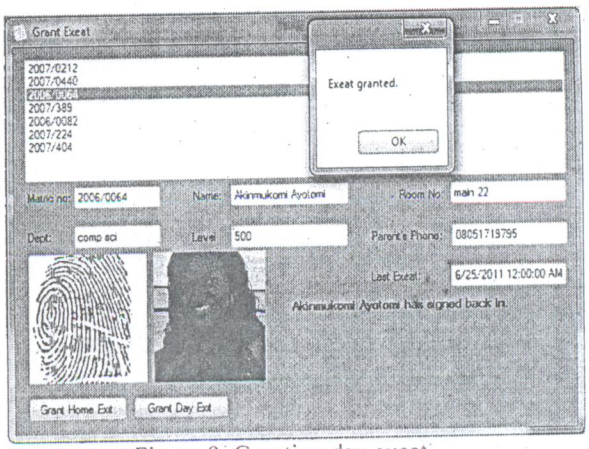

Figure 8: Granting day exeat

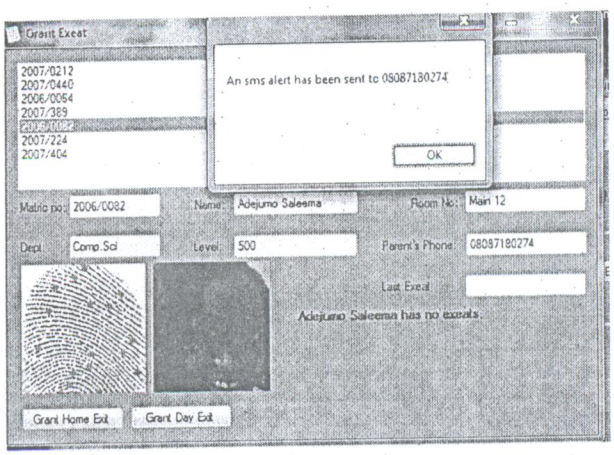

Figure 9: Granting home exeat.

A sample report page is shown in figure 10 and this page displays the student name, matric number, the type of exeat collected, expected date of return and finally if that student has returned or not. A returning student status is update once they confirm their return with their fingerprint thus, with this approach there is no problem of uncertainty as to whether a student returned or not as the system can automatically accurately monitor exeat.

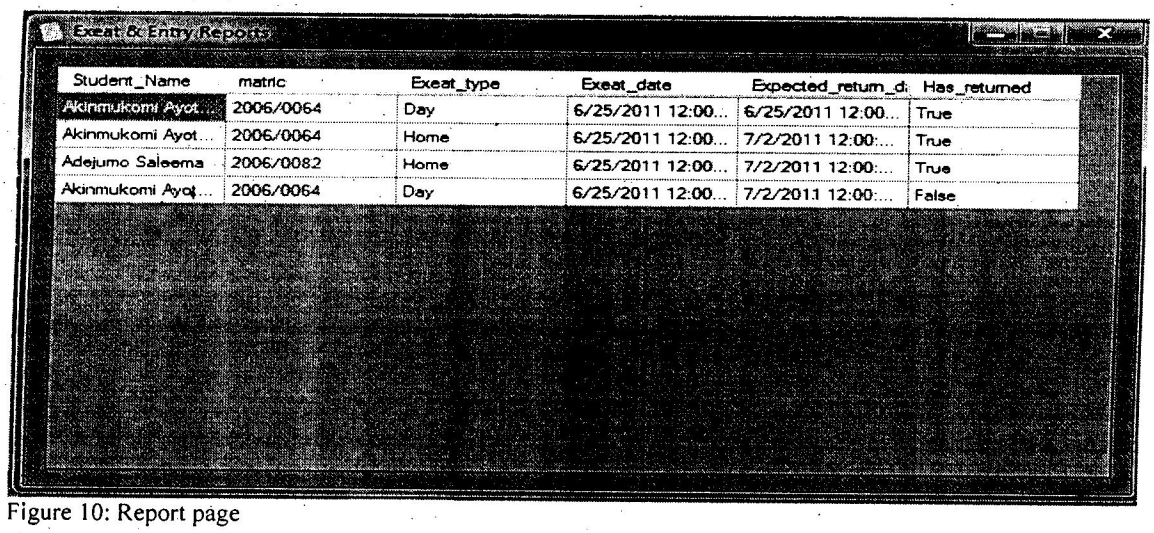

Figure 10: Report page

5. CONCLUSION

In this paper, the proposed exeat based system was developed to solve inaccuracy, insecurity and impersonation challenges of the current paper based exeat system in use in most privately owned University Halls of Residence. With aid of a fingerprint biometric authentication, impersonation of other students is eradicated. The biometric device authenticates each student before granting access; ensuring that no student can take more the required number of the exeat per unit time. The mobile short message service informs the guardians the current location of where their wards are. The proposed system has improved the existing system in the following ways: Provide electronic solution to the existing method of issuing exeat to student which is paper based; discourage and prevent impersonation; Allow guardians or parents to monitor or be aware of their wards movement when they leave school; Eliminates the cost of making several copies of paper exeat and allow the university administrator to have a report of the student's exeat activities.

REFERENCES

Abdul Kadir H, Abdul Wahab M and Siti Nurul A (2009),"Boarding Students Monitoring Systems(E-ID) Using Radio Frequency Identification", Journal of Social Sciences, Volume 5(3),pp 206-211.

Bochkov. Y, Chiem. J, Sai. Y(2007). Use Biometric Techniques in Combating Identity Theft. Loyola Marymount University Los Angeles.

Chander Kant & Rajender Nath (2005). Reducing Process-Time for Fingerprint Identification System. International Journals of Biometric and Bioinformatics, Volume (3) : Issue (1)

Frischolz, R.and Dieckmann, U.(2000). A Multimodal Biometric Identification System ,IEEE Computer, Vol. 33, No. 2.

Hua, W,, and Lili, S.,Yanchun, Z., and Jinli, C. (2004) *Anonymous access scheme for electronic services.* In: 27th Australasian Computer Science Conference (ACSC2004), 18-22 Jan 2004, Dunedin, NZ.

Khiyal M.S, Aihab Khan, and Erum Shehzadi.(2009).Software Engineering Dept.,Fatima Jinnah Women University,Rawalpindi, Pakistan.

Lee, H.C, and Gaensslen, R,E. (1991). Advances in Fingerprint Technology, Elsevier, New York.

Maltoni, D, Maio, D, Jain, A.K, Prabhakar, S.(2003). "Handbook of Fingerprint Recognition". Springer- Verlag,

Matjaž. G, Tušar. T (2007). Intelligent High-Security Access Control. Department of Intelligent Systems Jožef Stefan Institute.

Matyas.V., Riha, Z. (2000). Biometric Authentication Systems. Technical report. Retrieved from http://www.ecom-monitor.com/papers/biometricsTR2000.pdf.

Omidiora E.O (2009) A prototype of an access control system for a computer laboratory 4th edition international conference on ICT to Teaching Research and Administration (AICTTRA 2009), Ile-Ife, Nigeria 4: (114-120).

The Global Information Technology Report (2009). World Economic Forum and INSEAD. ISBN 978-92-95044-19-7

Thornton, John (2000). Latent Fingerprints, Setting Standards In The Comparison and Identification. 84th Annual Training Conference of the California State Division of IAI. Retrieved from http://www.latent-prints.com/Thornton.htm.

Vijay M. M and Dattatray V. J (2007). Review of Multimodal Biometrics: Applications, challenges and Research Areas. International **Journal** of Biometrics and Bioinformatics (IJBB), Volume 3, Issue 5. 90.

Vladimir G..(2007). Mathematical Models of Fingerprint Image On the Basis of Lines Description. Department of Applied Mathematics Chelyabinsk State University, Chelyabinsk, Russia.

Implementation of Voice over Internet Protocol (VoIP) Communication Service for Campus Environment

**Olaniyi, O.M, *Adewumi D.O, *Oluwatosin E.A, *Adeyiga J.A, * Sanusi A
**Department of Electronic and Electrical Engineering
*Department of Computer Science and Technology
Bells University of Technology, Ota, Ogun-state, Nigeria.
E-mail: engrolaniyi09@yahoo.com, adebisiash@yahoo.com

Abstract
This research work explores some of the issues related to PABX communication systems and how communication can be improved in a campus environment. The issues related to PABX systems include: the operational cost which is very high since the system is maintained by a third party, expanding the network is difficult since it requires the purchase of new hardware and running of additional cables, environmental factors such as wind, rain. The challenges will be overcome by deploying a scalable and cost effective VoIP communication system using a wireless Local Area Network and a wired network that would replace the conventional communication system used in a campus environment. Important parameters that were tested during implementation such as voice quality, latency and packet loss is also captured in this research. The effect of different codec on voice quality was tested such as the G.711 alaw, G.711 ulaw, GSM, iLBC and speex codec. At the end of the research, it was observed that G.711 alaw and G.711 ulaw generated high voice quality while it was impossible to communicate with GSM, Ilbc and speex codec.

Keywords: PABX, softphone, codec, G.711 alaw, G.711 ulaw, GSM, Ilbc, SPEEX)

1. INTRODUCTION

Communication is the process through which information is disseminated and Information is very vital for decision making. Inter-communication of voice related information is achieved through Public Address Branch Exchange (PABX) system and has recently been enhanced by variety of computer-based services, including voice mail and computerized telephone exchanged services like Voice-Over Internet Protocol (VOIP) based networking. VoIP is a technology allowing the user "to make telephone calls using a broadband Internet connection instead of a regular (or analog) phone line. Some VoIP services allow the user to only call those using the same service, while others allow the user "to call anyone having a telephone number—including local, long distance, mobile, and international numbers [Stephen, 2005].

Voice communication is quite expensive especially with PSTN line. Since VOIP uses the internet as the back bone, the only cost you incur when using it is the monthly bill to your ISP. These networks consist of many different parts, operated by many different companies, but are inter-connected using common signaling methods. The signaling between different telephone systems is done by switching, which has progressed from the simplest of hand operated switches through the more complex manual systems to the present packet switching systems.

The packet switching is a technology that splits data in a network communications into manageable small pieces, called packets. The Public Switched Telephone Network (PSTN) is the traditional telephone network that provides Plain Old Telephone Service (POTS), the network anyone could access by circuit-switch connection. This connection is a dedicated service that can guarantee the reliable, accessible and quality. PSTN converts voice into electrical signals and transmitted through the circuit-switched network (Amel, et al, 2008). There is no single template that can be followed when contemplating the use of this technology to a traditional phone system (Amel, et.al, 2008).This phenomenon has made a profound change in the world of telephone communications.

VOIP is simply the transmission of voice calls over IP-based networks. The Internet Protocol (IP) was originally designed for data networking. The traditional method of making calls the landline are being fast replaced by this technology that has taken the world by storm. Not only is this method economical as this does not involve the telephone company charges that are pretty heavy, it also gives better coverage. Other benefits of VOIP include: Fast implementation meaning cost savings realized immediately; Easy to manage from a web page where the entire voice service access can be controlled and

monitored; Unmatched system flexibility; Interoperability with off-the shelf components and applications; Leverages existing broadband or network connection for voice and data, future-proofed network which enables easy moves, adds and changes, conference calls, call forwarding, caller ID. (Ismail et al 2010) considered the deployment of VoIP in campus environments over wired networks on security during communication between two parties. The work analyzed SRTP performance on different VoIP codec selections over wired systems. This research work considered both wired and wireless network in a campus environment.

2. PROBLEM STATEMENT

The operating cost of PABX telephone systems are usually high as it requires hardware to operate and a third party to make adjustments, continuous configurations and maintenance on the telephone system. Furthermore expansion on the PABX system can be quite expensive as this might require the purchase of additional hardware and running of additional cables. The traditional PABX systems have a set of number of ports for telephones to plug into thereby restricting the number of users that can use the telephone in a particular office. It is also prone to environmental hazards such as rain.

The VOIP based telephone system can overcome the above mentioned challenges by providing a greater flexibility because it allows a number of "virtual users" through each network socket which makes it scalable. A VOIP based telephone system is based on reconfigurable software systems, easier to manage and maintain. Also in VOIP based telephone system, an enterprise can add more telephone lines and increase call capacity without running additional cabling.

2.1 Focus of the work

A communication system that is easy to manage and maintain which will also allow more telephone lines and increase call capacity without running additional cabling. Also a system that can overcome challenges of environmental hazards, reduce annual overhead cost of inter-office communication by management and expand inter-office communication link within the university is required. This study is mainly to deploy a cost-effective VOIP based telecommunication system to reduce operational cost and for effective communication. This was achieved by studying the existing telephone system of Bells University of Technology, Ota and carrying out extensive literature on the technologies of VOIP, the feasibility of the VOIP system if implemented in the campus network like Bells University of Technology, Ota, will reduce operational cost and expansion limitation of the existing PABX system

3. RELATED WORK

Voice over Internet Protocol (VOIP) is an emerging telecommunications technology that is already shaping the future of telephony. Over the past couple of years, there has been discussion in the industry about the convergence of data and voice and the pros and cons of transmitting data and voice over the same network (Akintola, et al, 2008). Voice over Internet Protocol (VOIP), is a technology that allows the transmission of voice packets over packet –switched IP networks (Richard et al, 2005).Basic VOIP access usually allows you to call others who are also receiving calls over the internet. Interconnected VOIP services allow you to make and receive calls to and from traditional landline numbers, usually for a service fee. Some VOIP services may require a computer or a dedicated VOIP phone, while others allow you to use your landline phone to place VOIP calls through a special adapter (Akintola et al, 2008).

Dar & Latif (2010) suggested, that before choosing a solution, organizations should consider both the required functionality and the potential issues. These considerations drive the protocol and equipment choices in designing the VoIP solution. Although the wide range of VoIP protocols has caused some confusion in the marketplace, it is precisely this protocol flexibility that makes VoIP-based systems so much more useful than legacy voice systems (Dar et al, 2010). In their work, they discussed the different security and quality of service issues for voice over IP networks and they propose solutions for these problems.

According to Werbach (2005), the most successful business implementations concentrated on two factors. Firstly, the implementation of the new technology benefited business objectives. Cost saving was not a primary objective. Instead, businesses used the advantages that VoIP offers over POTS to benefit their business and increase their competitive advantage. The second factor that successful adopters of the technology focused on was that they viewed everyone in their organizations as a resource, and implementing VoIP meant accessing those resources. (Lydia, 2009) Investigates the use of VoIP compared to plain old telephone system (POTS) as a communications tool in the South African business environment. The work identify major advantages, risks and provide management with insight into what VoIP is, what possible benefits it could hold for their business, and what the risks are. He classified risks under the following headings: Developmental issues, Operational aspects, Intrusion risk and Environmental risks.

Ajay (2006) Discovered in his work set of mechanisms to increase voice quality on data networks by decreasing dropped voice packets during times of network congestion and minimizing both the fixed and variable delays encountered in a given voice connection. According to Williams (2005) explains how computing technology was used to address the need for mobile communications among nursing staff. He examines how Voice over IP was applied to the mobile communications problem to produce a solution that satisfied nurse managers, nursing staff, physicians, and information technology staff.The article details how this technology was selected over several other communications technologies and used to implement wireless telephony over the hospital's existing computer network. It reviews key standards and technologies and issues surrounding their use. Finally, the article demonstrates how this computing technology improved patient care by facilitating mobile communications. Employee morale and physician satisfaction increased, and the hospital's IT and communication benefitted.

The components of VOIP include: end-user equipment, network components, call processors, gateways and protocols. End-user equipments are equipments which are used to access the VOIP system in order to communicate with another end point. Connection to the network may be physically cabled or wireless. The end-user equipment may be a phone which can be an IP phone or analog phone with adapter or a softphone application installed on a computer. Functions include voice and possibly video communication, and may contain instant messaging, monitoring and surveillance capabilities. Though end-user equipment is often deployed on an internal, protected network, it is not usually protected by security network devices such as firewalls and may be threatened if the equipment has vulnerabilities. The threat is dependent on the level of security that exists on the internal network. If the device is allowed to reach or can be reached from a public or unprotected network, there may be threats that are normally found on the internal network. Softphone software may have vulnerabilities, there may be vulnerabilities in the operating system it is running on, and there may be vulnerabilities of other applications running on the operating system.

Gateways can be categorized into three functional types: Signaling Gateways (SG), Media Gateways (MG) and Media Controllers. In general, they handle call origination and detection and analog to digital conversion. Signaling gateways manage the signal traffic between an IP network and a switched circuit network, while media gateways manage signals between the two. Media Gateway controllers manage traffic between SGs and MGs.

The most common gateway protocols are MGCP and Megaco. Both are composites or derivations of previously but now less used protocols (Greg, 2004) The protocol used by VOIP to send and receive voice as data packets over an IP network is the Internet Protocol (IP). There are several protocols used for VOIP but two are most common. They are H.323 and Session Initiation Protocol (SIP). (Akintola et al, 2008). H.323 is a protocol suite specified by the International Telecommunications Union (ITU) that lays a foundation for IP based real-time communications including audio, video and data. It was created for multimedia conferencing on LANs but due to its high implementation the company decided to expand its horizon, thus H.323 was later extended to cover VOIP. This standard specifies four kinds of components: Terminals, Gateways, Gatekeepers and Multi-point Control Units (MCU).

Terminals are the end-user equipment while gateways handle communication between unlike networks with protocol translation and media format conversion. Gatekeepers provide services such as addressing, authorization and authentication, accounting functions and calls routing. MCUs handle conferencing.H.323 uses different protocols to manage different needs. There are audio codec and video codec that encode and decode the audio and video data. (Akintola et al, 2008)

H.225 covers registrations, admissions and status (RAS) and call signaling that handles various functions between the endpoints and the gateway, including registrations and admission control. It also manages changes in bandwidth and disengages procedures (Greg, 2004). Session Initiation Protocol (SIP) is a signaling protocol specified by the Internet Engineering Task Force used to set up and tear down two-way communications session. SIP is an application layer control protocol for creating, modifying and terminating sessions with one or more participants.SIP is made up of the following components: User Agent (UA), Proxy Server, Registrar Server and the redirect server (Akintola et al, 2008).

The UA software contains client, and server components. The client piece makes outgoing calls and the server is responsible for receiving incoming calls. The proxy server forwards traffic, the registrar server authenticates requests, and the redirect server resolves information for the UA client (Greg, 2004).

4. MATERIALS AND METHODS

For the purpose of this work, real wireless network environment was setup to analyze important parameters such as bandwidth usage, delay, packet loss and voice quality with different types of CODEC

in the implementation of VOIP at Bells University of technology, Ota. This will answer the research questions listed below:

- How the choice of CODEC affect voice quality in a wireless VOIP network.
- The data transmission rate of each CODEC used in the wireless VOIP network.

A typical VOIP communication involves interaction between different VOIP clients and the SIP server. A typical VOIP model consists of a switch that will link all the communication equipment such as the SIP server, soft phones together to be in the same network. The SIP server software that was deployed for this research is a tribox based SIP server. It is an enterprise-grade, fully featured solution with integrated voice mail, Automatic Call Distribution (ACD), multiple auto attendants and a web-based system configuration and management tool, PSTN/IP gateways and end points. Some of the benefits of the SIP server include low cost, adaptability and flexibility, with the reliable solutions and support which enterprises require for voice applications.

This SIP server is also capable of supporting a remote worker solution which is ideal for supporting distributed and mobile professionals with full PBX functionality to any location that has a high-speed or broadband connection. These features allows mobile professionals to carry their extension numbers along with them wherever they go enabling them to be reached with the same extension number as long as they remain within the university's WAN. The suite is backed by a robust support and service infrastructure that can be accessed through a web-browser. The SIP server runs on a combination of the following software; CentOS 5.1 kernel, Asterisk 1.4, FreePBX 2.3,Web MeetMe 3. This different software works in synergy.

The soft phone that was used for this paper is the counterPaths's soft phone client. CounterPath's soft phone clients are built on open standards, leveraging SIP (Session Initiation Protocol) to create, run and terminate multi-media sessions. They are built on International Telecommunication Union (ITU) codec standards for voice and video (for example, G.711,G.722.2, G.723) and the SIP SIMPLE standard for Instant Messaging.

4.1 Methods

The Voice Over internet protocol Network (VOIP) server was implemented on an existing data network in a campus environment (Bells University of Technology Ota). The quality of the voice calls was measured through a subjective measure using the Mean Opinion Score (MOS) which is based on individual judgment. The measurement was done both on wireless and wired network in the campus.
The voice quality was measured on different codec; G.711alaw, G.711ulaw, GSM, ilbc, SPEEX

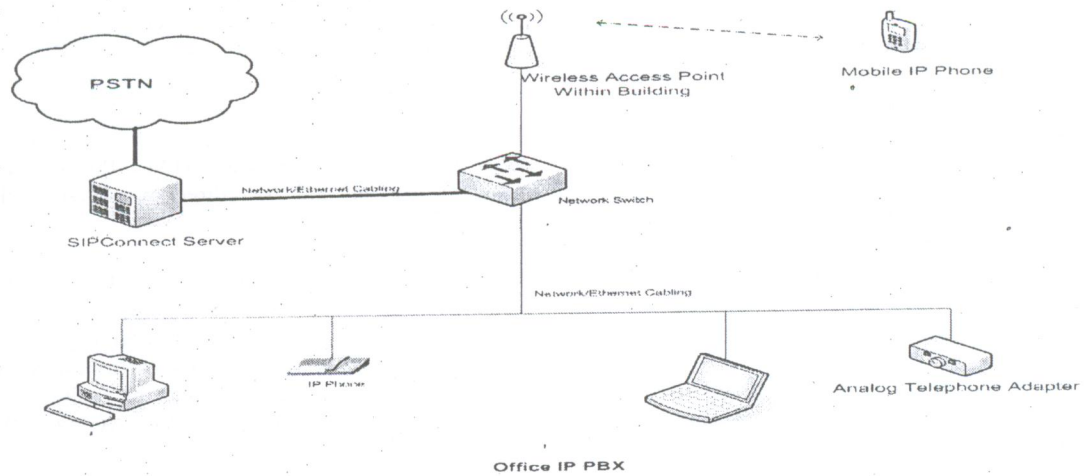

Fig 1: Conceptual Framework of the VOIP network for Bells University of Technology

A tribox SIP server was used which was directly connected to the switch with a cat5 twisted pair cable. All the devices in the VoIP network communicated through the switch to the VOIP server.

5. RESULT AND ANALYSIS

This section explained the implementation of the VOIP based telecommunication system and the parameters to evaluate its performance. It describes the functionality of the various interfaces provided by the tribox software and how the interfaces function to achieve the aim of the system. It helps further to

explain the various functions of each page and the ways each user would work and interact with it. This section also measures and compares VOIP voice quality over the choice of CODEC. It also measures the Data transmission rate for different type of CODEC. The voice quality test was done using a subjective measure. A subjective measure is a measure that is based on individual judgments which is a numerical method of measuring voice and video quality called Mean Opinion Score (MOS). Mean Opinion Score is expressed in numbers ranging from 1 to 5. 1 is the worst while 5 is the best. This is based on the International Telecommunication Union (ITU) Standard.

Table 5.1: Mean Opinion Score (MOS) Ratings for voice communications.

Mean Opinion Score (MOS) ratings	
Excellent	5 (Perfect. Like face-to-face conservation or radio reception)
Good	4 (Fair. Imperfections can be perceived, but sound still clear. This is (supposedly) range of cell phones)
Fair	3 (Annoying)
Poor	2 (Very annoying. Nearly impossible to communicate)
Bad	1 (Impossible to communicate)

System implementation covers a broad spectrum of activities from a detailed workflow analysis to the formal go-live on the new system. Therefore, in the systems implementation phase, overall working feature and conditions of the system is to be highlighted and components are described.

5.1 A scenario for two users to communicate remotely

Before two users can communicate, an account need to be setup for both user on the tribox SIP server with a unique extension number and a secret code. After, the client's soft phone will be setup with the extension number given to the user by the administrator and the secret code. The IP address of the tribox server must be entered to the soft phone setup page then the two users are connected to the same network with the tribox server using a switch or a wireless LAN where applicable. Once the soft phone client connects to the network, it synchronizes with the server to authenticate itself and if this is done successfully, the user can now make calls to one another.

5.2 Communication between six users in different locations within the campus

In reference to appendix c, Six users were selected and an account was setup on the tribox server to allow them communicate over the wireless network to measure the voice quality on different codec and also measure the data rate for each codec.

User 1 and user 2 located at the administrative block of the campus, user 3 and user 4 located in the e-library and the main library respectively, user 5 and user 6 were inside the software laboratory and computer resource laboratory respectively. User 1 called user 6, user 5 called user4, user 3 called user 2 and the voice quality was determined by each users with the International Telecommunication Union (ITU) Mean Opinion Score standard. A Cisco wireless router was used to connect all the soft phone clients with the tribox server.

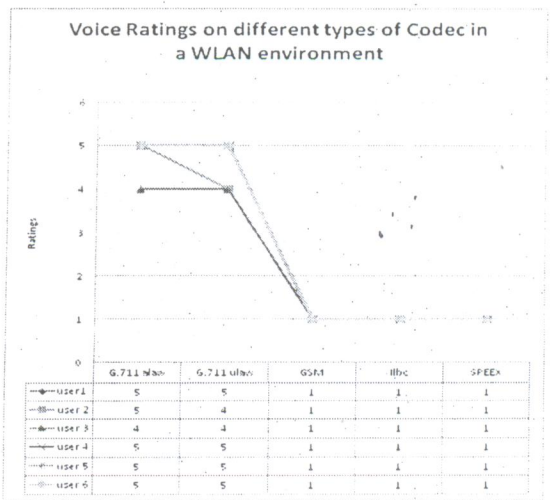

Figure 5.1: Voice ratings of different codec

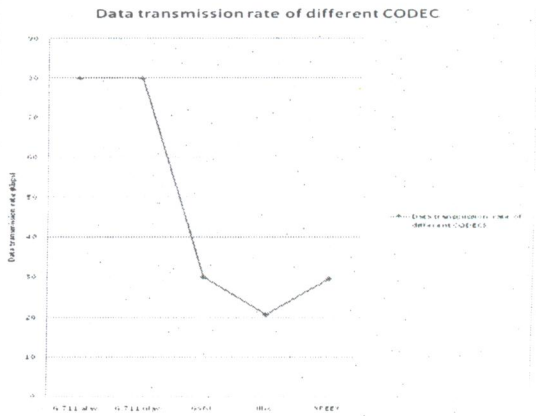

Figure 5.2: Data transmission rate of different codec

5.3 Analysis

The average Mean Opinion Score (MOS) for G.711 alaw is 4.8, for G.711 ulaw is 4.7, for GSM is 1, ilbc is 1 and for SPEEX is 1. Therefore G.711 alaw and the G.711 ulaw are the only codecs that are able to improve voice performance over a wireless network while the SPEEX, Ilbc and GSM, makes it impossible for users to communicate over the wireless network. Therefore when considering the kind of codec to use in a wireless network for voice communication, G.711 alaw and G.711 ulaw are the most reliable codec that improve voice quality in a wireless network.

The data transmission rate for G.711 alaw is 80kbps and which can support transmission for 675 calls on the 54Mbps wireless LAN device, for G.711 ulaw is 80kbps which also supports 675 calls on the same wireless LAN device, for GSM is 30kbps which supports 1800 calls over the 54Mbps wireless LAN, ilbc is 29.5kbps which supports 1830 calls on the 54Mbps wireless LAN device and for SPEEX is 23kbps which supports 2347 calls on the 54Mbps wireless LAN device. The codec with the lower transmission rate supports more calls but have low voice quality. In summary, the G.711 accommodates the least amount of calls because of its high data transmission rate but produces the best voice quality during communication.

The results obtained from the test shows that G.711 alaw, G.711 ulaw codec are able to generate high quality VOIP conversation in a one-to-one conversation on the wireless network. The MOS analysis also indicated that it is impossible to make voice conversation with the GSM, Ilbc and SPEEX CODECS in a one-to-one conversation over the wireless network.

It is therefore recommended that Bells University network administrator should adopt the VoIP system for use in the University, for Effective Communication. This will eliminate the high operational cost and maintaining the PABX system. Wireless LAN network should be adopted for easy expansion of the network.

It is also recommended that the university should encourage the students to investigate the system further, concerning the bandwidth and latency issue as the system expands.

REFERENCES

1. Ajay K, 2006 "An overview of Voice Over Internet Protocol (VOIP)" Journals from Rivier College. volume 2, pp 1.
2. Akintola K.G, Adeola S.O and Boyinbode O.K 2008. "Application of Information Communication Technologies to Teaching, Research and Administration". Proceedings of the 3rd International Conference on Voice over Internet Protocol (VOIP). vol.3, pp 195-204.
3. Amel C, Jakia A, 2008 "Analysis of Telephone System of a University Campus and Design of a Converged VOIP System" Journal of Computer and Information Science. Vol.1, pp. 4
4. Bur, G 2002. "Voice over Internet Protocol". Proceedings of the IEEE. Vol.90, pp. 9.
5. Dar & Latif, 2010 "Issues of implementation of Voice over Ip with Quality of Service: An Overview" International journal of Computer Science and telecommunications. Vol. 1, Nov 2010.
6. Greg, 2004. "Voice over Internet Protocol". Cisco articles.
7. Ismail, M.N 2010. "Implementation of secure Real Time Transport Protocol on VoIP over Wired In-campus Network Environment". Pacific Journal of Science and Technology. 11(1):287-293
8. Lydia Uys, 2009. "VOIP as a communication tool in South Africa business" African journal of business management. Vol 3(3) pp. 89-94 March 2009. Available online at www.academic journal. Org/AJBM.
9. Richard D. K, Thomas J. W, Steffen F, 2005. "Security Considerations for Voice Over IP Systems". National Institute of Standards and Technology. 800-58.
10. Stephen E. Blythe, 2005."The regulation of VOIP in the United State, The European Union and the United Kingdom" Journal of High technology law. Vol 5 No 2 2005.
11. Werbach. K, 2005. "Using VOIP to Compete" Harvard Business Review. Sep 2005, 83(9) pp. 140-147.
12. Williams Johnson, 2005. "Voice over IP: How Computing Technology is being used in Mobile Communication" Journal of Healthcare Information Management" Vol.19 No 4, 2005.

Volume 6 No. 1, September 2010.

LAUTECH

Journal of Engineering and Technology

iSSN: 1597-0000

Special Issue on the First International Conference on Engineering and Technology Research 2010.

Published by the Faculty of Engineering and Technology,
Ladoke Akintola University of Technology, Ogbomoso, Nigeria.

Lautech Journal of Engineering and Technology (LAUJET)
Volume 6 Number1 (September, 2010)

CONTENTS

ISSN: 1597-0000

Prudence Print Media (PPM) - 08069019894

1597-0000