SECURITY CONCERN OF SMALL-MEDIUM ENTERPRISES ON CLOUD COMPUTING ADOPTION

(TWO-STEP AUTHENTICATION SOLUTION)

By:
Osei Eric Opoku

A Thesis submitted to the Department of Computer Science, Kwame Nkrumah University of Science and Technology in partial fulfillment of the requirements for degree of

MASTER OF SCIENCE

Information Technology

June 2013

DECLARATION

I hereby declare that this thesis is my own work towards the Master of Science 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 or elsewhere, except where due acknowledgement has been made in the text.

STATUS	NAME	SIGNATURE	DATE
Student	OSEI ERIC OPOKU **(PG6559411)**	………………………	10/5/13
Certified by **(Supervisor)**	DR. J.B HAYFRON-ACQUAH	………………………	16/5/1
Certified by **(Head of Department)**	DR. J.B HAYFRON-ACQUAH	………………………	…………

ABSTRACT

Cloud computing is an agile evolution in ICT world to facilitate virtual application deployment. We all use cloud: emails and social networks are services provided using cloud. However, the new idea is to leverage this virtual subscription concept into everyday enterprise business. Service providers offer to corporate clients: *Infrastructure-as-a-Service, Software-as-a-Service, and Platform-as-a-Service*; all at pay-per-use and without initial Capital-intensive demand. Cloud offers better economic advantages over the traditional in-house-acquired IT infrastructure. The two architectures have similar setback of Trusted-security, but cloud has high migration risk.

The Trusted-security problems under discussion involved the difficulty working with unknown cloud system administrator and insufficient protection for data access at user end workstation. The discussion prompted a research question to redesign system login architecture that offers sufficient protection at user-end workstation, so that domain intrusion is blocked on real-time.

We designed a new login architecture using the 2-step authentication concept. Unique feature introduced to this concept was the use of logic "AND" gate mathematical model for interlocking user computer to mobile phone. We adopted system development life cycle as research method.

On experiment, user must login with cloud username and password on computer as step-1 key to do access request. The user has to complete login using biometric authentication as step-2 key. The authentication server picks the request by step-1 password key "AND" embeds login link to a pre-defined user mobile phone for biometric scan. There is backdoor login process; link is sent through E-mail account so that computer with biometric scanner is used to authenticate user.

Result indicated that a hacker holding user-password, user-phone or any biometric computer, cannot access enterprise cloud data without authorised fingerprint scan to authenticate access. We recommended eye and fingerprint scans (multi-nodal scanning) to reduce authentication failure rate and argued conclusively that this re-design work can improve cloud trusted-security.

Keywords: Cloud computing, Security, Login Access control, 2-step Authentication, Biometric

ACKNOWLEDGEMENT

First, I thank God, the almighty, for his divine guidance coupled with the gift of creativity and innovation that has won me over six technological innovation accolades in my current employment at MTN-Ghana.

I am indebted to DR. J.B HAYFRON-ACQUAH, my thesis supervisor. Under tensed schedules as the Head of Department, he supported to turn imagination into realization. May God continue to bless you for your time, inputs and apt for excellence.

To MTN-Ghana: Admittedly, I can see far and admire a brighter career future because giants allowed me stood on their shoulders. If I presume to be excited about how far I have come in my career, then it is because MTN-Ghana, the company I have worked for seven **(7)** years, allowed me to work and study simultaneously. Not just that KIND privilege, the company also supported my personal development in CASH for my school fees subvention.

I am grateful to my interviewees: Wilfred Bruku (facts on SMS transmissions), Edgar Zormelo (Cloud system administration) and Eric Afanu (I.T security consultant) for immense contribution gathered from their experiences.

I am grateful to my wife and Children, as they have to sacrifice to let me have more concentrated hours to finish my work on schedule.

Finally, I cannot hold back my appreciation to all the lecturers at the Department of Computer Science. I own them due acknowledgement for their contributions. God bless contributors.

DEDICATION

I dedicate this thesis to my wife and children. Admittedly, I took major part of the family time to complete this research. You have shaped me to appreciate and understand the need for a balance life between academics and family responsibilities.

God bless you.

TABLE OF CONTENT

ABBREVIATIONS

SLA	*Service* Level Agreement	1
CIO	Chief Information Officer	4
IaaS	Infrastructure-as-a-Service	5
SaaS	Software-as-a-Service	5
PaaS	Platform-as-a-Service	5
XaaS	Everything-as-a-Service	5
OS	Operating System	7
VPN	Virtual Private Network	7
TCH	Traffic Channel Availability	8
D-Gate	Double Gate Access Control	9
SDLC	System Development Life Cycle	10
OTP	One Time Password	20
SSL	Secure Socket Layer	23
TOTP	Time-based One Time Password	23
AWSMF	Amazon Web Service Multifactor Authentication	23
IAM	Identity & Access Management	25

FIGURES

TABLES

CHAPTER 1

1.0. Introduction

This chapter introduces the background of the research topic and provides information about the knowledge gap which this topic is about to fill by discussing the previous research around this subject. Cloud computing is the new evolution to expand ICT for development and virtual applications. We all use cloud: emails and social networks are services provided using cloud. However, the new idea is to leverage this virtual subscription concept into everyday enterprise business. Service providers offer to corporate clients: *Infrastructure-as-a-Service, Software-as-a-Service, and Platform-as-a-Service*; all at pay-per-use and without initial Capital-intensive demand. Cloud offers better economic advantages over the traditional in-house-acquired IT infrastructure.

1.1 Theoretical Background and terminologies in cloud

In the late 1960's, the computer scientist John McCarthy once brought the concept of utility computing into the technology world, predicting that the life cycle of technology will not only stick as tangible products. From the background of utility computing, one can admit that cloud computing is an innovation from the utility computing. In utility computing, simply put, utility computing allows customers to receive computing resources, hardware or software, from a service provider and "pay –as-you-go"; much as you do for your water and electricity services at home. The very near concept of today's cloud computing was called grid computing. The intangible difference between cloud and grid is that cloud comes with service Level Agreement (SLA) between customer and the provider. Aside from being SLA-driven there is no concern to user to see the nature and location ~~of the un~~derlying infrastructure for clouds. Cloud computing is a flexible, cost-effective and proven delivery platform for providing business or Consumer IT servi~~ces ov~~er the Internet. Cloud resources can be rapidly deployed and easily scaled, with all processes, applications and services provisioned "on demand," regardless of user location or device. Away from cloud, the term grid computing also originated in the early 1990s as a metaphor for making computer power as easy to access as an electric power grid. The power grid metaphor for accessible computing quickly became canonical when Ian Foster and Carl Kesselman published their seminal work, "The Grid: Blueprint for a new computing infrastructure" (2004). Grid environments are tons more modular and do not have single point of failure. If one of the servers or deskstop in the grid fails, there are tons of other resources ready to pick load. Roles can immediately restart if a failure happens. More specifically, the results of all processes are sent first on all nodes within the grid, and then collaboratively assessed. Before the final assessment is made, it is not possible to define or to declare a final outcome. This is particularly a problem when talking about time sensitive projects. Furthermore, another important disadvantage of grid computing is that it relies heavily on dispersed data management (which is a very important concept in cloud computing) and connectivity (connectivity errors may occur unexpectedly). We can now examine the milestones of the cloud over the grid sytem.

In 2008, Geva Perry of Gigaspace technologies listed below features and characteristics to best describe cloud computing. An infrastructure is uniquely classified as cloud computing for its-

- ***Self-healing*:** In case of failure, there will be a hot backup instance of the application ready to take over without disruption (known as failover). It also means that when I set a policy that says everything should always have a backup, when such a fail occurs and my backup becomes the primary, the system launches a new backup, maintaining my reliability policies.
- ***Data, Data, Data*:** The key to many of these aspects is management of the data: its distribution, partitioning, security and synchronization.
- ***SLA-driven*:** The system is dynamically managed by service-level agreements that define policies such as how quickly responses to requests need to be delivered. If the system is experiencing peaks in load, it will create additional instances of the application on more servers in order to comply with the committed service levels, even at the expense of a low-priority application.
- ***Multi-tenancy*:** The system ~~is built~~ in a way that allows several customers to share infrastructure, without the customers being aware of it and without compromising the privacy and security of each customer's data.
- ***Service-oriented*:** The system allows composing applications out of discrete services that are loosely coupled (independent of each other). Changes to or failure of one service will not disrupt other services.
- ***Virtualized*:** Applications are de-couple from the underlying hardware. Multiple applications can run on one computer (virtualization a la VMware) or multiple computers can be used to run one application (grid computing).

- ***Linearly Scalable***: Perhaps the biggest challenge; the system will be predictable and efficient in growing the application. If one server can process 1,000 transactions per second, two servers should be able to process 2,000 transactions per second, and so forth.

Transition from the traditional in-house server computing to public or private cloud computing has some good results. There is no need any more for worrying about the machines running the application as the service provider is now taking care of that. Secondly, there is no need for devotion of time and resources to develop and maintain the applications that is used.

However, there are disadvantages that come along with this kind of transition:

- ❖ One-size-fits-all approach might not work for all enterprises with complex requirements
- ❖ Other companies might not like the idea of processing the data outside their firewall
- ❖ The subscription model does normally not align the costs of usage. Hence, companies wanted the convenience and simplicity of software as a service.
- ❖ With the concept of virtualization, servers could be utilized more efficiently, while applications and IT infrastructure are independent allowing servers to be easily shared by many applications running virtually anywhere.

Security is critical in any virtual application like the cloud computing. Vitalizing the application involves packaging the application bits with everything it needs to run, that could include security controls, database, middleware and operating system. This self-contained unit of virtualized application can run anywhere (Armbrust et al., 2009).

In terms of metering, the cloud is a computing service that charges based only on the amount of computing resources that are used (Motahari-Nezhad et al., 2009). This pay-per-use feature is one of the big marks of today's cloud computing and one of the things that sets it apart from traditional IT services (Armbrust et al., 2009).

In wrapping up this section, there is no need evaluating whether cloud computing is worth the investment, if an entity decides to move from the in-house computing to the cloud. It is obviously the cheapest; but why business enterprises have adopted a "wait-and-see" approach in moving unto the cloud?

Adam Maguire published a survey conducted amongst Chief Information Officers (CIO's) and I.T Directors during the 2010 pricewaterhouseCoopers forum (www.irishtimes.com, 2010). The publication provided feedback that clearly shows "Security" as the biggest concern for enterprises thinking about the cloud evolution. It is now very interesting to go back one-step in time before cloud computing to find literatures on cloud securities. It is important to understand existing security measures on cloud platform, as well as, what some stakeholders think about cloud security. After that it can be discovered whether the literature evaluations of the security solutions raised by key stakeholders can lead to different security control approach that can build more trust for enterprises to confidently move on to the obvious cost-effective computing platform.

Existing Research papers on cloud computing

Cloud Computing as an academic keyword is emerging in the last few years (2007), even though disciplines that are the base of cloud computing as grid computing, virtualization, software oriented architecture, web services, utility computing and distributed computing have been a theme of a vast number of researches (Motahari-Nezhad et al., 2009). There are several papers captioned under the old names than the contemporary buzzword, "Cloud Computing". A fact that could be noticed in the searching for previous studies is that most of the technical –driven research conducted until now were conducted by private research institutes such as Gartner and Forrester, the IBM laboratory. India is doing well with cloud computing research; however most of the papers focuses on the business case and future prospects for enterprises ready to use cloud computing. However, one thing that stands tall in many of the recent cloud papers irrespective of the dimension of objectives captures the word- Security. As much as possible the only security papers captioned under cloud computing technology shall be reviewed in this work to provide focus and common language. This means that closely related papers such as grid computing security, utility computing security, distributed computing security, web services security, and virtualization security would not be used in the literature review.

Definition of Theoretical Terminologies of cloud

1. **Cloud computing:** - The term, "cloud computing", was first used in 1997 by information systems professor, Ramnath Chellappa. Basically it is the use of computing resources (Hardware and Software) that are delivered as a service over the internet.

2. **Private Cloud computing: -** Private cloud is “A form of cloud computing where service access is limited or the customer has some control/ownership of the service implementation.” (Tom Bittman, May 2010)
3. **Public Cloud Computing:-** When the customer does not see the implementation behind the boundary, and the provider doesn’t care who the customer is, you have a public cloud service. A typical example is Yahoo and google email and other services.
4. **Hybrid Cloud Computing: -** A composition of at least one private cloud and at least one public cloud (Bill Claybrook, 2011). For example, a multinational-group banking institution that has on-premise datacenter serving global branches may choose to interconnect with Google public cloud using Safe connection or Virtual Private Network for effective security. The bank may choose to run “mission critical operations on their private datacenter/cloud and run peak workloads on the public cloud to harness scalability. The summary of the differences are shown as in table 1.1.

Table 1.1 Cloud Topologies – Benefits and Risks

TOPOLOGY	BENEFITS	RISK
Public Cloud	-Low investment hurdle -Scalability for Applications	-Multi-tenancy security threat -Loses data Control
Private Cloud	-Sustain in-house security policies -Retains data Administrative control	-High infrastructure cost -High operation/maintains cost
Hybrid Cloud	-Operational swap flexibility -Scalability & Network Availability	- Few in real use/Adoption -Some Public cloud security threat

5. **Cloud Infrastructure-as-a-Service (IaaS):-** This is one of the three main services in cloud computing. Providers offer to clients computers, servers and transmission medium resources.
6. **Cloud Software-as-a-Service (SaasS):-** Sometimes referred to as "on-demand software", is a software delivery model in which software and associated data are centrally hosted on the cloud. SaaS is typically accessed by users using a thin client via a web browser.
7. **Cloud Platform-as-a-Service (PaaS):-** In this model, the consumer creates the software using tools and/or libraries from the provider. The consumer controls software deployment and configuration settings. Server co-location, office space are all platform services

Evolutional Technologies to the Cloud concept

1. **Utility Computing: -** It is the packaging of computing resources, such as computation, storage and services, as a metered service. Cloud computing added the idea of applications and network as a service on demand.
2. **Cluster and Grid Computing:-** Cluster, Grid and cloud are all distributed classified as distributed system and they share common characteristics. Their commonalities are resource pooling and broad network access. One significant difference is that we use network access topologies for both cluster and grid computing internally by specific large corporate entity with distributed departments or branches. Cloud computing extend this internally distributed corporate network access to cover public network access (internet), using VPN for corporate consumers to achieve data privacy.
3. **Virtualization: -** The usual goal of virtualization is to centralize administrative tasks while improving scalability and overall hardware-resource utilization. With virtualization, several operating systems can be run in parallel on a single central processing unit (CPU). This parallelism tends to reduce overhead costs and differs from multitasking, which involves running several programs on the same OS. Cloud, cluster, and Grid systems of operations are all forms of virtualisation. The summary of characteristics between Cluster, Grid compared to cloud are shown as in table 1.2

Table 1.2: Characteristics of Cluster, Grid and Cloud

Characteristics	Cluster	Grid	Cloud
On-demand Self Service	No	No	Yes Services are Dynamic, unlike the pre-reserved services in Cluster & Grid
Broad Network Access	Yes	Yes	Yes
Resource pooling	Yes	Yes	Yes
Rapid Elasticity -	No	No	Yes Call it Pre-paid offer- Customer can procure low or high computing power needed anytime.
Measured Service	No	Yes	Yes Pay-per –use metering is accurately and transparently measured in Grid & Cloud

General cloud Terminologies

1. **Cloud Service Provider:-** I.T service suppliers such as Amazon, Google, Microsoft, Salesforce, force.com, MTN in Africa and Balti-airtel etc
2. **Cloud Client/Consumer:-** An entity that subscribes to this virtual services
3. **Cloud User:-** Any principal holding credential to access cloud applications
4. **Data Confidentiality:** - A term use to prevent the disclosure of information to unauthorized individual or a system. In cloud all data transmissions on the internet and storage are encrypted with public key. There is breach of confidentiality, if an authorized person or system obtains access to the data in transit or data-at-rest or data-in-process.
5. **Data Integrity**: - In security, this means data-in transit or data-in-motion cannot be modified undetected in the cloud platform. Integrity is violated when unauthorized party actively modifies data.
6. **Data Availability:** - This means that the computing systems used to store and process the information, the security controls used to protect it, and the communication channels used to access it must be functioning correctly with 99.99% of systems availability.
7. **Authenticity:** - Any reliable method to validate that parties inter-connected to exchange information are who they claim to be per definitions in the security and access control unit. One recommended authentication method for to boost trust for cloud computing and subscription is the D-Gate access control technology under-investigation in this research work.
8. **Public-key cryptography**: This data protection technology refers to a cryptographic system requiring two separate keys, one of which is secret and one of which is public. Although different, the two parts of the key pair are practically impossible to derive one key from the other key. One key locks or encrypts the plaintext, and the other unlocks or decrypts the ciphertext.
9. **Sandboxes:** - A sandbox is a security mechanism for separating running programs. Used in all virtual systems including the cloud, the sandbox typically provides a tightly controlled set of resources for guest programs to run in, such as scratch space on disk and memory. Network access, the ability to inspect the host system or read from input devices are usually disallowed or heavily restricted. This also reduces the threat in using multi-tenancy platforms such as the cloud.

1.1 Problem Statement

In order to attract enterprises to appreciate cloud Trusted-security, service providers have to share system administrative (login) control with clients to block domain intrusion on real time. The use of 2-step authentication concept at the user-end workstation can offer a visible security control for a client to appreciate secured data on the cloud platform.

Very few cloud providers have added authentication layer to support password at the user-end workstation. However, it has recurring limitations that allow intrusion success using either keylogger software, stolen PIN code and/or stolen authentication device such as mobile phone.

If service providers fail to implement robust authentication layer at user-end workstation, hacking intrusion will upsurge and thus downgrade the adoption of cloud computing over in-house IT infrastructure.

We proposed 2-step/multifactor authentication using biometric to overcome the three limitations and block intrusion on real time. Our proposal will argument the use of cryptography as dominant security option in the cloud. Cryptography model seeks to protect data at rest and data in transit/motion from or to the cloud platform; but the 2-step authentication option stands gallantly at the user-end to improve access protection.

Until now, cryptography is the major security technology for data protection in the cloud. Research laboratories of large vendors such as; Google, HP, IBM, and Amazon concentrates on investigating how best to advance data encryption and decryption algorithms to improve confidentiality, Integrity and Availability on the platform. Research works are ongoing to make cryptography security applications robust. However, many hackers, cyber criminals and some novels always finds alternative means to make the security algorithm vulnerable. Such vulnerability affects either data in transit or data at rest that has been protected by encryption algorithms. Encryption and decryption protection for data are currently the major alternative to convince customers to transfer enterprise data unto the cloud platform. *Many articles purported to speak for the consumer of cloud services do complain about the vulnerabilities in cryptographies and the fact that a client loses administrative control entirely on enterprise data, after moving to the cloud business solution.*

We named our work as "Conjunction 2-step biometric authentication method" due to the use of AND logic function to conjoin user workstation to mobile phone to complete authentication.

1.2 Research Question

1. What improvement on Two-step authentication method would ensure that a hacker in possession of authorized username, password, PIN code and the stolen mobile phone cannot access corporate data sitting on cloud computing infrastructure".
2. In what way can SME's subscribing to cloud computing administer security control against real time intrusion on the multitenant cloud platform to inprove trusted security.

1.2.1. Aim

The long-term goal is to compose basis for cloud security research and investigations that attempts to return at least 60% of system administration and security controls on data back to enterprises after making transition from their in-house computing to the cloud-computing platform.

1.2. 2. Objective

The specific objective of the study is to:

- Develop by experiment, double authentication security software, where cloud user has to validate access credentials on two unique but integrated workstations of a user.

1.2.3 Scope of Research

This study primarily investigated existing 2-step authentication security methods and observed how to improve the method for cloud computing implementation.

1.2.4 Limitation

1. Ambiguous undefined terms – The term Cloud is quite new in the information Technology cycle. Sometimes being too technical when asking interview questions can force people to respond based on their understanding, which may not give reflection of exact information gathering needs. To reduce such limitation, the scope of technical language associated with cloud computing was reduced to ensure clarity of questions to the respondents.

1.3 Research Methods

Qualitative and quantitative research methods were used. The literature review chapter involves secondary data collected solely from online digital libraries of cloud-based industry players' using the 2-step authentication system. Most academic and journal papers reviewed on two-step authentication have to deal with network paths and address protocols using 2-step methods. These papers were avoided as part of data collection in chapter two of this paper to reduce scope deviation. Primary data collection was captured through unstructured interviews with I.T security experts, cloud administrator and a mobile switching engineer to improve on the research question as well as the software design methodology. The System Development Life Cycle (SDLC) approach for software development process was adopted. Typical model of SDLC used in this work was the revolutional waterfall and the cycle is shown as in figure 1.

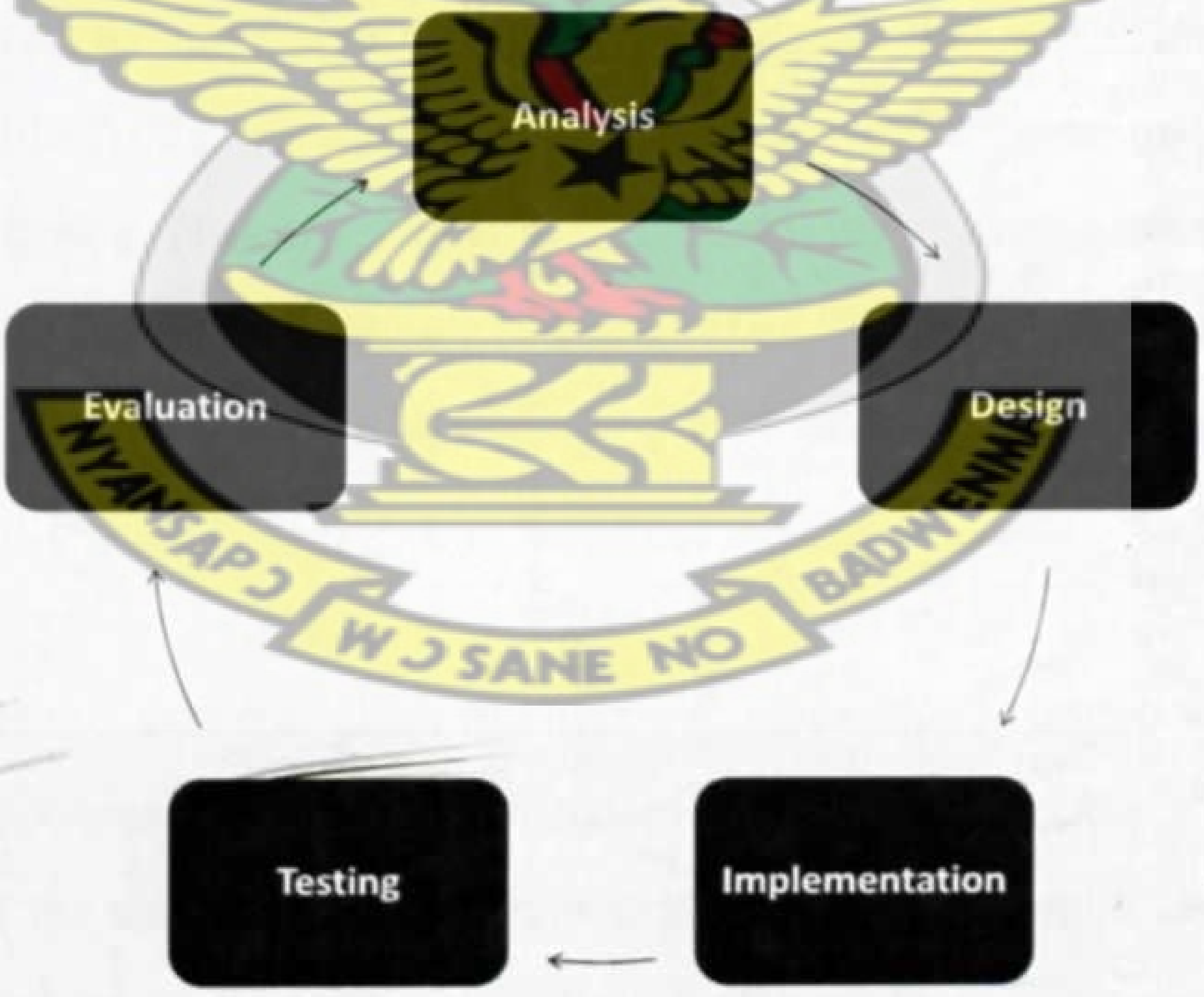


Figure 1: System Development Life cycle (SDLC) –Revolutionary Waterfall Model

Chapter 2
LITERATURE REVIEW

2.0. Introduction

In this chapter, there was the need to understand the fundamental journey made so far in two-step authentications at user-end workstation by various researchers to help build strong theoretical framework for this new work. The terms, verification and authentication, have been widely interchanged by various research groups; however, the convergent description of their methods are similar in application. The current researcher prefers the use of authentication in referencing the idea.

There are two main categories of researchers advancing the Two-step authentication method. The first classification of cloud security researchers' attempts to deepen knowledge in Double authentication within routing protocols in a network and cryptographic key usage. Their architecture simply involves user terminal (computer) and the authentication server. Major papers such as "A Double Authentication Scheme to Detect Impersonation Attack in Link State Routing Protocols" **(Dijiang Huang, 2003)**; "A Double-Way Authentication Access Control Scheme Based on Harn's Digital Signature" (**Rong Hua,2001**); "Study on Cloud Computing Security- Credible Access control (FENG et al, 2011) are all journal papers with common direction.

The second and the most current classification of researchers under this same Two-step authentication method focuses on how to do verification through mobile phone; where a secret code is generated from the authentication server and sent to the mobile device before used as input on the user terminal to complete access authorisation to data. Their architecture is made up of mobile phone, an authentication server and user terminal. So far, papers under this path are typically of direct experimental implementations in use by some specific cloud-based companies. Some companies captured in this direction are Google Account-"Two step authentication", Dropbox-"Two-factor verification", Microsoft/Hotmail- "Microsoft account security code", Barclays Internet Banking- "Secure code", Amazon-"AWS multifactor authentication".

The interest of the current researchers is to advance the latter dimension of 2-step authentication methods completed through mobile device. All papers reviewed under this chapter cover the Two-step authentication method that uses mobile phone/device to complete verification.

2.1 Rationale

The review of related work on two-step authentication using mobile phone/device helped the current researcher:

- Know what areas have been covered and what is yet to be covered in order to know how to contribute and provide scholarly results.
- Understand and use the relevant terminology in writing the thesis.

2.2 Two-step Authentication at Fujitsu Limited

S. Sotashi (2009) patented two-step authentication architecture at Fujitsu Limited to improve data security as shown in figure 2. They discussed that an authentication system includes a user terminal to perform authentication based on a password corresponding to a seed number generated in accordance with a predefined rule. The system further includes a password issuance apparatus to issue the password in response to reception of a request message including the seed number as shown in figure 2.

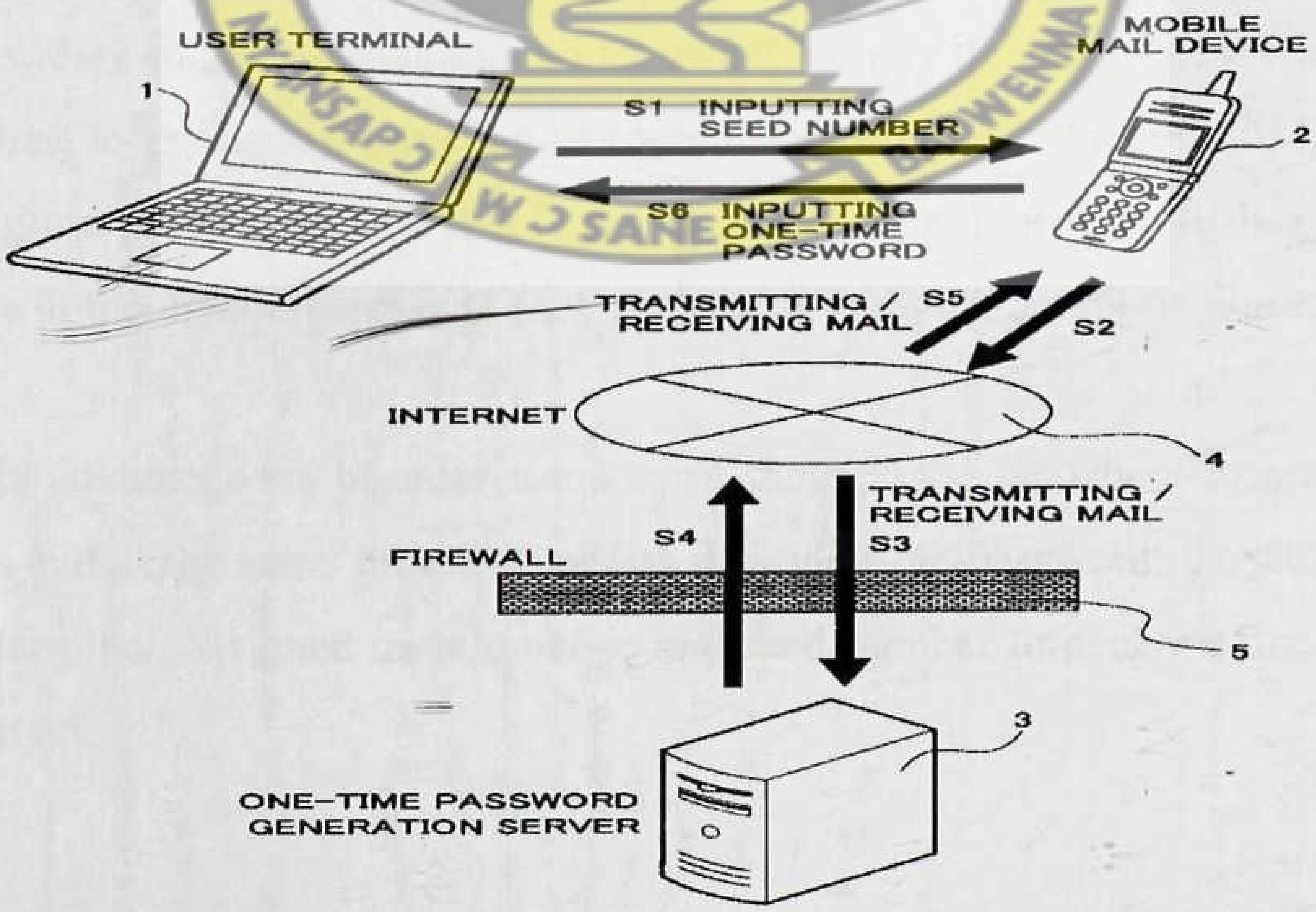

USER TERMINAL
1
MOBILE MAIL DEVICE
2
S1 INPUTTING SEED NUMBER
S6 INPUTTING ONE-TIME PASSWORD
TRANSMITTING / RECEIVING MAIL
S5
S2
INTERNET
4
TRANSMITTING / RECEIVING MAIL
S4
S3
FIREWALL
5
3
ONE-TIME PASSWORD GENERATION SERVER

Figure 2: The implementation of Two-Step Authentication as used by Fujitsu Limited

The method of design has three main device segments: User terminal, Mobile device, Server, and transmission medium (internet). Figure 1 shows that:

1. The mobile device has software uploaded to communicate with the authentication server.
2. Each user has a code called seed number; user enters that seed number on the mobile device and the seed number transmits to the authentication server.
3. The authentication server compares SIM number sending the request and Seed number assigned to that authorize user. If SIM and SEED numbers corresponds to pre-defined numbers on the server, then server grants the request to transmit one-time- password to the phone.
4. Authorized user can now obtain password and use it to log-in through the computer domain to access corporate data on business operations server.

[Patent Document 1] Japanese Laid-open Patent Publication No. 2007-58469]

Satoshi argued that the common practice of pre-defined password to a computer user is insecure; they are of the view that a user who is afraid of forgetting the password may write it on the body of the user terminal or on a piece of paper carried by the user. The written password may be sneaked a look at for unauthorized use. Especially, when a user carries a portable user terminal such as a notebook computer, the risk of unauthorized use of the password may increase.
In their findings, they suggested that an authorized user of any information system terminal must do a server request to generate a one-time-password only for use at the point of login and then it elapses after log-out to improve data security. In conclusion, authorised user has to do password request from the authentication server ~~at each~~ attempt to login using mobile phone to do request.

The ap~~proach~~ is advantageous because users carry their phone anywhere to make calls, check personal emails and at the same time to generate this one-time-password. Unauthorised user has to burgle user terminal, assigned mobile phone and seed number to generate one-time-password to open the domain.

The major problems associated with this approach are as follows:
First, if such application software needs to be downloaded to cellular phones, it will incur great cost for its both development and distribution. It should be noted that, although cellular phones are very popular, there are multiple manufacturers of cellular phones and people have various types of cellular phones. The application software for enabling cellular phones to operate as a one-time password generator may need to be adapted to each type of cellular phones. For example, android phone may pose compatibility challenge.

Secondly, the application software may be downloaded from a software distribution server connected to the Internet to each cellular phone. The software distribution server, if it is made accessible from the Internet, may face more risk of unauthorized accesses than a server connected in an intranet protected by a firewall. Thus, the software distribution server usually requires constant effort for maintaining a high level of security, the effort including applying security patches, for example. The operation of the software distribution server connected to the Internet is often outsourced to an external service provider in order to distribute the application software safely, which incurs additional operation cost.

Finally, eavesdropping risk becomes high. The method described in which a cellular phone and an authentication server are used requires the authentication server to store generated one-time passwords. The one-time password is sent at least twice, that is, from the authentication server to the cellular phone and from the operation server to the authentication server,(both servers finally communicates to verify password input by user) which increases the risk of eavesdropping.
In their conclusion, they conceded ~~it is an~~ object in one aspect of the invention to provide a new authentication system and method that solves at least one of the problems described with the use of cell~~ular ph~~one to complete two-step authentication. It is to be understood that both the foregoing general description and the following detailed description are exemplary and explanatory and are not restrictive of the invention, as claimed. The flowchart for executing the authentication process as in fujitsu work is shoen as in figure 3 and figure 4.

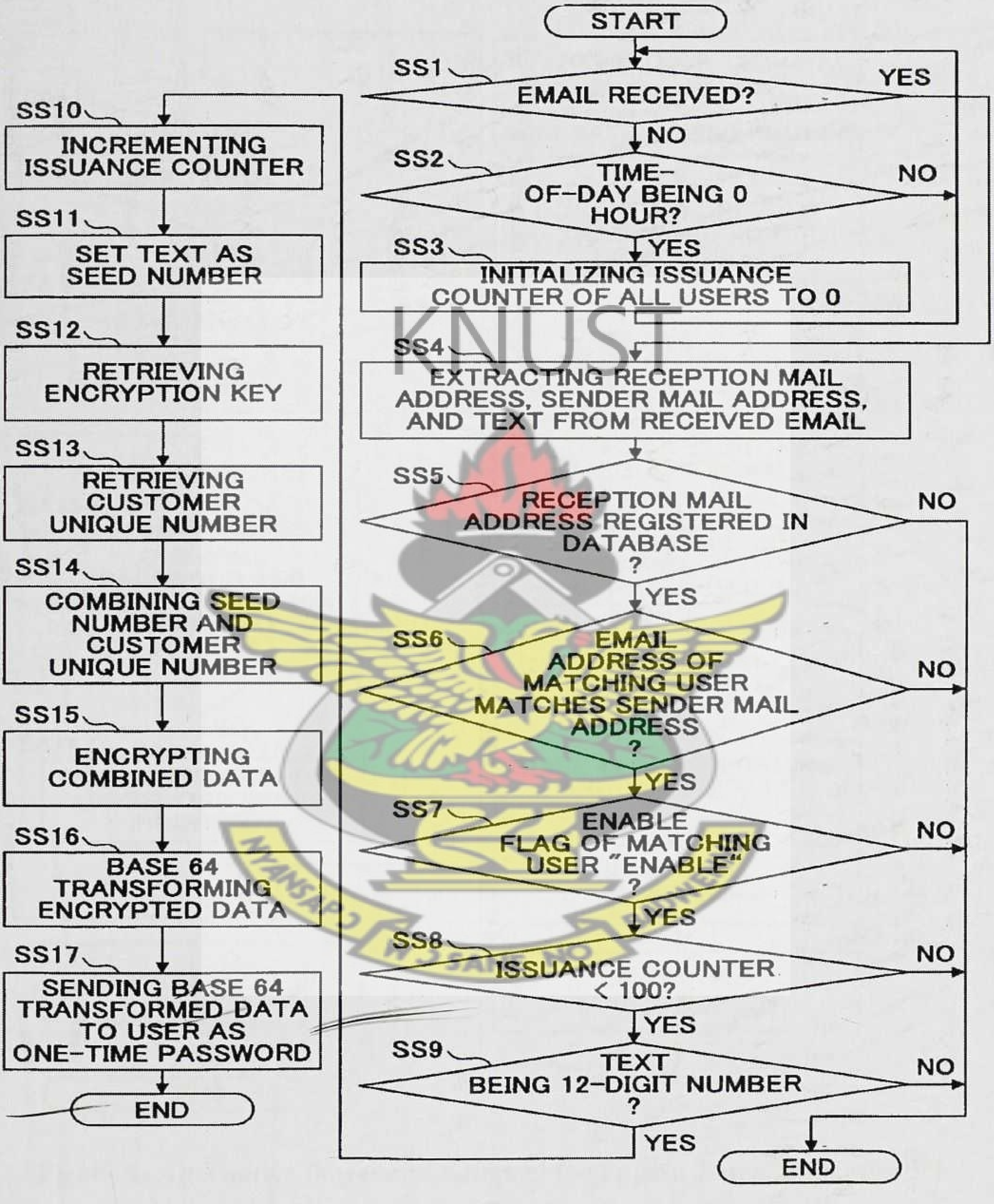

START
SS1
EMAIL RECEIVED?
YES
NO
SS2
TIME-OF-DAY BEING 0 HOUR?
NO
YES
SS3
INITIALIZING ISSUANCE COUNTER OF ALL USERS TO 0
SS4
EXTRACTING RECEPTION MAIL ADDRESS, SENDER MAIL ADDRESS, AND TEXT FROM RECEIVED EMAIL
SS5
RECEPTION MAIL ADDRESS REGISTERED IN DATABASE ?
NO
YES
SS6
EMAIL ADDRESS OF MATCHING USER MATCHES SENDER MAIL ADDRESS ?
NO
YES
SS7
ENABLE FLAG OF MATCHING USER "ENABLE" ?
NO
YES
SS8
ISSUANCE COUNTER < 100?
NO
YES
SS9
TEXT BEING 12-DIGIT NUMBER ?
NO
YES
END
SS10
INCREMENTING ISSUANCE COUNTER
SS11
SET TEXT AS SEED NUMBER
SS12
RETRIEVING ENCRYPTION KEY
SS13
RETRIEVING CUSTOMER UNIQUE NUMBER
SS14
COMBINING SEED NUMBER AND CUSTOMER UNIQUE NUMBER
SS15
ENCRYPTING COMBINED DATA
SS16
BASE 64 TRANSFORMING ENCRYPTED DATA
SS17
SENDING BASE 64 TRANSFORMED DATA TO USER AS ONE-TIME PASSWORD
END

Figure 3: Flowchart design by Fujitsu Limited for 2-step authentication

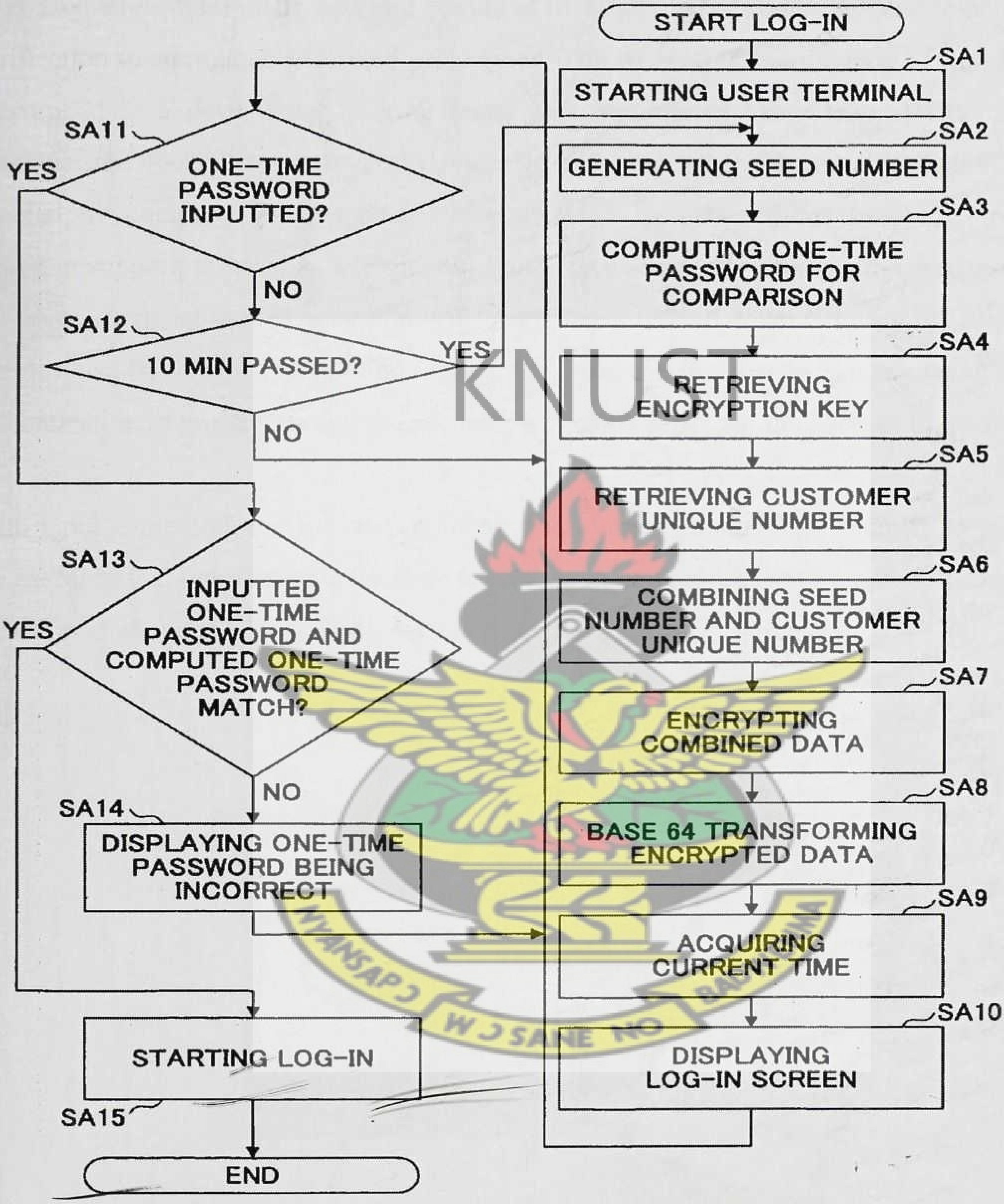

START LOG-IN
SA1
STARTING USER TERMINAL
SA2
GENERATING SEED NUMBER
SA3
COMPUTING ONE-TIME PASSWORD FOR COMPARISON
SA4
RETRIEVING ENCRYPTION KEY
SA5
RETRIEVING CUSTOMER UNIQUE NUMBER
SA6
COMBINING SEED NUMBER AND CUSTOMER UNIQUE NUMBER
SA7
ENCRYPTING COMBINED DATA
SA8
BASE 64 TRANSFORMING ENCRYPTED DATA
SA9
ACQUIRING CURRENT TIME
SA10
DISPLAYING LOG-IN SCREEN
SA11
ONE-TIME PASSWORD INPUTTED?
YES
NO
SA12
10 MIN PASSED?
YES
NO
SA13
INPUTTED ONE-TIME PASSWORD AND COMPUTED ONE-TIME PASSWORD MATCH?
YES
NO
SA14
DISPLAYING ONE-TIME PASSWORD BEING INCORRECT
STARTING LOG-IN
SA15
END

Figure 4: Alternative flowcharts designed for Fujitsu 2-step authentication

2.3. Google Account Two-Step Authentications

Alex Dobie (Google) made editorial comment in August 2012 about the need to adopt two-step verification to strengthen password protections. The writer referred the case of Mat Honan, who succumbed to a devastating hacking attack that annihilated his iCloud, Twitter and Google accounts and locked down several devices in the process. In Honan's case, the attack were enabled by compromised personal information, as well as failures by Amazon and Apple customer support, rather than a traditional brute-force attack or contact with malware.

However, a crucial part of what allowed the attackers to take down not only his Apple accounts and devices, but also his Gmail and Google stuff was the fact that he was not using the two-step authentication to protect his Google account; it became easier for the hackers to get information.

With Google method, the two-step authentication adds extra layer of security to password. On the user terminal (computer), a user has to enter both correct password and secret code sent to the pre-defined phone to get access to data as shown in figure 5.

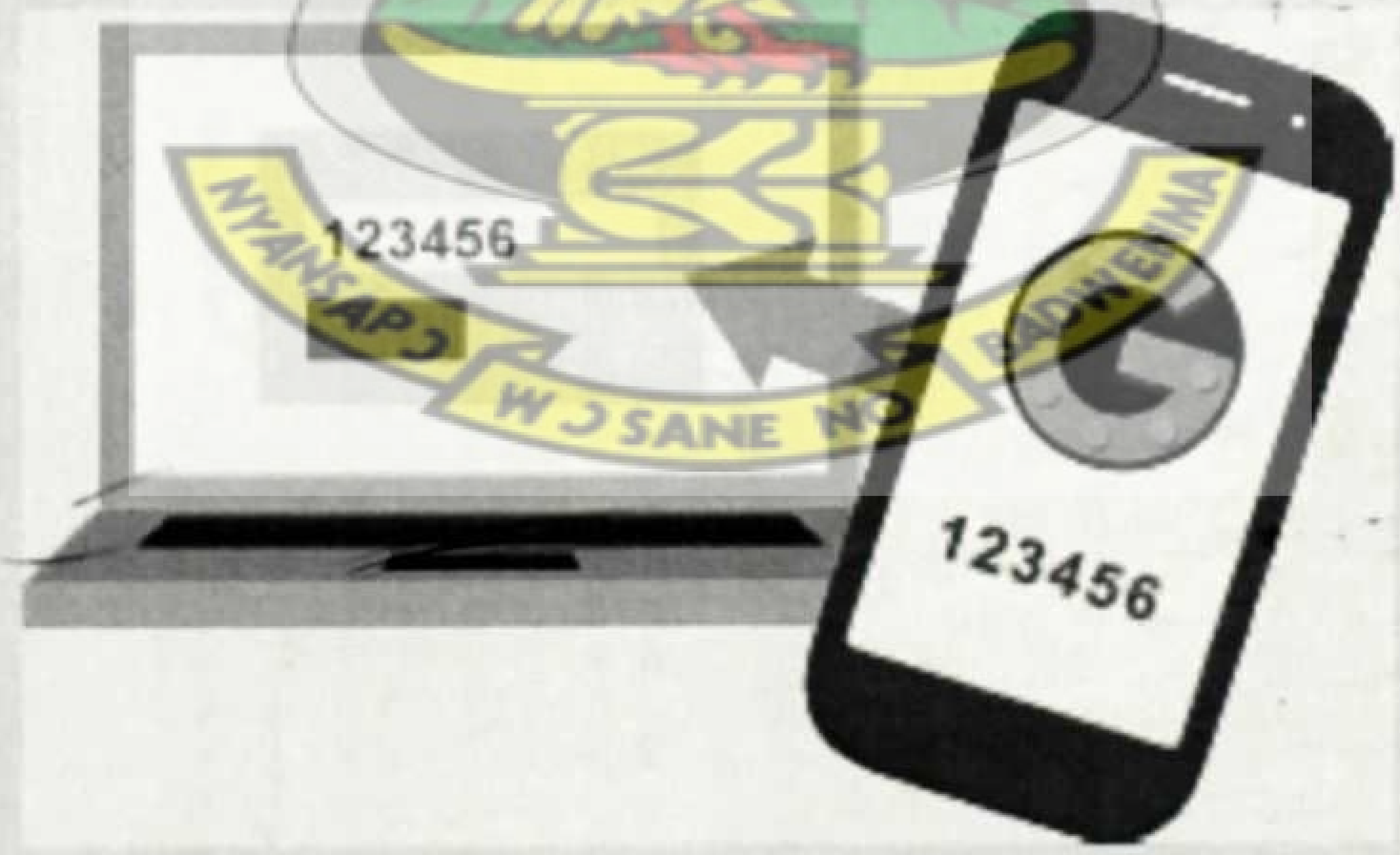


Figure 5: 2-step verification adds an extra layer of security to your Google Account

1. On your Gmail account go to sign in page and enter your normal username and password as shown in figure 6.

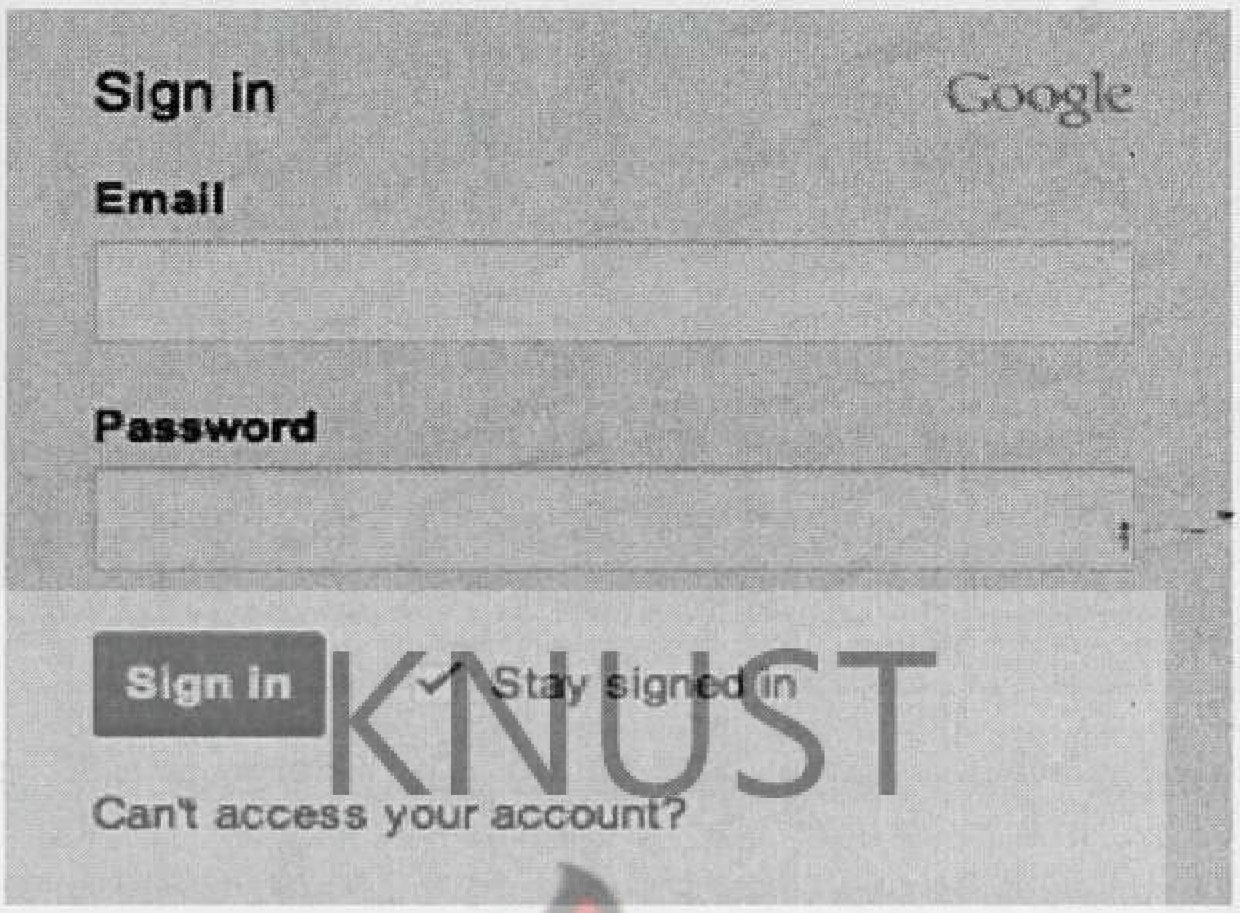
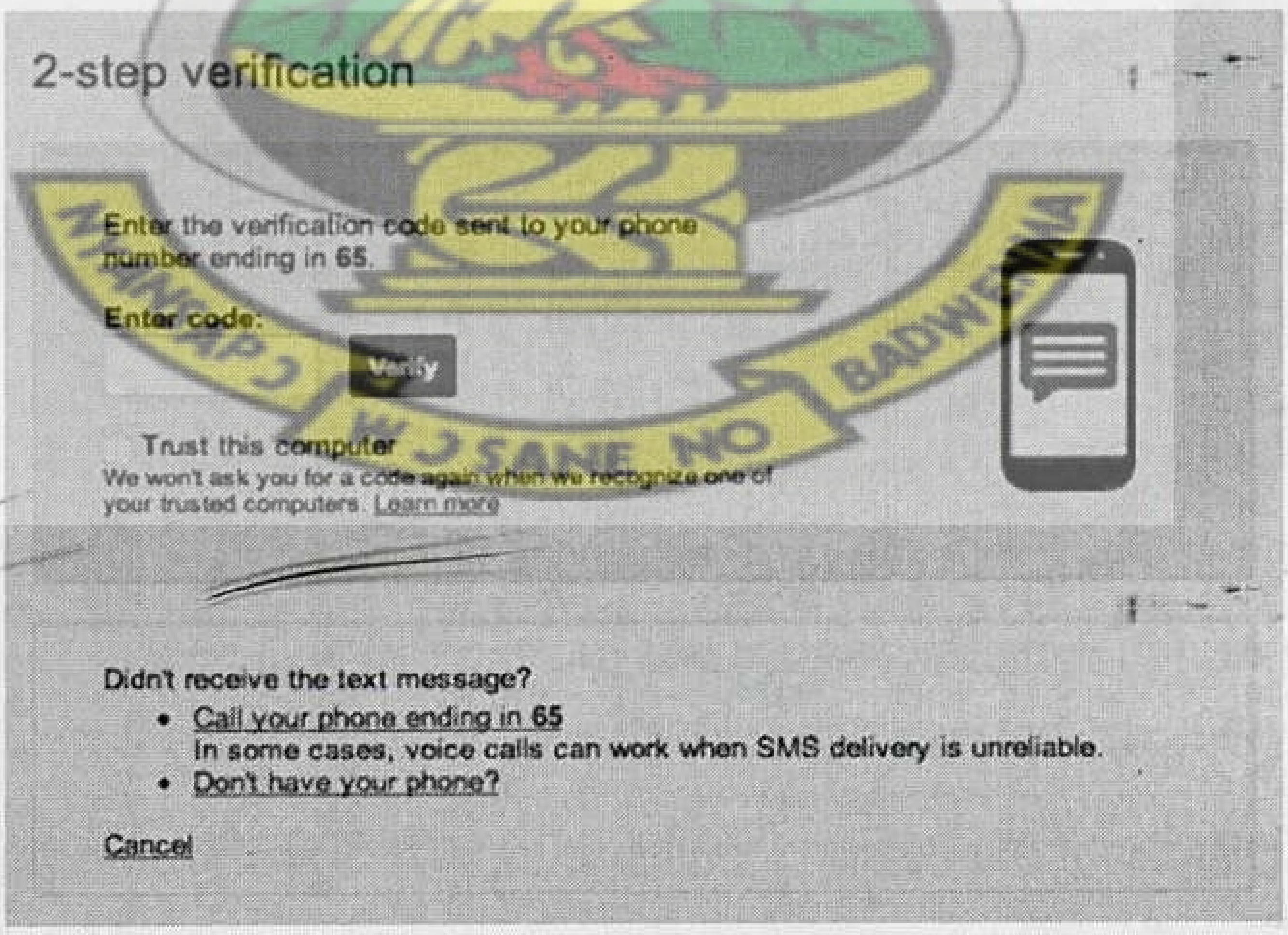


Figure 6: Gmail sign in page

2. After a click of sign in button, a verification page would appear. Then it will ask for a six-digit code, which you'll get from your phone. If you want, when you enter your code, you can choose to trust your computer -- this means you will not be asked for a code again when you sign in from this computer. If an authorised user sign in from another computer, however, it will still ask for the code as shown in figure 7.



Enter the verification code sent to your phone number ending in 65.

We won't ask you for a code again when we recognize one of your trusted computers. Learn more

Didn't receive the text message?

- Call your phone ending in 65
  In some cases, voice calls can work when SMS delivery is unreliable.
- Don't have your phone?

Figure 7: Gmail verification page

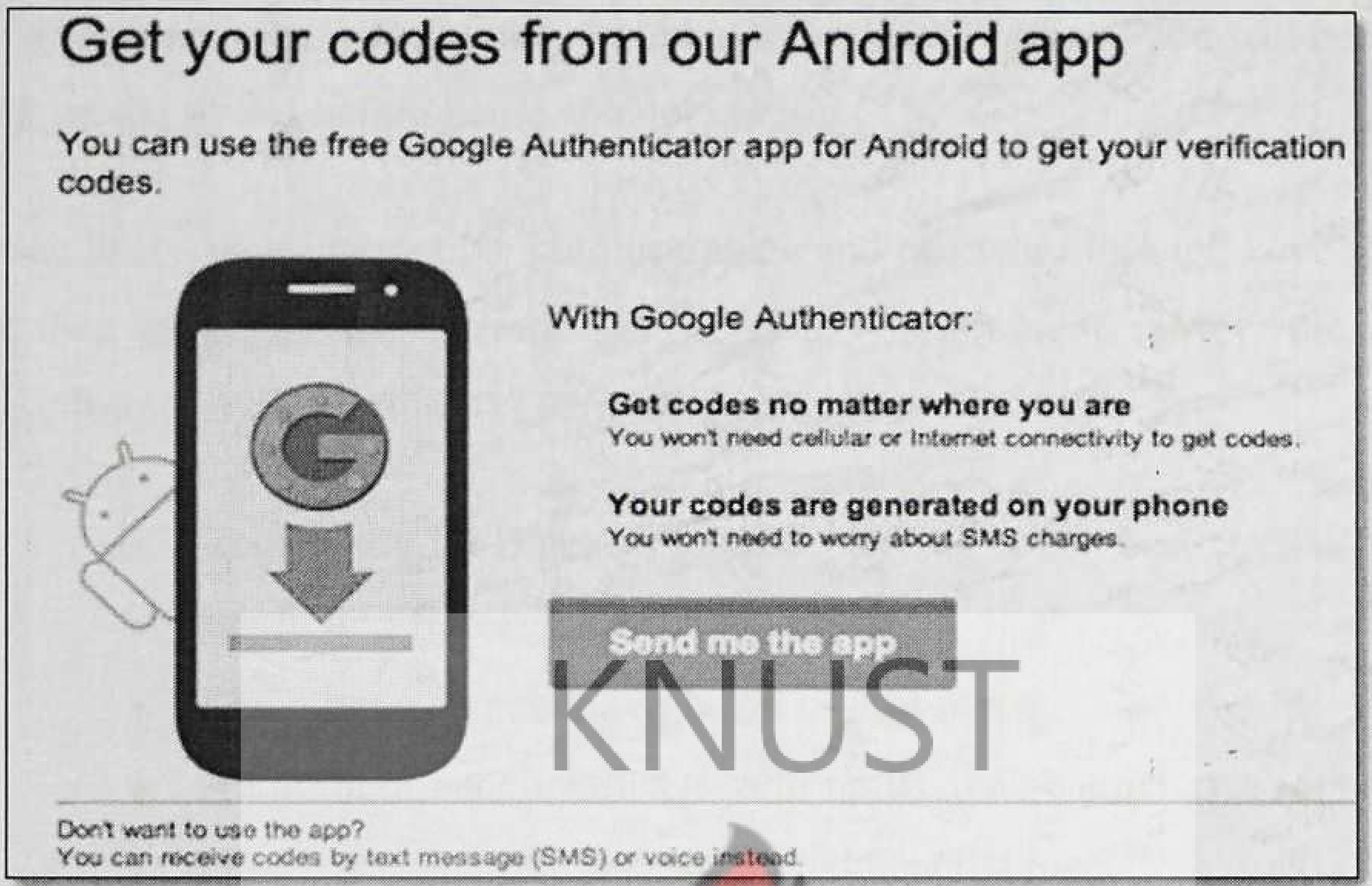
The result of Goggles' work is that even if your password is cracked, your account should still be safe. Chances are whoever is trying to break into your account from afar also does not have your phone in their possession, so they cannot get that secondary code sent to your phone by SMS. Admittedly, Alex acknowledged that Two-step authentication technology for secured access to data is good, but it is not flawless- ***What if your pre-integrated phone is stolen, for instance?*** Contingency Answers provided to this question are the need to define a backup phone number to receive your secret code in case you lose your phone/SIM card and there is that urgency to login.

The second approach is the use of a backup secret code that will be given during your first sign-in to the service. A user has to keep this back up secret code at the most confidential environment in your room or hidden place; only to be used once your primary phone and back up phones are indisposed. When you use the one time secret code to enter, you can then reset your account with new phone numbers and another "one-time secret code" sent to user.

To further the discussion on the flaws, attacker or possibly a person who leave with you in a room, can reset your account temporarily to divert the secret code generation from your phone to another phone. This temporal reset by unauthorized user is possible, if the person gets hold of your username, password and the special secret code kept in your "confidential" suitcase/room. They recommended that since SMS link are unavailable sometimes from the telecom service provider, it is critical to send both SMS and automatic voice call to announce the secret code to

How did Google solve SMS or cellular network failure to send code to user?

Users who only access their Google Account from Android devices without alternative usage of other computer terminals at some point in time can use a short walkthrough to set up the Google Authenticator application on their phones. With Google Authenticator, you can generate verification codes on your phone even if your phone is not connected to a cellular network. If the Google Authenticator is used instead of cellular link dependency, click "Send me the app" to install the app on your phone and follow the instructions on your screen to complete the setup process. The application software installed on your terminal would generate the internal secret code which is pre-configured on Google servers as authentic unused codes powered by Google. Once code is used, Google server flashes out the code from your device to avoid re-use.



Get your codes from our Android app

You can use the free Google Authenticator app for Android to get your verification codes.

With Google Authenticator:

Get codes no matter where you are
You won't need cellular or Internet connectivity to get codes.

Your codes are generated on your phone
You won't need to worry about SMS charges.

Don't want to use the app?
You can receive codes by text message (SMS) or voice instead.

Figure 8: Google authenticator software downloads to Andriod phones

As shown in figure 8, authenticator software advantage is that cellular or internet connectivity failure will not delay your request for data access codes. This speeds up your request for secret code, but the technical prove is that you still require internet availability and connectivity to open your Gmail and other accounts.

Whether a user opts to install the authenticator software or depends on cellular connectivity to receive the secret code never provides complete solution to expected robust access control on cloud environments such as Google and others because a hacker can use key-logger software to listen to the codes as buttons are pressed on the keyboard. Aside from that users have to keep one time secret code that can be stolen by a roommate.

2.4. Barclays Bank Two-step verification

Industry players operating one or two forms cloud-based architecture are adopting the two-step verification to ensure user trust on their platform. With Barclay's internet banking, customers can access their accounts with their username and password at the convenience of their home. Users' accounts are secured with additional "One Time Password" (OTP) and the use of virtual keyboard to prevent activities of key-loggers.

The one Time activation PIN called OTP; a new security feature that helps us to recognize that it is really you making the transactions. OTP is a unique code that will be sent to your mobile phone via SMS whenever you use certain features on Internet banking. You will be prompted to enter the OTP on the screen before being able to proceed.

When someone hacks your internet banking username and password through key logging or any other means, then the person may have to get access to your phone to retrieve the OTP sent by SMS. The activities that will require OTP authentication are:

- Registering for Barclays Internet banking
- Login into Barclays Internet banking
- Changing a forgotten password or user name
- Addition of beneficiaries to your registered beneficiaries address book
- On-off transactions to unregistered beneficiaries

For transmission security, the Barclays online Banking uses 128-bit digital certificate from VeriSign for encryption of the Secure Sockets Layer (SSL) session. SSL is the industry standard for encrypted communication and ensures that customers interaction with the Bank over the Internet is secure. While we appreciate security assurance at each layer on data communication path in cloud computing, the attention of this paper is on the user end protection as it is the most workstation highly vulnerable to hacking activities. The use of Encryption and Virtual LAN (VLANS) for multi-tenant server platform has reduced security risk at the server side. If there is any security adoption that would provide trusted-security and assurance to the cloud client, then it is provisions such as the 2-step authentication which the user plays a role to block access to unathorised entry.

Nothing has changed. Barclay's internet banking security using the OTP sent via SMS to user mobile device still carries the limitation in Fujitsu and Google two-step authentication. The underlining problem is a hacker holding someone's username and password in addition to the stolen mobile phone can execute unethical cybercrime before the telecom operator deactivates the SIM.

Practically, in countries where SIM registration is optional, the hacker can impersonate before the telecom operator at 16:45 GMT and pretend to be owner of a lost mobile phone/ SIM.

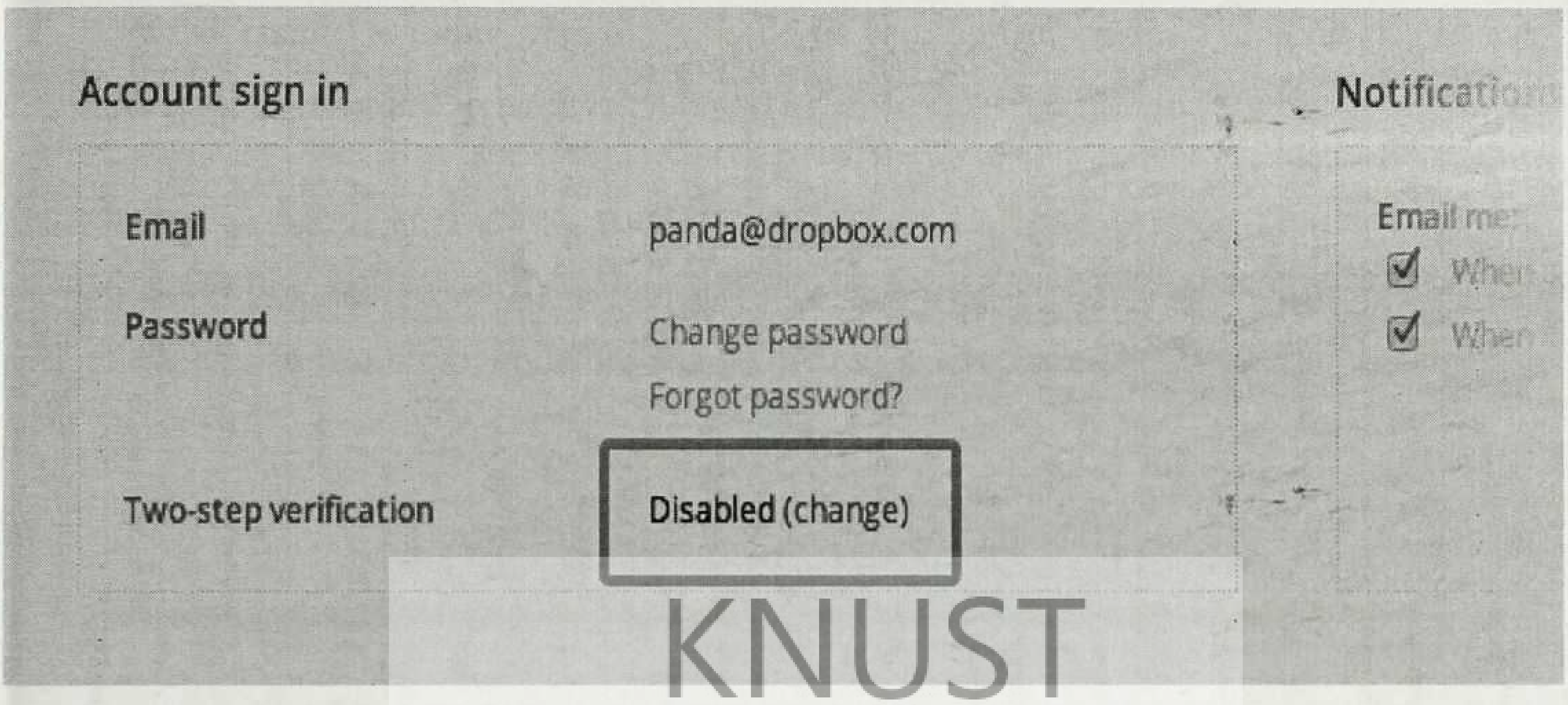
Hacker may request for deactivation of the original SIM; make a SIM change at those odd closing hours and get a new SIM to represent the assigned mobile device used to receive the OTP code. By the dawn of another day, one million dollars sitting in user account would have been transferred to several un-traceable user accounts to effect immediate transactions through ATM and E-marketing.

2.5 Dropbox Two-step authentication

Dropbox introduction of barcode scan opens the discussion for the proposed work in this paper. The barcode scan used by Dropbox did not solve the main problem: i.e. **"what if my mobile phone is lost to my hacker"? The answer is that whether barcode or OTP, a hacker with the stolen mobile phone may succeed to access data stored on Dropbox cloud-based architecture.** However, the mentioning of barcodes mounts the foundation on how to advance existing Two-step authentication methods using barcode systems.

In Dropbox method, a user may opt to receive barcode and scan to get access to data instead of receiving the secret code that can be trapped by key logger software. This is additional option but do not solve the problem question: Dropbox increased options that must be pre-configured to be used at each point of need and on emergency. Several options to access data from your domain are **Barcode scan**, OTP, Alternative phone, Emergency backup code.

Two-step verification is an optional but highly recommended security feature that adds an extra layer of protection to your Dropbox account. Once enabled, Dropbox will require a six-digit security code in addition to your password whenever you sign in to Dropbox or link a new computer, phone, or tablet as shown in figure 9.



Account sign in

Email panda@dropbox.com

Password Change password

Forgot password?

Two-step verification Disabled (change)

Notificatio

Email me

☑ When

☑ When

Figure 9: Dropbox two-step verification interface

For security reasons, you will be asked to re-enter your password to confirm your decision to enable two-step verification. Once you do, you will be given the choice to receive your security code by text message or to use a mobile app.

If you choose to receive your security codes by text message, you will need a phone capable of receiving text messages (carrier rates may apply). Whenever you successfully sign in to Dropbox using your password, a text message containing a security code will be sent to your phone.

The use of mobile authenticator application

Several mobile apps are available that will generate a unique time-sensitive security code you can use to finish signing in to your Dropbox account. Any app that supports the Time-based One-Time Password (TOTP) protocol should work, including the following:

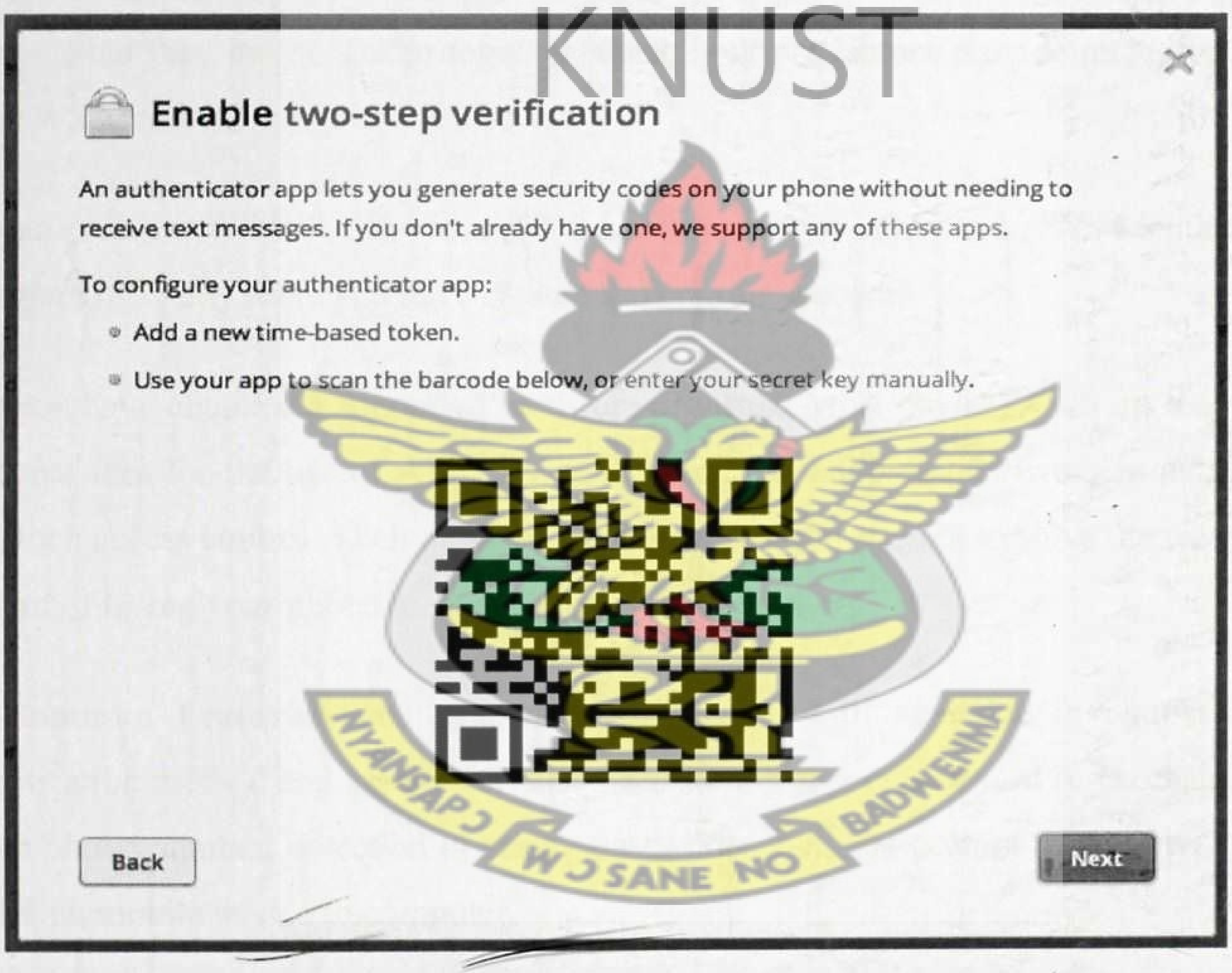
- Google Authenticator (Android/iPhone/BlackBerry)
- Amazon AWS MFA (Android)
- Authenticator (Windows Phone 7)

To use one of these apps:

1. Select **Use a mobile app** during the two-step verification setup.

2. You can choose to either scan the barcode (if your app supports it) or click **enter your secret key manually** to be given a secret key you can type into the app.

3. Once your app is configured, you will need to enter a security code generated by your authenticator app to verify setup and enable two-step verification. The application allow user to use secret code or scan a barcode to conclude authentication as shown in figure 10.



Enable two-step verification

An authenticator app lets you generate security codes on your phone without needing to receive text messages. If you don't already have one, we support any of these apps.

To configure your authenticator app:

- Add a new time-based token.
- Use your app to scan the barcode below, or enter your secret key manually.

Figure 10: Scan the barcode or enter a secret key manually

Storing your emergency backup code

Before enabling two-step verification, you will receive a special 16-digit backup code. It is very important that you write this key down and store it somewhere safe. If you ever lose your phone or cannot receive or generate a security code, you will need this backup code for emergency access to your Dropbox. Most apps will generate security codes even when cellular/data service is not available - useful when traveling or where coverage is unreliable.

2.6 Amazon Web service Multi-factor Authentication (AWS-MFA)

AWS Multi-Factor Authentication (AWS MFA) also provides an extra level of security that you can apply to your AWS environment. With AWS MFA enabled, when a user signs in to an AWS website, they will be prompted for their username and password (the first factor – what they know), as well as for an authentication code from their AWS MFA device/phone (the second factor – what they have). Taken together, these multiple factors provide increased security for your AWS account settings and resources.

You can enable AWS MFA for your AWS account and for individual AWS Identity and Access Management (IAM) users you have created under your account.

Once you have obtained a supported hardware or virtual MFA device, AWS does not charge any additional fees for the use of AWS MFA. Amazon has adopted this two-step authentication to strengthen access control. Their application is by no way an attempt to solve the existing possible problem of losing your phone to your closed relation hacker.

2.7. Common Features: The following features are still available in almost all two-step authentication method and application discussed in this paper: Password reset, change password, change phone number, detection of strong passwords, frequent prompt to change password, link and unlink mobile device to computer.

2.8. Summary of Discussion

It has been observed that Two-step authentication is a unique method of improving domain access control for cloud-based application to give confidence to users on cloud adoption. If the issuance of secret code or OTP through mobile device is powerful to some extent, then the use of biometric scanning on the mobile device to complete the second factor authentication would be a great potential to hype interest for small medium enterprises to adopt cloud computing.

Again, it was noted that a hacker who steals the configured mobile phone in addition to username and password could fully access every data because of the use of OTP codes. We can resolve this problem with the use of biometric productions. A typical of it would be biometric authentication (Thumbprint scan) or the Iris scan (scan of the eye). Therefore, for small and medium enterprises to hook unto cloud business solutions, each corporate user requires specialised biometric compatible mobile phones that can be used to scan the thumbprint or the eye as in the iris scan technology. A hacker holding username, password and stolen mobile phone cannot access data as the life body of the authorized user may still be required to complete the second factor authentication.

It was also observed that Google, Dropbox and Amazon allow user self-services to decide what option and when to change options. There could be nothing wrong with self-service; however, in the situation for small medium enterprise, an in-house data-manager must have the administrative control to grant user choice for enterprises to track user behaviour. An in-house data administrative controller has to be an intermediary to manage authorised user activities such as; password reset, change of phone ~~number~~/SIM, link and unlink mobile device to corporate computer that communicates with the cloud-provider server.

In conclusion, we believe that the experience obtained from observing the trailing of existing software packages and discussions with others have enhanced the development of our ideas to implement two-step authentication software.

CHAPTER 3

ANALYSIS AND DESIGN OF SYSTEM

3.0. Introduction

The System Development Life Cycle (SDLC) approach was used for the software development process. According to Thomas Vian (2002), designing an interactive website; the writer eluded the fact that using most SDLC models in programming projects offer best option due to easy way of iterating a process to check errors and achieve high performing software production.

3.1. The system Development Life cycle (SDLC)

We introduced the SDLC –Revolutionary waterfall model in figure: 1.0.1, as our research method for the software development process. The same SDLC is presented in figure 1.0.2, to explain how to walk through each stage within the cycle to complete the software development.

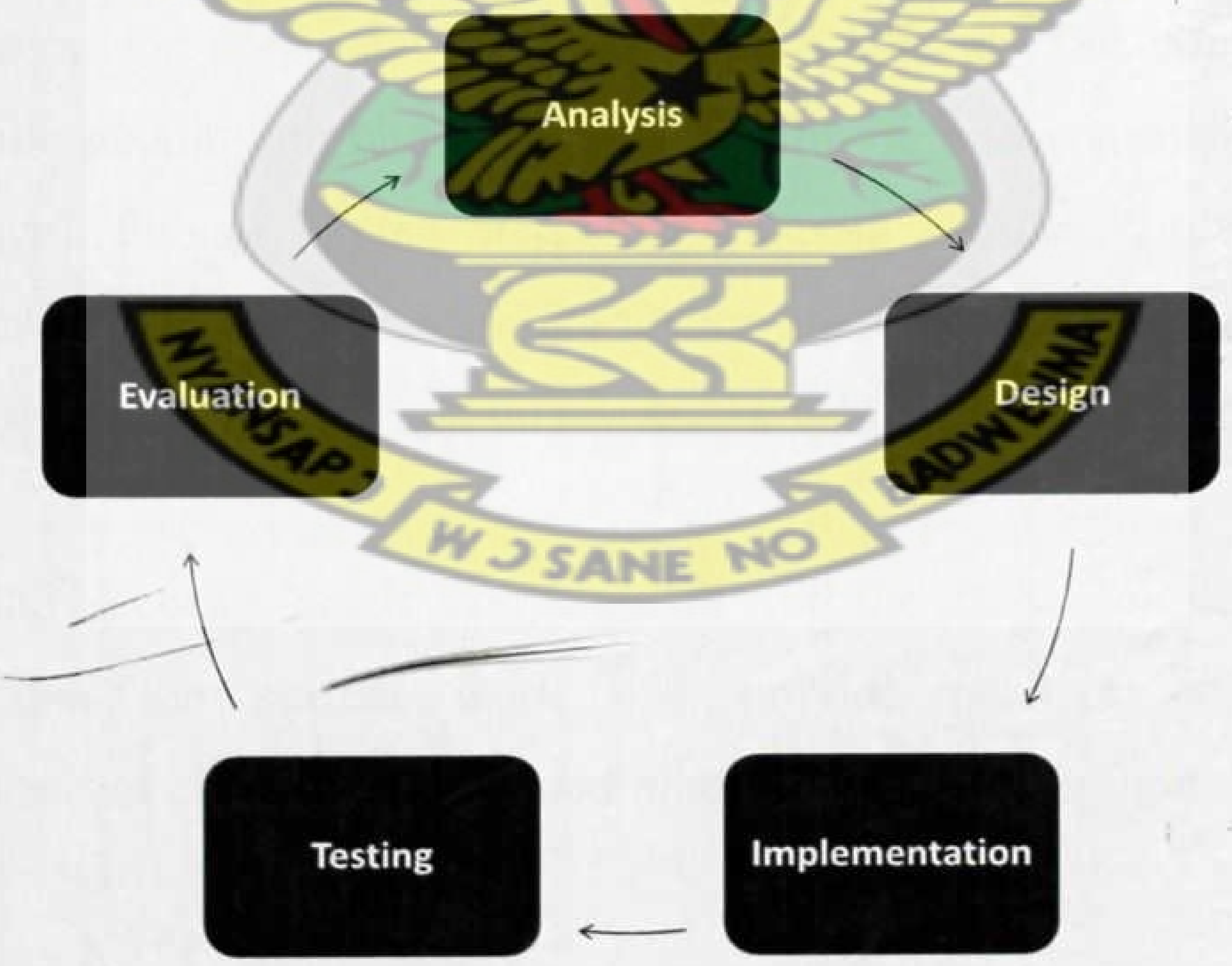


Figure: 1.0.2 System Development Life Cycle-Revolutionary waterfall model

3.2. Analysis of Design

We did analysis of the problem and a small study to measure the worth of investigation. We found worth investigating; especially knowing for the fact that cloud giants such as Google, Amazon, Dropbox, Barclays and Fujitsu companies have all turned to improve user-domain access security with the 2-step authentication method through mobile phone. The feasibility was on three points: Technical, Social and Economic.

3.1.1 Technical Feasibility: we saw the viability to resolve gaps in the existing 2-step authentications and flexibility to implement and use the software. Latency in processing biometric data was considered acceptable

3.1.2 Social feasibility: we successfully ruled out any effect on people involved from data collection to the implementation and testing stages. DNA data was ruled out to protect ethical standard. With DNA scanning, the data collected can be use to check diseases and medical status of a particular user.

3.1.3 Economic feasibility: This area predicted high cost for such customized implementation and distribution for corporates adopting cloud platform. The implementation required special mobile phone with biometric compatibility to either scan fingerprint or perform Iris scan (eye). Phones having biometric scanning features cost about $ 199.00. and Laptops with similar bometric scanning feature cost around $ 499.00 in current market. The other cost is the software and this would be estimated based on proprietory.

However, the security needs compensated for the initial implementation cost. We concluded that the current work will provide positive improvement on data confidentiality and integrity in the cloud platform as shown in figure 11.

3.3. Design of system

Figure 11: The use of biometric for authentication

As a scenario to describe the design concept in this paper, we used the conjunction door-key engine system shown in fig. 11 for clarity of the innovation. Banks make use of this two-in-one key system to lock moneybox or the "strong room".

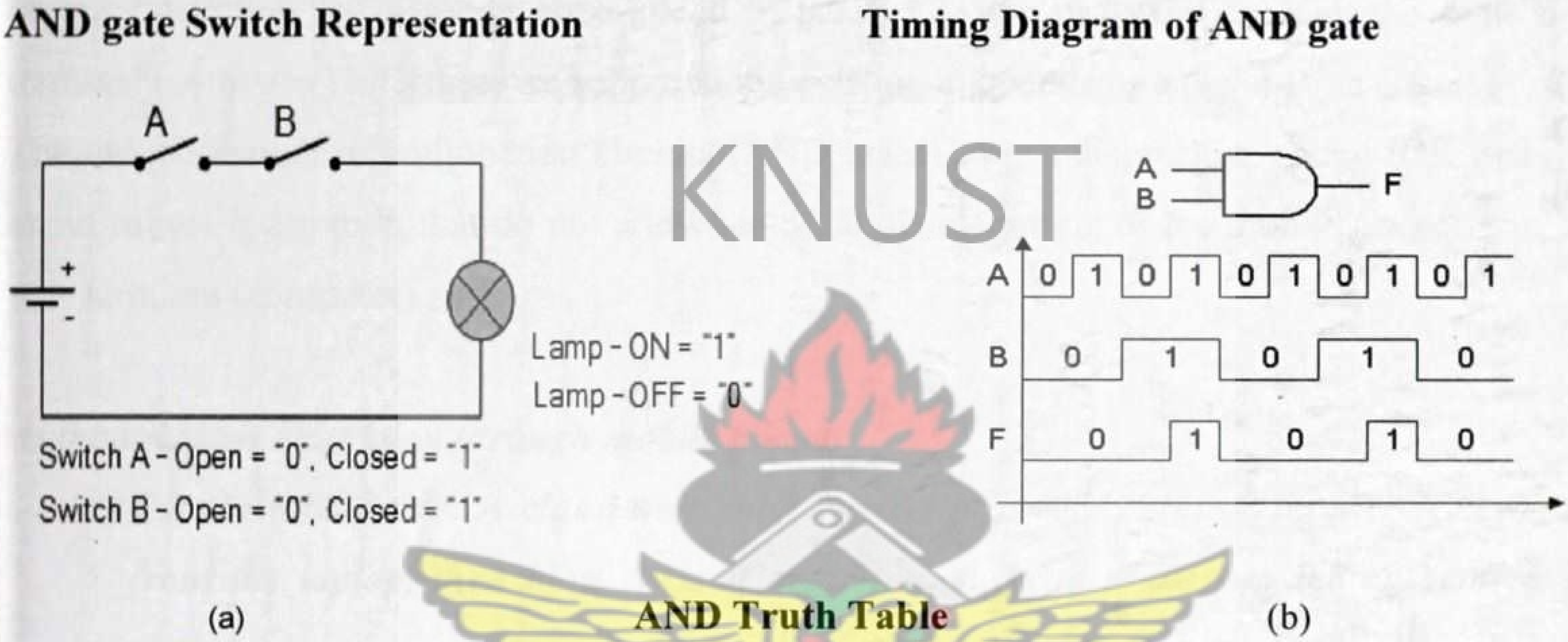
The Finance manager has one side of the key solely in custody, while the branch Manager also holds one side of the key entirely. The moneybox can only be opened if the two authorized key holders come into agreement and provide their unique keys to open their side of the savings box. If the branch manager opens his side at any point in time, without the finance manager doing it at his side, the branch manager cannot access the savings box.

3.4. Application of AND logic functions

Mathematically we represented the two-in-one key system using Boolean algebraic expressions. Boolean algebra has been fundamental in the development of computer science and is yet the basis of the abstract description of digital circuits. It is also used in digital logic, computer programming, set theory, and statistics. Claude Shannon observed that one could also apply the rules of Boole's algebra in this setting, and he introduced **switching algebra** as a way to analyze and design circuits by algebraic means in terms of logic gates. Shannon already had at his disposal the abstract mathematical apparatus, thus he cast his switching algebra as the two-element Boolean algebra.

We adopted the AND gate Boolean operation (A.B=AB*)* for our design. What happens with AND gate is that the two keys work in the conjunction operation method.

Comparative to our design, the truth table expresses similar security protocols that must be fulfilled before authorised user can access data. This is demonstrated in the truth table shown in figure 12.



AND gate Switch Representation

Timing Diagram of AND gate

AND Truth Table

2 Input AND gate		
A	B	A.B
0	0	0
0	1	0
1	0	0
1	1	1

(c)

Figure 12: AND gate truth table

The simplest form to understand the truth table is the use of the switch diagram in figure.12a and its corresponding timing diagram generated by digital oscilloscope as shown in figure 12b. The two switches connected in series or conjunction mode to ensure that lamp lights "ON" only if switch A **AND** B are closed. From the truth table, only the last condition would permit authorized user to access data in the cloud domain.

Unlike our design, the existing 2-step authentication designs used by Google, Barclays and others did not show direct relation with any of the seven logic gates Truth Tables (AND, OR, NOT, NAND, NOR, EXOR, EXNOR).

The only conclusion is that the existing design operates under disjunction mode, because one has to enter correct password (A) to trigger the generation of "Additional" ***(+ operation)*** secret code (B) to serve as second input before getting output result that will allow user to access data. Based on the "Addition" of a secret code added in parallel to the password through the same user terminal (computer) interface, we supposed the existing to operate as a disjunction circuit (+).

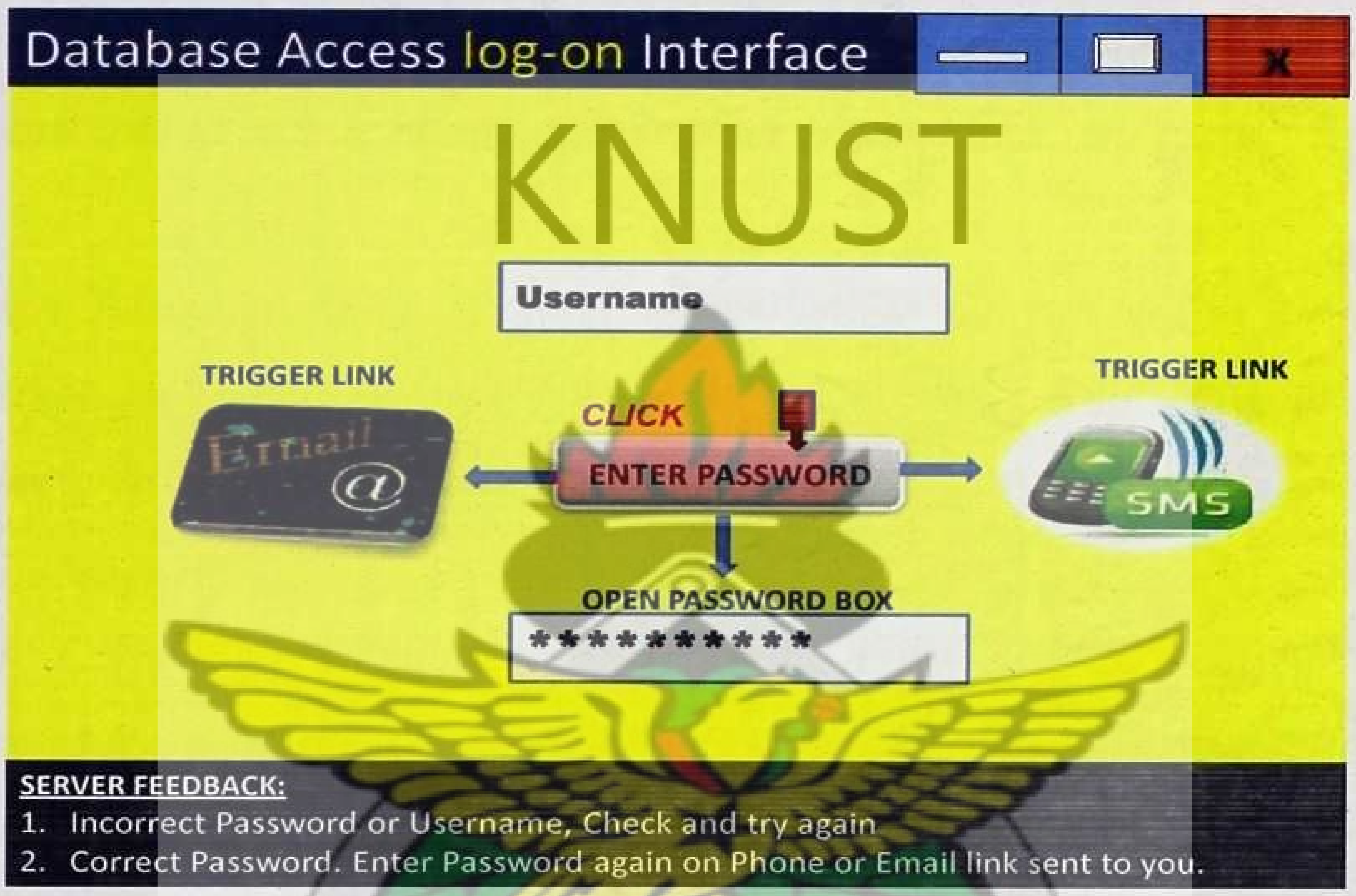
The unique feature of conjunction circuits (AND gates) over a disjunction circuit (OR gates) is about robust integration that do not allow temporal disintegration of the mobile phone from the user terminal (computer).

Authentication Execution through mobile phone:

- ***User terminal side: A cloud user enter correct password through on-screen keyboard from the laptop, then by a click of enter button, send request to the authentication server.***
- **Cloud authentication server:** ***The cloud authentication server receives correct username and password to direct authentication request to the interlocking phone.***
- ***Wrong user Password Entry:*** *If cloud authentication server receives a wrong password with correct username, it will trigger a voice phone call alert to the authorise "username". User account blocks after third wrong password insert.*
- ***Biometric compatible phone: By receiving the SMS text on assigned user phone, the user opens the embedded link ~~to scan~~ the fingerprint or perform the Irish scan (eye). After successful biometric scan, the user then sends the scanned print by clicking on the ~~enter~~ button on the phone.***
- ***Cloud authentication Server: The security authentication server receives a feedback message from the mobile phone to compare the fingerprint barcode received from the mobile phone with the pre-defined barcode stored on the security server to complete authentication for the authorised user to now access data.***

3.5. The backdoor Access method

Imagine you lose your biometric compatible phone in a car; ***what alternative can ensure business continuity in the cloud by such victimised user***? Backdoor entry is important in any access design and programming. Figure 13, shows the routing of backdoor link to E-mail account.



SERVER FEEDBACK:
1. Incorrect Password or Username, Check and try again
2. Correct Password. Enter Password again on Phone or Email link sent to you.

Figure 13: Backdoor Authentication routing on user E-mail account

Before we explain the solution provided for this question, it is important to reiterate the application of this security design. ***The application is for SME's moving into cloud computing business solutions to help improve data trust on the multi-tenant platform***. SME are failing to adopt cloud computing due to security threat on corporate data. Our focus is to design a customised security-wall that assures data confidentiality, Integrity and a return of proportional system administration functions back to the enterprise users to administer individual access control. This we proposed, would give SME's a substantial confidence in the cloud-based solutions, reduce the fear of data hacking and challenge of working with an unknown cloud system administrators managing the multi-tenant platform.

Aligning our thoughts and application of the design within the corporate environment, we created a backdoor entry through user terminal (computer) that is biometric compatible.

Authentication Execution through backdoor E-mail Account

- ***User terminal side: A cloud user enter correct password through on-screen keyboard on computer, then by a click of enter button, sends request to the authentication server.***

- ***Cloud authentication server: The cloud authentication server receives and directs the request to the backdoor E-mail account through a link.** (NB) **One authentication request link sent to mobile phone and another request link sent to user E-mail account.***

- *Wrong user Password Entry: If cloud authentication server receives a wrong password with correct username, it will trigger a voice phone call alert to the authorise "username". User account blocks after third wrong password insert.*

- ***Biometric Compatible Computer: By receiving the backdoor authentication link the computer user opens the E-mailed link to scan the fingerprint or perform the Irish scan (eye). After successful biometric scan, the user then sends the scanned fingerprint by clicking on the enter button on the on screen or keyboard.***

- ***Cloud authentication Server: The security authentication server receives a feedback message from the user Email account to compare the fingerprint barcode received from the authorised E-mail with the pre-defined barcode stored on the security server to complete authentication for the authorised user to now access data.***

3.6. Summary

Prototyping the design has been the major choice. The advantage is to give chance to both the designers and potential users suggest improvement to the project completion.

It was important to determine the testing standard suitable for this design to pre-inform the implementation stage of this cycle. There are three basic testing methods: Top-down, Bottom-up and Ends-in and we selected the Top-down approach.

Top-down is a method in which a programmer joins the overall skeletal structure of the program before performing test. Next, the programmer would 'load in' the reviewed codes in some sections and then test it again and so on until the final program is completed and tested. The advantage of this method is that the programmer is always looking at the whole problem in one go, as all the parts of the program are related to each stage of execution.

CHAPTER 4
SYSTEM IMPLEMENTATION

4.0. Introduction

Implementation has to do with how the final solution will fit into the existing system using known and available tools for construction. In the context of login architecture re-design, we used the Java API platforms. Creating password dialogue box was made by a combination of the JOptionPane class and the JPasswordField class to allow step-1 key (username and password) to be entered. The Java card supported the biometric implementation to allow step-2 authentication key to be used. In the final arrangement, we interlocked or serialized the two Java application programs with a string command; to ensure that output of password dialogue box becomes input to triggers biometric platform. After biometric authentication key, the output that will be produced depends on the function AND logic gate (A.B=F) as shown in figure 14.

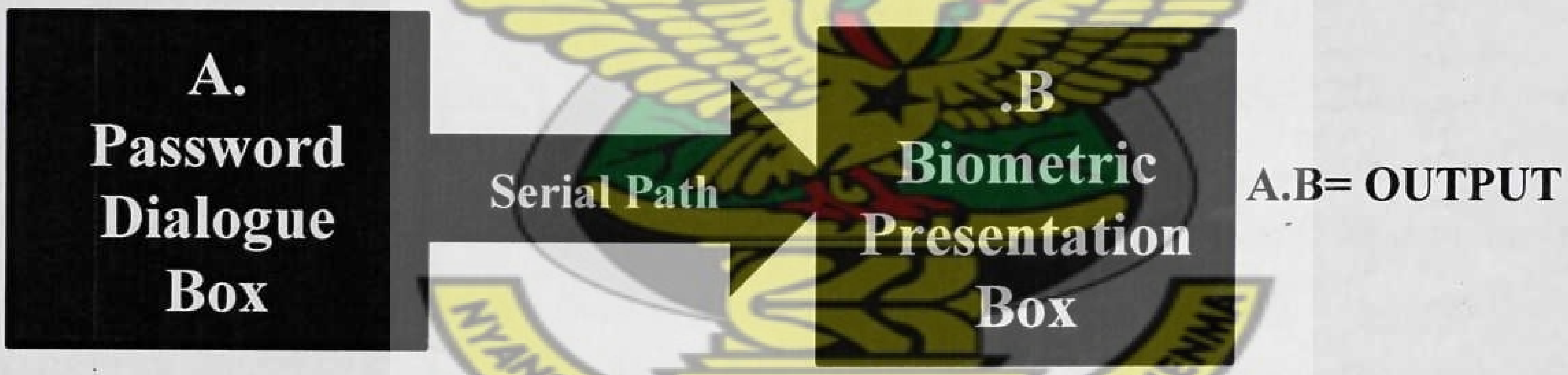
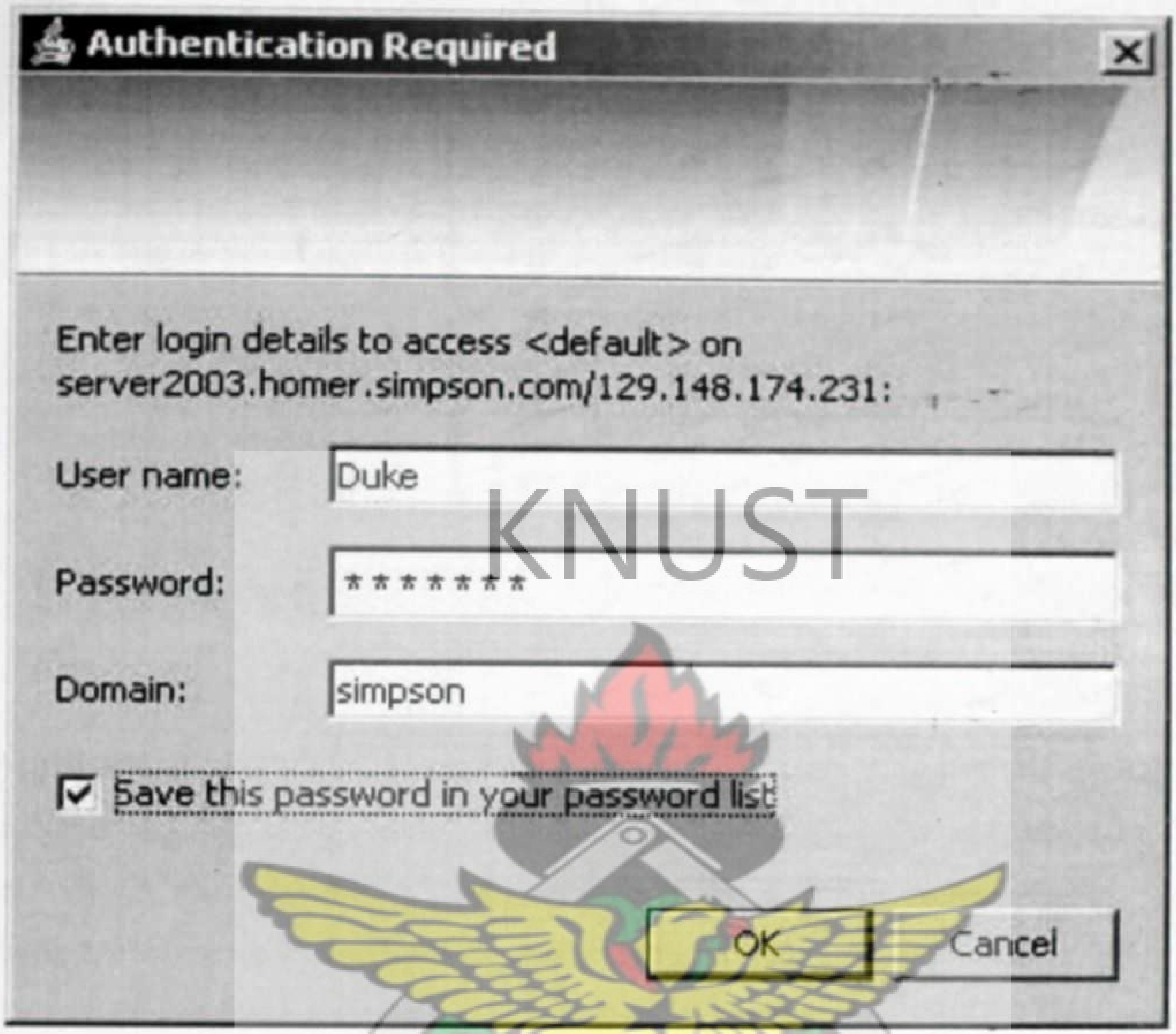


Figure 14: The serialised login dialogue boxes

4.1 Password dialogue box development

Java ~~code~~ supports how to make a password dialog box. This program uses a combination of the JOptionPane class and the JPasswordField class. When this program is run a JOptionPane is shown containing a JPasswordField, a JTextField, an OK and Cancel button. Sample of the password dialogue box is shown in figure 15.



Enter login details to access <default> on server2003.homer.simpson.com/129.148.174.231:

User name: Duke

Password: *******

Domain: simpson

☑ Save this password in your password list

Figure 15: sample password dialogue box

The JFrame behind the JOptionPane uses a text area to provide feedback about the input the user has made and what buttons have been pressed. For this Java program to work it is saved in a file called PasswordDialog.java. Appendix A2 provides the flow of all the psuodocodes for excution.

Sample Psuodo-code for creating password dialogue box:

Load internet browser with service provider address; https://www.mtncloudservices.com

```
START
        Initialize and add the screen objects in the password dialogue box
        Initialize soft-keypad on screen under password dialogue box
        Type on screen keypad the assigned cloud Username and Password
        Press enter on screen keypad to send access request to authentication server
```

```
When enter key is pressed authentication server should respond
    If username and Password are correct as in the server
        Say please authentication required to login
        Server should send embedded login page link in SMS to user mobile phone
        Server should send same embedded access page link to user E-mail account
        Trigger voice alert call to credential holder after 5min delay to authenticate
    If username correct and Password wrong in the server database
        Say Please check password and try again
        Trigger automated security alert voice phone call to authorized username holder
    If username wrong and Password correct
        Assume ideal state and do nothing to respond the request
    If username and password are wrong compared to stored credentials
        Assume ideal state
END
```

4.2. Application of "AND" logic function

The password (A) "AND" biometric (B) input interfaces have been interlocked to provide feedback message when any of the four attempts shown in the table is performed by the user. We arrived at the four login attempts that require action response from the authentication server using the mathematical index formula, $2^n-2^2=4$ to create the switching AND logic truth table as shown in Table: 3. Login (output) is successful only if input switch A and B are all in state "1". This is the only login attempt for user to get access to data. The feedback response that should be generated by the authentication server is listed in the ACTION column as in the table.

Table 3: Application of "AND" logic function

A (Password)	B (Biometric scan)	F (login success report)	ACTION
0	0	0	Ideal state
0	1	0	Do nothing
1	0	0	*Send SMS, E-mail links *Trigger voice alert call in 3-min authentication delay
1	1	1	Open domain for user

The psuodocode shows conditions to activate the interlocking string

```
START
    Initialise the serial string to interlock password and biometric input dialogue boxes
    Make serial string a uni-direction path from key-1 box to trigger key-2 box

        If username and password are correct activate string to transfer authentication link
        If username and password are not correct don't activate serial path
END
```

4.3. Biometric dialogue box development

Biometric authentication programming starts from input where bio-scan is captured, and walks through transmision medium, signal processing, storage and decision to produce an output.

4.3.1 Biobuilder class for Template creation. (Application Programming Interface)

NIST/Biometric Consortium (2002) discussed in conference, about the improvement required with the use of Biobuilder. The proposed that with the new OwnerBioTemplate, once an object is created, enrollment may commence. The following biometric types are defined in the initial version of the bioBuilder: facial feature, voice print, fingerprint, iris scan, retina scan, hand geometry, written signature, keystroke dynamics, lip movement, thermal face image, thermal hand image, gait style, body odor, DNA scan, ear geometry, finger geometry, palm geometry, vein pattern. BuildBioTemplate method will reject requests for biometric types that are not supported on a card.

The use of Java Card has benefited from interoperability both at the binary and the Application Programming Interface (API) level. Biometric technologies can build on this foundation by way of a high level API. As Java Cards grow into today's smallest standardized computing platform, developers wish to ensure the interoperability of many biometric technologies with Java Cards, and to allow multiple, independent applications on a card to access the biometric functionalities requried for specific development.

Java Cards increases both computing power and storage capacity; with these developments comes the potential to include ever-more advanced biometric technologies on a Java Card. Particular among these developments is the ability to support multiple biometrics on a single card, for instance allowing a card to choose between recognition of a eye or a fingerprint.

4.3.2 Biometric Identification Process

Research on biometric has increased in recent times. However, no single bodily or behavioral scan is able to satisfy acceptability, speed and reliability of authentication. In real application the recent trend is therefore towards multi-node system. Simply put, we want biometric system that can sense, store as well as process data collection from at least two different bio-sources such as the fingerprint and eye. More research investment are made currently to advance the multi-nodal. With the objective of cloud serving day-to-day urgent business application, multi-nodal biometric data collection is a good news to improve trusted-security for cloud computing. The process to complete biometric authentication is shown as in figure 16.

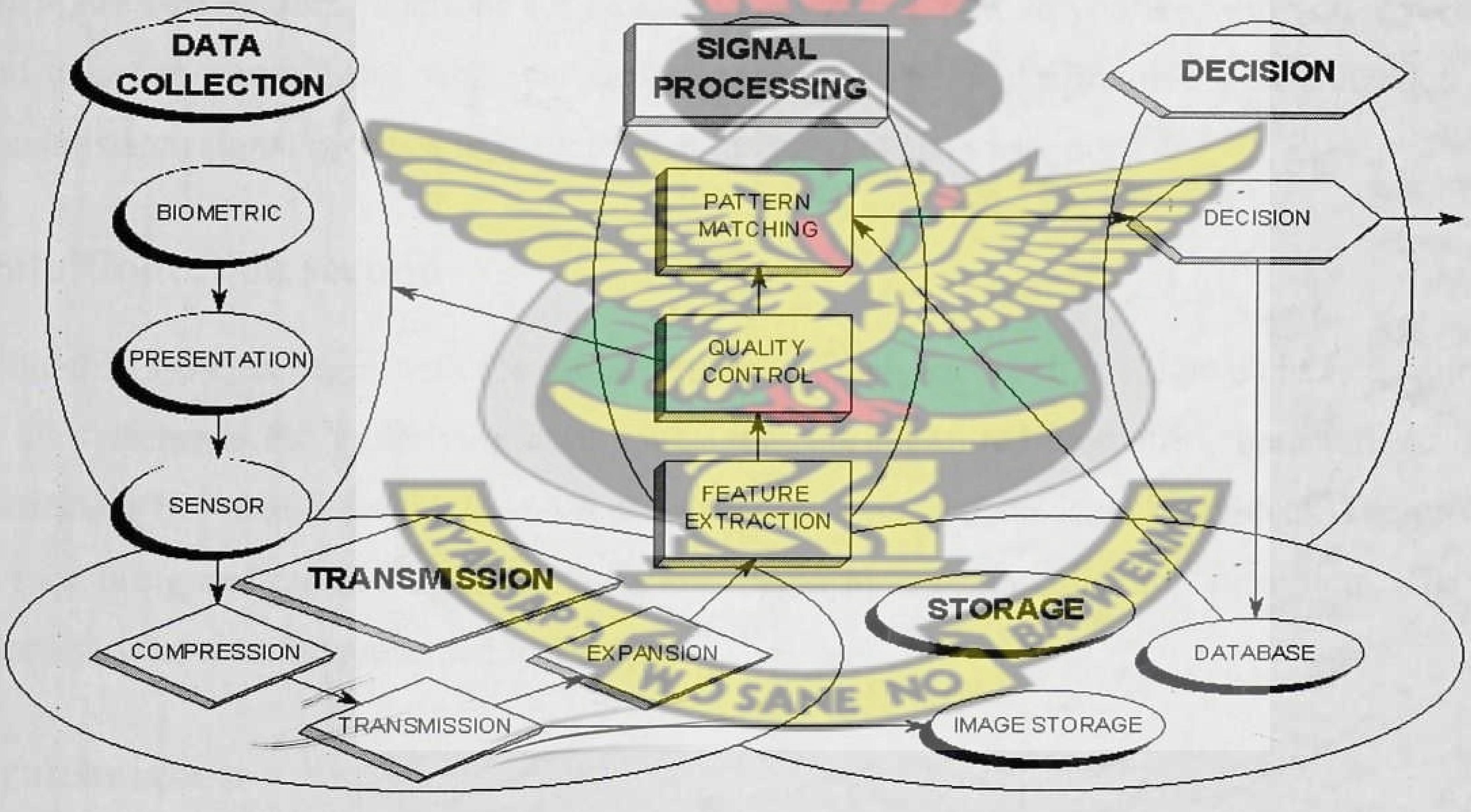


Figure:16 Biometric identification Process

Brad Wing (2011), depicted figure 16 in a paper, "overview of all INS Biometric projects" to explain the function of each stage in the authentication process. As shown in the diagram, the biometric coding is divided into three: client side, server side and proxy side scripting. Each side requires specific algorithms to run successfully.

The two basic operations performed by a general biometric system are the capture and storage of enrollment (reference) biometric samples and the capture of new biometric samples and their comparison with corresponding reference samples (matching). This figure depicts the operation of a generic biometric system although some systems will differ in their particulars.

The primary components for the purposes of this discussion are "capture," where the sensor collects biometric data from the subject to be recognized; the "reference database," where previously enrolled subjects' biometric data are held; the "matcher," which compares presented data to reference data in order to make a recognition decision; and "action," where the system recognition decision is revealed and actions are undertaken based on that decision.

4.4.1. Identification stages

There are two distinct functions for biometric devices: To prove you are who you say you are; and to prove you are not who you say you are not. The stages involve data collection point, transmission, signal processing, pattern matching and decision support.

Data Collection section

Biometric systems begin with the measurement of a behavioral/physiological characteristic. Key to all systems is the underlying assumption that the measured biometric characteristic is both distinctive between individuals and repeatable over time for the same individual. The problems in measuring and controlling these variations begin in the data collection subsystem. The user's characteristic must be presented to a sensor.

Transmission

Some, ~~but not~~ all, biometric systems collect data at one location but store and/or process it at another. Such systems require data transmission. If a great amount of data is involved, compression may be required before transmission or storage to conserve bandwidth and storage space. The process of compression and expansion generally causes quality loss in the restored signal, with loss increasing with increasing compression ratio. The compression technique used will depend upon the biometric signal.

Signal Processing

Having acquired and possibly transmitted a biometric characteristic, we must prepare it for matching with other like measures. Figure 1 divides the signal processing subsystem into three tasks: feature extraction, quality control, and pattern matching.

If the feature lacks good quality or are insufficient in some way, we can conclude quickly that the received signal was defective and request a new sample from the data collection subsystem while the user is still at the sensor. The development of this "quality control" process has greatly improved the performance of biometric systems in the last few short years. The feature is finally sent to the matching pattern.

Pattern matching

The purpose of the pattern matching process is to compare a presented feature sample to a stored template, and to send to the decision subsystem a quantitative measure of the comparison

The term "enrollment" refers to the placing of that feature "sample" into the database for the very first time. Once in the database and associated with an identity by external information (provided by the enrollee or others), the feature sample is referred to as the "template" for the individual to which it refers. In all other cases, the pattern matching process compares the present sample to multiple templates from the database one-at-a-time, as instructed by the decision subsystem, sending on a quantitative "distance" measure for each comparison.

Decision

The decision subsystem implements system policy by directing the database search, determine "matches" or "non-matches" based on the distance measures received from the pattern matcher, and ultimately make an "accept/reject" decision based on the system policy. Storage

The remaining subsystem to be considered is that of storage. There will be one or more forms of storage used, depending upon the biometric system. Feature templates will be stored in a database for comparison by the pattern matcher to incoming feature samples.

4.3.3 Testing Biometric Projects at lab

Testing of biometric devices requires repeat visits with multiple human subjects. Further, the generally low error rates mean that many human subjects are required for statistical confidence. Consequently, biometric testing is extremely expensive, generally affordable only by government agencies.

Few biometric technologies have undergone rigorous, developer/vendor-independent testing to establish robustness, distinctiveness, accessibility, acceptability and availability in "real-world" (non-laboratory) applications. Over the last four years, the U.S. National Biometric Test Center has been focusing on developing lower cost testing alternatives, including testing methods using operational data and methods of generalizing results from a single test for performance prediction over a variety of application-specific decision policies.

The goal of the scientific community is to provide tools and test results to aid current and prospective users in selecting and employing biometric technologies in a secure, user-friendly, and cost-effective manner.

Finally, the science of Biometric is still infantile and it promises a secured environment for many information technology applications.

4.4 Psuodocode for implementation

4.4.1 ProPassword interface

Load internet browser with service provider address; https://www.mtncloudservices.com

```
START
        Initialize and add the screen objects in the password dialogue box
        Initialize soft-keypad on screen under password dialogue box
        Type on screen keypad the assigned cloud Username and Password
        Press enter on screen keypad to send access request to authentication server

      When enter key is pressed authentication server should respond
          If username and Password are correct as in the server
               Say please authentication required to login
               Server should send embedded login page link in SMS to user mobile phone
               Server should send same embedded access page link to user E-mail account
               Trigger voice alert call to credential holder after 5min delay to authenticate
        If username correct and Password wrong in the server database
            Say Please check password and try again
            Trigger automated security alert voice phone call to authorized username holder
        If username wrong and Password correct
            Assume ideal state and do nothing to respond the request
        If username and password are wrong compared to stored credentials
            Assume ideal state
END
```

4.4.2. ProgInterlock Password AND Biometric interfaces

```
START
      Initialise the serial string to interlock password and biometric dialogue boxes
      Make serial string a uni-direction path from key-1 box to trigger key-2 box
          If username and password are correct activate string to transfer authentication link
          If username and password are not correct don't activate serial path
END
```

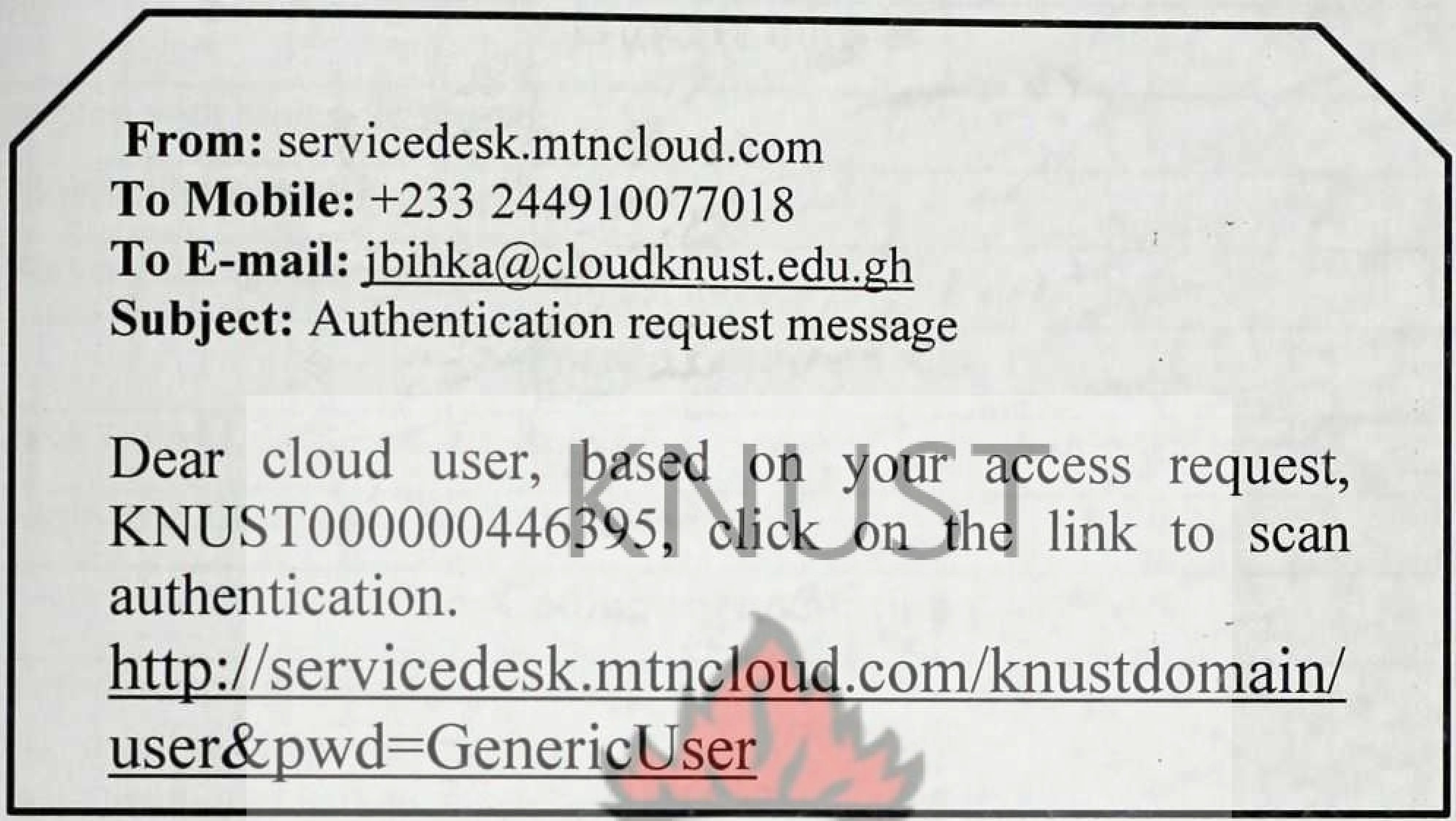
4.4.3 ProgMobilePhone authentication link

```
START
      Initialises to add mobile phone screen objects
       When mobile phone receives authentication request from server
            Save text message in the SMS inbox
            See embedded login interface after opening the link inside SMS
         If link open to show login interface then scan fingerprint
         If scan complete
             Send to authentication server by pressing OK button
             Say, waiting, whiles the server compares biometric enrollment to stored image
             Say, scan successful, after comparison completed
         Else
            Say scan unsuccessful if enrollment scan contradicts  stored image
            Say scan unsucceeful if comparison interfered by another signal
END
```

4.4.4 ProgE-mail authentication

```
START
        Initialises to add E-mail account objects on computer screen
        When backdoor E-mail account receives authentication request from server
                Save E-mail message inside the E-mail inbox
                See embedded login interface after opening the link inside the message received
            If link open to show login interface then scan fingerprint on laptop
            If scan complete
                 Send to authentication server by pressing OK button
                  Say, waiting, whiles the server compares biometric enrollment to stored image
                 Say, scan successful, after comparison completed
            Else
                Say scan unsuccessful if enrollment scan contradicts  stored image
                Say scan unsucceeful if comparison interfered by another signal
END
```

4.4.5 ProgAutomated intrusion alert voice call

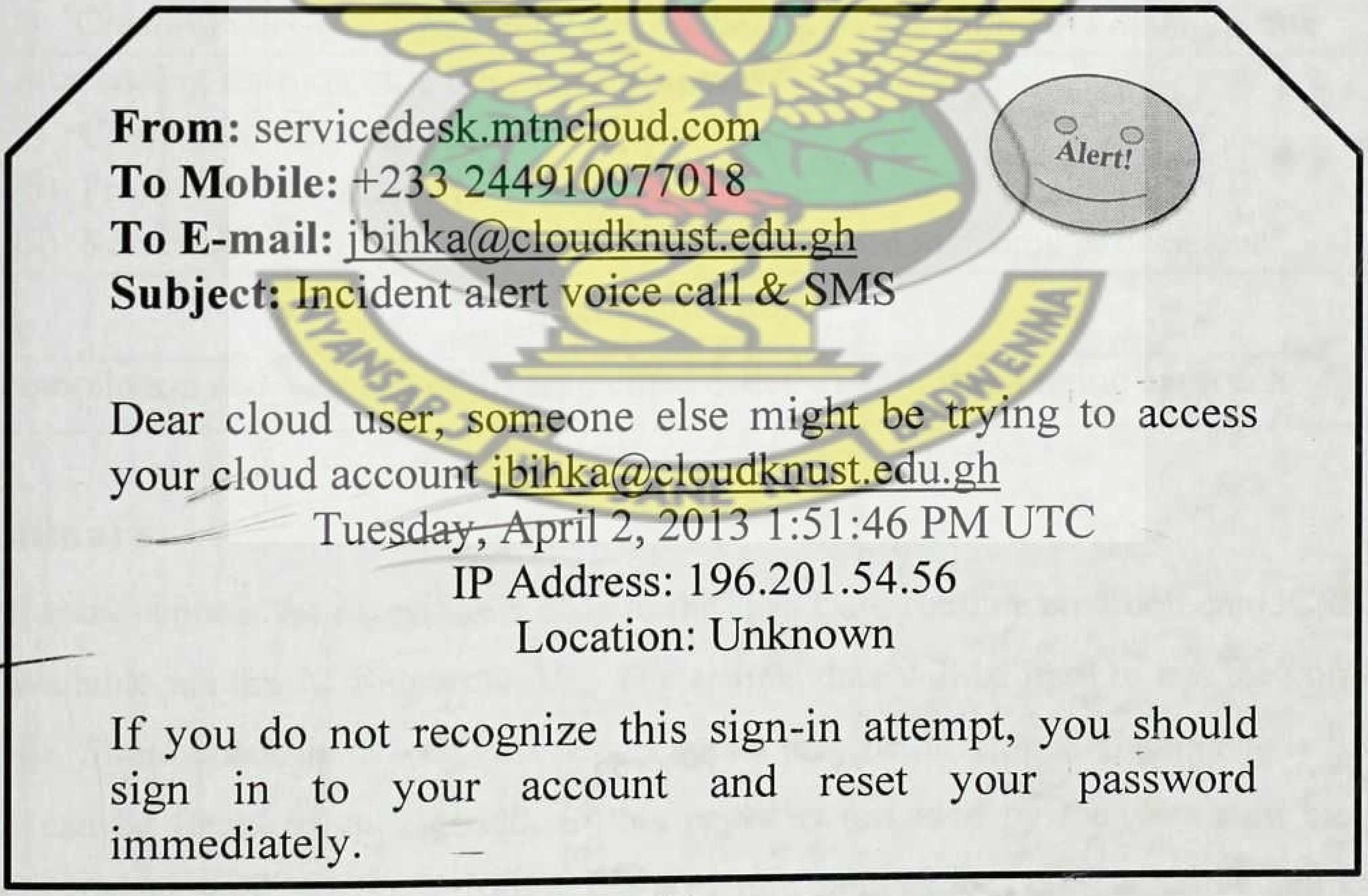


From: servicedesk.mtncloud.com
To Mobile: +233 244910077018
To E-mail: jbihka@cloudknust.edu.gh
Subject: Authentication request message

Dear cloud user, based on your access request, KNUST000000446395, click on the link to scan authentication.
http://servicedesk.mtncloud.com/knustdomain/user&pwd=GenericUser

(a)

4.4.6 ProgAutomated server authorisation Message - Voice call &SMS



From: servicedesk.mtncloud.com
To Mobile: +233 244910077018
To E-mail: jbihka@cloudknust.edu.gh
Subject: Incident alert voice call & SMS

Dear cloud user, someone else might be trying to access your cloud account jbihka@cloudknust.edu.gh

Tuesday, April 2, 2013 1:51:46 PM UTC
IP Address: 196.201.54.56
Location: Unknown

If you do not recognize this sign-in attempt, you should sign in to your account and reset your password immediately.

(b)

Figure 17 a & b: Automated SMS correspondence to user actions

4.5. Requirement for Laboratory implementation

Table 4: Requirements at implementation laboratory

Hardware devices
1.. Laptop with biometric sensor
2.. Mobile phone with biometric sensor
3.. Server-Internet connectivity set-up
Software requirements
4.. Java 7.0 API, JavaCard -BioBuilder
5.. Biometric Testing lab-platform & Simulator
Coding segmentation
6.. Top-down programming and testing a) creating password interface b) Creating of mobile phone link c) Creating E-mail link d) Creating authorised message e) Creating intrusion alert through voice call &SMS f) Creating interlock serial path between password and biometric dialogue box
7.. Java coding for biometric device implementation i) Client side scripting –data collection ii) Proxy side scripting-Bio-Transmission iii) Server side scripting- for template storage, pattern matching & decisions
Compilation
8.. compilation and Test run of all segmented codes –Top-down Testing approach

4.5. Summary

The developers connect the algorithm's code to the Java Card runtime environment (JCRE), and make it available via the JC Biometric API. The sample data will be used to test the port of the native code. Simultaneously, a biometric server applet may be developed. Sample code for such an applet can be found in an appendix to this paper as provided by the Java card biometric consortium (Document#: 02-0019, 2002). The API stub sources for compilation and export file for conversion can be found in: http://www.javacardforum.org/Documents/biometry and may be used for the development of the biometric server and client applets.

CHAPTER 5

EVALUATION OF SYSTEM

5.0. Introduction

This chapter discusses how well the final solution solves the research problem. Performance measurements Test are for the basic scientific factors: Speed; Throughput; Bandwidth; Latency.

- Speed of SMS and E-mail transfer from authentication server to mobile phone,
- Throughput of data transmission and receiving each node forming the circuit.
- Bandwidth of biometric image transmission on the traffic channel path.
- Latency on how long a time is taken for network path to hold data in transit

5.1. Success of the program in solving the problem

The architecture development is based on existing Java Application Programming interfaces common to many developers. All the innovations introduced in the work have existing template and functions in the Java platforms. Laptop Computers using biometric sensors are available in the market; though not highly patronized. Mobile phones embedded with biometric sensors are also available and becoming popular in terms of market patronage.

Result indicated that a hacker holding user-password, user-phone or any biometric computer, cannot access enterprise cloud data without final user-fingerprint scan to authenticate access. The security experts and software developers that came on board through design showcase and unstructured interview discussions thought that it was interesting and promising to improve IT data security.

The application can be used in any virtualize network platform; be it an in-house or cloud infrastructure to improve access control. Financial institutions promoting internet banking can reduce business risk for their corporate clients working towards cashless community. With this 2-step authentication approach, companies that handle huge employee salary data can do self-service through internet banking to credit the accounts of its staff and procurement transaction without submitting data copies to individual banks before processing accounts payable.

The Java library or the applet used in the development has firm foundations that can be extended upon to improve work in future.

The multi-nodal biometric input scanning rests the criticism associated to possible failure of the authentication process, as compared to secret code and one-time-password (OTP) generation. The multi-nodal implies that if user eye, fingerprint, and ear barcodes are stored in the database, the probability of either one passing the authentication is high to grant access to domain.

5.2. The weakness of the program

Telecommunication Network availability and dependency is still a challenge in most countries. However, the situation could be handled in the development by having two unique networks SIM connected in master slave circuit. If the preferred SIM fails to deliver the SMS link on time, then after 5-minutes of delay to authenticate, then the server should trigger a voice alert call to the preferred SIM-1. During same time delay another SMS should be transferred from the server to the alternative-slave SIM-2. Consider a user not having biometric laptop computer to authenticate from backdoor (E-mail account). It is obvious user biometric phone should be a dual SIM type to override the weaknesses associated to network failure rate.

5.3. Summary

In February 2013, the Department of Defense (US) paid AOptix **$3 million** to develop an enhanced solution smartphone that can serve as biometric scanner. The latest lunch uses multi-nodal biometric development proposed in this current research; so that at least five different features on the human organ are accepted for authentication. The hardware and software system, the first of its kind for the iPhone~~, is called~~ AOptix Stratus, which comprises both the iOS app, which will **cost $199** AOptix will also release a software development kit to its customers so they ~~can~~ customize the app to their own needs.

Finally, the new lunch and its reduced cost of the handset have given economic credibility for any cloud provider to adopt this work with ease of implementation.

CHAPTER 6

COMPARISON OF WORK AGAINST PREVIOUS WORK

6.0. Introduction

This section compares current work with other authentication methods.

Table 5: Comparison of current work against previous works

CURRENT WORK	PREVIOUS WORK
Verification method We used biometric to verify authorized user in the domain	**Verification method** Previous implementations verified authorized domain user; by possession of secret code and One-time-password generated through user mobile phone.
Connectivity to mobile: "AND gate" User computer is in permanent conjunction (AND function) with user mobile phone on the authentication server. Conjunction is not by self-service If you enter (username, Password) successfully, it will trigger the key-2 engine (biometric login interface) to accept biometric scan.	**Connectivity to mobile** With previous work, user may detach mobile phone from authentication server on self-service without the notice of the service provider who is hosting and protecting the client data. If you enter correct username and password, it will trigger secret code generation unto mobile phone.
Backdoor Authentication If user-1 lost biometric mobile phone, authentication is done on user-1 computer compatible to read biometric barcodes. (*Thin client was produced to support virtualization; everything is done on the server side).* Therefore user-1 can still login and authenticate with enterprise user-2 biometric computer, whiles waiting for phone replacement.	**Backdoor Authentication** Aside the secret code or One-time-password generation, a user on the first day of sign in, is given a confidential PIN code that should be kept in the hollow of confidential wall-drop; only to be used when you have lost mobile phone during the time you have attached to the authentication server.

6.1 Conclusion

The outstanding contribution of this work is the introduction of biometric technology into the two-step authentication method.

The next contribution is the use of AND logic function to permanently conjoin the two login interfaces on the authentication server and in a unidirectional operation. (i.e., the step-1 Login interface accepts only username and password). If the credentials are correct, it will trigger a link to prompt user to authenticate through the mobile device.

Finally, a hacker holding correct user-password, user-phone or any biometric computer, cannot access enterprise cloud data without final user-fingerprint scan to authenticate access.

The development meet the aim set out in the introduction and title of this thesis and it improves trusted-security. This is an innovation to improve cloud trusted security and further attract enterprises to migrate unto the cloud with the hope of sharing security control to access enterprise data process through cloud computing platform.

6.2 Recommendations for future work

With a little further study, this 2-step biometric authentication would become one of the trusted-security to counterpart cryptography in securing cloud computing platform. At present cryptography support the cloud for data in transit and data at rest. The two-step will support access control at the user-end terminal which is found to be the most culpable for security compromises due to user behaviour and negligence.

In the near future work, attension would be investigating encryption and decryption algorithms to secure biometric data transmission from the mobile phone to the authentication server.

Advanced studies are underway to encourage multi-nodal biometric systems. A multi-node biometric sensor can accept more than one unique feature of the bio-data from human anatomy. The advancement is to almost eliminate biometric authentication failure. It is important to follow this work with biometric studies so that authentication on the user mobile phone is also enhanced to accept multi-nodes (ear, eye, and fingerprint) at all times. If one or two inputs fail during authentication, there will still be options to scan on the unique human organs for authentication.

References

- Débora DG & Brunzel T, (2010) cloud Computing Evaluation-How it differs to Traditional IT outsourcing, Jönköping, 1-29, 70-pages Thesis

- Cloud Security and Privacy: An Enterprise Perspective on Risks and Compliance, by Tim Mather, Subra Kumaraswamy, and Shahed Latif; O'Reilly Media Inc, 2009, Chapter 5, identity and access management, pages 338.

- Cloud Computing: Implementation, Management, and Security, by John Rittenhouse and James Ransome; CRC Press 2010, Chapter 1 Introduction, pages 340.

- Multimedia Encryption and Authentication Techniques, by Borko Furht and Darko Kirovski, Auerbach Publications 2006, Chapter 1,8 ; pages 383.

- Perfect Password: Selection, Protection Authentication Illustrated, by Mark Burnett and Dave Kleiman, Syngress publications 2005, Chapter 1, 2, 13 pages 182.

- Difference between clusters, Grid & Cloud. Available from: <http://gigaom.com/2008/02/28/how-cloud-utility-computing-are-different/> Accessed on 6/03/2013 .

- Clarifying Private cloud, Hybrid Cloud & Public cloud. Available from: <http://blogs.gartner.com/thomas_bittman/2010/05/18/ > Accessed on 6/03/2013

- Definitions of theories associated with cloud computing. Available from: <http://en.wikipedia.org/wiki/Cloud_computing/> Accessed on 6/03/2013

- Differences explained: Private vs. Public vs. hybrid cloud computing. Available from: <http://www.mcrinc.com/Documents/Newsletters/201207/> Accessed on 6/03/2013

- Understanding differences in cloud, Cluster & Grid computing. Available from: < http://www.cloud-competence-center.com/> or www.aisec.fraunhofer.de Accessed on 7/03/2013

- Cloud computing and Passwords. Available from: <http://sociamediapedia.se/2011/01/23/cloud-computing-and-passwords/> Accessed on 17/03/2013

- Dropbox support-2-step authentication system; Available from: <https://www.dropbox.com/help/363/en /> Accessed on 21/03/2013

- Google support- 2-step verification system; Available from: <http://support.google.com/accounts/bin/answer.py?hl>Accessed on: 04/02/2013

- Barclays Bank Ghana internet banking (2010)-step authentication system; Available on <http://barclays.ghana@barclays.com /internet banking/OTP> Accessed on 15/03/2013

- Sotashi Samba (2009) Fujitsu limited 2-step authentication system and method < http://www.google.com/patents/EP2131302A2?cl> Accessed on 11/02/2013

- Amazon web services (2009) Multifactor authentication system; Available from: < http://aws.amazon.com/mfa> Accessed on 28/02/2013

- The History of cloud computing (Jan 2013); Available from: <http://en.wikipedia.org/wiki/Cloud_computing/> Accessed on 4/03/2013

- ECE 171 lecture notes (1999)Logic AND gate timing diagram lecture notes <http://web.cecs.pdx.edu/~mcnames/ECE171/Lectures/Lecture06.html> Accessed on 6/04/2013

- Gail Koehler, "Biometrics: A Case Study – Using Finger Image Access in an Automated Branch", Proc. CTST'98, Vo. 1, pg. 535-541 < http://www.docstoc.com/documents/most-recent/> Accessed on 7/04/2013

- J.M. Floyd, The functions of Biometric Identification Devices", Proc. CTST '96, < http://angelinvestornews.com/ART_Biometric.htm/> Accessed on 5/04/2013

- Brad Wing, "Overview of All INS Biometrics Projects", Proc. CTST'98, pg. 543-552 < http://angelinvestornews.com/ART_Biometric.htm/> Accessed on 9/04/2013

- L. Franceschi-Bicchierai, How to turn your phone into a biometric scanning machine <http://edition.cnn.com/2013/04/16/tech/mobile/mashable-biometric-iphone scanner/index.html? hpt=hp_mid. Accessed on 5/04/2013

- NIST/Biometric Consortium (2002), Biometric Interoperability, Assurance, and Performance Working Group Accessed on 6/04/2013 <http://www.biometrics.org/bc2002/4_bc0109_KsheerabdhiBrief.pdf/>

- Thomas Vian (2002), Design an interactive website to help teach maths, to Year Two, Key Stage One children, Academic thesis, Pages 82. Accessed on 2/04/2013

APPENDIX A

From: Edward Appiah [mailto:eddappiah@ddr2013.com.gh]
Sent: Friday, February 08, 2013 2:02 PM
To: eoosei@gmail.com
Subject: DDR CONFERENCE 2013 Abstracts

Dear E. O. Osei,
I write on behalf of the review committee and happy to announce acceptance of your abstract for the DDR 2013.
Please submit your full paper according to the reviewers' suggestions below (should there be any), and make sure it is formatted correctly, according to the guidelines on the website and indicate the sub-theme of your paper. Author(s) details should be on separate sheet as a cover. This is of great importance for the double-blind peer-review process.

Please note that:
- All authors' names and references are inserted on a separate sheet
- The reference style is Harvard
- The paper is proof-read (for non-English speaking countries, we may want to overlook certain aspects)
- Your revised paper should be in WORD format
- Please submit paper as an attachment to **submissions@ddr2013.com.gh**
- Check that your user account details are correct

See also the Conference Submission Guidelines
The deadline for full papers with corrections is **March 30, 2013**.
We are very much looking forward to seeing your full paper,

Eddie Appiah
Conference Coordinator
DDR 2013, Kumasi
Ghana

CONTRIBUTION DETAILS

ID: 20007
Title:
Cloud Computing Access Control Re-design- How it address security challenge of SME's on cloud adoption
REVIEW RESULT OF THE PROGRAMME COMMITTEE:
This contribution has been accepted.
OVERVIEW OF REVIEWS
Review
========

Evaluation of the contribution

Overall Recommendation (100%): B+
Total points (out of 10) : 7
Comments for the authors

Quality of Content: Good
Originality : One step forward
Presentation : Above average; author(s) must provide relevant keywords

Pseudo-code Program design:

```
START
      Load internet browser with provider address; https://www.mtncloudservices.com
      Initializes and add the screen objects
      Type on screen keypad the assigned Username and Password credentials
      Press enter on screen keypad to send access request to authentication server

      When enter key is pressed authentication server should respond
        If username and Password are correct as in the server
            Say please authenticate required to login
            Server should send embedded login page link in SMS to Eric mobile phone
            Server should send same embedded access page link to Eric E-mail account
        If username and password are wrong in the server
            Say sorry is wrong try again
        If username correct and Password wrong in the server database
            Say Please check password and try again
            Same time trigger automated voice phone call to correct username holder
        If username wrong and Password correct
            Say sorry username is wrong try again

     When mobile phone receives authentication request from server
            Save text message in the SMS inbox
            See embedded login interface after opening the link inside SMS
         If link open to show login interface then scan fingerprint
         If scan complete
             Send to authentication server by pressing OK button
             Say, waiting, whiles the server compares pre-defined & sent finger barcodes
             Say, scan successful, after authentication completed
         Else
            Say scan unsuccessful
  When backdoor E-mail account receives authentication request from server
            Save E-mail message inside the user inbox
            See embedded login interface after opening the link inside the E-mail
         If link open to show login interface then scan fingerprint on laptop
         If scan complete
             Send to authentication server by pressing OK button
             Say, waiting, whiles the server compares pre-defined & sent finger barcodes
             Say, scan successful, after authentication completed
         Else
            Say scan unsuccessful
END
```

APPENDIX B:

Interview with Cloud Service Provider-MTN-Ghana

Interviewer: Eric Opoku Osei
Interviewee: Edgar Zormelo (MTN-cloud services coordinator)
Type of interview: unstructured face-to-face
Date: 10th April 2013
Duration of interview: 25minutes

About the company:

MTN is a global Telecommunication Company operating in about 22 countries. The company renders cloud services to the public. They are into Infrastructure-as-a-service, Platform-as-a-service and currently lunched software-as-a-service.

We agreed on a favourable date and time, for such discussion. During the day of interview, we familiarised ourselves with the thesis topic and proceeded as follows:

Question1:

What cloud services are offered by your company to their clients?

Answer:

MTN is actively engaged in all the three basic cloud services IaaS, PaaS and SaaS to the Ghanaian public.

Question 2

What are some critical questions your customers inquire for their decision to migrate enterprise data unto the cloud services?

Answer:

Security! The interesting thing is that MTN has contracted Jamcracker who is the Global Leader in Cloud Service Brokerage.

Regarding Security, Data resides in state of the art data centers across Africa, USA and Europe. The platform conforms to approved and accepted security standards to ensure data integrity and compliance to agreed security policies.

MTN has also engaged auditing firms such as KPMG and PWC for regular auditing of their platforms to ensure that the platform is secure. Several Penetration and vulnerability testing are carried out in this regard.

Question 3:

How do you track intrusion or unauthorised user of a customer account?

At firewall level, that wouldn't be a problem for MTN; however it will be quiet difficult to track intrusion at the user-level unless the client report suspicious events. The client is responsible for user level protection; however, for us to deepen trusted security for our cherished clients, we are considering a multi-factor authentication. I can't be very specific which authentication approach to adopt, but it will be one of the robust designs.

Question 4:

How do you see cloud adoption in Ghana, especially the SaaS?

Is all about time; I believe the SMEs would benefit massively. I know of a local company subscribing to one international cloud provider for their applications; this is precedence and so would other local enterprises adopt the MTN SaaS.

Interview with I.T Security Professional

Interviewer: Eric Opoku Osei

Interviewee: Eric Afanu (MTN-Manager)

Type of interview: unstructured face-to-face

Date: 10th April 2013

Duration of interview: 30mins

About Afanu:

Mr. Eric Afanu is an I.T security Expert of MTN-Ghana with over 10-years' experience. He also serves as a security consultant for some SMEs in Ghana.

Interview:

We initiated the conversation from a cordial interaction. We familiarised ourselves with the thesis topic and proceeded with the interview as follows:

Question1:

What are your views on cloud computing security for enterprises in respect of data CIA?

Answer:

Data CIA highly depends on the kind of service provider hosting your data. I will recommend cloud for SMEs in terms of cost. I will suggest that larger companies build their own datacenters.

Question 2

How do you see the use of multi-factor authentication method? Can you envisage some pros and corns of multi-factor authentication when executed through a mobile network?

Answer:

Multi-factor authentication is good for user-level protection. There are three important questions to answer right to choose a strong and robust multi-factor implementation. What I know; what I have; what I am. It is important for the service provider to test the environment and see which one would provide trusted security and at the same time smart availability for authentication.

Question 3:

What measures would you advice a service provider to manage well on cloud multi-tenant platform?

Answer:

VLAN configuration is critical for multi-tenant platforms such as the cloud. These are my reasons; VLAN that is not strong can easily be compromise. One tenant on the server can penetrate through the wall into another user domain and that is a security breach.

Interview with Telecom Engineer, MTN-Ghana

Interviewer: Eric Opoku Osei

Interviewee: Wilfred Kofi Bruku (MTN-SMS &voice switching Engineer)

Type of interview: Questionnaire submission

Date: 10th April 2013

***1. My work uses SMS** for login authentication; please can you brief me on **SMS routing in a GSM/WCDMA network** and some challenges that are faced by this service?*

Answer:

SMS routing is quite broad so I will like to break it down into the following:

- SMS overview
- Mobile terminated SMS
- Unsuccessful Mobile terminated SMS
- Mobile originated SMS
- SMS queuing

SHORT MESSAGE SERVICE (SMS) Overview

SMS is a means of transferring a text message consisting of up to 160 alphanumeric characters from one point to another. SMS should not be confused with the SMS-Cell Broadcast Service, which transfers text messages point to multi-point from the BSC/RNC.

Short messages can either be transferred from a short message Service Center (SC) to a MS/UE, referred to as mobile-terminated; or from a MS/UE to an SC, referred to as mobile-originated. Only the signalling network transfers a short message. No traffic devices or channels are allocated.

MOBILE-TERMINATED SMS

The mobile-terminated SMS has the capability to transfer a short message from the SC to a MS/UE. In addition, it provides information about the delivery of the message through a delivery report, which confirms the delivery of the short message, or through a failure report, which informs the originator that the short message has not been delivered and the reason why. If the short message is not delivered, a specific procedure for later delivery is

used. The mobile-terminated short message can be input to the SC from a variety of sources, for example, speech, internet, or other MS/UE as shown in figure 1.

Unsuccessful Mobile-Terminated SMS Delivery

1. When a mobile subscriber is unreachable, the message waiting flag is set in the MSC/VLR.An error message is then sent to the SMS-GMSC
2. When the SMS-GMSC receives the error message from the MSC/VLR, the Set Message Waiting Data message is sent to the HLR. This message requests the HLR to transfer the SC address to the message-waiting data list. The message contains the MSISD of the called subscriber and the SC address. If the MSISDN is known and the message waiting data list is not full, the HLR includes the SC-address in the list
3. After receiving the answer to the Set Message Waiting Data message, the SMS GMSC sends a negative acknowledgment to the SC.

MOBILE-ORIGINATED SMS

The mobile-originated SMS provides the means to transfer a short message from a mobile to an SC. This can be carried out either when the mobile is idle, or when a connection (such as speech or fax) already exists. For both successful and unsuccessful deliveries, the mobile receives a delivery report.

SMS QUEUING

This function enables queuing of mobile terminated short messages. The short message is queued in the MSC/VLR server for a short time. The function is invoked in MSC/VLR server at unsuccessful delivery of a mobile terminating short message due to ongoing MS activities

Question 2:

How closely knit together are Computers and mobile phones? How may this close link help in secured 2nd factor authentication?

Mobile phones have progressively been improved to become smarter and more sophisticated. Modern mobile phone Operating systems have made this even better by their robustness and ease of update. To see how closely knit smart phones and PC are, I will like to compare a phone that uses on of commonest mobile phone OS's today, Android, to a PC running MS Win7.

I use the HTC one X smart phone which runs Android version 4.0.4 and a Toshiba satellite pro which runs Win7. These two devices share a lot of similarities that it is hard to separate them in terms of basic functionality. They both have big processors, Wi-Fi compatibility, strong password protection, access to thousands of software (Android store for the HTC one X smart phone and MS site and 3rd party sites for the PC). Both OS's can be updated and they have equal accesses to the internet. It is therefore not surprising that more smart phones were shipped out from manufacturer than PCs in 2012. In my opinion, Smart phones will have an edge over PCs in the near future because of their portability.

Now that the close link between PCs and Smartphones has been established, it lends strong credence to the fact that they can both be used almost seamlessly in a 2 way authentication of any computer system.

Question 3:

Have you ever used 2-step authentication? If yes what limitations have you observed.

My bankers use this 2-step authentication where after logging into their E-banking system with your password, another one-time password is sent via SMS to your phone. The onetime password is a six digit unique password which is always required to have access to your account. Without the cell phone it is virtually impossible to log in. I also realised the system used https, which will encrypt any data that is sent via the internet. Packet listening tools might capture the packets being sent, but will not be able to interpret them. The cell phone authentication adds even security.

The limitation to me is when the same cell phone (usually a smart phone) that is used for the second authentication is used for the first login.

The cell phone might keep some cookies to the site and this makes the system a little bit vulnerable. A hacker who has the cell phone might try to look at the cookies and try to get the first pass word; the second authentication will not be a problem since he has the cell phone already. So to make the system more secured for myself, I try as much as possible not to use my smartphone to log in to the site, so I don't expose myself to any security issues.