KWAME NKRUMAH UNIVERSITY OF SCIENCE AND

TECHNOLOGY, KUMASI, GHANA

IMPROVING NETWORK SECURITY USING KEY-STROKE DYNAMICS

A CASE STUDY AT ANGLICAN SENIOR HIGH SCHOOL

BY

Boakye Obeng Michael (B.Ed Information Technology)

A Thesis Submitted to the Department of Computer Science,

College of Sciences

In partial fulfillment of the requirement for the degree of

MPHIL INFORMATION TECHNOLOGY

November, 2016

DECLARTION

I hereby declare that this submission is my own work towards the MPHIL and that, to the best of my knowledge, it contains no material previously published by another person, nor material which has been accepted for the award of any other degree of the University, except due acknowledgment has been made in the text.

BOAKYE OBENG MICHAEL (GP 5093910) …….. ……

Student Name & ID Signature Date

Certified By:

MR. DOMINIC ASAMOAH ……

Supervisor(s) Name Signature Date

Certified By

Head of Department Name …… …….

Signature Date

……

ACKNOLEDGMENT

My first appreciation goes to the Almighty God whose protections and guidance has made it possible for me and to complete this work.

I wish to express my sincere gratitude to my supervisors: Mr. Dominic Asamuah, Mr. J.K Panford, Michael Asanti and J.B Hayfron-Acquah for the directions and suggestions which assisted me to complete this research.

My profound and special gratitude goes to Anglican S.HS Head Master and my H.O.D

Special appreciation goes to Mr. Partey Benjamin, Mr. Abiew Nuku Atta and Mr. Laud Macmills for their inspirations

ABSTRACT

System administrators and safety professionals know that relying on only “userID” and “user Password” to validate users is basically not virtually efficient, particularly where system safety is at stake. A procedure known as keystroke dynamics (or, typing dynamics) is rising as an helpful way to fortify user certification. Keystroke dynamics is a thorough explanation of the timing of key-down and key-up proceedings when users enter usernames, passwords, or any other cord of lettering. Because a user's keystroke timings are as individual as handwriting or a autograph, keystroke dynamics can be used as part of a proposal to confirm a user's uniqueness. That is the idea after keystroke dynamics. Some researchers and developers have built many techniques more or less using this keystroke dynamics biometric as a form of validation to Web-based applications, e-mail and networks.

This research project seeks to provide improved technique over the works of these researchers and developers, providing second layer of security to user’s identity authentication and verification process, using keystroke dynamics on the user’s computer rather than inculcating in network server authentication process. A resultant software application from this research project is named “BioNetLogon” developed in VB.Net environment. It comes with interfaces that authenticate users (against database of users keystroke patterns) after windows logon stage, whilst controlling the user’s computer network services to ensure that only successful authenticated user gets access to the Windows desktop as well as network resources of his/her computer. Otherwise, the user is blocked from getting access to the network environment with the network services disabled.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

ABBREVIATIONS

ALT- Alternative

ATM - Automated Teller Machine

CCTV - Closed-circuit Television

CER- Cross-Over Rate

DNA- Deoxyribonucleic acid

EER - Equal Error Rate

E.G - Example

ER -Entity Relation

FAR - Falls Acceptance Rate

FNMR - False Non-Match Rate

FRR - Falls Rejection Rate

ID - Identity

IDE - Interactive Development Environment

IEEE - Institute of Electrical and Electronics Engineers

IP- Internet Protocol

IPR - Impostor Pass Rate

PC - Personal Computer

PIN - Personnel Identification Number

RAD - Rapid Application Development

SDK - Software Development Kit

SDLC - Software Development Lifecycles

TCP - Transmission Control Protocol

CHAPTER 1

INTRODUCTION

1.0 BACKGROUND

Institutions are challenged every day to make sure applications and networks are protected and maintained in equilibrium between usability, safety and cost. Information should be available all the time through different computing nodes and networking infrastructures for the flowing number of students, teachers, and non-teaching staffs. These problems with significant safety necessities verify identities, protecting information, ensuring confidentiality, conformity of standards and preventing the school from internal and outside swindle.

The most important mission of an invader who has infiltrated a system is to initiate growth of rights that is how an invader attempts to expand more right of entry from the reputable foothold that they have fashioned. After a growth of rights has occurred, there is small left to prevent an impostor from whatever objective that invader has. Attackers can use many diverse mechanisms to accomplish a growth of rights, but above all they engage compromising existing accounts, particularly those with administrator the same rights.

The majority businesses or commercial networks frequently make use of some measure of safety controls over normal user accounts, but frequently do not bring to bear many controls over service accounts, in that way making such accounts susceptible and well-liked targets for intruders. After an intruder has compromised a system to the level where a significant account with high rights is compromised, the whole system can in no way be measured as totally dependable again unless it is crushed and entirely recreated. Consequently the level of safety for all types of accounts is a

very significant feature of any network safety proposal. Aside from the risks that outside intimidation pose to a commercial network, inside intimidation also have the possibility to cause a enormous deal of damage. In-house intimidation embodies not only hateful users but also those who might cause unplanned destruction. The seemingly harmless attempts to avoid safety procedures by users that seek access to resources are but one instance. All too often, users and services are approved access to greater rights than required for reasons of expediency. Even though this approach pledge users have right of entry to the resources they require to do their jobs, it also increases the danger of a flourishing attack upon the system. Network administrators and professionals use ID and password to validate users, this is known to be in adequate to successfully validate a person.

This is some of the attacks (pushing, spyware, keystroke copying and simple brute force password crack.) Private and community network, with susceptible valuable information gain attention. Commercial organizations are ensuring safety strategy to incorporate multi-factor procedures something you know. Password or passphrase with something you are a biometric or something you have a smart card.

A system known as keystroke dynamics, typing dynamics is now emerging as a useful tool to intensify user verification. Key stroke dynamics can be explained as timing of key down and key up events when users enter user name and password, or other characters because user key strike dynamics timing is unique as their handwriting or an autograph. Key stroke dynamics can be used as a plan to validate users individually. The idea of key stroke dynamics has been in existence since World-War11. Every individual who uses the computer also uses a keyboard.

The keyboard is placed disjointedly in frontage of the monitor, attached within the laptop or even in the smart phones. Some people write leisurely, others quickly. The typing tempo might modify over occasion, subject to the temper and period of the day. Biometric keystroke appreciation is the expertise of distinguishing persons from the mode they type. By using diverse statistics investigation methods, it might be that each user has an exclusive technique of typing.

Exploring at diverse procedures to analyse the structures of keystroke is growing since the World War II and becoming common region of exploration in keystroke biometrics. Feature mining from typing is critical for the competent keystroke appreciation. Throughout history, numerous diverse structures were used such as latency, duration, pressure, etc. A study of several investigation works shows that there are two types of keystroke dynamics. The first one is static keystroke dynamics in which the keystrokes are analysed only at explicit times e.g. during login. The second one is endless keystroke dynamics in which the typing features are analysed during a whole session. Static methods deliver vigorous system-user confirmation as opposed to normal passwords. Nevertheless static methods do not offer endless safety, specifically they cannot perceive replacement of the user after the preliminary confirmation. Endless confirmation monitors the user's typing performance throughout the session. Therefore it can be used to spot abnormal typing tempo instigated by say sleepiness. A lot of intelligences can be established on keystroke dynamics dealing with a static confirmation. Fewer can be originated on Keystroke dynamics based on endless confirmation.

1.1 Objectives

An individual's typing arrangements can be as matchless as a thumbprint or autograph. That's the impression behind keystroke dynamics. Some scholars and designers have developed many procedures around using this keystroke dynamic biometric as a form of confirmation to Webbased

applications, e-mail and other systems. This research project seeks to provide an improved method to user uniqueness certification using keystroke dynamics that will check to ensure that only authenticated users have entrance to the network and without wasting network bandwidth by processing all the keystroke dynamics issues on the workstation or local machine. On failure to confirm authentication, the authentication system or application will block the workstation machine desktop, thereby preventing the intruder from logging on to the system.

1.2 Problem Statement

Access to ATM is usually controlled by passwords or PINs. After the user enters his users-ID (his card) in an ATM machine, the user will be asked to enter his PIN or password. The main problem appears when a user loses his card and the card falls in the wrong hands, the guessing of PIN or password can be possible after many tries. So getting hold of a card (without knowing the password) does not necessarily allow access to the card owner account. However, currently if an imposter gets both the card and password of an account owner, there is no way to stop the imposter from using the card and cashing money from the account. The user-ID (card) and PIN (password) are available to the legitimate user and to the imposter, how to stop the imposter and to allow the legitimate user to access the system. In the same manner, if a hacker succeeds in having access to a networked computer nothing can stop him from pretending to be an authorized user on that computer, and inherit all the privileges of the user whose account he has hijacked. This scenario can afford the cracker some rights to launch malicious attack on the network resources. Except somehow all user activities (on the computer) are stopped, or deactivated pending current user's verification and authorization. Constant checking of a user's behaviour is an indispensible component of user identity authentication using keystroke dynamics in network security. Because of the conventional password-based systems used today, there is practically no way to verify that

the user originally authenticated is the user still in control of the keyboard. Network security is usually focused on essential network resources such as servers, networked computers, data storage devices, input and output devices. User authentication part of the network security usually occurs at login stage. Continuous authentication is practically out of the way in a server-client model. There is no way the network gateway (or servers) or firewall may periodically request for any form of user authentication in other to ascertain that the user initially genuine is the same user still in control of the keyboard. Implementation of this may increase network latencies, access to server or network resources may be interrupted unexpectedly, and sometimes cause packet retransmission, creating heavy traffic in the entire network. Therefore, theoretically it will be expedient to rest the authentication technique on the workstation rather than on a network server or terminal. Currently, the keystroke dynamics techniques or methods in the market were not developed with continuous network-based remote authentication in mind. It is upon this problem that this research project turns to provide an improved solution for steadier network security.

1.3 Research Questions

- Can an entire network logical connection becomes less busy, with load of keystroke dynamics authentication traffic, trying to authenticate everyone on the network?
- The use of behavioural peculiarity rather than physiological characteristics as a sign of distinctiveness has limitations, can keystroke dynamics solve this problem?
- Can keystroke dynamics implementation made cheaper since the single hardware essential is a keyboard, which makes it almost free?

1.4 Background

Access to only valid users and surviving attack of pretenders is one of the tests in computer safety. User ID and password are the greatest commonly used technique for validation in computers. The technique has much flair such as password distribution, brute force, shoulder surfing, destroys attack, pushing and guising and many more.

Keystroke dynamics is the cheapest behavioural biometric which recognize the legitimacy of a user when he/she is using a keyboard and not a prey to malicious hacking or cracking feat.

User verification precludes unsanctioned information access when information provided is safe. This is completed for the resolution of execution of reliable network parties.

User information is in three groups

(1) Knowledge

(2) Object or Token

(3) Biometric

Biometric is the arithmetical examination of natural explanations of phenomena. Measurements of Biometric can be classified under physical and behavioral. Keystroke Dynamics, being a behavioral measurement is an arrangement displayed by a person by the use of an input device with a dependable routine. Measurements previously accessible by the keyboard can be operated to regulate. Dwell time is the time a user keeps a key pressed and flight time in the time a user takes to jump from one key to another.

Difference in algorithms is between complete and relative timing. The data is then examined to control collective fairs like rhythm, spatial correction, content and consistency. This is put through an autograph processing routine. It infers the principal accompanying patterns for future confirmation. User validation is one way to realize this. The biometric methods do not have

problem with losses, stealing and memory difficulties. They are not completely fault free. It includes two kinds of mistakes. False Accept Rate (FAR) which signifies rates that a pretender is permitted access. False Reject Rate (FRR) also signifies the degree at which the genuine user is deprived of access.

Key stroke dynamics previously were found in numerous zones in some few years earlier. This knowledge has enable users safety. One of the many ways to improve network security is to control network access on network clients, by controlling network services and protocols running on the client. Client-server models usually involve the client initiating connection to the server through special authentication token. On meeting specific conditions, the client node is either approved or snubbed access to the network (or the server) resources.

However, a network node which is physically connected to a network, can be configured with the network IP/TCP credentials (in case of static IP configuration) in other to have access to the network. Getting access to resources available on the other network nodes (including the server) depends on conditions available on that network node. Through many available hacking and cracking techniques, unauthorized network node being introduced to a network in this manner may be free to launch malicious attack on the network itself (or on specific targets) thereby compromising the network security. Keystroke dynamics authentication can be applied to improve network security by controlling user access on network node through authentication and verification mechanism.

1.5 Justification

Validation and confirmation of users for computer security are zones which require attention and consideration. A motivation for it is as a result of extraordinary number of attacks which previously genuinely. Users account is used to gain access to forbidden materials or rights.

Password predicting/pilfering, period hijacking or perimeter controls are examples of ranges where normal conformation has failed. A password and username is the most extensive validation and confirmation structure used. Biometrics are accepted as one of the harshest confirmation structures to interruption, because they are the toughest to takeoff or replica, unlike user IDs and passwords, which can be simply pilfered and used. Merging two validation features together generates an extra layer of protection for a network. If attackers break done one feature, they still have the additional one to crash until acquiring hateful access. In this research work, keystroke dynamics application (in Microsoft Windows .Net platform) is developed as an additional security layer for user's system and the network in which the user's PC is to be connected to. Thus, it forms second security layer, after windows usual logon authentication process. This technique is necessary, because it ensures that:

- Proper security authentication and authorization is ensured at the user level on each PC in a network.
- Unauthorized persons are not allowed into the network (or the server resources) through legitimate computers in the network.
- During authentication, network services are totally disabled (on the user's computer) until the process is successful. In the event of an unsuccessful authentication or verification, the user's computer will still remain connectionless.

- The following chapter will review various researched works in improving network security using keystroke dynamics, their failures, flaws and specific strength.

1.6 Methodology

Understanding of the problems of the network authentication at the Anglican Senior High School, calls for the gathering of information through observation of the existing authentication system, interviewing of the users and testing of the existing system, to expose the various authentication problems. Since this is not the first time such a researc h is going to be conducted, a number of research works on keystroke dynamics should be reviewed to get better ideas to solve the problem at hand. This will lead to an appropriate software development life cycle, resulting into successful algorithm. After t hat Visual Basic will be used to develop a software called BioNetlogon. BioNetlogon software will be installed at the school after a successful testing.

1.7 Limitation

The research is limited to using keystroke dynamics authentication system to secure the local area network at Kumasi Anglican Senior High School.

CHAPTER TWO

LITERATURE REVIEW

A review of prevailing keystroke dynamics procedures, metrics, and diverse styles are given in this chapter. This chapter also deliberates around the numerous network safety topics and tasks confronted by keystroke dynamics.

2.1 Biometric Measurements

Measurements figures are deliberated as statues which produce an accurate match. Partial matches are mostly as a result of inconsistency in the capture procedures, as insertion portion of a finger on a fingerprint device. Physical biometric are DNA, Retina, Iris, Head geometry, fingerprint and vein structure. Behavioural biometrics describes distinctive characters unveiled by an individual that can regulate individuality.

Measurements which are accepted dynamically results in confidence matches. The superiority of measurement is diverged behaviorally and exterior issues being measured. Behavioral biometric examples are; voice, handwriting, speech, gait, language, typing patterns and gestures. Key stroke dynamics as a behavioral measurement is designed to exhibit an individual input using a method in a reliable fashion. New measurements previously available by keyboard can be used to regulate Dwell time. Disparities of procedures Reliability. This is then put into an autograph dispensation routine, which gathers the principal (and additional) designs for future confirmation. There are many challenges facing Keystroke dynamics. One contest is that the identical individual's typing rapidity can differ significantly on diverse processors or diverse periods, even on the same

processor. Another is how to ensure that the right person is still the same person using the same system after sometime. There's also the problem of what occurs when an individual halts a hand or finger. The greater challenge is how to authenticate users seeking access to a network resources, or network node. Keystroke biometrics is still less popular than other procedures of biometric verification since not sufficient individuals are acquainted with it yet. Like other biometrics, keystroke dynamics is presently not a faultless explanation, as compared to other forms of user/system authentication solution. Hence further research and improvements are required. Utmost safety specialists approve that exhausting layered procedures is the finest. Keystroke dynamics can be one portion of a collection of confirmation approaches, or as add-on to operating system authentication mechanism. This research work seeks to study, analyse and propose method to improve network security using keystroke dynamics (Joyce et al, 1990).

2.2 Research Field and Subject of Study

This section briefly reviews the challenges facing development of keystroke dynamics techniques as a subject of study in this research. Recognising the fact that research in this field has not been widely appraised over the last decade, this section briefly highlights some of the issues that contribute to its unpopularity. Keystroke dynamics is habitually appropriate to confirmation, but likewise documentation is possible. In confirmation it is recognized who the user is expected to be and the biometric structure should authenticate if the user is who he assume to be. In documentation, the biometric method should recognize the user deprived of any supplementary information, using just keystroke dynamics. Utmost uses of keystroke dynamics are in ground of confirmation. One of the most probable conceivable uses for Keystroke Dynamics in the corporate and information domain today would be for user documentation commitments. By having the

explicit user standardised to typing a precise expression or password, the investigative software would be able to translate whether or not the user is the permissible foundation based upon reluctance and swiftness of the stroke. Thus basically typing the password or pasting it within the suitable area would not work since the flight time and dwell times would not match. This would exclude safety threats to an information structure even if the genuine text or character permutation was discovered to an external foundation. Furthermore, this software could be used to differentiate one individual from another in signal based communications, such as typing or transmitting, where the user is physically recording the pointers conferring to their own regular patterns. Even though not able to recognise fresh users, the system can associate input pointers to reputable models and regulate whether or not the anticipated user is the one communicating the gesture. Keystroke appreciation, however, is apparently a more semi-prominent biometric than fingerprint. It gives the likelihood to recognize human-beings in-front of a computer without any "real" direct unambiguous collaboration with the computer. For example, while a person is typing something on the computer, the computer will extract features and analyse the keystrokes where the user doesn't need to think of the authentication. In case of weak quality features, it would be more sufficient to have it as second security authentication (at application level), whilst operating system log-in precedes as the first security authentication layer. This is because keystroke appreciation is still under investigation to be a durable and vigorous biometric. However, until now the keystroke recognition can be used as a supplementary technique for growing safety by prominent and intermittent re-confirmation of an individual personality (Magnus, 2009).

2.2.1 Ease of Use

The foundation for challenging or witnessing one's pattern for typing is the recurrence of typing so that variances can be noted and designs witnessed between words. Presently most answers, comprise original comprising of the user typing a sequence of words over lengthy periods to break

up the time. Compulsory typing due to repetitive strain wound, over lengthy periods of time can encourage exhaustion, pressure, and other issues, such as modest typing mistakes, which may inhibit the template's accuracy. When properly regulated, the pattern is certainly able to differentiate whether the conventional user is typing or not by equating the flight and dwell periods to those set on the pattern Monrose et al, (1997). It can therefore be deduced that the disappointment of comfort in respects to using keystroke dynamics method is what prevents its uses from the unrestricted arena. Locating a sequences of recognized users is time overwhelming and centered on the trainings of one specific learning, may be hard to replica by that user than by that of another user. Also, the disappointment of the program to definitely recognise fresh suitable user while in place confines its use. While advances are actuality made to formulate the program for such cleverness, it has not yet been merged.

2.2.2 Features Used with Keystroke Dynamics

Keystroke dynamics embrace numerous diverse capacities which are perceived when users presses keys on the keyboard. The imaginable measurements embrace the following

Latency in successive keystrokes

Length of keystroke, held time

Complete keystroke rapidity Occurrence of mistakes

The practice of using supplementary keyboard, example typing numbers with numerical pad.

How the user press keys if writing block letters, shift or letter key greed first.

The energy required to strike a key while typing.

Data can be universal. Data can be collected for all key or keystrokes distinctly. Many organizations don't automatically enjoy all the features. Most programs calculate just latencies among successive intervals of keystrokes. These are vibrant variances in latencies and typical deviations. Latency among keystroke during writing word 'password' let say three individuals, characters are typed numerous times. Latencies between keystroke and the length of keystrokes are generally calculated because it can easily be calculated with standard PC hardware.

Together key press and release keystroke dynamics statistics has nevertheless scarce difficulties. Numerous keys pressed at the same time means that the user punches the succeeding key before freeing preceding one. This frequency occurs relatively regular when typing quicker. Subject to what is calculated, there could be negative time among freeing a key and punching the succeeding ones. It improves marginally to difficulty for the key stroke dynamics application.

2.2.3 Typing Speed

Additional contest is that there is an identical extensive variation of typing talents, and the biometric application must labour for all operators. First of all, the rapidity of typing can be largely diverse among diverse individuals. A qualified touch-typist inscribes effortlessly numerous tens of times quicker than an amateur using "hunt-and-peck" smartness with one finger. Similarly the predictability of a skillful writer is much superior – there is no necessity to stop and meditate where certain characters are positioned on the keyboard. The typing can also be affected if the user is on a minor stage of vigilance, for instance drowsy or sick. Users will moreover occasionally have injury and subsequently write in an abnormal technique for a few months when a hand is covered, or type with singly hand when holding food in other hand and so on. Shifting keyboard to a diverse

model or using a mobile phone in place of a normal computer can also disturb keystroke dynamics immensely. All these reasons have to be considered when planning a keystroke dynamics application (Monrose et al, 1999).

2.3 Technologies

Biometric machineries are defined as computerised approaches of confirming or knowing the uniqueness of an existing individual grounded on biological or behavioural features (Anil et al, 2004). Due to the advance security associated with the use of Biometrics in combination with existing security approaches the approach has really gain grounds and acceptance in the security sphere. The phenomenon comprises individual traits or actions and these features is nearly separated as biological and behavioral categories (O'Gorman, 2003). Biological features here points to what nature or naturally is bounded to an individual and records of physical structures of an individuals' body particular instances of which includes Thumbprints, Hand Geometry, Vein Testing, Iris Scanning, Retinal Scanning, Facial Recognition, and Facial Thermo gram. Behavioural features are associated to what an individual does, or how the individual uses the body. Speech print, gait identification, Autograph Identification, Mouse Dynamics and keystroke dynamics, are respectable instances of this collection. Keystroke dynamics is considered as a robust behavioral Biometric founded Confirmation application (Awad et al, 2005). It is a procedure of examining the manner an operator or system user punches at system terminal via watching the terminal keyboard to recognize operators founded on typical Keystroke Dynamics designs. Furthermore, different biometric application, whose installation could be better off. The whole concept is virtually priceless since Keyboard as a hardware module is the sole prerequisite.

2.4 Verification Techniques

Keystroke verification techniques can be classified as either static or dynamic (continuous) (Monrose et al, 1999). Static confirmation method examines keystroke authentication features simply at explicit periods as long as a supplementary safety as the customary username/password.

Static methods deliver additional vigorous operator authentication than normal passwords nonetheless the recognition of an operator modifies after the logon verification is intolerable. Uninterrupted confirmation, on the other hand, observers the operator's keying conduct throughout the progress of the communication. In the continuous way, the operator is checked on a consistent basis during the period he/she is punching on the keyboard, permitting a live period investigation (Monrose et al, 1997). This implies that even after a successful login, the typing patterns of a person are constantly analyzed and when they do not match the user's profile, access to the system is blocked.

2.5 Methods and Metrics

Earlier lessons have recognized a collection of statistics collection procedures and punching rubrics with which the concept of keystrokes examination is founded. Succeeding segment abridges a simple approach and rubrics used (Shanmugapriya et al, 2009).

2.5.1 Static at Login

Static keystroke investigation validates a keying design founded on a recognised keyword, phrase or some other prearranged characters. The keying design accepted is equated alongside a beforehand documented keying designs saved throughout system acceptance.

2.5.2 Periodic and Continuous Dynamics

Dynamic keystroke examination validates an operator on the foundation of their typing throughout a registered gathering. The document, which is recorded in the registered assembly, is then equated to a saved typing arrangement to conclude the deviances. In an intermittent arrangement, the verification can be perpetual; either as portion of a scheduled administration. Uninterrupted keystroke examination spreads the documents collection to the complete period of the recorded period. The uninterrupted structure of the user observing gives meaningfully additional facts upon which the confirmation finding is founded. Moreover, an imitator could be noticed previously in the period than under an occasionally watched application.

2.5.3 Keyword and Application-Specifics

Keyword-specific keystroke investigation prolongs the nonstop or interrupted observing to deliberate the metrics connected to particular keywords. Further checking is prepared to discover probable misapplication of delicate instructions. Static examination could be used to precise keywords to obtain a progressive self-guarantee assumption. Application-obvious keystroke examination further outspreads the uninterrupted or intermittent watching. It could be conceivable to improve isolated key stroke designs for diverse programs. In calculation to a variety of application situations, changes in keystroke rubrics or metrics are probable.

Succeeding are rubrics commonly applied by in the field.

2.5.4 Digraph and Trigraph Latencies

Digraph latency refers to rubrics normally applied and calculate in most cases the interruption among key-ups and the subsequent key-downs happenings, fashioned throughout standard keying

(e.g. pressing letter T-H). Latency in Trigraph spreads latency in digraph rubrics to deliberate scheduling for a third stroke (A typical example. punching characters T – H – E).

Latency in Keyword deliberates latency generally for comprehensive (www.the freedictionary.com)

2.6 Performance Measures

Presentation of Keystroke examination is classically calculated in relations of numerous mistake degrees, specifically "False Accept Rate (FAR) and False Reject Rate (FRR)". The concept of FAR revolves around an impersonators' likelihood posturing in the position of lawful operator with the intelligence to achieve entrance into to a protected network effectively according to Guven et al, (2003). In mathematics, this is assumed a Type II mistake. FRR on the other hand calculates a proportion of lawful operators who are founded by Keystroke Dynamics

Confirmation and disallowed been tagged as impersonators and mathematically assumed as Type I mistake. These two instances must be rated straight away zero percent (0%). Type II associated mistakes must not be given room for any unlawful user authentication logging in although Type I mistakes as well must be irregular due to chances of lawful operators going irritated because the system discards their credentials mistakenly. Among the normal calculation in biometric program involves degree associated with the combinational receipt and discard mistakes are identical. The following terms are associated with these instances thus "Equal Error Rate (EER), or the CrossOver Error Rate (CER)" the value of which depicts a proportionate equivalence between false acceptance and rejections thus the variance in EER and accuracy in the Biometric system. (www.webopedia.com)

2.7 Keystroke Analysis Approaches

A number of studies have already been conducted in the field of biometric but at the front line are;

- Arithmetical procedures
- Neural system procedures

The straightforward indication of the arithmetical method associates a reference “typing set” features associated with definite operator and comes with keying features test of the same user or set for an intruder. At any point in time, the space or gab between the two sets should not be more that a convinced minimum either than that the operator is accepted as an intruder. Artificial Neural

system procedures initially figures a forecast model from past records, and implements the idea to forecast a conclusion of a newer experiment. Granting readings inclines a difference in methodology evidential in keystroke exploits to trending classification methods used. All of which should to explain associated tricks of coming out with vigorous and cheap verification tools.

Table 1 gives a summary of main the investigation methods completed

Table. 1: Approaches in Keystroke Analysis

Study	Classification	Technique	Operator (Users)	FAR (%)	FRR (%)
Joyce et al, 1990	Static	Statistical	33	0.25	16.36
Leggett et al, 1991	Dynamic	Statistical	36	12.8	11.1
Brown et al, 1993	Static	Neural Network	25	0	12.0
Obaidat et al, 1993	Static	Neural Network	24	8	9
Napier et al, 1995	Dynamic	Statistical	24	3.8 (Combined)	
Sadoun et al, 1997	Static	Statistical	15	0.7	1.9
		Neural Network		0	0
Monrose et al, 1999	Static	Statistical	63	7.9 (Combined)	
Cho et al, 2000	Static	Neural Network	21	0	1

Furnell et al, 2000	Static	Neural Network	14	9.9	30
Bergadano et al, 2002	Static	Statistical	154	0.01	4
Guven et al, 2003	Static	Statistical	12	1	10.7
Sogukpinar et al, 2004	Static	Statistical	0	0.6	60
Dowland et al, 2004	Dynamic	Neural Network	35	4.9	0
Cho et al 2004	Static	Neural Network	21	0	3.69
Gunetti et al, 2005	Static	Neural Network	205	0.005	5
Clarke et al,2007	Static	Neural Network	32	5(Equal Error Rate)	
Cho et al, 2007	Static	Neural Network	21	0.43 (Average Integrated Errors)	
Pin et al 2008	Static	Statistical	50	6.36(Equal Error Rate)	

With the exception of Pin et al (2008) most of the current researchers prefer the use of neural network technique. Majority of the good results of False Accept Rate (FAR) and False Reject Rate (FRR), are from the neural network technique. In terms of classification almost all the good results came from static even from the beginning of the research into keystroke dynamics

2.8 Security of Keystroke Dynamics

Minute investigation has been directed to examine keystroke dynamics regarding safety. The use of keystroke dynamics to network access safety is comparatively fresh and not extensively used in practice. Evidence on factual report of violation keystroke dynamics verification program does not occur. Keystroke dynamics systems are examined concerning customary attack methods in the subsequent segment. The customary attacks can be categorised as:

- Shoulder Surfing
- Recording Users Information
- Social and Engineering
- Guessing Brute Force
- Dictionary Attack

2.8.1 Shoulder Surfing

A modest method to acquire a user's password is to look at him throughout verification. With the coming into the existence of CCTV installations in the security sensitive establishments, an intruder now do not need to be closer or at the same office to be able to watch someone when he or she is typing a password. CCTV installations do record, therefore an intruder can copy and playback the video recording from the CCTV installation which is termed as "shoulder surfing". With the advent and implementation of keystroke dynamics shoulder surfing is no more a major threat to system breach or intrusion in which instance passwords do not come into play in recognition scenarios and as such authentication details would not be pilfered. What is significant and highly conclusive is the design of the keystroke in which case an aggressor been intelligent to acquire an operators user credential will still find it difficult to hack the system. Nonetheless, the phenomenon confirmation is a two-way confirmation machinery since the design should still equate the log credentials.

2.8.2 Recording Users Information

Spyware is an application that registers facts about operators or users unknowingly and they are undoubtedly a great and cool technique to break application with keystroke dynamic verification. With spyware operators user credentials as well as keystroke latencies and durations can easily be recorded to replicate a user associated keystroke design and as such further investigation in this realm is anticipated.

2.8.3 Social Engineering

Social engineering is the rehearsal of finding personal evidence by mental management of genuine operators. A social engineer will usually use the phone or Internet to deceive individuals into giving out delicate records or convincing them to do something that are in contradiction of classic procedures.

Phishing simply is another form of social engineering through internet, system response and other automated methods. Social engineering is not highly conceivable to keystroke dynamics since no user credentials can be easily given out freely. Requesting user credentials via phone and creating a lawful impression to the user cannot be easily achieved.

Nonetheless, the use of Internet for social engineering could be a means to trick users or operators to leak out their credentials (keystroke pattern). Aggressors in most of these phishing act may represent a dependable individual, requesting operator credentials to gain access into a system. Upon gaining access, the aggressor may go ahead and save the patterns associated with the keystrokes. Nonetheless, the accomplishment degree perhaps would be actually small and the

operator therefore must punch or key in the user credentials several times to get an understandable keystroke design.

2.8.4 Guessing and Brute Force

On the average system users are likely to use normal or every day words as password and this leaves majority of user credentials stand the chance of been replicated. There are numerous ways of predicting passwords of users or operators notwithstanding that keystroke dynamics prediction is intolerable. In a brute force attack, an impostor attempts all potential groupings of words to break user credentials. The further multifaceted a systems or user credential is the harder it is to be hacked or guesses. The best move to fight against brute force attack is to have a lengthier password thus the longer the combination of characters, the more secured a password is but this attack is unbearable to keystroke dynamics. The troubles associated with programs are the mechanical creation of keystrokes design and the reproduction of human participation. A system therefore becomes more secured with the combination of keystroke dynamics and the usual user password

2.8.5 Dictionary Attack

Dictionary attack involves a procedure to overpower confirmation machinery through deciding to pass expression in a way to examine a big number of potentials. In disparity brute force attack, wherever an examination is done through comprehensive analysis, dictionary-based attack only attempts likelihoods that furthermost brings about possibility to thrive, normally resulting in a list of characters in thesaurus. For dictionary attacks, it is unfeasible and scarcely unbearable to transfer dictionary-based attacks to canter keystroke dynamic verification devices (Benny, 2007).

It is possible to use a dictionary attack which contains an overall keystroke designs, but an mechanical dictionary attack will be extra multifaceted than a text founded dictionary attack. Again the attack applications must mechanically produce keystroke designs and reproduce human-inputs. In a nutshell, brute-force attacks and dictionary-based attacks are not very much successful on keystroke dynamics.

2.9 False Alarm and an Imposter Pass Rate

Commentary of examination into Keystroke Dynamics initiated in the early 1980's with the frequently quoted groundbreaking publication by Gaines et al (1980), from RAND Corporation. The calculations done proofed that efficiency of Keystroke Dynamics structure by two factors which is still in use today. FAR, which is the keyboard pattern rate is wrongly known as fitting intruder. IPR which is the rate an intruder's keyboard pattern is mistakenly acknowledged as fitting a genuine operator (Bergadano et al, 2002). The perfect condition for a successful implementation of dynamics is to have these two factors far from anything thinkable and the best out is to have more FAR than IPR for the safest situation.

In Gaines et al, (1980), the test carried on seven typists to rekey equally three sections within two diverse periods over a four month period and have it mastered by the dynamics. Their fallouts associated exhibited a FAR of 4% and an IPR of 0%. This showed the theory of documenting user keyboard timing as feasible and a challenge appraisal of efficiency of the implemented approaches owing to inadequate test measures.

Another study proofed that their uniqueness 'Verifier' founded solely on keystroke techniques. In their tests, thirty three operators each delivered an orientation autograph by keying login

credentials a number of times. Operators' records are gathered for the five occasions he/she tries to login to their account. Six out of the thirty three operators performed as intruders or pretenders and tried gaining access into the remaining twenty seven accounts. This resulted in an FAR of 16.7 % coupled with an IPR or 0.25% suggesting a rejection of one out of six logins. Joyce et al, (1990) annotated that a higher IPR considered acceptable would reduce FAR and also noted that a reduction in FAR could be gained considering a little increase in IPR with a modification in thresholds in certain ways

Cho et al, (2000) reported that "a FAR of 1% which is within the specification for acceptance by users suggested by Robinson et al, (1998)". However rejection of results by slow and unprofessional typist which is acclaimed to improve FAR still leaves room for further investigation. Yu et al, (2004). This reflects on this work and identified two major issues thus:

1. Excessive training time 2.

Larger data inputs

A proposed solution to curb the situation while still maintaining similar FAR and IPR results.

2.10 Keystroke and Durations Latencies

Duration is the length of time keys are pressed. Whiles latency is the time between successive keystrokes. Monrose et al, (1997) acknowledged the work of Joyce et al, (1990) and extended their research work by:

- Probing the use of keystroke durations in addition to keystroke latencies. ▪ Discovering the extensive periodic keystroke dynamics records over months;
- Recording keystroke dynamics with operators own computer system.

All the three features were feasible through the outcomes exhibited. Specific attention is their basis effort on the pattern of a dynamic confirmation method (Leggett et al, 1991) which confirms an operator concluded in a period through the formless character keyed in by an operator as a day to day rehearsal. Obaidat et al (1997) echo that "on their effort using keystroke durations, latencies and neural nets to regulate a user's individuality founded exclusively on their user ID". These researchers insisted that a minute FARs and IPRs aided to find out the extra importance associated with keystroke duration or hold times over the latencies. Meaningfully, a decent accomplishment is made in appreciation using very small cords (5 words). What is still not obvious from their publication is quantity of exercise needed before their program will be clever to accomplish the confirmation appreciation that they appealed. Furthermore it is of anxiety that together the pretender's and legitimate t user's keying designs were applied for learning which is not appropriate to most system circumstances.

There appears to be considerable indication that Keystroke Dynamics as a technique of confirmation is established to be feasible. On-going examination is obviously desirable to decrease together FAR and IPR to levels that become obvious to the operator.

2.11 Latency Patterns

Researchers who analysed keystroke latency patterns to recognize the individual keying on the keyboard were Perrig et al, (1997). Unlike previous works which concentrated on pleasing one mention model and undertaking user verification founded on one acknowledgment.

Perrig et al, (1997) applied uninterruptedly tester operator input and applied the aggregate facts for determination of the correct operator. They also did not require the perfect number of times. In many

circumstances, an operator may vacate his system without switching it off or padlocking the system. This allows an impostor an opportunity to operate the keyboard and the operator's logon to access the computer. In their project report they were able to demonstrate a tool to deliver uninterrupted validation of the operator by constantly watching the operator keying design. Immediately an unalike keying design is noticed, the system is blocked and the mistrusted impostor is questioned to key in a password. This procedure can be convenient in numerous situations, for illustration, notebooks. It can also be applied as an extra biometric validation technique in an extraordinary safety organization. Their methodology was to authenticate operator individuality at all periods by endlessly watching keystrokes. Each keystroke is taken through X-windows server and administered either to direct the system or to calculate a possibility that the present operator is the identical to the operator on whom the system was educated. The program is applying the keystroke deferrals to design a procedure equivalent to a

Markov chain which models the models and adjustment of the deferral among two keystrokes. The program considers all the permutations of two succeeding keys and save the data. To recognize an operator, the application validates which operator's model exploits the probability of the current key-presses.

2.12 Latency Observation

Perrig et al, (1997) define latency observation as the monitoring of all the important proceedings that operator keys. In their method, keying a single key generates a couple of key procedures: press and release, which they call a key stroke. They had the latency among pressing and releasing a key for each key that is typed, which is called PR-latency. For each two uninterrupted keys punched, they had the latency among the release incident of the first key and the press incident of the next

key, which is called RP-latency. PR-latency is permanently positive, since a key can simply be released after it's pressed. RP-latency can be negative, because the second key can be pressed before the first key is released.

2.13 Typing Error

The relational position of tripgraphs is the basis for calculation the distance or gaps between two samples. In each sample, the relational position is always dependent on that tripgraph's duration. Due to that, any comparison made between two samples must have the same tripgraphs.

Nonetheless, the argument made doesn't necessarily mean the two samples keyed in should be the same text or characters. The two samples are simply filtered before comparison is made between them for their distance in order to keep a shared tripgraph and the value of the tripgraph brings meaning to the value of their distance. Calculations can still take place provided the tripgraphs kept for the two samples is of a greater value. These experiments gave the operators the free will of typing to have a natural setting paving way for correction of errors. (Bergadano et al, 2002).

There are consequences associated with the involved tripgraphs in comparison of two samples because no samples were discarded for their typing mistakes. Though the experimental text amounted to 350 different tripgraphs, the actual number shared for two samples amounted to 272 on average. " The entire set of samples used in these experiments virtually has no pairing of samples with distinct set of trigraphs though it must be noted most experiments found in the literature rejects erroneous samples" (Bleha et al, 1990, Brown et al, 1993 and Obaidat et al, 1997). According to, Leggett et al,(1988), "samples are kept even if they contain typing errors, while no information is available for the experiment described".

2.14 Classifications of Users

Given some set of operators and typing samples of the same text from these operators and a new sample from a fresh operator, Bergadano et al (2002) and Claudia (2005) did studies on the Classification of users. They wanted to be in the know of who typed. Averagely, they expected the actual distance that lied between the two samples of the same operators to be lesser than that of different operator samples. Oltsik (2006) said that the advantages of Keystroke Dynamics in authentication software delivers a solution that is fast, accurate, scalable to millions of users, requires no change in user behaviour and is immediately deployable across the organization and the Internet without the need for expensive tokens, cards or other specialized hardware.

2.15 Typing Task

Some researchers work on login-type authentication while others work on in session authentication. Among research on login-type authentication, where subjects type the same sequence repeatedly, the sequence ranges from a 7 character password to a 50 character sentence (Cho et al, 2000). Among research on in session authentication, where subjects type long spans of text, some researchers have subjects transcribe text (e.g, a passage from a novel), while others monitor keystrokes during subjects day-to-day activities (Bergadano et al, 2002). Because research has found some digraphs to be better than others for accurate keystroke dynamics (Janakiraman, 2007), the system knows that the error rates depend on the typing task. Perhaps these different typing tasks explain why different researchers get different error rates.

2.16 Reliability of User Authentication

Keystroke dynamic is most appropriate way of checking Reliability of operator Verification. The truth is that individuals can be recognised by their keying behaviour, previously acknowledged in the initial days of the telegraph became significant in World War II. The Morse code comprising dots with dashes, with each having a defined interval has no duplication effects in the know of those recommended intervals exactly (Magnus, 2009). The difference of positioning extending these dots with dashes, denote a rhythmic unique identity of an operator known as the user's first. The key fundamental clue of the arithmetical method involves associating a link keying features of particular operator coupled with some set of keying features of no difference to the operators' or of an intruder.

The concept of data mining revolves around collection and gathering various methods procedures and techniques in expert systems, artificial intelligence (AI), pervasive computer (PA), neural networks and machine to machine learning. The procedures and techniques naturally initially develop an expectation ideal from past records, and then integrate the ideal to forecast consequence of a fresh test. In figures divergence, the concept of data mining does not make prediction about figures. The major variance among arithmetical and approaches in data mining is consequently applied as the evidence. Example the likeliness among operators or users in a data mining approach are deliberate, notwithstanding design variances associated with designs detected in ideal constructions. This is where the program constantly observes an operator's keying design. The system tends to shut down or request for operator to re-login when design does not equal records logged-on. This approach uninterruptedly modifies and observes records of a logon.

Magnus in 1999 goes on to say that differentiating among actual operators and intruders is regarded as “a one-class identification difficulty” wherever an attempt to differentiate a group of operators from the rest of operators (hackers) by educating from a recorded set comprising merely the items of that group. One difficulty with the realistic submissions is the absence of statistics and the learning shift-key designs. His set of data comprises of one thousand, two hundred and fifty four (1254) members are given the chance to enter their user credentials for ten (10) times apiece. Nonetheless, set of data is tagged huge and sufficient for educational purpose. Magnus (1999) said “when a probable partaker the website, a ‘session’ is created”. Three hundred and forty-seven (347) meetings were thus initiated for the approach. Connection of significant link and copying applet to the operator’s workstation is the initial step or action for any partaker. The new applet is needed to keep track of important records throughout the linking stage and centered on timer of any partakers’ workstation or system.

Primarily the action happens on the partaker’s workstation thus the client side and not the server side (website server) and consequently methodological difficulties like latency in network transmission or server congestion are scrapped off. Logically, various prospective partakers don’t copy the new applet and usually that does not log them off instantly without noting down records. This contributed to 64% sessions and ended us with 125 sessions where data have been noted. The partakers were asked to use a user ID (38 atrick) and Password (water80), the identical for all partakers and a request to punch their user credentials for 10 times.

Each of the 10 efforts to login from figure 1 below for a punch (P) and release I clock time of 14 character were noted given$(P_i, R_i) for\ i = 1, \ldots \ldots 14$. With these figures, he was able to compute dwell times (D) and flight times (F) as$D_i = R_i - P_i$ $F_i = P_i - R_{i-1}$. The time of dwell or dwell

time (D) thus accounts for key held pressed period where as the time of flight or flight time stands in for the time exactly between two (2) consecutive presses. F1 clearly thus has no significant meaning since it leaves no importance to elapsed time between last letter of user name and first of password giving a 14 dwell times with flight time of 12 per login attempt. Flight time therefore seen natural to be defined as $F_I^* = P_i - R_{i-1}$ in order to break up login period independently and non-overlapping. It is no good an idea as it is mostly negative though the flash applet keeps track of the press and release time. Characters registered by the system are only engineered by the exact moment there is a press on key and not the release period and as such one is likely to press the second key when the first hasn't been released yet.

2.16.1 Dwell and Flight Time Calculations

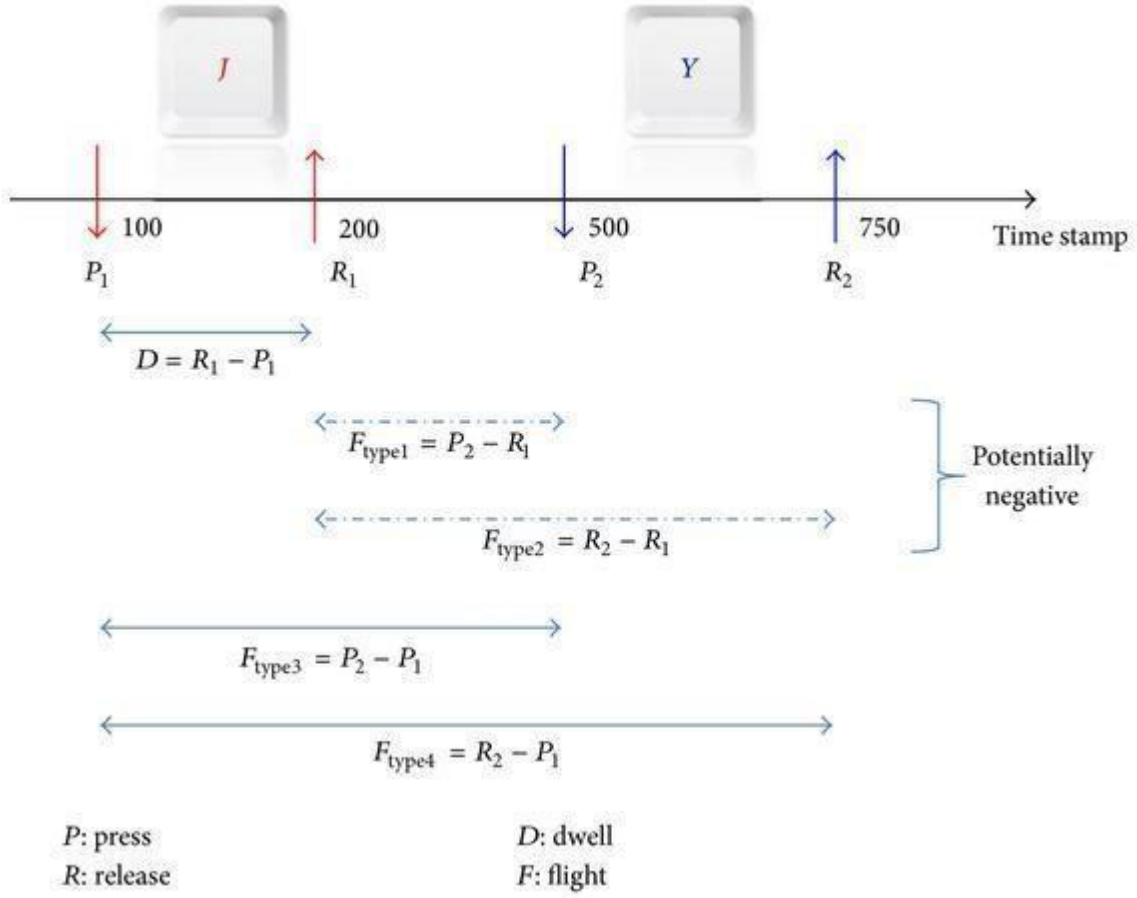

Figure. 1: Dwell and Flight Time Calculation ***(Source:*** Ankur Kumar , Abhijeet Patwari , Sagar Sabale ***October 2014)***

If all partakers would finish their session (10 logins) and make no keying mistakes, when he had 26×10×125=32500 data points. Some partakers stopped wi llingly (they stopped their computers) or unwillingly (their machines stopped), so that they could not finished all 10 logins. Furthermore, partakers made keying mistakes. If a keying mistake occurs in User ID, that leaves no records since all dwell and fl ight times are erased off leaving no room for correcting a mistake. The use of backspace with two fingers will only have a longer flight time on the average that a person who uses ten all ten fingers.

2.17 Password Hardening

Password Hardening is any one of the variety of measures taken to make it more difficult for an intruder to circumvent the authentication process. Password Hardening may take the form of multifactor authentication by adding some components to the username / password combination or may be policy based (Margaret et al, 2007).

(Cho et al, 2000) Exploration concerned with enhancing the safety of passwords is offered in this segment. These applications incorporate and extend the safety delivered by traditional username/password structures. The suggestion was that, a server-side java applet application used in confirming legitimacy of user credentials via keystroke dynamics and neural networks for examination.

This is the description of the application. When a workstation makes an attempt to long on to a home page, for instance, say a manufacturer's online shop, which is on a server, the customer keys the previously recorded operator ID. After that the server uses Java applet to sends the workstation a code that can examine the operator's password keystroke timing vector. When the Java applet is processing on the workstation computer, it collects the operator's keystroke timing vector, it moves results back to the serving computer. Before the auto associative neural network positioned in the server can confirm if the operator is the individual he/she assertions to be. Since the code is coded in Java, any customer computer that has a Java browser installed on it can be linked to the server.

Monrose et al (2002) offered an application with an operator's duration and latency keystroke joined with user or operator's credentials to harden the password and make it more protected than the usual conservative passwords. The system routinely accepted a steady variation in an

operator's keying designs while constantly upholding the similar toughened password through various logins. First of all, the password is as safe as a predictable password and is regularly toughened as biometric data becomes accessible. They recognize the foremost restriction of their application that is the condition where an operator, whose keying designs alternate substantively among succeeding logins, probably because of an unacquainted keyboard could not produce the precise toughened password and is protected out of the computer.

Monrose et al (2002) too boast that their application advances on other prevailing password toughening application, in specific the marketable BIOPASSWORD application, through creating a key that is repeatable and coined through the biometric component which is more protective than the usual password in use. With other applications, the argument was the ability to conceded if the toughened passkey is taken and an attempt made to attack, though someone might presume accommodating meaningfully lengthier than a conservative password. Whereas the outcomes remain actually promising the system delivers a warning statement depicting a restriction of 10 operators and 1 password as a pilot stage. They seriously endorse extra investigation done in line of study. Whereas investigations on securing the passkeys with keystroke dynamics is restricted, it has proven to be perfect as a method to enhancing safety of user credentials verification whereas operating around prevailing structures, the technique is feasible in a networked situation.

2.18 Commercial Implementation of Keystroke Dynamics

Few software houses made an attempt to come out with products on keystroke dynamics. The most popular one is the BIOPASSWORD (www.biopassword.com). It is a profitable application of

Keystroke Dynamics for safeguarding systems, and separate computers with normal user login credential. This happens to be an intermediate device to substitutes the ordinary logon display of computer systems. Vended by BioNet Systems who freshly purchased the associated privileges with the requisite knowledge from Net Nanny Inc. BIOPASSWORD ideology is dubbed from the original effort directed by The RAND Corporation and is protected by a number of patents (Gaines et al, 1980). Within a network environment the system is integrated by a superior server program with Windows NT/2000/2003 domain controller that overlooks the logon of domain members. Fresh operators are expected to user credentials 10 times to gain access into the documentation of the keystroke dynamics. This process is referred to as "The training cycle". A safety stage can thus be agreed for each and every operator and becomes the beginning of harmonizing FAR and IPR. (Patrick et al, 2004).

BIOPASSWORD has expected an amount of satisfactory assessments from the Information Technology press. It would appear that assessors in total discovered the safety presented by the application to be dependable and operational with none of the assessors capable to produce Imposter Pass errors. Assessors likewise establish the learning stage to be tolerable. There was varied point of views on the simplicity of setting it up with one assessor commenting on the high awareness of Windows Domain configurations needed. Since the middleware architecture of the application, one critic was clever to circumvent safety by combining 'run as' credentials – nevertheless it was proposed that would be solved in a later editions of the application. Specific concern is the scheduling of the assessment publications which all transpired during the inauguration of the software in 2001/2002. There was similarly an amount of declaration type publications printed during this period also. Subsequently the BIOPASSWORD application appears to have remained basically overlooked by the Information Technology and common press

houses. This could be deduced to understand that it has not however made the business permeation that was propagated in its preliminary publication, nevertheless it could also show that the press has merely switched its consideration to more interesting matters – Only time will tell the outcome. (Altman, 2002 and Bragg, 2002).

2.19 Applications Under Keystroke Dynamics

There are numerous applications of the concept of keystroke dynamics in the field of computer security one of such instance of a static approach is in restricting master server hosting with respect to root access level. When a user accesses a network, there is the tendency of been promoted or queried for a pass phrase in addition to their user credentials to be given full access.

Access is given if and only if their pattern of typing corresponds to reasonable threshold of an acclaimed identity.

As effective as it could be for such an instance since root access is normally given to users at console logins. Nonetheless, monitoring continuously or dynamically of interactions of operators in the course of accessing restricted files or executing instruction set in alerting environments normally is a unique cases for keystroke dynamics verification and authentication. The keystroke dynamics phenomenon could be deployed for detecting unrealistic rhythmic typing in the operator notification third party apps. Magnus (1999) concluded by addressing the essentials of the phenomenon as biometric for workstation access authentication.

The whole concept of keystroke dynamics involves analyzing the manner operators keying characters by carefully tracking inputs from the keypad or keyboard and authenticating them based

on habitual patterns of rhythm. The author analyses the current state of the phenomenon and postulates classification procedures with respect to matching of templates and Bayesian likelihood models and further agitates that although the use of a behavioural trait as a sign of identification has limitations, when implemented alongside traditional schemes, the phenomenon stands a greater chance allowing design of a more robust and powerful authentication systems than traditional password alone. The limitations associated with deploying keystroke dynamics for user authentications comes about as a result of the nature of reference signature and the its connection with recognizing operators based on habitual trend in their key press patterns performance and traits depending on the rhythm as a function of operator environmental factors. The issues associated are the known traits that are uniquely carrying discrimination details unlike non-static biometrics. In past years studies has proven that results of different individuals depicts characteristics in their key press pattern which are pushing individuals and can be successfully exploited and use for identification purposes. His classifiers performance on 63 datasets of users ranging from 83.22% - 92.14% accuracy depending on approach adopted is significant variability with which typists produces digraphs.

He therefore proposes adapting digraph-specific processes of unevenness rather than single lowpass filters. Moreover, he stands for the use of structured text opposed to allowing users type arbitrary free text in identification process. Whereas free-text based on identification may be more favorable, its recognition evidently varies under great operation situations and for a fact that associated inputs are unhindered, operators may be act contrary the uncontrolled environmental factors with limitations on expected free-text recognition. They believe is that

Magnus (1990) point of view of using 'free test' to learn is the best because some character may not be commonly used or typed by some group of people. For the example an Akans tribe in Ghana do not commonly use or type letters like q,c,z,x,j. So it is better to allow for 'Free Text'.

2.20 Lessons and Conclusion

Notwithstanding the countless potential of biometric procedures applying Keystroke Dynamics as a method of refining verification, there appears to have made a unreasonably little permeation of the technique into conventional verification of operators of systems. Approximately all the data studied in this examination work, protest on this condition. An amount of conceivable explanations can be presented that pinpointed everywhere in the theme, which once a Keystroke Dynamics structure of verification is setup, human existence is made further problematic for everybody added including operators, managers, and backing workers. For instance:

- The knowledge regularly needs the fixing of middleware which is an extra cost and further depleting on computer managerial and support assets. Middleware presents additional complication into the logon technique and generates a superior chance for disappointment and problem directions (Bragg, 2002). With the system to be developed, there will be no middleware.
- The expertise makes the logon technique extra problematic for operators, predominantly when FAR are high. This will affect the Help Desks, previously getting half their assignment as password associated questions. Patrick, (2002) who could risk bringing even extra password-associated aid calls.

- The application of such biometric procedures require to be harmonised around an operator set and this necessitates installation and conservation means. The application of such methods, with its superior dependence on satisfactory password creation may uncover prevailing flaws in IT (Information Technology) strategy and application in a office.

- The knowledge is fresh and there could be a confrontation and absence of belief towards such a novelty. Traditional administrations might be waiting till new establishments approve such processes.
- There is undoubtedly an absence of government/judicial necessities/enticements to advance verification to the stage accepted by Biometric Keystroke Dynamics

CHAPTER 3

METHODOLOGY AND DESIGN

3.1 Review

The motivation for using keystroke features to strengthen password -based authentication comes from numerous research efforts that validate the hypothesis, that certain keystroke features are highly repeatable and that significant variation exist between users (Gaines et al, 1980). While researches on network security authentication applying keystro ke dynamics are imperfect, it is obvious that as a way of refining network safety verification while still operating around current structures. The approaches are feasible in a networked setting. The system will:

- Generate ID and key stroke pattern
- Design an efficient way of saving and retrieving password
- Code database in binary format to avoid password hacking
- Help users to learn password pattern
- Provide efficient and secure way of accessing the network
- Providing local authentication

The system will be analysed, designed, developed tested and implemented at the Anglican Senior High School to handle activities at the following departments:

- Administration
- Academic
- Domestic

3.2 System Analysis

This is the need to consider all sides of the constraints in other to come up with an accurate solution. System analysis requires the study of the system and how it interacts with other entities both inside and outside. Detailed specification was gathered in other to come up with solution based on the requirement given. The user requirement was proposed based on a student project work. System development has two major components.

- Looking at the problem and its new requirements.
- Looking at the pros and cons of new areas of the system.

3.3 Requirements Gathering

In the effort to really understand the current system being operated at the School, An existing problem were known by going to the school to find out the problems the School was facing, to come out with alternative solutions and finally choose the best solution for the School, Various techniques were adopted in achieving the main aim of system. The under listed techniques were adopted:

3.3.1 Sampling of Existing Documents and Events

Various samples of documents and events that occur at the School concerning the school network security system were collected included the following;

- Intrusion to administration records
- Alteration of students marks

In depth analysis of these documents had been conducted which forms the basis of the generation of the entity relational diagram.

3.3.2 Interview with the Staff of the School

The headmaster was the main source of information in regards to knowing about the problem domain. The context diagram as part of this document was generated during the interview with the School Headmaster. He actually made us understand that the Schools have not had any meaningful security policy or systems to manage their School network. In his view, being able to outline some of the requirements of the proposed system was a bit of a problem as the users have been so used to the old ways of working. There were staffs without computer access due to the fear that they may interfere with the existing system. Staffs with access, have unlimited access which is also dangerous in terms of security. Student records manipulation in the accounts office was some of the cited issues.

3.3.3 Observation of the Working Environment

Several visits have been conducted at the School, especially the accounts, administration department and the Computer laboratories. Being at the administration was important for us to understand how the non-teaching staffs perform their administrative procedures on the network. Various scenarios on network log on and logout were captured, which will form the basis of capturing of authentication history into the system.

3.3.4 Testing of the old system

After the observations and interviews , there was the need to practically test for the ability of the system to secure the network. The test was done to compare with the new system to do a better analysis of both systems, which will result in drawing a better conclusion as to the direction the school must take. Five working days were used.

3.3.4.1 Shoulder Surfing Attack

Shoulder surfing is an attacking technique whereby an intruder secretly watch a user types his/her password with the intension of using it later. This attack usually occur in an open office where typing of password is exposed to surrounding on lookers. This was how the shoulder surfing test was conducted. The test was conducted continuously for five working days. Ten intruders where asked to watch users as they type their passwords.

- Users were not aware that they were being watched.
- After five days the intruders were made to try to enter what they were able to capture by watching the users type their user name and password.
- The table 2 explains the result (what occurred on the concurrent days with the same preamble).

Table. 2: Summary of test results for shoulder surfing attack experiment

Days	Number of Intruders	Success	Failure	Remarks
Day1	20	11	9	Fair authentication
Day2	20	18	2	Poor authentication
Day3	20	10	10	Fair authentication
Day4	20	5	15	Good authentication
Day5	20	13	7	Weak authentication
Total	**100**	**57**	**43**	**Fair authentication**

This was how the experiment was conducted

On the first day, twenty users were watched as they typed their user names and passwords. Eleven intruders were able to produce those they watched, thus user names and passwords. Therefore they were able to enter their victim's computer. Preamble continuous up to the fifth day as indicated in the table above.

Observations

Out of 100 experience performed with shoulder surfing attack on the old system 57 of the intruders were successful, which means that more than 50% of the intruders where successful.

3.3.4.2 Brute-Force Attack

With brute-force attacks, an impostor attempts combinational character permutations to break a login credential. Passwords tend to be more secured against brute-force attacks when they are

multifaceted and the greatest means to defend a system password against a brute-force attach is to implement a lengthier password to generically increase the time associated with the permutation of characters.

Table. 3: Summary of test results for guessing and brute force attack experiment

Days	Number of Intrudes	Success	Failure	Remarks
Day1	20	17	3	Poor authentication
Day2	20	9	11	Fair authentication
Day3	20	10	10	Fair authentication
Day4	20	3	17	Good authentication
Day5	20	0	20	Good authentication
Total	100	29	61	Good authentication

This was how the experiment was conducted

- Twenty intruders were made to guess the password of users in the school, using word and phrase like their name, telephone numbers, names of their spouses and sample numbers like 0 to 9.
- Brute force Attack programs (like John the rapper)were used to automatically search for user name and passwords

From the table above, on the first day, twenty intruders were allowed to use guessing and attack programs to gain access to the user's machine. The result was that seventeen of the intruders were successful and three of the intruders failed. The preamble continuous up to the fifth day as indicated the table above.

Observations

Out of hundred experiment perform on the old system twenty nine intruder were successful which account for 29% of success. But in network security terms it is bad rate, it should be 0% success rate.

3.3.4.3 Social Engineering Attack

Social engineering is the practice of obtaining confidential information by manipulating of legitimate users. This is how the experiment was conducted. Twenty of theintruders were made to call the users and just ask them of their password. The intruders also send form through email to users to fill and in the form, they were supposed to enter their user name and password on their machine and some of them did. The password was assume to help the intruder to install programs like games, antivirus and many attractive programs for free for the users, and some of them were tricked in that process to give out their user names and passwords

Table. 4: Summary of test results for social engineering attack experiment

Days	Number of Intruders	Success	Failure	Remarks
Day1	20	12	8	Fair authentication
Day2	20	11	9	Fair authentication

Day3	20	15	5	Weak authentication
Day4	20	10	10	Fair authentication
Day5	20	8	12	Fair authentication
Total	**100**	**56**	**44**	**Fair authentication**

The table 4: explain the experiment

On the first day twenty of the intruders used both telephone call and email tricks to obtain user name and password twelve of the intruders were successful and eight of the failed. The preamble continues up to fifth day, as show in the table above.

Observations

Out of hundred experiments performed for social engineering attacks (impersonation) fifty six of the intruders were successful, that account for more than50% intruder success rate which is bad.

3.3.4.4 Recording user information Attack

Recording user information is the use of spyware software in recording data concerning a user, typically devoid of their awareness.

How the experiment was conducted

Spyware application or executable files were installed on user's machines. A spyware called mediacces.exe was installed on twenty of their machines with the intent to copy the information like user name and passwords.

Table. 5: Summary of test results for recording user information attack experiment

Days	Installed spyware on computers	Success	Failure	Remarks
Day1	20	18	2	Poor authentication
Day2	20	16	4	Poor authentication
Day3	20	18	2	Poor authentication
Day4	20	17	3	Poor authentication
Day5	20	17	3	Poor authentication
Total	**100**	**86**	**14**	**Poor authentication**

Table. 5: explain the experiment

On the first day twenty of the machine on which the spyware ware installed were checked, nineteen of the machine data was successful recorded, one couldn't record the information. The preamble continues up to fifth day, as show on the table above.

Observations

Out of the hundred experiments conducted for recording user information 84 of the spyware was able to copy the user information leaving only 14. Therefore it means that there was almost 90% successful rate in the attack. All the results of the experiments performed above already goes to prove that the old system have a lot of defects which need to be solved.

3.4 Description of the new System

The Keystroke Dynamics authentication System is designed to prevent users at the School from gaining access to network without authorization. In addition, the system is expected to require users to learn keystroke dynamics to create a key stroke pattern which should be unique to any user in addition to their password. The system should be designed such that the administrator logon first and personally creates an account for users. After which users are required to learn the key stroke dynamics with the system. After a successful learning of the key stroke pattern, the user is allowed to logon. Meanwhile at any point in time the computer screen is covered until a successful logon.

3.5 The Software Development Lifecycle (SDLC)

The software development lifecycle (SDLC) covers the whole life of the software project. That is from feasibility study, analysis, specification, design, development and even the aspects which take place after the system has been accepted by the end user that is operation, maintenance and enhancement. For the purpose of this project, the waterfall development model was used as a guide to develop the Keystroke Dynamics authentication System, since this is a small-scale project. The Waterfall model is one of the most common software development lifecycle models available. It is very simple to understand and use. Each next phase in this model must begin only after the previous phase is completed.

Waterfall software development model may be applicable to projects where:

- Software requirements are clearly defined and known as in the case of this project
- Software development technologies and tools are well known

3.6.1 The Waterfall Model Diagram

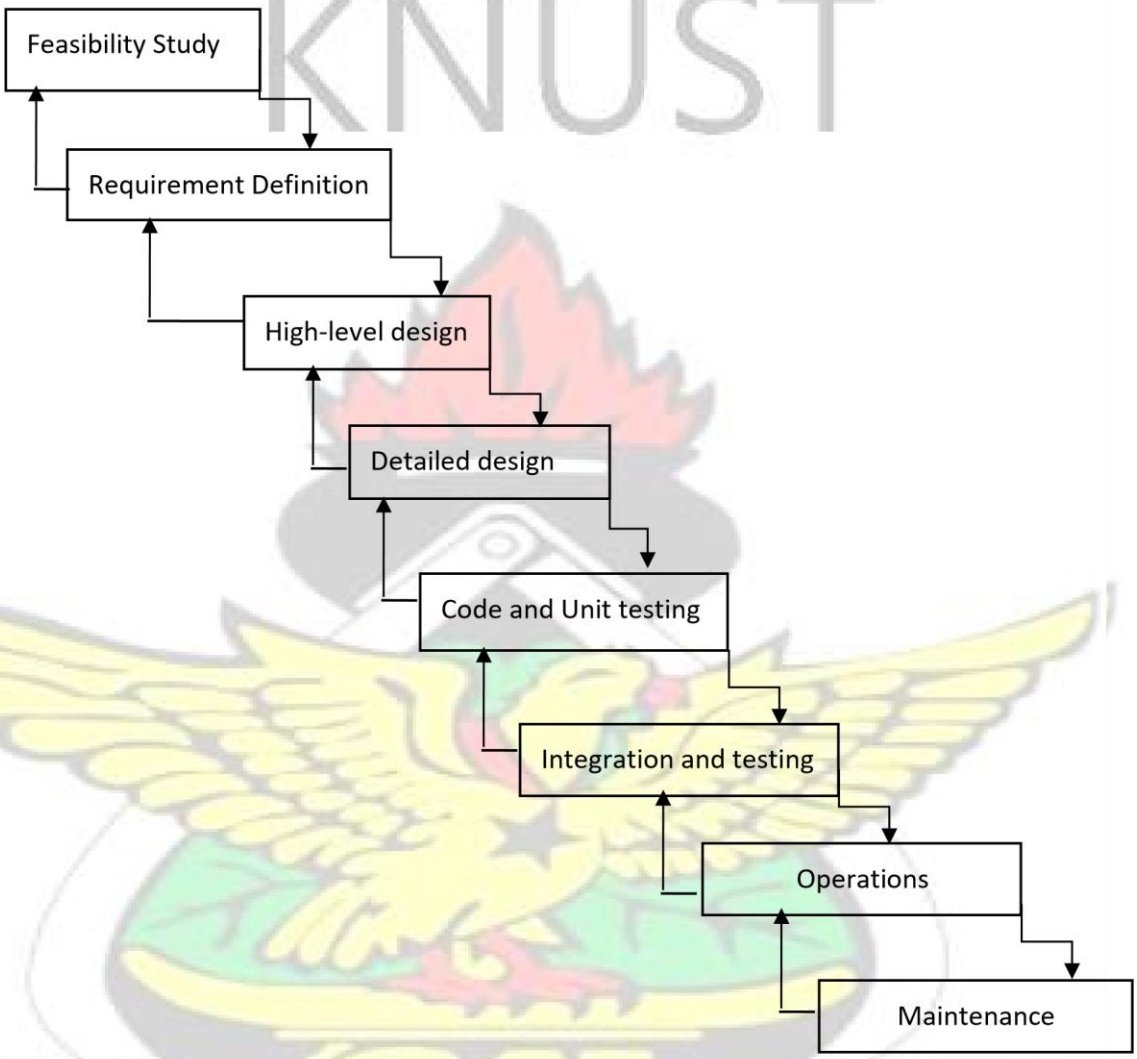

Figure.2: The Waterfall Model Diagram

3.6.2 Project Version of the Waterfall Model

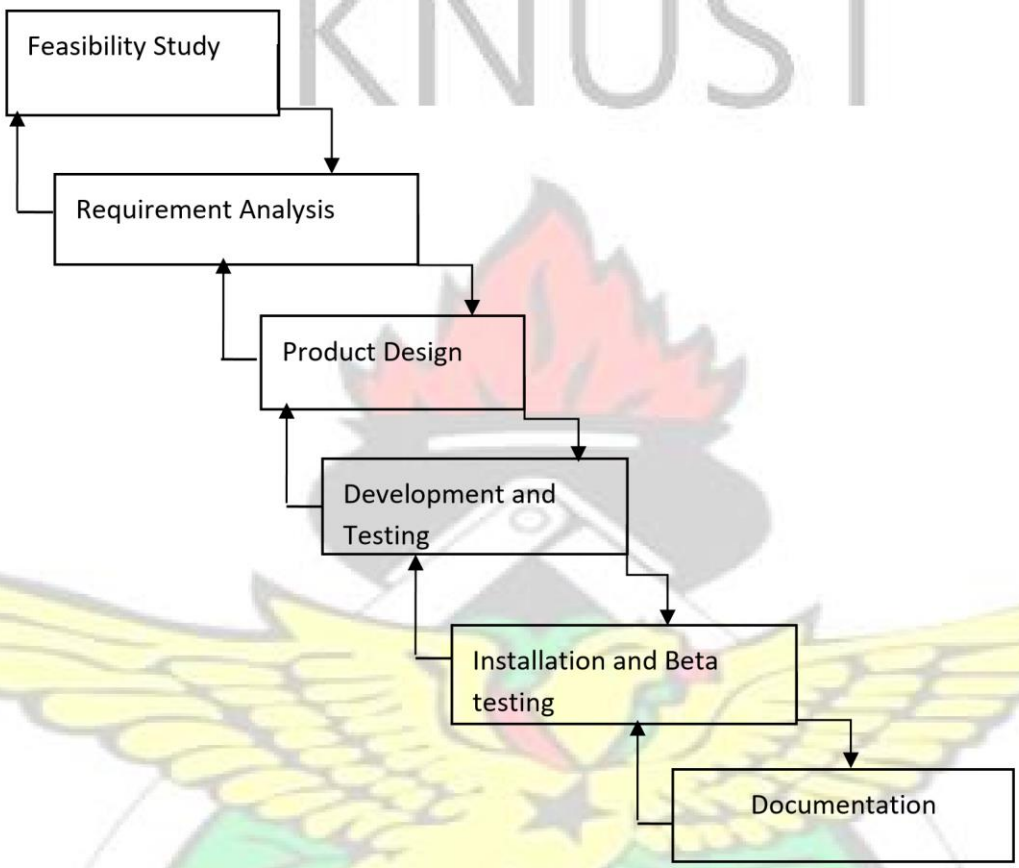

Figure.3: Project Version of the Waterfall Model

For the purpose of this project, the waterfall model has been modified to suit the nature of what this system wants to achieve within the project constraints.

3.7 Explanation of Modified Waterfall Model

This project is for academic purposes, hence requires that the software to be produced at the end of it all will be analyzed, designed and implemented. Looking at the time constraints, the believe is that, the system will not have the luxury to see the project through its entire life cycle, hence a modified version of the development model.

3.8 Non-Functional Requirements of the System

In order for the project to succeed, the system is expected to be easy to use by users at the School. The Software shall provide an easy to use graphical user interface that is intuitive and shall give a graphical representation of the action that user perform. The Keystroke Dynamics authentication System would be adaptable enough to allow for future changes should the business processes of the School change. This system should be able to expand to meet future business needs. This should include increasing the number of computers that can connect to use the application. The system should include technical support and provide upgrades whenever possible.

The Keystroke Dynamics authentication System will be capable of integrating with any other system that the School may wish to introduce later. The system shall provide secure protection to network. The system is expected to perform very well and enable the appropriate users to Logon to the system, with a username and password. Administrators shall be given full rights to view the system, add and delete users in the system. Users are also required to learn keystroke dynamics in order to have access to the system.

3.8.1 Business Rules

The following business rules shall be followed and implemented in the system.

Systems Owner and Administrators should have extra privileges.

Only Information needed by a particular staff shall be made available to them.

Users shall have three attempts to enter user names and passwords, after which the systems logon screen shall be closed.

3.9 Functional Requirements

The actual functionalities of the system to be developed are outlined using the Unified Modeling Language (UML) Use case models as detailed below in a use case survey:

3.10 The Use Case Models

The system will use UML Use Case modeling technique to identify all the relevant actors and the particular type of functions that the system can offer each actor. In general, the use case models shall help to identify the scope and functionality of the Keystroke Dynamics authentication System.

3.10.1 Use Case Survey

Table.6: Use Case Survey

NAME OF ACTOR	DESCRIPTION
Administrator	The only person responsible for creating user accounts
Non-teaching staff	This actor learns keyboard dynamics and logon
Teachers	This actor learns keyboard dynamics and logon

Students	This actor learns keyboard dynamics and logon

3.10.2 Use Cases Description

Table 7: Use Cases Description

USE CASE	DESCRIPTION
Create account	This use case describes how the administrator creates accounts for users
Learn Dynamics	This use case describes how users learn their keystroke dynamics.
Logon	This use case describes how the user logon into the system.

3.10.3 Use Case Diagram

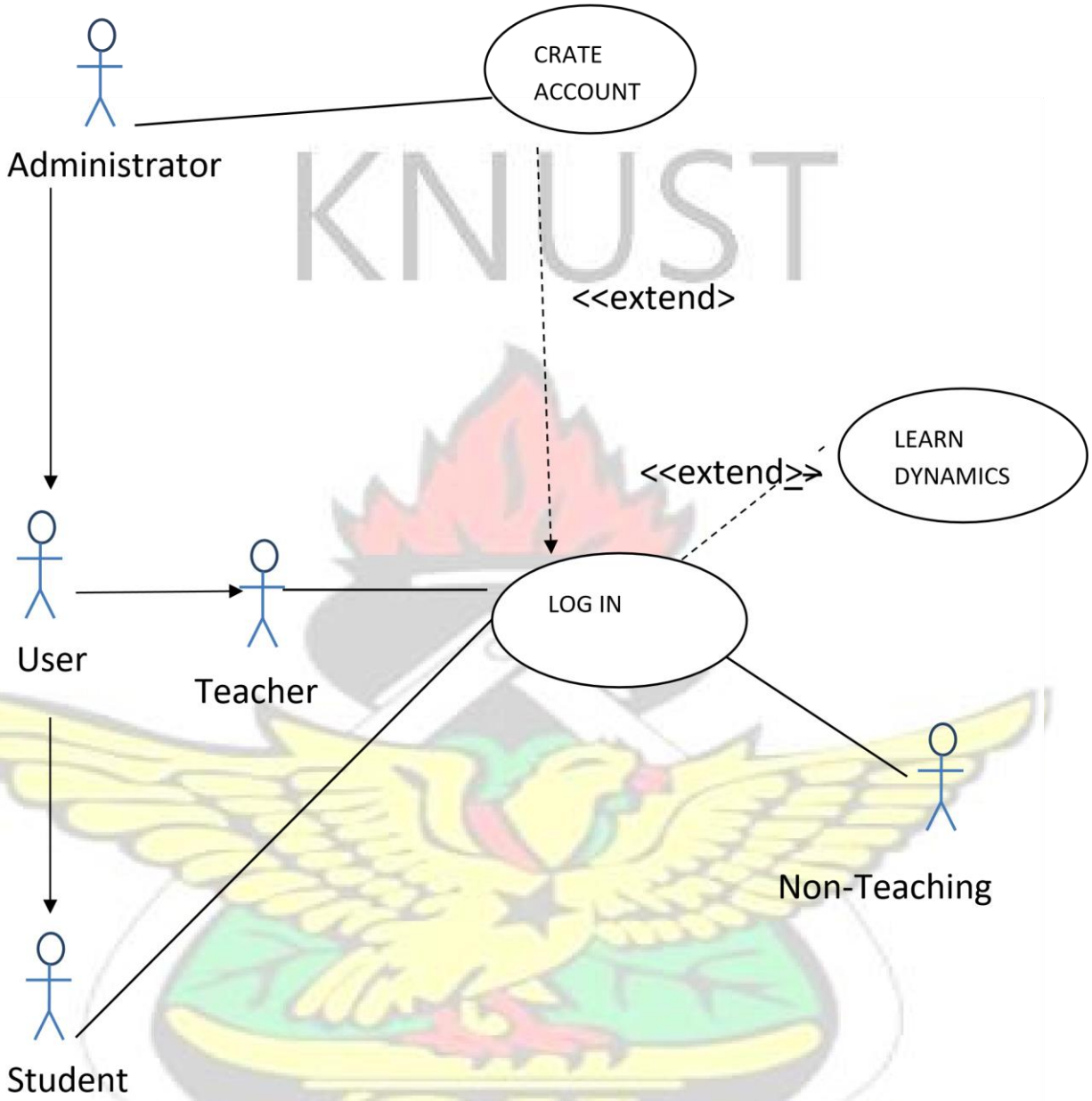

Figure.4: Use Case Diagram

3.11 Context Diagram, Data Flow Diagrams and Entity Relational Diagrams

All the relevant documents that are in use at the School will be gathered, which will form the basis of the entity relational (ER) diagrams and data flow diagram. Followed by the initial context diagram for the system to be developed for the School. The context diagram shall be used to depict the system and its external entities. Dataflow diagrams will be used to depict the processes involved in delivering logon authentication system. It will include the following:

- Creating password
- Learning password pattern and
- Authenticating users

The purpose of the requirements analysis process is to produce requirements specifications document,

3.12 Data Flow Diagram

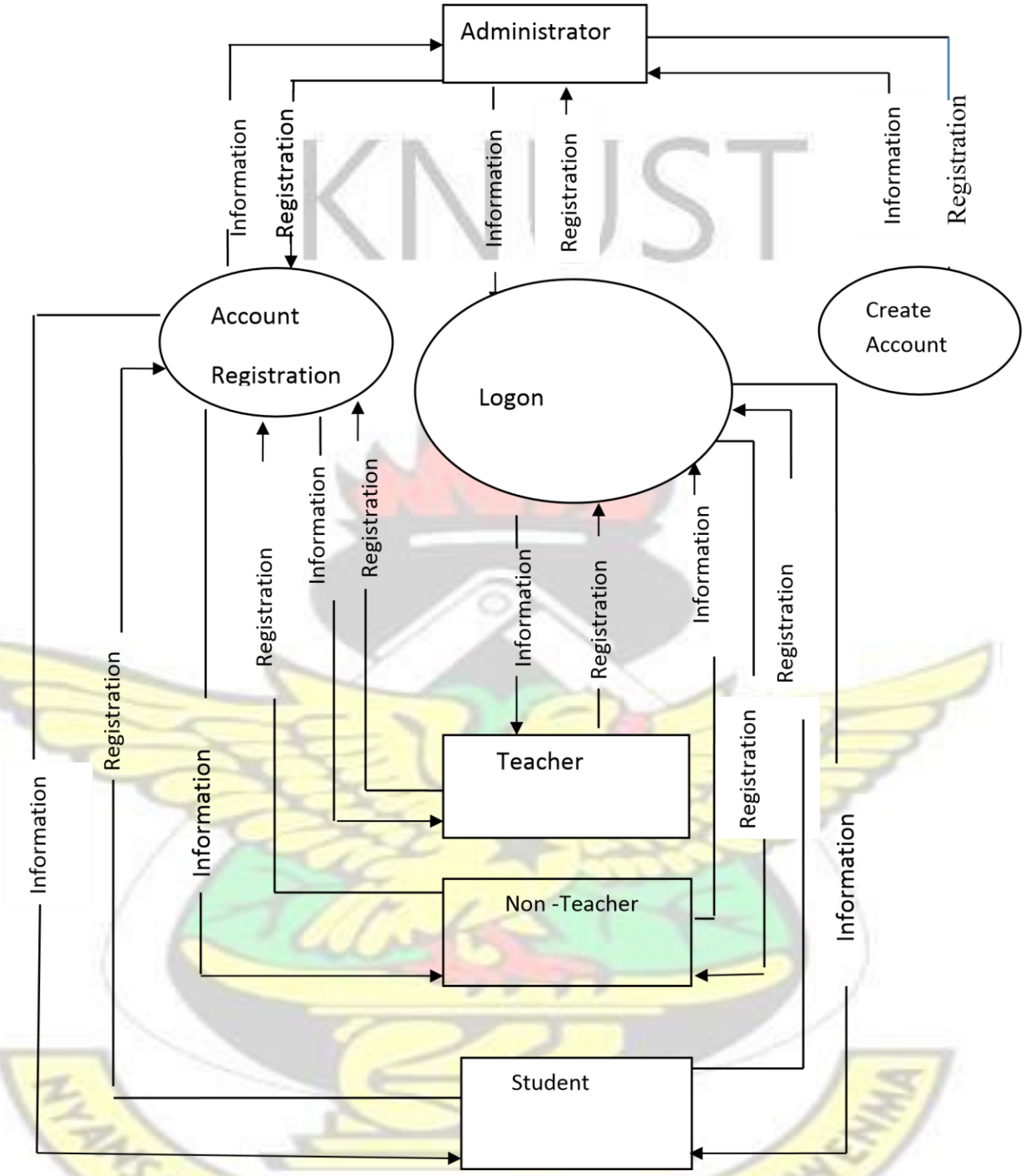

Figure.5: Data Flow Diagram

3.13 Main Architecture Design

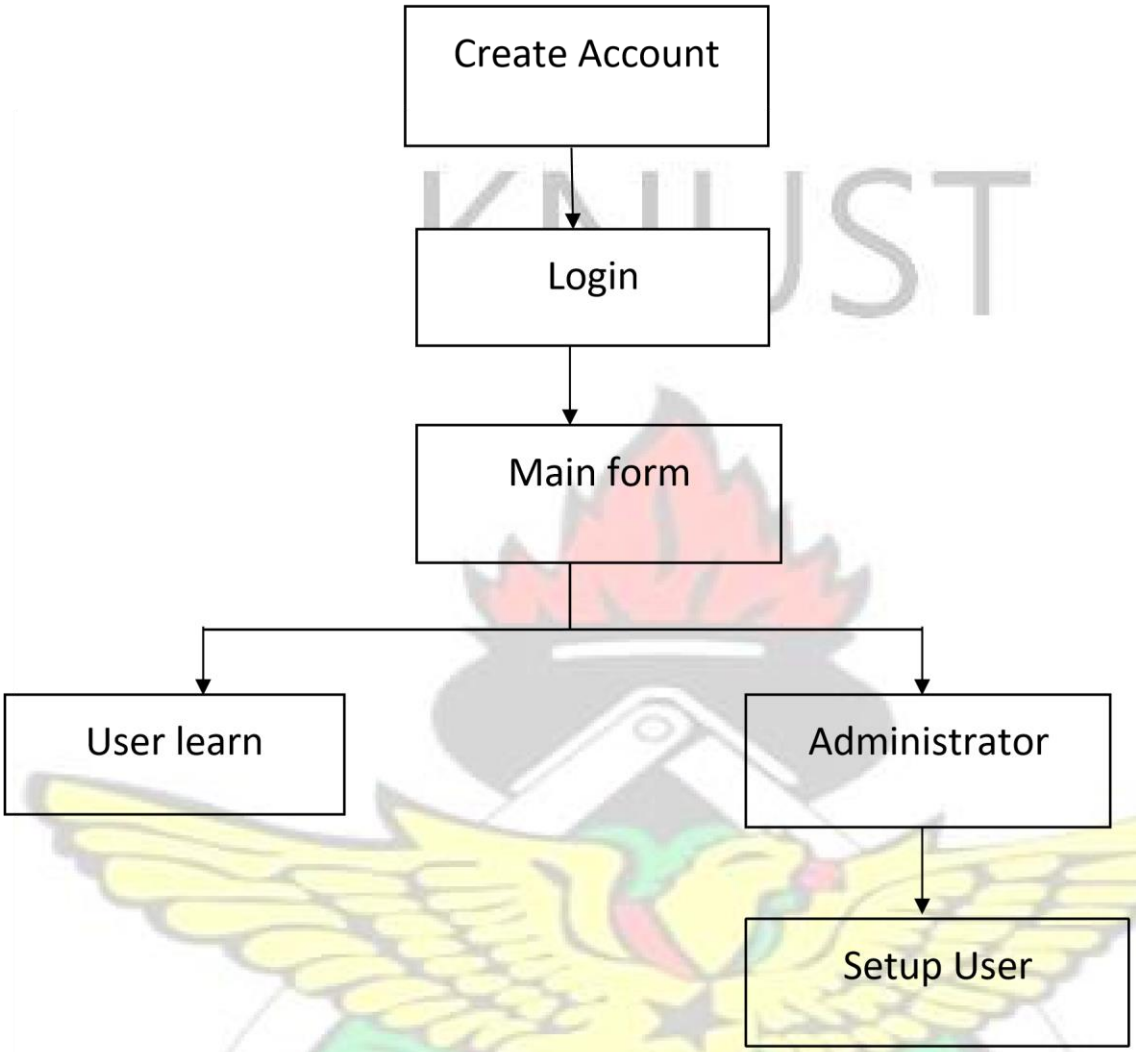

Figure.6: Main Architecture Design

3.14 Process Analysis

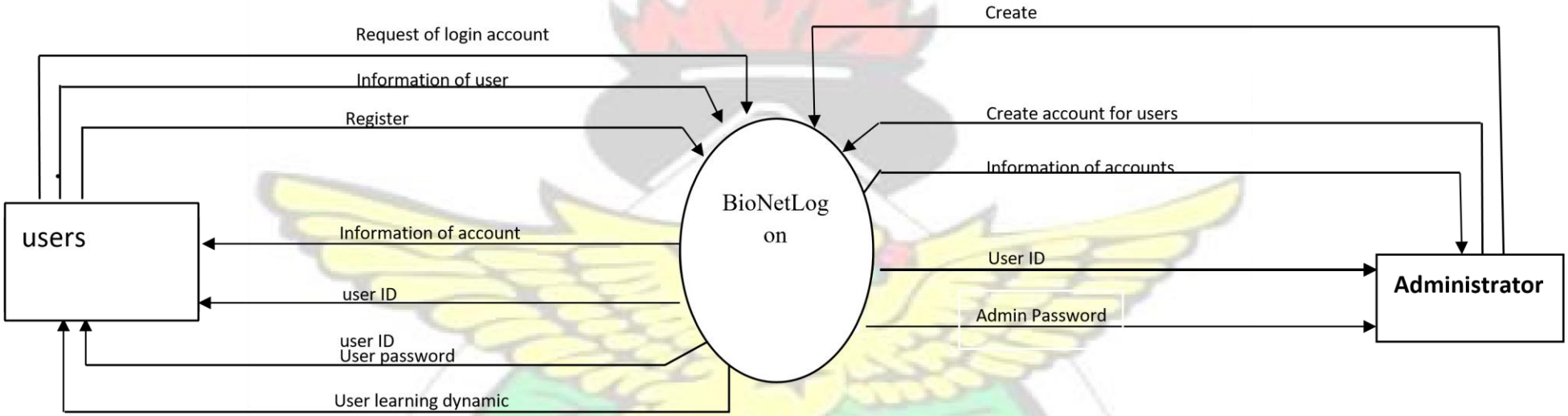

Figure.7: Process Analysis

KNUST

3.15 The Algorithm

The algorithm of the existing system in the client's organization should be known. To build an algorithm, the system analyst need to obtain a detailed understanding of each process and analysed it in greater details This project work considers the use of d ata flow diagrams to model the algorithm for the school new system.

3.15.1 The System Algorithm

Due to implementation of the proposed system, few changes will occur in the existing algorithm.

Step1. *Start*

Step2. *While network Is Availablegoto3 else 15*

Step3. *Disable Desktop and Windows access*

Step4.*Get admin key value from registry*

Step5. *If Admin Key Value is nothing go to 9 else 6*

Step6. *Enter Admin Username and Password*

Step7. *Confirm Password*

Step8. Create *Admin Key Value in registry go to 10*

Step9. *Display No Administrator Found Error Message go to 6*

Step10. *Enter Username and Password*

Step11. *If user is Admin go to 12 else 14*

Step12. *Display Create New User Form*

Step13.*Create New user*

Step14. *Allow Windows Access*

Step 15.Minimize to Taskbar Step 16. Stop

3.15.2 System Flow Chart

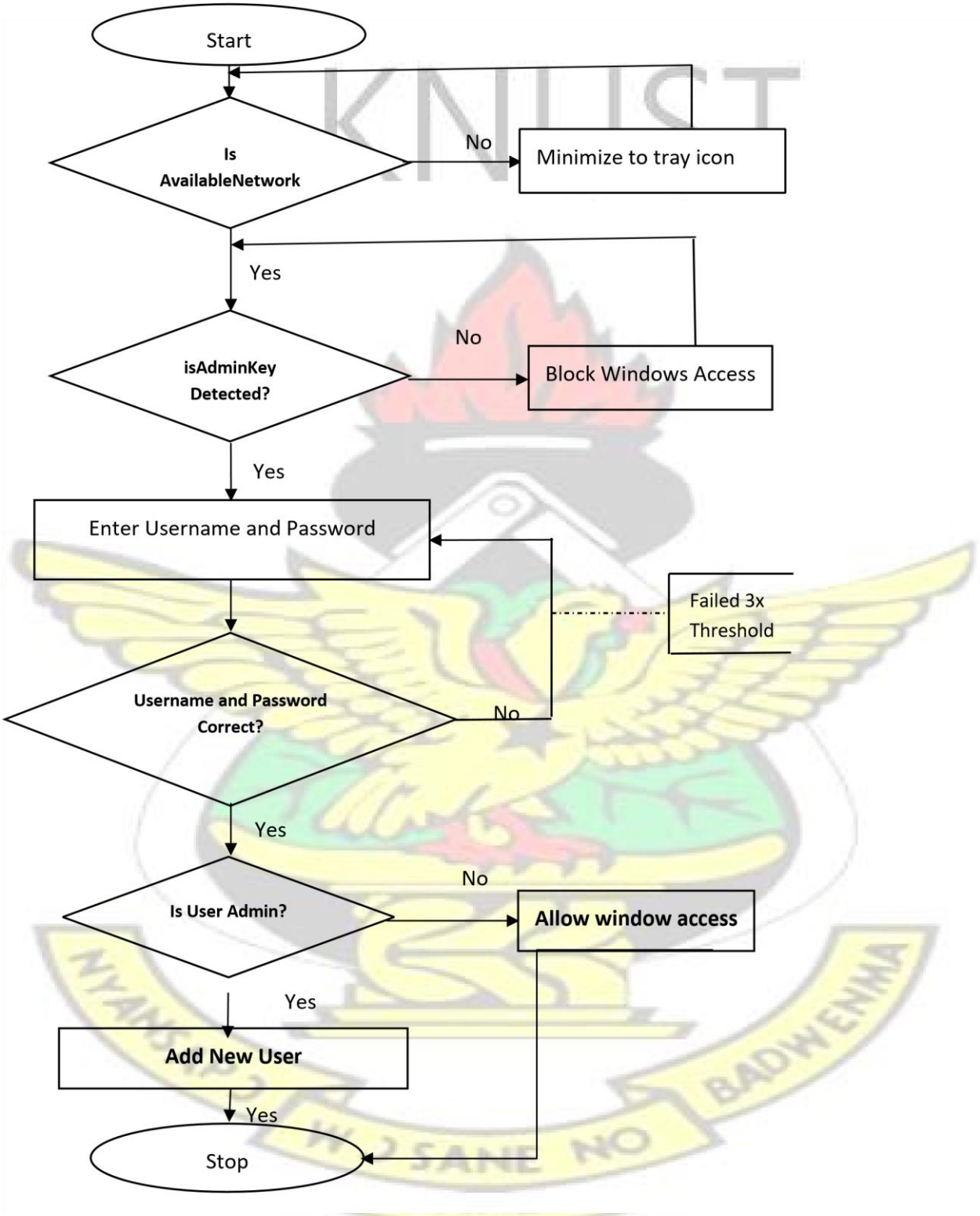

Figure.8: System Flow Chart

3.16 The Logon Process

The scope of the system to be developed includes accepting user password and logon in keystroke dynamics. The administrator creates accounts for users, with the new system and helps them to go through the keystroke dynamics learning processes, to obtain a well-practiced password rhythm with the new system. The system prevents the user from having access to the school network until a correct user name and password is typed in a particular pattern which is recognised by the system. A teacher will have a new password and user name together with his keystroke dynamic pattern, which will help him authenticate with the new system. The new system will prevent other teachers who don't have permission to use the network to enter it. It will also help in reducing network traffic which is a serious problem for networks. The nonteaching staffs are going to be assured of the fact that intruders are not going to interfere with their data due to the new authentication system. Student are only allowed to the system when they are authenticated, this reduces the network traffic drastically and improves system efficiency.

3.17 Back-End Design

The system will use binary file as the backend that is a file whose content must be interpreted by a program or a hardware processor that understands it. Binary file format has the advantages;

- The file is smaller due to the format.
- Binary formats also offer advantages in terms of speed of access
- Binary files are more efficient, in terms of memory storing values using numeric formats, such as IEEE 754, rather than as text characters, which tends to use more memory.

Code database in binary format to avoid password hacking.

3.18 Front-End Design

Microsoft Visual Basic.Net 2008 IDE will be used for the front end design, the reasons being that:

- The structure of the Visual Basic.Net programming language is very simple, particularly as to the readability of the executable codes.
- VB.Net provides the DotNet framework that is not only a language but primarily an integrated, interactive development environment ("IDE").
- The VB-IDE has been highly optimized to support rapid application development ("RAD"). It is particularly easy to develop graphical user interfaces and to connect them to handle functions provided by the application. Since the choice of users are mainly average computer literates, the flexible visual interface will allow to develop prototypes as quickly as possible, to help solicit users view in modifying the modules as and when they are developed.
- The graphical user interface of the VB-IDE provides intuitively appealing views for the management of the program structure in the large and the various types of entities (classes, modules, procedures, forms).

3.19 Technical / Hardware Requirements

The front-end application software (which would be developed using Visual Basic.Net 2008 version) shall be installed on all client computers at the School (administration, and academic department s). Back-end database will be written to binary file.

In order for the installation of the application to be successful, the system shall require the following hardware equipment to be installed at the School:

3.20 Hardware Equipment

Table.8: Hardware Requirements

Item Name	Minimum Specifications
HP Pro Liant G5 Server M360	3.6 GHz Speed, 2 GB Memory 4x146 HDD, Rack Mountable, Supports Raid 5 Windows 2008 Server operating system
Client workstation	Intel 1.8 GHz speed, Windows XP operating system 1GB Memory,80 HDD
Local Area Network (LAN)	Network speed of about 100/1000 Mbps
Switch	Supports up to 100/1000 Mbps
Powerful Network Printer	To be placed at the administration to print students reports

3.21 Testing

The general aim of testing is to affirm the quality of software systems by systematically examining the software in carefully controlled circumstances. Testing should have the major intent of finding errors. The system used both unit and integrated testing Each module of the application developed has been tested thoroughly to ensure that it suits the design specification. The tested modules have been integrated using test data to ensure that the modules can operate together without any problems. One of the tests that was very important to the school was system test. Hardware and

software testing ware conducted to ascertain how the "Bionetlogon" will function on windows operating system and the minimum hardware requirement that will be needed .The following Steps were followed for testing.

3.21.1 Static and Dynamic Testing

Static testing includes review of documents required for the software development.

- All the documents related to customer requirements and business rules that are required for software design and development should be handed over to the project work supervisor.
- The documents were reviewed. The reviewing of documents includes comprehensive and thorough study of the documents. Discrepancy found in them were noted and figure out why such discrepancies, so that it will not occur again.

Dynamic testing deals with specific methods for ascertaining and or approximating software quality through actual executions, i.e. with real data and under real (or simulated) circumstances. After these Test cases and test scenarios are prepared. A Report of bugs was prepared, which helped in the further debugging of the codes.

The system shall first be implemented on the Anglican Senior High School network after testing. Believe is that more institutions will express interest in the system if it able to serve its purpose.

3.22 Implementation

After successful testing of the new authentication system, NetBiologon software was implemented to test against the traditional attacks discovered at the school, thus Anglican secondary school, which included:

- shoulder surfing
- Recording user information
- Social engineering

- Guessing and Brute force

3.22.1 Shoulder Surfing

The surest way for one to have user credentials of an operator is to sight him through authentication. It was observed that user passwords were being spy on by others, because of the fact that their offices were an open one, which reduces confidentiality t o passwords. There were CCTV cameras at their store rooms, which facilitated shoulder surfing. With the implementation of Keystroke dynamics it was no threat to think of as someone may be should surfing or spying on you during a system login because user credentials alone (username and password) is not the sole means of accessing a system and as such login details cannot be compromised.

Table.

9: Summary of the Results of Tested Attack for Shoulder Surfing Experiment

Days	Number of users watched	Success	Failure	Remarks
Day1	20	0	20	Excellent Authentication
Day2	20	0	20	Excellent Authentication
Day3	20	0	20	Excellent Authentication
Day4	20	0	20	Excellent Authentication
Day5	20	0	20	Excellent Authentication
Total	**100**	**0**	**100**	**Excellent Authentication**

This was how the experiment was conducted

On the first day twenty users were watched and none of the intruders were able to produce keystroke dynamics pattern password of users they watched. Therefore they were able to enter their victim's computer. Preamble continuous to the fifth day as indicated in the table above

Observation

Shoulder surfing attack was tested with the new system, thus the keystroke dynamics

authentication system and the result was remarkable. 0% of the attackers were successful, which means 100% failure. The attackers were able to capture the password but were not successful because keystroke dynamics are not just about password, it also requires patterns and sequences.

They failed because they could not get the pattern and the sequences.

3.22.2 Recording User Information

Spywares are software that can record information about users during authentication. The use of internet at the school increases the chance of spywares attacks, which records users typing. Keystroke dynamics is not just about user name and password alone, it also about sequences and patterns which makes it difficult for these spywares software to record.

10: Summary of the Results of Tested Attack for Recording User Information Experiment

Days	Installed of spyware on computers	Success	Failure	Remarks
Day1	20	2	18	Excellent Authentication
Day2	20	0	20	Excellent Authentication
Day3	20	0	20	Excellent Authentication

Table.

Day4	20	0	20	Excellent Authentication
Day5	20	0	20	Excellent Authentication
Total	**100**	**0**	**98**	**Excellent Authentication**

This is how the experiment was conducted

Spyware application such as Trojan virus was installed on the twenty user computers, with the aim of recording their authentication information. On the first day only two of the user records were able to capture by the spyware virus. Preamble continuous to the fifth day as indicated in the table above.

Testing the recording of user information attack technique against keystroke dynamics authentication system was about 98% failure. Spyware is seen as the surest means to attacking keystroke dynamics system provided the intruder intentionally install a Trojan virus which records all information to reproduce the users' keystroke pattern.

3.22.3 Social Engineering

Social engineering is the practice of obtaining confidential information by the manipulation of legitimate users. Because of social bonding at the school, people entrust their password to friends. Others are able to trick peop le to given their password through telephone call and other forms of conversations. Initially, social engineering tends not to be feasible with keystroke dynamics in that identification stage password patterns that could literally be given out not even on purpose. Requesting for user credentials and posing to be the legit operators was not possible.

11: Summary of the Results of Tested Attack for Social Engineering Experiment

Days	Number of users watched	Success	Failure	Remarks
Day1	20	0	20	Excellent Authentication
Day2	20	0	20	Excellent Authentication

Observation
Table.

Day3	20	0	20	Excellent Authentication
Day4	20	0	20	Excellent Authentication
Day5	20	0	20	Excellent Authentication
Total	**100**	**0**	**100**	**Excellent Authentication**

Table. 11: explain the experiment

On the first day twenty of the intruders used impersonation type of social engineering attack on users, by calling and sending them Emails to trick them to give their keystroke dynamics authentication pattern password to the intruders. Although the intruders were successful in getting the passwords from the users, they could not be able to type in the pattern known to the new system. So therefore the intruders could not logon to the users computers. Preamble continuous to the fifth day as indicated in the table above.

Testing keystroke dynamics against social engineering attack, the success rate was 0%. Nevertheless the associated breakthrough tends to be low. Considering identification, no user credentials given out is feasible and note even on purpose.

3.22.4 Guessing and Brute-Force

With brute -force attacks, impostors use several conceivable character groupings to break the system and the extra difficult a login credential is, the further protected it is for bruteforce attacks. It was recognized that student at the school have tried and even on some instances been able to break into the school main server by continuously guessing and using combination of characters. To best protect a system against brute -force attacks one must have as a lengthier password. The length associated with keystroke dynamics is fairly good and almost unbearable for brute -force attacks. The invader or application should be habitually produce keystroke designs and emulate human input. When keystroke dynamics are applied in two -factor verification mechanism, that is password and keystroke. It was virtually incredible to override the safety scheme.

12: Summary of the Results of Tested attack for Guessing and Brute Force Experiment

Days	Number of users watched	Success	Failure	Remarks
Day1	20	0	20	Excellent Authentication
Day2	20	0	20	Excellent Authentication

Observation Table.

Day3	20	0	20	Excellent Authentication
Day4	20	0	20	Excellent Authentication
Day5	20	0	20	Excellent Authentication
Total	**100**	**0**	**100**	**Excellent Authentication**

This was how the experiment was conducted

Brute force Attack programs were installed on twenty user computers to automatically search for users keystroke dynamics pattern passwords.

From the table above, on the first day, the results were that none of the twenty intruder programs were able to capture the keystroke dynamics pattern passwords. The preamble continuous to the fifth day as indicated the table above.

In the guessing and brute force attach technique, 0% was successful against the keystroke dynamics authentication system. The attacker or program needs automated keystroke generation pattern and imitate the human input which is difficult to achieve. When the dynamics are used as two factor mechanism, it becomes more or less impossible to hack, thus keystroke dynamics patterns.

3.22.5 Dictionary Attacks

Dictionary attacks involve overcoming system authentications through a pass phrase against its database of possibilities. As opposed to brute-force attacks, when all attempts proofs futile, it then tries possible attempts likely to succeed and thus relying on words from the dictionary. In the school case, dictionary attacks have also been noted where students download softwa re from the internet to carry out these attacks. As for dictionary attack, it was impractical and barely impossible to carry it out against keystroke dynamics authentication mechanism.

CHAPTER 4

Observation

Analysis

The analysis will compare the results of both the old new systems experiments to establish the clear differences between the two systems with respect to security of authentication at the school network.

4.1 The systems experiment results.

The old and new systems were tested upon by attack mechanisms, thus social engineering shoulder surfing, brute force and recording user information.

Results for shoulder surfing technique attack.

For the old system, out of hundred intruders used in the experiment, as already stated in the experiment in chapter three, fifty seven of the intruders were successful while forty three failed in the attempt to authenticate, using the username and password obtained from the shoulder surfing technique. Since hundred users were used in the experiment, it means 57 users account for 57%, so invariably more than 50% succeeded in the attack. Whereas the new system also produced the following results from the test conducted. Out of the hundred users (intruders) used no ne of them were able to use the shoulder surfing technique to attack the new system. 0% successful and 100% failure.

Social engineering results

Out of hundred users used for the experiment for the social engineering attack on the old system, 56% of the intruders were successful, while 44% failed in the attempt to authenticate using the social engineering techniques. With the use of 100users, 56 accounts for 56% success. So invariably, more than 50% intruders were successful in the attack.

But the test on the new system using social engineering attack experiments produced the following results. Out of the hundred user used, none of the intruders could succeed in breaking into the new system. Therefore 100% failed and 0% successful.

Brute force attack results

In reference to chapter three, the old system experiment result shows that 29% intruders were successful, while 61% of them failed in the attempt to authenticate using brute force attack.

The test on the new system using brute force and guessing attack experiment brought about the following results. Hundred intruders were used, No intruder was successful in beating the new system, which imply that 100% failed and 0% succeeded.

Recording user information result attack

As already stated in the previews experiments, hundred users again were put to task and 86 of the softwares on the machines were successful and 14 of them failed in recording the user information. Using 100 machines for the experiment the result goes to prove that 86% of the machines were venerable to the attack while only 14% of them were able resist the attack.

The test conducted on the new system using Recording user information technique showed that, out of hundred users (intruders) used, only two of the installed spyware softwares were able to record keystroke dynamics patterns of the users. 98% failed and 2% were successful.

4.2 Conclusion of Analysis

From the experiment conducted for both old and new system, the old system had an average of 40% failure of the attack whiles 57% of the attacks were successful. 57% of success in attack to a system shows very huge risk to the system which will require a better system to stop this large security risk to the school networking system.

Upon the installation of the new system and test conducted, these are the results obtained.

An average 99.5% of the experimented attackers failed, it was 0.5% margin of risk. This risk margins was found in the Recording user information attack technique. Spyware is undoubtedly the paramount and cheapest technique to break into keystroke dynamics verification network. If on operator intentionally install an attacking software such as trojan horse virus which records all information.

4.3 Result After Implementation of Keystroke Dynamics

After the implementation of keystroke dynamics following general observations were made.

4.3.1 Uniqueness

Keystrokes incidents are calculated with milliseconds accuracy by programs and that makes it unreasonable for duplicating an operators' keystroke design at a great determination without voluminous strength.

4.3.2 Transparency and Non-invasiveness

One momentous advantage associated with keystroke dynamics biometrics is the amount of fairness it offers. The concept involves nobody or marginal modification to operator comportment meanwhile the record of keystroke design is executed through backend application execution. In majority of the cases, operator might not be even conscious that they are sheltered by an additional level of verification. This easiness not merely substantially favours application developers but also to those end operators with slight or no practical experience.

4.3.3 Increase Password Strength and Lifespan

System passwords have become the best extensively installed personality verification procedures, notwithstanding the methods that trust exclusively on only documents set organize feebleness and susceptibility. Scholars have recognized that keystroke dynamics biometrics possible solution to at least improve a further level of defense and increasing the survival of password. Keystroke dynamics biometrics conveys the proficiency to connect the cheapness of password design with better reliability associated with biometrics. By using keystroke dynamics biometrics, users can deliberate on producing a vigorous password however prevent being subdues by unrelated collections of password.

4.3.4 Replication Prevention and Additional Security

Keystroke schemes are tougher to be duplicated than printed signatures. This is because best safety schemes merely permit restricted wrong inputs efforts before closing user account. Moreover, combination of keystroke dynamics biometrics makes password prediction less feasible and as such stolen identity becomes completely irrelevant, since fruitful ownership of undisclosed key is only a simple criteria of the whole verification sequence. Even if it does acquire conceded, a fresh keying biometric stencil can be restored simply by selecting a fresh password.

4.3.6 Disadvantages

Lower Accuracy

The system was substandard in relations to verification precision because of discrepancies in keying pace that was instigated by marginal reasons such as wound, tiredness, or disruption. However, extra biometric applications are not spared by such factors either.

Lower Permanence

Most behavioural biometrics commonly involves lesser durability equate to physical biometrics. Keying design of a person could regularly metamorphose succeeding the personalisation towards a password, growing keying ability, variation to input devices, as well as environmental traits. Nonetheless, studies recommend constant updates to stored keystroke profile to make it more seucred.

4.3.7 System Evaluation Criteria

Keystroke dynamics based authentication systems are highly effective based on their rate of system recognition. However, to practically implement this technology, there is the need to consider important criterial show below

4.3.8 Effectiveness

This trait shows a system's ability to differentiate between genuine and fake user or an imposter. Performance pointers adopted by researchers are enumerated below.

False Rejection Rate (FRR) this pointer refers to percentage (%) ratio that lies between genuine users who are denied access against all genuine users gaining access into the system which is occasionally termed as Force Non-match Rate (FNMR) or type 1 error. A lower FRR implies less rejection and easier access by genuine user.

FAR as another pointer is the percentage (%) ratio between a falsely accepted user without authority coupled against imposters gaining access into the system. False Match Rate is also called type 2 error. An FAR of a smaller value depicts less imposter accepted.

To determine accuracy level and comparative measure against systems Equal Error Rate (EER) is usually used which is sometimes referred to as Crossover Error Rate (CER). Comparison of results shown in the next section mainly expresses with FAR, FRR, and EER.

4.3.9 Efficiency

The complexity of procedure engaged is what is referred to as Efficiency and is normally considered better if complexity is deemed lower. An expensive method for computation does not only put mounted strain to hardware but also frustrates user with longer waiting time.

4.3.10 Adaptability and Robustness

Adaptability on the other hand has to do with ability of a system to accept or tolerate gradual typing changes of user across time. Robustness shows the capability to work well with usersfrom diverse professions with dissimilar typing proficiencies.

CHAPTER 5

Conclusion

This project work addresses the practical significance of applying keystroke dynamics as a biometric for validating entree into workstations of a network. Keystroke dynamics is the procedure of examining the approach operators key in by watching keyboard inputs and validating them established on routine designs in their typing rhythm.

The present condition of keystroke dynamics and existing sorting methods centered on original corresponding and Bayesian probability model were revised. The disagreement was that, while the

use of a behavioural peculiarity (rather than a physiological characteristic) as a sign of distinctiveness has innate restrictions, when executed in combination with outdated systems. Keystroke dynamics tolerates for the proposal of further vigorous authentication systems than traditional password based alternatives alone.

The inherent limitations that arise with the use of Keystroke dynamics, as an authentication mechanism are attributed to the nature of the reference “signature" and its relationship to the user recognizing users based on habitual rhythm in their typing pattern uses dynamic performance features that depend upon an act (the rhythm is a function of the user and the environment). The problem with keystroke recognition is that, unlike other non-static biometrics (such as voice) there are no known features or feature transformations which are dedicated solely to carrying discriminating information.

Fortunately, in the past few years researchers (Joyce et al, 1990, Mahar et al, 1995, and Monrose et al,1997) have offered experiential results that display that diverse personalities display features in their keying rhythm that are extraordinarily distinctive and that these features can be successfully oppressed and applied for documentation purposes.

This exploration supports the remark of Mahar et al (1995) in that there is essential irregularity that user come out with a digraphs. Hence, the research suggests the adaption of digraph specific measures of unevenness rather than single low-pass filters. Moreover, the study postulates that of the usage of free text permitting operators to key in any characters of their choice during the

identification learning process while recognition based on structured text may be more desirable, structured text recognition was observed to vary greatly under operational conditions.

5.1 Summary of the Research

The summary of the research drawn based on the findings and recommendations made are discussed below ware focused on objectives of the research study.

5.1.1 Findings

- The argument is that although the use of a behavioural trait (rather than a physiological characteristic) as a sign of identity has inherent limitations, when implemented in conjunction with traditional schemes. Keystroke dynamics allowed for the design of more robust authentication systems than traditional password based alternatives alone.
- One of the problem with keystroke recognition is that unlike other non-static biometrics (such as voice) there are no known features or feature transformations which are dedicated solely to carrying discriminating information. Below are important factors that are openly connected to operator satisfactoriness to the expertise. The knowledge must give operator as much contented and clearness as conceivable by not disturbing operator with elongated inputs. Having to remember multifaceted strings, or deliver enormous volumes of boring input.

Other than the user and impostor typing style, none of the other tested traits (i.e., age, gender, or dominant hand) were found to have a significant effect on the experiment. The experiment continues to have the lowest miss rates (i.e., the chance of successfully evading detection), across

most feature sets, typing tasks, amounts of training, updating strategies, and impostor familiarity levels. Impostors who become familiar with a typing task often significantly increase their miss rate. Employing an updating strategy significantly reduces miss rates across the experiment and

typing tasks. In each investigation, we drew these conclusions by evaluating experiments under systematically varied conditions. We compared our findings to those of earlier works, in each investigation, by drawing inferences using different experiments. we were able to make discoveries and understand phenomena in ways that would not have been possible without this work.

5.1.2 Recommendations

System administrators should be encoura ged to use keystroke dynamics authentication system to secure their networks.

5.2 Area of application

This software is design to secure network from unauthorized user in a network environment. Network comes with a lot of benefit including sharing of res ources, but with inherent risk of hacking by an intruder. This has led to the development of this software, which is intended to prevent network intruders. An institution that are delicate and uses network infrastructures like banks, schools, military installations and many others can use this system to prevent intruders from their network.

5.3 Further work

- Developers of keystroke related systems should come out with the versions that can be installed on non- Microsoft Operating System software programs, such as Linux
- Developers should be able to come out with system that can periodically check to ensure that the current user is the same user authenticated earlier.

REFERENCES

Khosrow-Pour, MehdiAccess security", Computers & Security, 22, 695 –706, 2003, (accessed 2016 March 8).

Ahmed A Patel, M Taghavi, K Bakhtiyari, JC Junior et al. "Anomaly Intrusion Detection and prevension system in cloud computing, (accessed 2016 March 21).

Arun Ross and Salil Prabhakar2, "An Introduction to Biometric Recognitions". Information System Security Vol.No.5, pg 367-397, Nov 2005. (accessed 2014 March 21).

Fort Bragg, 2002, Distance-Educator.com, 2000, (accessed 2016 May 21).

Y Zhu, T Tan, Y Wang "Biometrics Proceedings of the IEEE", 2005, (accessed 2016 March 21).

TJ Brown, GA Churchill, JP Peter - Journal of retailing, 1993, (accessed 2016 March 27). M Brown, SJ Rogers - International Journal of Man-Machine Studies, 1993 – Elsevier (accessed 2015 March 2).

S.JCho, Bergadano Gunetti,Picardi and. R. Spillane, "Keyboard Apparatus for Personal Identifi-

Downland, et al, ,2004, (accessed 2015 March 3).

E Madenci, I Guven - 2015, (accessed 2016 March 12).

T Sim, S Zhang, R Janakiraman- IEEE transactions on 2007, (accessed 2016 July 10).

M Karnan, M Akil a – "Software and Networks, 2010.ICCSN'10. 2010 - ieeexplore.ieee.org, (accessed 2016 March 3).

D Shanmugapriya, G Padmavathi - IJCSNS International Journal …, 2011 - paper.ijcsns.org, (accessed 2016 June 21).

R Joyce, G Gupta - Communications of the ACM, 1990 - dl.acm.org "Identity Authentication Based on Keystroke Latencies", Communications of the ACM, vol. 39; pp 168 -176, 1990, (accessed 2016 March 2).

Lawrence O'Gorman, "Comparing Passwords, Tokens, and Biometrics for User Authentication", Proceedings of the IEEE, Vol. 91, No. 12, Dec, pp. 2019-2040, 2003. (accessed 2015 March 11).

J Leggett, G Williams, M Usnick "Dynamic Identity Verification via Keystroke Characteristics".International Journal of Man-Machine Studies, 1991, (accessed 2016 March 1).

K .Killourhy, R Maxion – "Why did my detector do that?!"2010,(accessed 2016 May 6).

F. Monrose, AD Rubi n "Keystroke Dynamics as a Biometric for Authentication".Future Generation Computer Systems, 16(4) pp 351-359, 1999. . (accessed 2016 July 16).

F. Monrose, AD Rubin "Authentication via Keystroke Dynamics", Proceedings of the 4th ACM Conference on Computer and Communications Security, p 48-56, April 1997.(accessed

2016 March 21).

MS Obaidat , B Sadoun, “Verification of computer users using keystroke dynamics”, IEEE Transactions on Systems, Man, and Cybernetics, Part B 27(2): 261-269, April 1997. . (accessed 2016 May 11).

D Shanmugapriya, G Padmavathi, “A Survey of Biometric keystroke Dynamics: Approaches, Security and Challenges”, (IJCSIS) International Journal of Computer Science and Information Security, ISSN 1947 -5500, Vol. 5, No. 1, 2009. . (accessed 2016 June 16).

R Napier, W Laverty, D Mahar, R Henderson “Keyboard User Verification: Toward an Accurate, Efficient and Ecological Valid Algorithm”. International Journal of Human -Computer Studies, vol. 43, pp213-222, 1995. . (accessed 2016 May 2).

S Furnell, A Buchoux, NL Clarke, “User Authentication for Keypad-Based Devices using Keystroke Analysis”.MSc Thesis, University of Plymouth, UK, 2000. . (accessed 2015 March 6).

MS Obaidat , B Sadoun, ,“Computer user verification using the perceptron,” IEEE Trans. on Systems, Man, and Cybernetics, vol. 23, no. 3, pp. 900–902, May 1993. . (accessed 2016 August 6).

I Soğukpinar, L Yalçin (2004), User identification at logon via keystroke dynamics, Journal of Electrical and Electronics Engineering,Vol. 4, No. 1, 995-1005. . (accessed 2016 May 23).

A Ross, AK Jain - Signal Processing Conference, 2004 - ieeexplore.ieee.org. . (accessed 2016 May 10).

E Yu, S Cho , "Keystroke dynamics identity verification and its problems and practical solutions", Computers & Security, 2004. . (accessed 2016 September 6).

S Furnell, A Buchoux, NL Clarke,, 'Authenticating mobile phone users using keystroke analysis' International Journal of Information Security, 6 (1): 1-14, 2007. . (accessed 2015 May 6).

D Mahar, R Napier, M Wagner, W Laverty ."Difference in Digraph Latency Distributions". Int. Journal of Human- Computer Studies, 43:579 592, 1995. . (accessed 2016 May 2).

JD Levy, A Ellsworth "Distance-Educator.com",(August, 2013). . (accessed 2016 June 6).

F Monrose, AD Rubin. Authentication Via Keystroke Dynamics. . (accessed 2016 july 6).

F Bergadano, D Gunetti, C Picardi . Fourth ACM Conference on Computer and Communications Security, Pages 48 56, 1997, (accessed 2016 May 20).

D Gunetti, C Picardi, " Keystroke analysis of free text", ACM Transactions on Information and

System Security, volume 8, pages 312–347, 2005. . (accessed 2016 May 16).

H Lee, S Cho, “Retraining a keystroke dynamics based authenticator with impostor patterns”, Computers & Security, 26(4): 300-310, 2007. . (accessed 2016 May 10).

Kevin S. Killourhy CMU-CS-12-100 January 2012. (accessed 2016 November 5).

Pin Shen Teh, Andrew Beng Jin Teoh, Thian Song Ong, Han Foon, “Statistical Fusion Approach on Keystroke Dynamics”, Third International IEEE Conference on Signal -Image Technologies and Internet-Based System”, 2007. (accessed 2016 May 6).

R Joyce, G Gupta. Identity Authorization Based on Keystroke. 2001, Latencies. Communications of the ACM, 33(2):168{176, February 1990.}, (accessed 2014 November 22).

RS Gaines, W Lisowski, SJ Pres s, N Shapiro.” Authentication by keystroke timing”: some preliminary results. Rand report R-256-NSF. Rand Corporation, 1980. (accessed 2015 January 8).

MS Obaidat, B Sadoun “Verification of computer users using keystroke dynamics”. IEEE Transactions on Systems, Man and Cybernetics 27 (1997) Pages 261 –269.2026. (accessed

2015 August 13).

F Bergadano, D Gunetti, C Picardi "University of Torino (2002) Transactions on Information and System Security", Vol. 5, No. 4, November 2002, Pages 367–397. (accessed 2014 June 3).

Wilhelm Magnus, S Blanes, F Casas, JA Oteo, J Ros (January 2009) (accessed 2016 November 23).

E Jaeger - J. Marshall J. Info. Tech. & Privacy L., 2014 HeinOnline 16. Margaret Rouse (accessed 2014 November 3).

D Shanmugapriya, G Padmavathi - arXiv preprint arXiv:0910.0817, 2009 - arxiv.org "A survey of biometric keystroke dynamics: Approaches, Security and Challenges" (IJCSIS) International Journal of Computer Science and Information Security, Vol. 5, No. 1, 2009. (accessed 2016 May,1).

I Vergote, R Verheijen, U Wagner - Annals of, 2005(accessed 2015 May 7).

A Peacock, X Ke, M Wilkerson, www.biopassword.com (accessed 2014 May17).

PI Good,WWW.Symetric.ca, (accessed 2015 June 19).

R Song, Z Luo, JY Nie, Y Yu, HW Hon- Www.thefreedictionary.com (accessed 2015 June 19).
S Keith, ME Martin-www.webopedia.com (accessed 2015 June 5).

Ankur Kumar1 , Abhijeet Patwari2 , Sagar Sabale " User Authentication by Typing Pattern for Computer and Computer based devices" (accessed 2016 May 19)

Appendix

User Manual

Windows® System Requirements

Minimum requirements:

Intel 1.8 GHz speed, Windows XP operating system

1GB Memory, 80 HDD

16X CD-ROM Drive

360MB Free Hard-Disk space*

16-bit colour monitor

800 x 600 Resolutions

Windows® compatible sound card

Windows® compatible mouse

A colour printer with 300dpi or better is recommended.

Installing "Bionetlogon" System

After installing the program from the CD, " BioNetLogon" the System runs from your hard drive. To complete the installation, 360MB free space is required on your hard drive to store program files. Close all programs and applications before installing.

When using "BioNetLogon" System under a typical installation, these instructions assume that the AutoPlay feature is turned on.

Windows

- Insert the "BioNetLogon" System CD in the CD-ROM drive.
- Follow the onscreen instructions to complete the setup process.

The setup program places "BioNetLogon" System file icons in the start menu.

Steps to Setups Administrator

- Enter administrator details into form thus username, password and confirm it.
- Click ok bottom to save.
- Restart the system for "BioNetLogon" software to start running.
- Enter logon details thus administrator username and password for authentication
- Use the logon learner window to learn the keystroke Dynamics pattern or rhythm.
- Save learnt keystroke pattern.
- Add new user to the system.

Steps to Setup User

- Enter user details into form thus username, password and confirm it.
- Click ok button to save.
- Use the logon learner window to learn the keystroke Dynamics pattern or rhythm.
- Save learnt keystroke pattern.
- Enter logon details thus username and password for authentication.