Improving the Security of the Internet Banking System Using Three-Level Security Implementation

Emeka Reginald Nwogu
Directorate of Information and Communication Technology,
Michael Okpara University of Agriculture,Umudike,
Umuahia, Nigeria.
nwogu.emeka@gmail.com

Abstract – The paper focuses on 3-level security for Internet banking systems using an internet banking dongle, Kerberos, Advanced Encryption Standard (AES) and Biometric Identification. Biometric identification will be used to implement access control to the dongle, which will provide a trusted path to the internet banking server instead of trusting the customers' computers. The preferred protocols for the implementation of this system are Kerberos and Advanced Encryption Standard (AES). Kerberos, being a third party authentication protocol, will allow a process (client) running on behalf of a principal (user) to prove its identity to a verifier (The application server). This implies avoiding the transmission of data across the network that might allow an attacker or the verifier to subsequently impersonate the principal. The system will require users to gain access to the Internet banking service by the use of a Kerberos ticket which can only be granted by a third party. AES on the other hand will provide additional security to this system, providing a shared key between the dongle and the Internet banking Server, which will be used for both encryption and decryption of transaction data.

Keywords: Biometrics, Advanced Encryption Standard, Kerberos, authentication, internet banking.

I. INTRODUCTION

Over the years, internet banking has transited different implementation, developmental and architectural stages; and consequently, there has been a wide acceptance of this service. As the service evolves, new functions and features continue to be added to it. This has reduced the time and resources spent conducting financial transactions, as one can just by logging into the internet banking website or system make huge transactions worth several millions in just a matter of seconds, without visiting a bank branch. Today, long queues in banking halls have either disappeared or reduced in most countries. Bank branches have been shut down and subsequently, savings made from reduced staff remuneration and branch office maintenance budgets [1].

The advancement of internet banking and its associated services has not been without an increased probability of attacks. Reference [2] reports that the trend of growth of online banking brings many security issues and increasing cost of implementing higher security system for both online banking users and the banks. Reference [4] claims that the wide use and application of information technology in the banking industries has also led to emerging threats and attacks, basically in the form of computer crimes and fraud. Also [3] writes that the adoption of electronic banking (e-banking) has brought major challenges to the banking industry in terms of risk exposure. This leaves customers with the choice of enjoying the ease, the service gives, with the resultant vulnerabilities that accompany it, or continuing with the traditional banking procedure which is often tedious and less user friendly while hoping that no one gains unauthorized access to their account and savings.

As more and more people are exposed to the information superhighway, privacy of information and the security that goes hand in hand with this information is crucial to the growth of electronic transactions [5]. Consequently, there is need to develop a more secure system that can solve most of the security needs and flaws that have been identified in the current internet banking systems. One such flaw is the threat posed by the "man-in-the-middle" attack, where an attacker hijacks an existing session after the legitimate party to that session has been authenticated by the server and logged in. When this happens, the attacker can then carry out their attacks with ease. This raises strong arguments about the effectiveness of systems that rely on trusting the client's computers, rather than using a secure device to create a trusted path from the client to the internet banking server.

The greatest challenge on internet banking security implementation is that security system developers tend to be reactive instead of active. Reference [6] discusses that, at different times, most of the defenses on Internet banking attacks have been reactive. Reference [7] also posits that the current internet banking models are focused on fraud identification instead of fraud prevention, which means that actions are taken only after a fraud occurs instead of performing a series of preventive procedures.

The overall motivation of this research-work is to propose and model an active system that solves most of the security related problems encountered on internet banking systems, employing a three-level security implementation by the use of a cheap internet banking hardware device that implements device access control using biometric information identification together with Kerberos and Advanced Encryption Standard for authentication and encryption.

II. CURRENT INTERNET BANKING SECURITY IMPLEMENTATIONS

In order to have a good understanding of this proposed Internet banking model, it is necessary to do a review of the current Internet banking security implementations and their shortcomings.

The current models in use on online banking systems are based on several security layers, with so many security mechanisms and solutions, all aimed at providing good security for internet banking systems, application and the transaction data, providing identification, authentication and authorization.

Reference [7] identified the current security implementations on online banking to include the following;

- **Digital Certificates:** Digital certificates are used to authenticate both the users and the banking system itself. This kind of authentication depends on the existence of a Public Key Infrastructure (PKI) and a Certificate Authority (CA), which represents a trusted third-party who signs the certificates attesting their validity.
- **One-Time Password Tokens:** One-Time Password devices are used as a second authentication factor. This kind of devices render captured authentication data useless for future attacks through the use of dynamically changing passwords which can be used only once.
- **Browser Protection:** In this model, the system is secured at the Internet browser level, which is used to access the banking system. The user and their browser are protected against known malware by monitoring the memory area allocated by the browser in order to detect such malware and hinder credential theft and capturing of sensitive information.
- **CAPTCHA:** Completely Automated Public Turing test to tell Computers and Humans is a method adopted to render automated attacks against authenticated sessions ineffective. This method requires the legitimate user to input information conveyed as scrambled images which are difficult for automated robots to process and recognize.
- **Device Identification:** Device identification is usually based on physical characteristics of the user's device through which it is possible to identify its origin and history information.
- **Pass-Phrase:** This is similar to PIN, but differs in that it consists of numbers, alphabets and strings. It is usually used as a second authentication method in transaction that involves money movement.
- **Transaction Monitoring:** This is currently applied in all online banking systems, using different techniques. Artificial intelligence, transaction history analysis, intrusion detection system, intrusion prevention system and other methods that identify fraud patterns in previously processed transactions are among the various approaches used.

Others include;

- **Spam Filtering :** Spam filters are classifiers that analyze emails and assign scores to them. Emails with scores above a particular threshold are discarded as spams. Spam classifiers work by trying to identify features in which legitimate email and spam differ.
- **Transport Layer Security (TLS) Protocol:** Transport Layer Security (TLS) protocol uses a key-agreement protocol such as Diffie-Hellman to establish a confidential channel with integrity guarantees between two parties. Authentication of the server is provided by an X509 certificate chain rooted in one of several trusted third parties whose

certificates are provided to clients out-of-band. TLS is a widely used mechanism on the Internet. Most sensitive data are protected using TLS while in transit across the Internet.

- **Password Wizards:** Most web browsers give the option to remember passwords for web sites and to auto-complete the log-in forms so that the users do not have to remember the password. This has been regarded as a security threat, since the password can be recovered from where it has been stored in the web browser. However, this sometimes improves security. The web browser is able to distinguish whether a site is the same site that it has visited previously. The user on the hand might be tricked by URLs which are similar, but not the same.
- **Onscreen Keyboard:** As a result of keyboard sniffing programs, most banks have introduced PIN entry with the mouse via an on-screen keyboard. An example of this is Citibank UK [9]. This is billed as foiling keystroke loggers since no keys are pressed.
- **Short Message Service (SMS) challenge:** This method has been applied in some banking systems to notify users about transactions requiring their authorization. It provides a second authentication channel for transactions that fit certain characteristics by sending to the user a set of characters which have to be entered on the system in order to authorize and process the transaction through the online banking system.
- **Private Identification Number (PIN):** In PIN, users are required to input some secret numbers only known to them in order to identify themselves. It is applied as a second authentication method.

A. CURRENT DEFENSE EFFECTIVENESS

After critically assessing the current security implementations on online banking systems, it was established that these defenses have not been able to solve the security needs of the internet banking systems. Reference [10] identified the four generally accepted security properties that one may require when establishing a secure channel between the user and the bank, and they are;

1. User/Server authentication – before sending sensitive information over the Internet, the user should be assured that they are communicating with the right bank; the bank should also be able to verify the identity of the user before processing the requested transactions.
2. Confidentiality – only the authorized entities (i.e. the user and the bank) should have access to the content of the messages being exchanged.
3. Data integrity – the user and the bank should be able to detect any manipulation (including insertion, deletion and substitution) or replay of data by unauthorized parties.
4. Non-repudiation – neither the user nor the bank should be able to deny previous actions; for instance, in case of disputes, the bank should be able to prove to a third party that the user has performed certain transactions.

Every internet banking system should be able to guarantee all four security parameters.

The table below lists the security issues associated with the current implementations.

Table 1 Security defects of the current internet banking security implementation

S/no	Security	Defects
1	Transport Layer Security (TLS) Protocol	Due to the costs associated with acquiring TLS certificates many sites have certificates which are not rooted in the trusted certificates shipped with the browser. When presented with such a certificate, browsers will typically prompt the user to accept the certificate. Such prompts do not provide information which will allow the majority of users to make an appropriate security decision since they do not understand the terms used.
2	Digital Certificates	Certificates could be exported and utilized remotely. They can also be used by more than one user at a time, thus allowing the use of stolen certificates.
3	OTP Card	Malwares and Trojans can collect passwords from users through phishing.
4	Onscreen Keyboard	Trojans and mouse loggers can capture input and transmit to the attacker.
5	Pass-Phrase	Screenloggers, keyloggers or mouseloggers can be used to capture the secret information. Social engineering and phishing may also be used.

6	CAPTCHA	The methods applied to scramble the information in the image are too simple, making it possible to extract the desired information using OCR software.
7	Browser Protection	New malware remain active until they are identified by the Model. Also counterfeit online banking system web pages which prevent the protection from properly loading can be used to make the user input their sensitive data (passwords) in an unsafe environment.
8	Short Message Challenge	Attackers may alter the mobile phone number to which the authorization messages are sent.
9	Private Identificati on Number	Phishing and social engineering may be used to harvest the secret number.

III. NEW SYSTEM DESIGN

Generally, the proposed Internet banking dongle is made up of two different modules, namely; the security module and the network/control module. The security module is the most important module in the proposed Internet banking dongle, and basically takes appropriate actions when the system is threatened. It is further segmented into three sub-modules. These sub-modules make up the three-level security proposed for this system, and they include;

- User authentication (device access control) module
- Device/Server authentication module
- Transaction data security (network security) module.

The network/control module is further segmented into two sub-modules, namely the network and the control sub-modules. The control sub-module is responsible for establishing the connection between the Internet banking Server and the Internet banking dongle. It also monitors the connection for anomalies and terminates the connection when such network anomalies are detected. Also flow control is done at this sub-module. The network module encapsulates the data to be transmitted. It also transmits and receives data from the Internet banking Server. The transmission is done using suitable Transmission Control Protocol/Internet Protocol (TCP/IP) and TLS protocols. This work does not cover a comprehensive analysis of the network module. Our main interest is on the analysis of the security module.

User authentication

The user authentication security sub-module ensures that only authorized users gain access to the internet banking system. This will be implemented using finger print information and user's private identification number (PIN). The Biometric reader reads and sends the client's biometric data to the network module for transmission to the Kerberos Server for authentication; the PIN reader on the other hand reads customer's PIN and equally sends such to the network module also for transmission to the Kerberos Server for authentication the system is designed in such a way that as information is captured, it is encrypted immediately to avoid sniffing of data at the application layer.

Device/Server authentication

The device/server authentication sub-module ensures that only authorized devices (dongles) access the internet banking server. This is to avoid the use of cloned devices. During authentication, the Kerberos server checks the device's encrypted Media Access Control (MAC) address, to be sure that tickets for access are only granted to authorized devices. The encryption of the MAC address and the fact that customers' finger print information together with the customers' PIN are sent to the Kerberos server for authentication guarantees the identity of the dongle device making sure cloned devices do not get authenticated. Also this guarantees non-repudiation, as the identity of the dongle device and the person who has made a transaction could be recorded and later accessed by authorized individuals. This is possible because dongle devices are registered with customers' information. The preferred protocol for the implementation device/server authentication is Kerberos.

Transaction data security

This sub-module ensures that transaction data are not accessible to any other except the dongle and the internet banking server. This guarantees confidentiality of data, eliminating any possible access to transaction data through man-in-the-middle attack and etc. Advanced Encryption Standard (AES) and Kerberos will be used to implement this module.

A. System Modules' Interaction

Figure 1 below gives a diagrammatic picture of the module interaction for the proposed system. The Kerberos client is embedded directly under the user interface such that once the device user access information (fingerprint and PIN) is captured, the Kerberos client encrypts the information and places it on the network/control module for transmission to the Kerberos server. This information together with the MAC address of the dongle device is used to authenticate the device and the user for subsequent granting of the Kerberos ticket.

Advanced Encryption Standard is implemented at the transaction data security module. This module sits directly under the device/server authentication module. It communicates directly with the internet banking server after the Kerberos ticket has been accepted by the internet banking server. This module ensures the confidentiality of the transaction information.

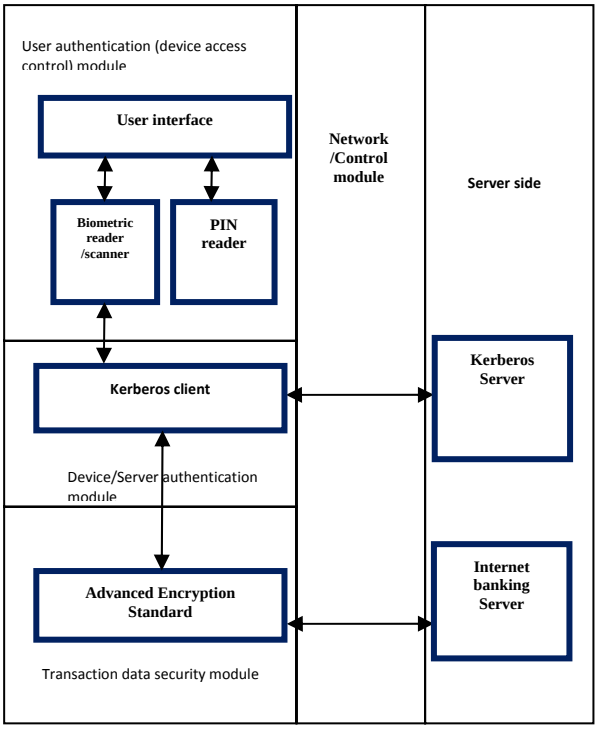

Fig. 1 Modules interaction for the proposed system

PIN entry

Because of the existence of Trojans and keyloggers, that can sniff keyboard inputs, we have proposed a virtual keyboard for the system. This keyboard will be embedded on the dongle application with random arrangement of keys. This will also protect against the sniffing of the customers' PINs by mouse-loggers, malwares and Trojans that have the ability of sniffing mouse inputs.

Fingerprint scanning

In order to avoid the sniffing of the fingerprint information at the application level, we have proposed a hardware device with inbuilt scanner. This will make it possible for the Kerberos client to encrypt the fingerprint information once captured, eliminating the possibility of sniffing the fingerprint information with the use of malwares and Trojans.

B. NEW SYSTEM'S ALGORITHM

In order to understand the information flow in the proposed system, we have represented the system operation with the following algorithm;

1. An intending user inserts the USB Internet banking dongle on a PC or tablet with Internet connectivity; the dongle user login interface is launched automatically.
2. The interface prompts the user to supply their PIN and fingerprint.
3. The preliminary security check (client level security) is conducted by the dongle application. And if this returns positive, the dongle application sends the information to the authenticating Kerberos server for ticket granting.
4. When the Kerberos server confirms the identity and permissions of the dongle device and the user, the ticket granting process begins.
5. If the ticket granting is successful, the dongle application automatically connects to the internet banking server using the ticket granted by the Kerberos server.
6. On the internet banking server interface, the user supplies their account login credential (username and password) to gain access to the internet banking menu where they can select operations to be performed.

7. For every transaction, the customers' initial access PIN serves as a transaction confirmation number, which they must input to confirm each transaction.
8. The internet banking server and the dongle use a symmetric key (Advanced Encryption Standard) known only to the two communicating devices to encrypt and decrypt transaction information.
9. Once the customer selects logout on the menu, the ticket expires, the communication between the server and the dongle terminates and the dongle application is closed automatically, after notifying the user, signaling the end of the operation.
10. Customer ejects their dongle from the computer.

C. NEW SYSTEM HARDWARE FEATURES

Low device cost

The proposed dongle in this research is a consumer device that is cheap and easy to use. This will be similar to the dial up modem device used by subscribers to access Internet connectivity from Telecommunication Service Providers. Another example of a cheap device issued to consumers by the banks is the smart card. These are sufficiently cheap that banks can issue them to all customers. If customers are well informed of the benefits of this dongle, they can sign up for its use. This proposed USB-attached device with a display interface is comparable in complexity and price, to USB dial-up modems which typically retail at around USD 30. We propose that the banks share the cost of this device with the consumers.

Transaction transparency

In the "man in the middle attack", the attacker spoofs the target so that the victim connects to the attack by mistake. The chosen protocol attack is, however, much more general than that. In some attacks, the attackers put up a web site dealing in pornography and entices the victims to access it. When accessing the pornographic site, the victim is asked to prove their age by signing some random values using their credit card. This has none of the visual clues of a spoofed banking site; the customer expects to be doing this and is on the site they wish to be. However, in parallel to this, the attackers are conducting a high-value transaction elsewhere. The "random value" which the victim is asked to sign is actually the authentication for this high-value transaction. A chosen protocol attack boils down to an authorization which the user thinks is for one purpose actually being used for a different purpose. Solutions for this involve ensuring that messages are unambiguous as to their purpose and destination and not allowing third parties to use the same authentication system.

Form factor

There are several form factors which could be used for this device. However, since USB is now the standard interconnect for computer peripherals and is supported in all major operating systems, together with the fact that it is cheap, easy to use and common, it is recommended for this dongle.

Device Input/Output infrastructure

The device presents a trusted user interface to the customer. This requires a screen to display details of the transactions and some method of authorizing or denying transactions. The minimum implementation of this is a pair of 'OK' and 'Cancel' buttons. Since performing transactions also requires logging into the bank's web site with the bank's provided credentials, this is already a two-factor authentication scheme; but this has been improved upon with the trade-off being increasing the cost of the device and a small amount of extra interaction with the device for the user. The option adopted here is the integration of biometric reader that reads customer's finger print information. This would reduce the exposure from a stolen device.

End - to - end connection security

The proposed system guarantees a secure end to end connection between the Internet banking site and the Internet banking dongle using symmetric key protocols.

D. PROPOSED SYSTEM AUTHENTICATION PROTOCOL

The proposed system will be achieved using Kerberos authentication protocol as the main protocol for its operation. The choice of Kerberos has been the added security the protocol provides. Kerberos was designed at the Massachusetts Institute of Technology (MIT). It is a trusted third-party

authentication protocol that can be used to provide a single sign-on solution and to provide protection for logon credentials. It relies upon symmetric key cryptography (Private Key Cryptography), specifically Data Encryption Standard (DES), and provides end-to- end security for authentication traffic between the client and the Key Distribution Center [11].

Kerberos authentication mechanism uses a trusted server (or servers) that host the functions of the KDC, Ticket Granting Service (TGS), and Authentication Service (AS). The central server that hosts all of these services is simply referred to as the Key Distribution Centre (KDC). All clients and servers are registered with the KDC, so it maintains the secret keys of all network members.

Kerberos uses timestamps to reduce the number of messages needed for basic authentication [12], and has a "ticket-granting" service to support subsequent authentication without re-entry of a principal's password, and different approach to cross-realm authentication (authentication of a principal registered with a different authentication server than the verifier).

Kerberos Ticket

Whenever a client authenticates itself to a new verifier (The party who demands assurance of the principal's identity, in this case, the Internet banking Server) it relies on the authentication server to generate a new encryption key and distribute it securely to both parties. This new encryption key is called a *session key* and the Kerberos ticket is used to distribute it to the verifier.

The Kerberos ticket is a certificate issued by an authentication Server and encrypted using the Server key. The ticket contains the random session key that will be used for authenticating the principal (The party whose identity is to be verified, in this case, the Internet banking user or client) to the verifier, the name of the principal to whom the session key was issued, and an expiration time after which the session key is no longer valid. The ticket is not sent directly to the verifier, but is instead sent to the client who forwards it to the verifier as part of the application request. Because the ticket is encrypted in the server key, known only by the authentication server (Kerberos Server) and intended verifier (Internet banking Server), it is not possible for the client to modify the ticket without detection. Kerberos tickets have specific lifetimes and use parameters. Once a ticket expires, the client must request a renewal or a new ticket to continue communications with a server.

The Kerberos Ticket granting process is as follows:

1. User types PIN and enters biometric information into the client.
2. Client encrypts credentials with DES for transmission to the KDC.
3. KDC verifies user credentials.
4. KDC generates a Ticket Granting Ticket (TGT) by hashing the user's information.
5. The TGT is encrypted with DES for transmission to the client.
6. The client installs the TGT for use until it expires.

Once this has been completed, the next process is the Internet banking service request and is as follows;

1. The client sends its TGT back to the KDC with a request for access to the Internet banking service.
2. The KDC verifies the ongoing validity of the TGT and checks its access control matrix to verify that the user has sufficient privilege to access the requested resource.
3. A Service Ticket (ST) is generated and sent to the client.
4. The client sends the ST to the Internet banking Server.
5. The server or service host verifies the validity of the ST with the KDC.
6. Once identity and authorization is verified, Kerberos activity is complete. The Internet banking Server then opens a session with the client and begins communications or data transmission.

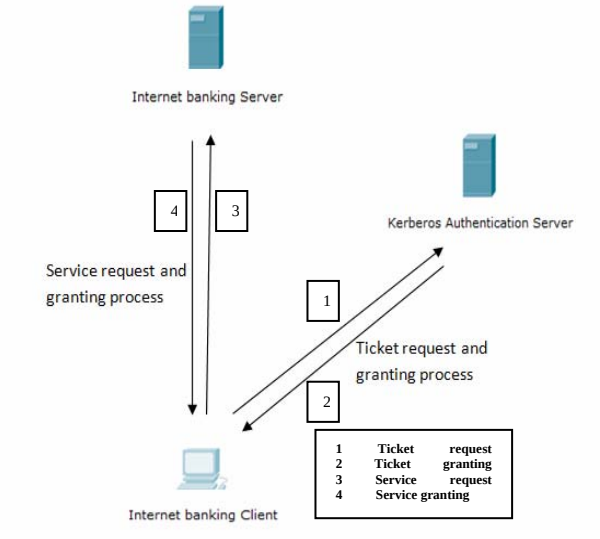

Fig. 2 Kerberos authentication process illustration

1. as_req: c, v, $time_{exp}$, n
2. as_rep: $\{K_{c,v}, v, time_{exp}, n, ...\}K_c$, $\{T_{c,v}\}K_v$
3. ap_req: $\{ts,ck, K_{subsession}, ...\}K_{c,v}$ $\{T_{c,v}\}K_v$
4. ap_rep: $\{ts\}K_{c,v}$ (optional)

$T_{c,v} = K_{c,v}$, c, $time_{exp}$ ...

Fig. 3 Basic Kerberos authentication protocol (simplified)
Source: Kerberos- An authentication Service for Computer Networks

Key Distribution Centre (KDC)

A Key Distribution Centre is a group of Servers that store, distribute and maintain cryptographic session keys. When a system wants to access a service that uses Kerberos, a request is made via the KDC. The KDC generates a session key and facilitates the process of connecting these two systems [13].

This work proposes a single KDC for all Internet banking transactions in each country irrespective of the Bank; with a couple of backup KDCs located at other locations. The backup KDCs will serve as failovers in the event of the active KDC failing. The KDCs will be synchronized to assure that data stored on all of them is the same and will be under the management of a single body that will be charged with the responsibility of administering the Key Distribution Centre services.

The KDC will use the dongle's Media Access Control (MAC) address and the user's credentials (PIN and finger print information) to authenticate the user and issue appropriate ticket to the user. With this, we are sure that the use of wrong credentials on a dongle will result in denial of service from the Internet banking site, since the KDC will ultimately issue no ticket to the principal. This makes it impossible to use another person's dongle to access the Internet banking service.

When users obtain the Internet banking dongle from their banks, the dongle is registered with the Key Distribution Centre, with users supplying their PIN and finger print information to the Key Distribution Centre. The MAC address of the dongle is then associated with the users PIN and finger print information, and is subsequently used to authenticate the user and issue Kerberos ticket on request. During the registration process, users are also required to supply their picture and security information which is stored at the Key escrow, making it possible to track the owner of a particular Internet banking dongle. In this way, the security information of anyone who performs any transaction on Internet banking sites will be identified.

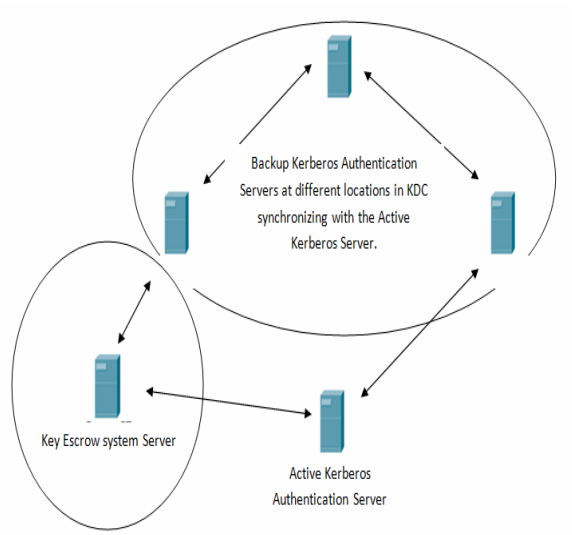

Fig. 4 Kerberos Servers and Key escrow synchronization

Key Escrow System

This is a cryptographic recovery mechanism by which keys are stored in a database and can only be recovered by authorized key escrow agents in the event of key loss or damage [11]. In this design, we have adopted a key escrow system that does more than normal key storage. The proposed key escrow will be able to keep a history of customers' usage of the Internet banking dongle, since a customer could decide to use more than one internet banking dongle. This is known as accounting. Such history can also be made available to authorized individuals when needed, especially during investigation of a particular Internet banking activity. The Key Escrow will checkmate repudiation attempts by criminals, fraudsters and attackers, since customers' and users' security information can easily be accessed. The key escrow will record and keep every Internet banking transaction.

When a customer loses their Internet banking dongle, the customer acquires a new dongle and subsequently the issuing bank registers it with

the KDC. All registered dongles have their information stored at the key escrow.

Transaction data security using Advanced Encryption Standard

Once the dongle has been authenticated and a ticket issued, the dongle can now exchange transaction information with the Internet banking Server using both the Kerberos ticket and the Advanced Encryption Standard (AES). AES algorithm is a symmetric block cipher that can encrypt (encipher) and decrypt (decipher) information [14]. AES will encrypt both the Kerberos information and the transaction data, adding an additional layer of security to the system. The dongle and the internet banking server share a symmetric key known only to them, which is used for the encryption and decryption processes.

IV. RESULT ANALYSIS

There is no doubt, the system proposed here performs much better than the current systems. In analyzing the proposed system for possible security flaws, we have based our analysis on the four criteria, a system must meet before it is deemed secure. These criteria include user/server authentication, confidentiality, data integrity and non-repudiation.

User/Server authentication test

The system proposed here ensures strong authentication of the communicating parties – the user, the internet banking dongle (client) and the internet banking server before communication can begin. The use of customers' PIN, known only to the customer and biometric information ensure the right user, not the attacker is allowed to access the service. This makes stolen dongles worthless and useless, since fraudsters cannot gain access to the service even after gaining access to customers' dongles. The Kerberos server on the other hand ensures that not only authorized customers but also authorized devices can access the service. This makes high level attacks by the compromise of communicating systems impossible. Such attacks as replay attacks, man-in-the-middle attacks and etc. can be stopped. Replaying an entire protocol run using an old initialization message is prevented by the inclusion of an incrementing counter for each run of the protocol. The server keeps track of these and aborts connections with repeated counters. Duplicate transaction request messages may be sent and will be accepted by the device, however they will not correspond to an outstanding transaction when a reply is received by the bank and will have no effect. At worst case scenario, even when the attacker has succeeded in sniffing the customers PIN and biometric information (which is practically impossible with the use of Kerberos), the use devices' encrypted IMEI numbers by the Kerberos server for device authentication ensures ticket isn't granted by the Kerberos server.

Confidentiality test

The system proposed here uses strong authentication and encryption protocols to ensure data confidentiality. Even if attackers succeed in sniffing data on the network, the strong encryption made possible by both Kerberos and AES protocols makes the information unintelligible, since the attackers would not have access to the symmetric keys shared by the server and dongle used for encryption and decryption of transaction information.

Data integrity

The proposed system makes insertion and substitution of data by unauthorized parties impossible. This is because messages are protected by a message authentication code with a different key from the encryption which is also generated for each session. The MAC provides integrity protection against modifying the message. All the messages include their message type and destination along with a unique value for that run of the protocol. This prevents messages being used in different runs of the protocol other than that intended.

Non-repudiation

Non-repudiation ensures that none of the parties (the user and the server) denies their activities by keeping a log of every transaction. Our proposed key escrow will be able to keep a history of customers' usage of the Internet banking dongle, customers' registration and security information and all transactions performed by any particular key. The internet banking server also will be able to log all transaction information, thereby making it impossible to repudiate any activity. This is called accounting.

V. CONCLUSION

As the crave for a more secure Internet banking system and service continues to rise, there is no doubt that the development and deployment of the system proposed in this work will go a long way in solving our Internet banking security needs. The system proposed here will guarantee a trusted path to the customer rather than trusting the customers' computers. This will eliminate any possible occurrence of the "Man in the Middle" attacks or other attacks which have been recurrent. This proposed system will not only solve our security needs, but will also make Internet banking affordable to the majority of the world population, guaranteeing security of customers accounts and information.

REFERENCES

[1] Nwogu Emeka Reginald, "Internet banking implementation in Nigeria; security issues analysis and solutions," unpublished.

[2] Hole, Moen and Tjostheim, "An analysis of the online banking security issues," Department of Computer Science, University of Auckland, 2013.

[3] Abaenewe Zeph, Ogbulu Onyemachi and Ndugbu Michael, "Electronic banking and bank performance in Nigeria," West African Journal of Industrial & Academic Research Vol.6 No.1, 2013.

[4] Friday Wada, Olumide Longe and Paul Danquah, "Action speaks louder than words – understanding cyber criminal behavior using criminological theories," Journal of internet banking and commerce, vol.17, no.1, Aril 2012.

[5] Yi-Jen Yang, "The security of electronic banking," 2010.

[6] Matthew Johnson and Simon Moore, "A new approach to e-banking," In U´ lfar Erlingsson and Andrei Sabelfeld, editors, Proc. *12th Nordic Workshop on Secure IT Systems (NORDSEC 2007)*, pages 127–138. Retrieved. May 14, 2012 http://www.matthew.ath.cx/publications/2007-Johnson ebanking.pdf.

[7] Laerte Peotta, Marcelo D. Holtz, Bernardo M. David, Flavio G. Deus and RafaelTimóteo de Sousa Jr., "A formal classification of internet banking attacks and vulnerabilities," International Journal of Computer Science & Information Technology (IJCSIT), Vol 3, No 1, February
2011.

[8] Dandash O., Dung P. and Srinivasan B., "Security analysis for internet banking models," Eighth ACIS International Conference on Software Engineering, Artificial Intelligence, Networking, and Parallel/Distributed Computing, 2007.

[9] Sarah Hilley, "Citibank cuts off bank spies with virtual keyboard," Infosecurity Magazine February 2005, retrieved Feb 17, 2012 from http://www.infosecurity-magazine.com/news/050216_Citibank_keyboard.html.

[10] Hyoungshick Kim, Jun Ho Huh and Ross Anderson, "On the security of internet banking in South Korea, 2012.

[11] James Michael Stewart, Ed Tittel, Mike Chapple, "Certified information systems security professional study guide, 3rd edition, 2005.

[12] D. E. Denning and G. M. Sacco, "Timestamps in key distribution protocols," Communication of the ACM, 24(8):533-536, August 1981.

[13] Emmett Dulaney, "CompTIA Security+ study guide," 2009.

[14] Federal Information Processing Standards Publication 197, "Announcing the Advanced Encryption Standard (AES)," November 2001.

AUTHORS' PROFILE

Nwogu Emeka Reginald is a staff of Michael Okpara University of Agriculture, Umudike, Nigeria. He holds a Bachelor of Engineering Degree in Electrical and Electronics Engineering (Telecommunications option) and a Master of Science Degree in Information Technology. He is also a recipient of the following certifications: Cisco Certified Network Professional (Routing and Switching), CompTIA Security +, CompTIA Network + and Cisco Certified Network Associate.

He has worked as an ICT professional since 2005 and has published a number of works in some renowned international journals. He currently researches on computer, network and information security.