Journal of Scientific Research & Reports

23(1): 1-14, 2019; Article no.JSRR.47953
ISSN: 2320-0227

Improved Online Security Framework for e-Banking Services in Nigeria: A Real World Perspective

O. Sarjiyus[1*], N. D. Oye[2] and B. Y. Baha[3]

[1]Department of Computer Science, Adamawa State University, Mubi, Nigeria.
[2]Department of Computer Science, MAUTECH, Yola, Nigeria.
[3]Department of Information Technology, MAUTECH, Yola, Nigeria.

Authors' contributions

This work was carried out in collaboration among all authors. Author OS designed the study, performed the statistical analysis, wrote the protocol and wrote the first draft of the manuscript. Authors NDO and BYB managed the analyses of the study. Author BYB managed the literature searches. All authors read and approved the final manuscript.

Article Information

DOI: 10.9734/JSRR/2019/v23i130113
Editor(s):
(1) Professor Luigi Giacomo Rodino, Mathematical Analysis, Dipartimento di Matematica, Università di Torino Via Carlo Alberto 10, I-10123 Torino, Italy.
Reviewers:
(1) Wael Omran Aly, High Institute of Computer Sciences and Information Systems New Cairo Academy, Egypt.
(2) Fouad Omran Elgahwash, University of Az-Zawia, Libya.
(3) Adebayo Omotosho, Landmark University, Nigeria.
(4) Mudasir M. Kirmani, Sher-e-Kashmri Unviersity of Agricultural Sciences and Technology of Kashmir, India.
Complete Peer review History: http://www.sdiarticle3.com/review-history/47953

Original Research Article

Received 17 January 2019
Accepted 29 March 2019
Published 10 April 2019

ABSTRACT

Internet technology has given Banks the opportunity to provide customers robust, convenient and flexible banking services including, but not limited to fund transfers, account checking and payment of bills. Despite these huge benefits, e-banking has given rise to so many security concerns arising from countless threats. The rise in security threats against e-banking has caused a decline in the use of online banking and has negatively affected customer confidence in the ability of banks to protect their money and information and are looking up to the banks to fix the problems. This research, Improved Online Security Framework for e-banking services is geared towards developing an improved security framework that solves the issues of authentication, confidentiality, integrity and non-repudiation as it pertains to online banking attacks. Data was collected from primary and secondary sources ranging from interviewing relevant stakeholders that use internet banking to consultations of related journals articles and technical reports. Design and modeling tools such as UML usecases, Entity relationship (E-R) diagrams, process flow modeling and MySQL for a robust database design were used to capture basic system functionalities and

**Corresponding author: E-mail: sarjiyus@gmail.com;*

artifacts required. The entire design was implemented on Visual studio platform. Upon running and testing on a XAMPP server, the system was found to meet all design objectives and operationally effective.

Keywords: Security; testing; functionalities; design; effective.

1. INTRODUCTION

Internet banking has demonstrated a speedy and tremendous growth in recent times. It has become a key player in every business activity. A major development in this dimension is traced to the banking sector where fixed operating costs are minimized by providing un-interrupted forms of banking services [1]. Online banking is expected to grow due to the dramatically increase in using e-commerce applications in businesses by Internet users [2].

Online banking is projected to grow geometrically because of the dramatic increase in the number of customers using e-commerce applications by adopting Internet Banking, banks can boost of having the comparative advantage of winning customer loyalty, gaining a larger share of the marketing, improving services, providing value added services, increasing efficiency and decreasing costs operationally [3].

Internet banking has in recent times enabled banks to provide their customers relatively convenient and flexible banking, also known as e-banking or online banking. This term does not yet have a precise definition, as many researchers have defined e-banking differently. In general, e-banking refers to bank customers using the Internet to perform financial services such as financial transactions [4]. These services now come in a wide range, including but not limited to conducting fund transfers, managing a checking account, and bill payments. Additionally, e-banking enables customers to gain access to the various banking services without having to physically visit the bank [5]. Internet banking has benefited both banks and customers. The banks are benefiting because the Internet has allowed banks to cut down their operational costs in terms of decreasing physical facilities involving human resources, paperwork, and supporting staff, while the customers are benefiting because e-banking has accorded them speedy access to various financial activities, such as money transfer, payment for utility bills, checking account management [6,7].

As cited by Safeena [8], bank customers can use banking in three overarching ways. The first use is to obtain simple information about services provided by the bank through its website, such as products and policies [9]. The second and third uses are simple and advanced transactions, respectively. Transactional websites are types of Internet banking that enable customers to expressly conduct simple transactions, such as account inquiry. The Simple transactions do not allow users to transfer funds. An advanced transactional website allows customers to transfer funds and access other online financial services and conduct other types of transactions. Today, many countries have integrated the use of the Internet into their traditional banking system. Since the advent of the Internet technology, many banks around the globe are offering Internet services, for instance, Bank of America, Zenith Bank in Nigeria, Citibank, Nations Bank, etc., [10]. These banks offer their customers convenience and flexibility of use, thus contributing to the growth of the bank and popularity of e-banking.

Despite numerous benefits that banks are offering to their customers through online services, online banking has also raised many security issues [11]. Computer hackers, who are persons with specialized skills in illegally breaking into a system or a network for malicious purposes, have developed a variety of elusive methods for stealing online bankers' money. Although there are many advantages of online banking, these security issues often discourage customers from using it, as many customers have found that using e-banking could make their money and other valuable assets prone to risk [11,12]. Since most banks are now offering services to their customers through the Internet, an increasing number of hackers have found it worthwhile and appealing to dedicate their time to carry out fraudulent activities through online banking system. It has been observed in many research studies that security issues, such as "phishing attacks," have been used by hackers to breach customers' e-banking accounts [12,13].

Banks will be putting their customers at risk and eventually drive them away if they do not strengthen the security of their e-banking, as this will make customers not to trust the Internet banking system or diminish customer confidence in the system.

According to Alsayed and Balgrami [14], financial institutions should pay particular attention to securing the information of their own organization, their users, and their finances, which are all forms of sensitive information which hackers can take advantage of, by blocking every security loophole. In terms of phishing, banks must protect their users' confidential data from unauthorized individuals or groups who could inquire after users' bank accounts to conduct fraudulent and malicious activities such as stealing customers' private information, data and ultimately the money. Unfortunately, the current lack of security protection amongst most online banking is conducive to phishing attacks, for example an unprotected system may prone to virus and Trojan attacks, in that a Trojan which drops a link and appears with its class ID to be a browser helper object can intercept any user information entered into a web page even before it is encrypted and sent on transit [15].

Online banking transactions involve sensitive customer data and are carried out via public network and this introduces challenges for security and trustworthiness. Hackers can take advantage of any security lapse on a public network and launch attacks. Hackers have become increasingly proficient in unleashing terrible attacks such as spoofing, phishing, pharming and keystroke capturing [16]. Any Internet banking technology must solve the issues of authentication in order to curb the menace of impostors by using a tamper resistant smartcard to identify legitimate users and it means the system must ensure that only legitimate persons can be granted access to online banking services; Confidentiality, which means, customer information cannot be viewed by any person accept the legitimate owner of the account. Integrity, which means the information cannot be modified by third unauthorized parties; and non-repudiation, which means, any online transactions carried out by two or more persons cannot in any way be denied by any of the parties involved [17]. All banking identification and authentication procedures may be grouped according to their tendencies resist major forms of attack such as offline credential stealing attacks, online channel breaking attacks and content manipulation (Man-in-the browser) [18].

This research focuses on designing a new online security framework that solves the issues of authenticity, confidentiality, integrity and non-repudiation in an e-banking system.

1.1 Research Motivation

The need for stronger online security system in an Internet banking environment has become necessary to ensure customers security, confidence, and acceptance of this widely used channel for financial institutions. For instance, the standard means of user authentication such as username and password are no longer strong enough to ensure appropriate access control to customers' account and personal information. Hence, this research is motivated by need for financial institutions to be able to strengthen user authentication and address other security challenges in an online setting in order to protect customers and boost their confidence.

1.2 Conceptual Framework

The term Online Banking System can be thought to mean a service that enables customers to carry out financial transactions. Online banking can be used to implements a designed software which allows clients to have access to critical information anywhere, any time. A fundamental feature of e-banking software is its ability to track various transactions ranging from making deposits, withdrawals, to making transfers, etc. and at what period of time the transact takes place. When an internet banking system is created it gives customers the unique access and ability to maximize the use of all the unique features from anywhere without the need to physically visit the banking hall [19]. Moreover, customers have the liberty to gain access to a comprehensive overview or complete statement of their financial status and also undertake various other transactions like fund transfer. The term e-banking is used to describe the new age banking technology [18]. E-banking is synonymous with online banking which is an off shoot of PC banking. E-banking relies on Internet as its measure delivery channel through which the conduct of banking operations are effected. For instance fund transfer, payment of bills, checking savings account balances, payment of mortgages and purchase of financial instruments and deposits of financial certificates [20]. However, it is difficult to categorically state who enjoys convenience more than the other between the banks and customers; but one paramount thing is that it contributes immensely in increasing efficiency and effectiveness of all banking operations thereby giving convenience to the side of the customers; thus making it possible for customers to carryout transaction in different parts of the country among different banks. This is the reason for the explosive growth of e-banking making it go a long way in the transformation of traditional banking practices [21]. According to Maholtra and Singh [22], this transformation has led to a paradigm shift in marketing practices and resulting to excellent performances in the banking industry. Service delivery in the banking world can be provided efficiently only where the background parameters are operationally efficient. Efficient background operations may be conducted conditionally if they integrated by electronic system. The essential components making up the system includes data, software, hardware, network and people-ware. Online banking customers derive satisfaction if the system provides them with needed convenience in the cause of transaction with the bank, while relaying on Internet enabled electronic system to facilitate the process of fetching operations result [23]. In an online banking environment, the most significant and critical element to be secured is the customer's information (mainly customer's banking credentials). Hence, the customer (user) is the weakest link in the system and is often vulnerable to attacks. This why the entire online banking system is usually built with very strong security since even, a very slight attack against it could pull down the whole system with devastating effect. Most a times, the context of online banking the bank server is usually built with the strongest security level techniques so as to make it less vulnerable to threats and attacks [24]. The bank's database is usually not kept on a single server, but in parts across the network on different system. This makes a case for distributed database generating high security concerns due to more systems becoming prone to attacks.

In online banking, the probability for the end user to be vulnerable and exposed to threats of attacks by hackers is very hard. A recent study revealed that end-users stand to lose the confidentiality of very critical and important banking information as a result of fraud or any malicious and authorized access to its record [25]. A similar study conducted by Jassal and Sehgal [26], revealed that the end-user always expresses concerns that his personal data could be corrupted due to the unhealthy activities of viruses, hackers and system crash. These trends could in turn cause end users to lose confidence and trust in maximizing the use of online banking. Other threats against online banking include phishing, pharming, man-in-the-middle-attack, man-in-the-browser-attack, and malware attacks. Phishing, entails any activity that makes the user surrender his banking credential or related personal information to fake websites while pharming is concern with the activity of modification of DNS entries which may result in making users to be directed to a wrong website [27]. Man-in-the-middle (MitM) attack is a kind of attack where hackers tend to listing to communication flows between the client and the server by standing in between the sender and receiver so as to access and control information flow causing undue modification and forwarding it to the receiver as a form of threat and this could be avoided using a public key infrastructure (PKI, say a tamper resistant smartcard) with some trusted digital certificate authority issuing matching digital certification that prevents the session from being hijacked [28]. One way attacker use is to involve the pharming attack since it installs malicious code into the system in order to compromise the DNS and redirect users to spoofed websites which has the tendency of trapping customer credentials and provide enabling environment for malicious activities to the detriment of the user [29]. Man-in-the-browser (MitB) on the other flip clearly depict a scenario where a Trojan horse lunches attacks by redirecting the user to a fake site with the aim of getting access to the customer credential or other useable information and this could be prevented by using an offline smartcard in a card reader so that user credentials a pre-encrypted before they are entered into the browser [30].

End- users may be concerned with malicious attack since it can "poison" the system's host files and the DNS – and this is made possible since the attacker is able to trap user credentials and other information. In view of the instances cited, security and privacy issues regarding online banking should be handled seriously. This is important so as to develop a comprehensive, reliable and well defined security parameters that give end-users the desired confidence and trust in online banking [31].

Generally, attacks directed at the banking server are usually not successful except a very common attack, denial of service which ensures that resources never get to the intended users [19]. This happens whenever the network is flooded with request. In other words, it is also referred to a scenario in which a resource, for instance, e-mail or a website that does not seem to be functioning correctly. A user could have the authentication credentials of his account which the hacker is targeting directly. It can itself be hacked using credential stealing attack. It can in many ways be hacked by using credential theft, phishing, pharming and social engineering. In credential stealing attack the user's personal information (used in authentication process) is stolen. This kind of attack can only be successful if a weak authentication is used [32]. Credential stealing employs the use of malicious software to carry out the attack in which case, disruption of the normal operation of the user's computer and gathering of user's sensitive letter is carried out by the malicious software. They are also referred as malware. Malware takes different forms such as script, code, or software. One of the commonly used method of intruding security is termed social engineering [33]. In social engineering, laymen are usually targeted. It has to do with tricking users so as to break into their security. It is imperative that for the attacker to succeed using social engineering, he must gain to an extend the confidence and trust of the user. Social engineers capitalize on the ignorance or weakness and general helplessness on part of the people (user) to inflict damage. An important aspect that also promote social engineering has to do with the peoples laxity in keeping up with modern information technology trends. Social engineering also depend on the fact that online banking users are not well informed about the value of their information and they do not care much about protecting it [19]. These social engineers are always in search of dumpsters to get valuable information, try to memorize access codes and always looking guessable passwords based on the fact that people have a natural flair for choosing password that are related to their date of birth, social security numbers e.t.c. it attacks are made possible because social engineering does not require any technical skill, except some simple trick [19]. Another attack method for accessing username, password, credit card number and other vital information is called Phishing [33]. It takes place when e-mails containing malwares are sent to user's computer. In this case the user is made to trust a fake website that looks exactly the same as the original one and made to log into it. Immediately the user logs onto the fake sight his confidential information disappears phishing uses the log in page of fake website that is similar to the actual website and in most cases, the link of that web page is contained in the e-mail being sent to the user and as soon as the log into that web page all personal information becomes hacked automatically [19]. Supposed after checking your e-mail you discover that there is a message from your bank say, Big Bank, even though you have been getting e-mails from the bank before but this one appears to be suspicious as it threatens to close down your account if you do not reply as soon as possible. This is a clear example of phishing- a known method of online identity theft. Apart from stealing personal and financial data, Phishers have the tendency to infect computers with viruses [31,32].

2. METHODOLOGY

2.1 Materials and Methods

The approach used in this research, is the object oriented analysis and design (OOAD) method since the system components captured for the design are closely related and the use of UML as a visual language allows for modelling of processes, software and system in order to clearly express the design of the system architecture.

Interview was administered to 120 bank IT staff and Internet banking customers (32 IT staff and 88 customers) drawn from 21 out of the leading 25 new generation banks in Nigeria. Also, observation of the operations of the existing system was carried out all in a bid to elicit the needed information to develop the new system. In addition, about 40 journal articles relating to Internet banking security were reviewed.

In order to derive the purpose of actualizing the set aim and objectives of this research, Security Framework for Online Banking system was developed. For this research, the framework was actualized using Hypertext Markup Language (HTML5), Cascading Style Sheet (CSS3), JavaScript, PHP, and Structured Query Language (MySQL). In designing the front- end interface, the Hypertext Markup Language (HTML 5), Cascading Style Sheet and JavaScript were used and for the back-end, PHP server side scripting, MySQL runs on the server. The system was tested using XAMPP server.

2.2 Building the System

The architecture employed for this system is made up of a complete range of robust high performance client and server platforms with integrated enterprise application and data extendable to banking customers in real-time.

The client system include a Personal Computer (PC). A server is used to maintain connectivity to enterprise resources for the online banking solution that includes the customer's service, standing order and payment of bills.

Also an offline card reader was used to generate customer's RESPONSE; as PKI- tamper resistant smartcard is entered, the customer ID_C and the CHALLENGE using cryptographic mechanisms, are encrypted to generate the appropriate RESPONSE string. This RESPOND string so generated together with other banking credentials were encrypted using AES algorithm and this encrypted data are embedded in an

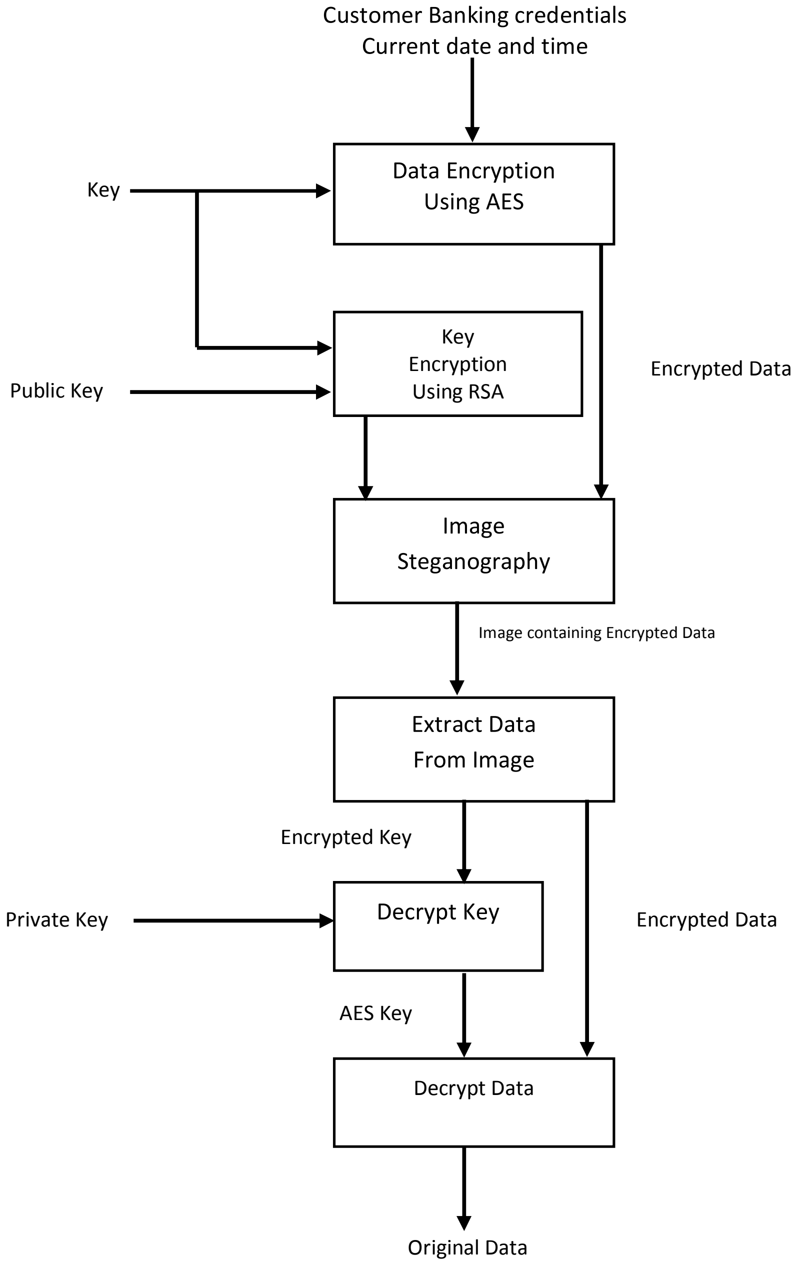


Fig. 1a. Encryption and steganographic process flow modeling

image using the Least Significant Bit (LSB) algorithm. The choice of the LSB algorithm is not far from its simplicity and being truly secure as it is not easily possible to extract data from the image without the key. This image is used by the client to carry out the banking transaction, thus guarantee that the client's details are securely transmitted over the network. After the process above, the encrypted user details and credentials are then extracted using AES decryption technique after which a validation of the client's credentials is carried out. In general, the CHALLENGE-RESPONSE system would be built upon a tripetite security model which is made up of the SSL (layer 2) tunnel and two other tunnels given one at the IP layer (IPsec) (layer I) and another, the application layer of TCP/IP networks (ALS) (layer 3) as shown in Fig. 1(a) and 1(b).

2.3 Analysis of the Existing System

The existing system for online banking requires the user to enter his card details it the system web browser. The information entered is then encrypted with higher end key and the entire encoded details forward and sent to the bank server over the Internet network. However, even the manner of encrypting data and algorithm utilized for the system is certified to have a very high level of security, they could still be hacked by seasoned hackers. It is basically so because the data just got encrypted with a key and it will not be difficult to hack the key. Apart from using encryption mechanism to hide the key, there are no other mechanism to consolidate the hiding of such data. Adding a new stronger, security feature termed one time password (OTP) is provided and sent to a registered mobile phone number tied to the card. All these are to guarantee that any person who uses the card is a legitimate owner and no fake. The generation of OTP, however, does not take place on specified international sites and because of network problems in many cases. Given such events the user is expected to turn to the use of his master key so as to complete the transaction. One major snag of using the master key has to do with the fact that there is no OTP generation pattern for the given transaction so, hacking the master card may be utilized for so many fraudulent and malicious transactions.

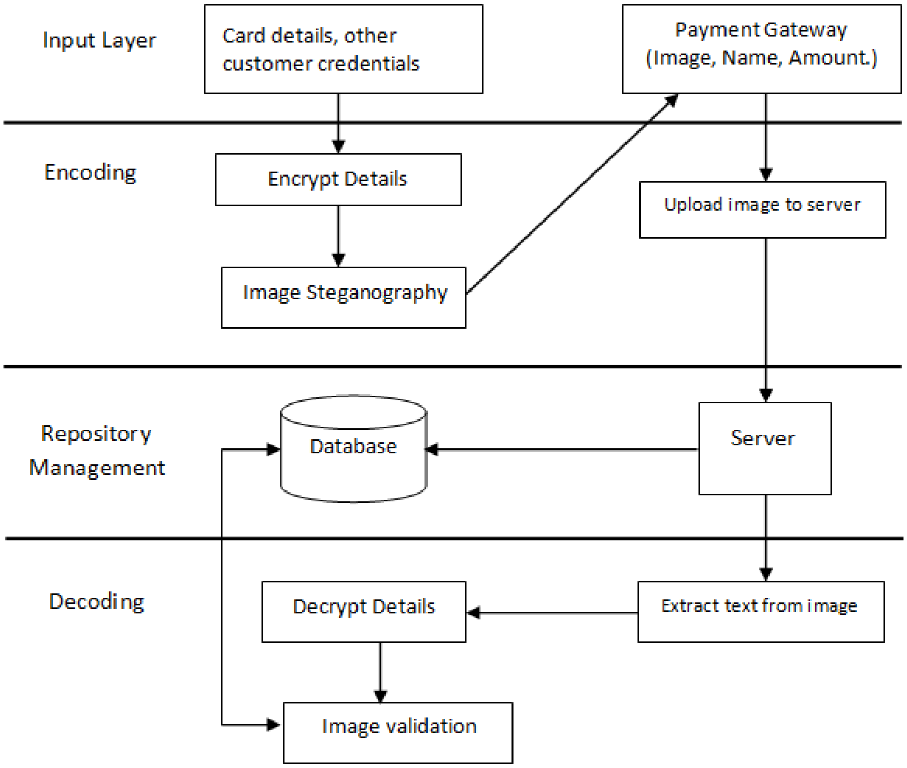


Fig. 1b. Network system architecture to ensure user details are securely transmitted over the network

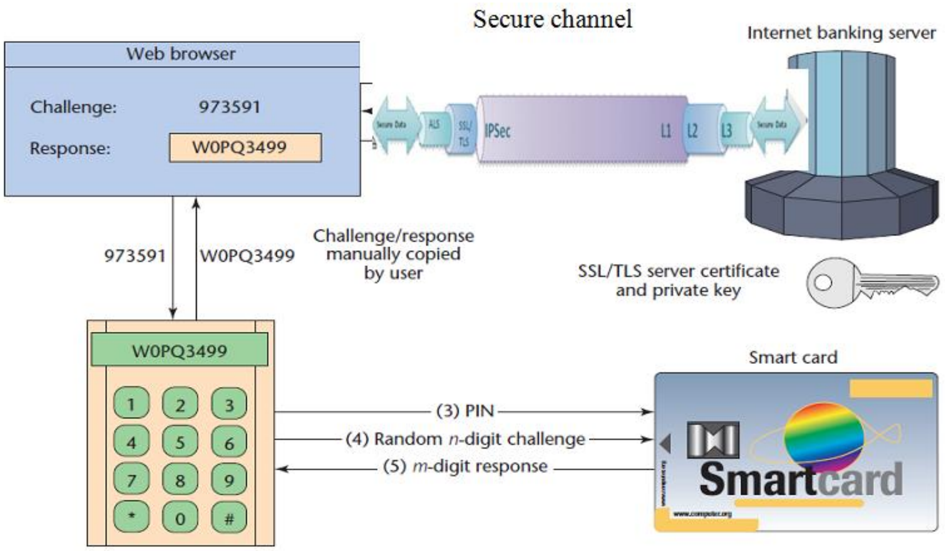


Fig. 2a. Challenge – response based on tripartite security framework [15]

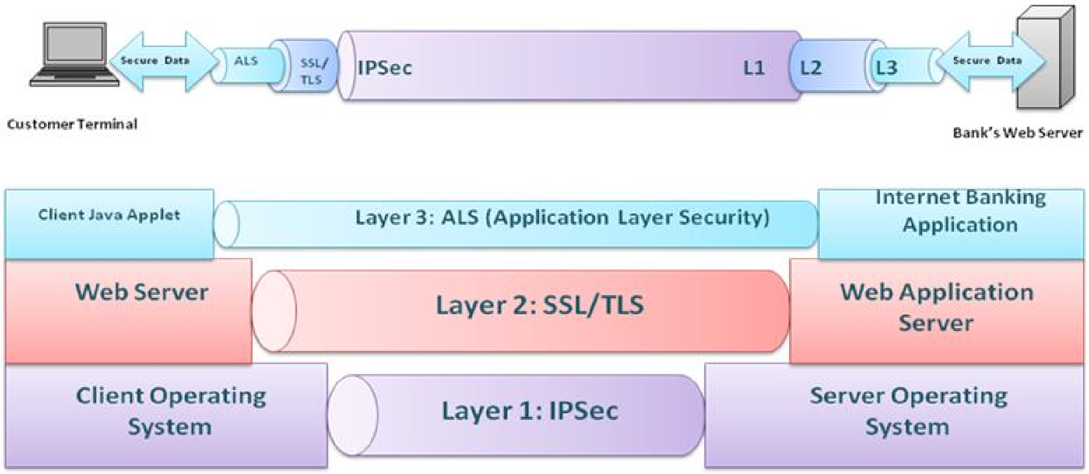


Fig. 2b. Tripartite security framework for internet banking [34]

2.4 Analysis of the Proposed System

This system deals with preventing fraud using cryptography for the encryption user card details and other banking credentials in conjunction with steganography hiding the encrypted details in an image which is responsible for actualizing the transaction. The steganographic mechanism used prevents the possibility of hacking customer credentials which is a major drawback of the existing system.

Also, customer credentials are never sent directly into the browser before encryption. This is because pre-exposing user credentials makes them vulnerable to Trojan, man- in- the – browser- attack and so many other related attacks; instead credentials are first encrypted in the card reader before entering them for transaction. The security strength and improvement of the new system is based on strengthen SSL tunnel with two other tunnels – an arrangement which put one at the IP layer and another at the application layer of TCP/IP networks.

2.5 UML Modeling for the Proposed System

The unified modeling language (UML) was used in capturing and modeling some of the functionalities and artifacts in the application.

This is because the UML serves as a visual language that provides a means to visualize, construct and document the artifacts of software systems. The use case diagram used for the system is contained in Fig. 3.

The Use Case UML diagram for the Proposed Challenge-Response security system is shown in Fig. 3.

2.6 Process Model for the Proposed System

Step 1: Connect browser to sever.

Step 2: Enter account number

If account number exist in database

Then, Server supplies CHALLENGE#
Else, the message, Invalid account number is prompted

Step 3: Insert smart card into card reader.

Step4: Enter PIN# to authenticate smart card.
If PIN# is correct

Then a welcome message is prompted

Else the message incorrect PIN# is displayed

Step 5: Enter CHALLENGE# into smart card.

Step 6: Enter encoded “Response” If “RESPONSE” match CHALLENGE# Then customer is authenticated. Else GOTO step 2.

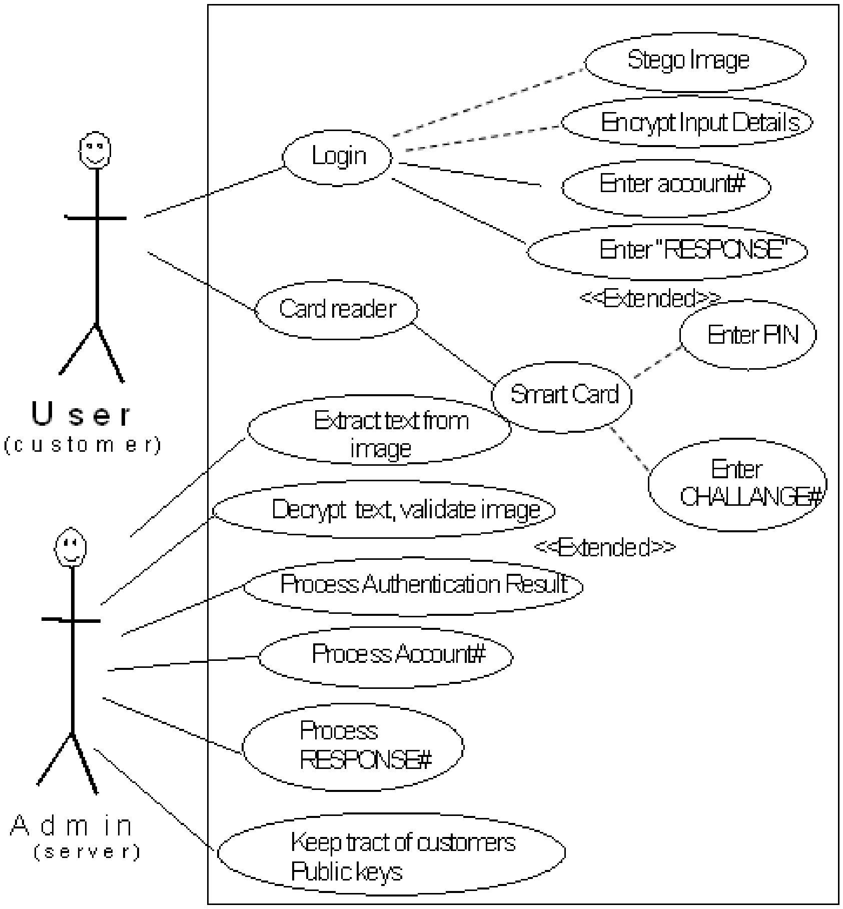


Fig. 3. UML use case diagram for challenge-response security system

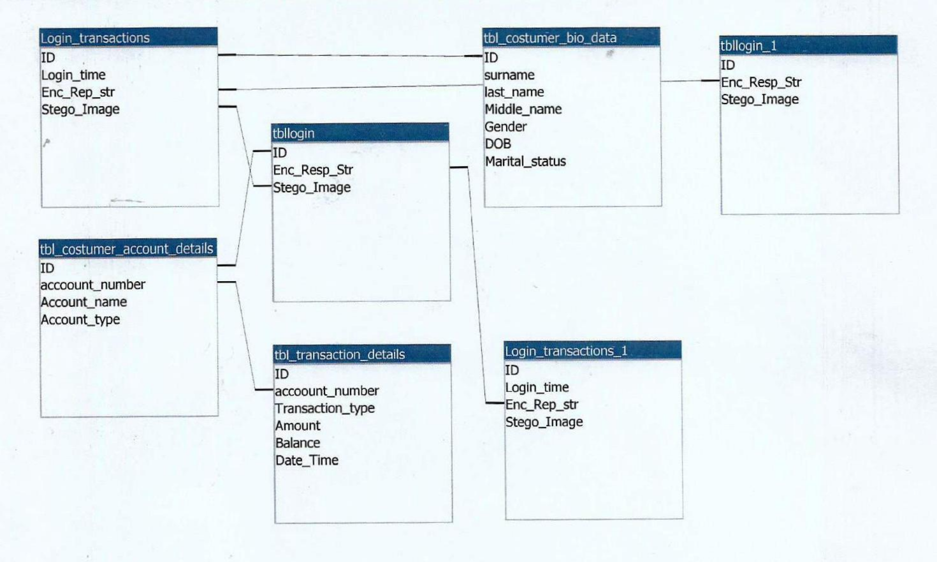
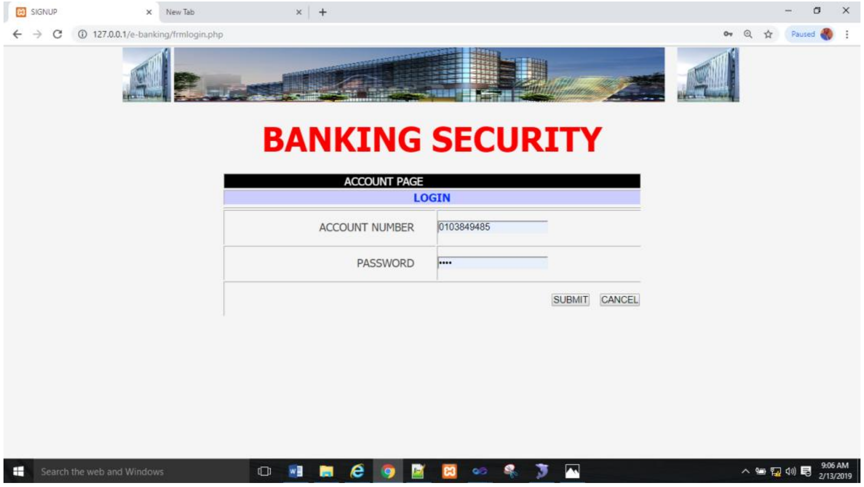


Fig. 4. Entity relationship diagram (E-R) of the system

2.6.1 Captured screen shorts during implementation

The implementation stage involves the transformation of the research aim and objectives using modelling tools such as UML usecases and the process flow model into real process flow of information. The various screen shots captured during the implementation of this system are given below:



BANKING SECURITY

ACCOUNT PAGE

LOGIN

ACCOUNT NUMBER 0103849485

PASSWORD ••••

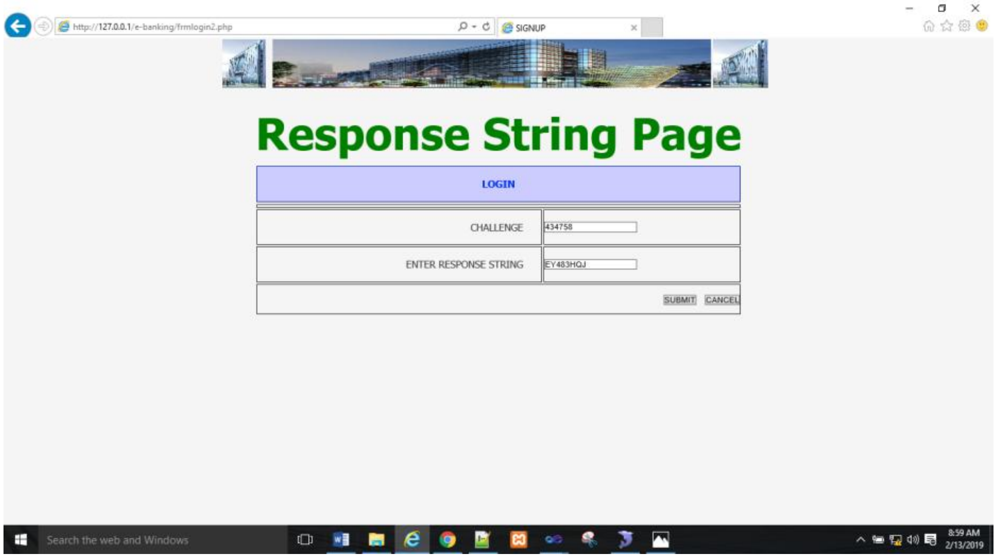
SUBMIT CANCEL

Fig. 5. CHALLENGE generation page (where customer enters his account number to generate the CHALLENGE)

3. DISCUSSION OF RESULTS

From Fig. 5 shows the challenge prompt page, was obtained by successfully entering the customer account number in the account confirmation page. After a successful login, the bank server gets the account number and then checks to ascertain its validity in the database, if it is a valid account number the server supplies CHALLENGE (N) which is bound to the account number it received, otherwise an error message is prompted.

The RESPONSE string confirmation page as shown in Fig. 6 was obtained by entering the CHALLENGE (N) obtained, into the offline smartcard and encrypting it with the customer identity (IDc). The RESPONSE string could only come from that specific customer device and could only be based on the use of that particular bank-issued smartcard. This encrypted message (using AES and encryption key using RSA) (RESPONSE string) is embedded in an image generated and sent to the web bank server and upon receipt, bank authentication serer decrypts the stego-image containing the data, extract the data, decrypts it and validate the image using the shared secret key and compares the result with what the customer has sent. If there is a match with prestored details in the database, then the customer is authenticated in to Transaction page, which is in conformity with the assertion of [34] who stated that building a trusted and secured environment entails crating a Challenge-Response scheme that authenticates both the customer and the bank.


http://127.0.0.1/e-banking/frmlogin2.php
SIGNUP
LOGIN
SUBMIT
CANCEL
Search the web and Windows
8:59 AM
2/13/2019

Response String Page

CHALLENGE 434758

ENTER RESPONSE STRING EY483HQJ

Fig. 6. RESPONSE string entry page. (Where the CHALLENGE generated is used to produce the RESPONSE string)

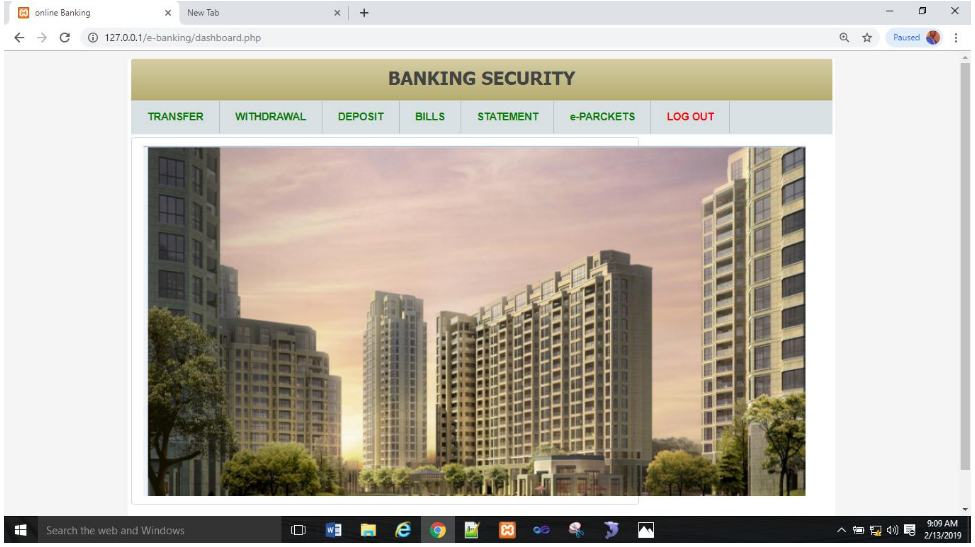
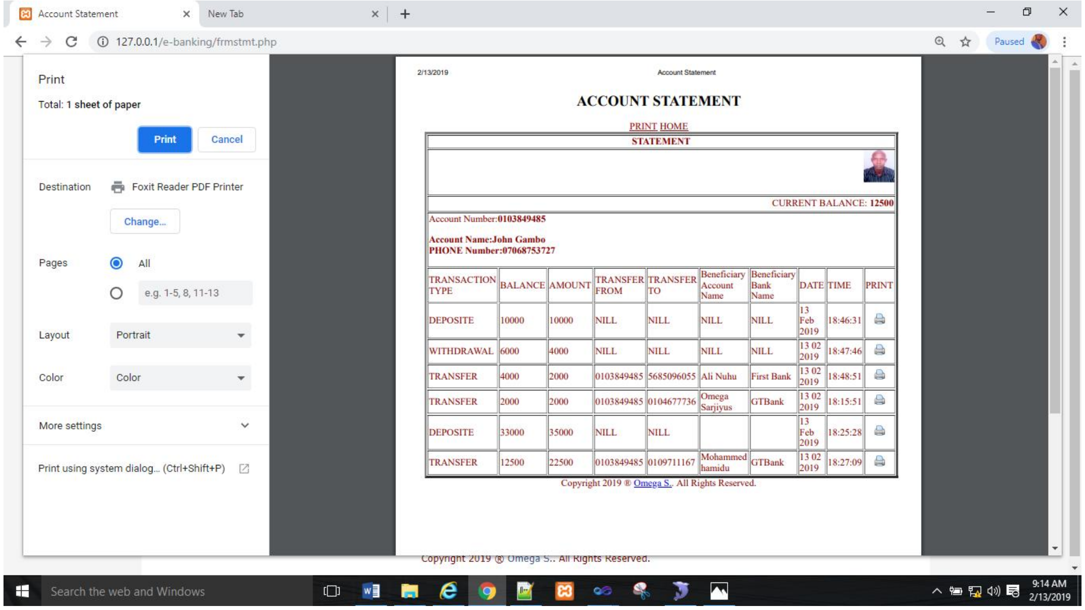


Fig. 7. Customer transaction page. (Which is obtained after successful authentications between customer and the system)


Account Statement
New Tab
127.0.0.1/e-banking/frmstmt.php
Paused
Print
Cancel
Change...
More settings
Print using system dialog... (Ctrl+Shift+P)
Search the web and Windows
9:14 AM
2/13/2019

Print

Total: 1 sheet of paper

Destination Foxit Reader PDF Printer

Pages ● All ○ e.g. 1-5, 8, 11-13

Layout Portrait

Color Color

2/13/2019 Account Statement

ACCOUNT STATEMENT

PRINT HOME

STATEMENT

CURRENT BALANCE: **12500**

Account Number:**0103849485**

Account Name:John Gambo
PHONE Number:07068753727

TRANSACTION TYPE	BALANCE	AMOUNT	TRANSFER FROM	TRANSFER TO	Beneficiary Account Name	Beneficiary Bank Name	DATE	TIME	PRINT
DEPOSITE	10000	10000	NILL	NILL	NILL	NILL	13 Feb 2019	18:46:31	🖨
WITHDRAWAL	6000	4000	NILL	NILL	NILL	NILL	13 02 2019	18:47:46	🖨
TRANSFER	4000	2000	0103849485	5685096055	Ali Nuhu	First Bank	13 02 2019	18:48:51	🖨
TRANSFER	2000	2000	0103849485	0104677736	Omega Sarjiyus	GTBank	13 02 2019	18:15:51	🖨
DEPOSITE	33000	35000	NILL	NILL			13 Feb 2019	18:25:28	🖨
TRANSFER	12500	22500	0103849485	0109711167	Mohammed hamidu	GTBank	13 02 2019	18:27:09	🖨

Copyright 2019 ® Omega S.. All Rights Reserved.

Copyright 2019 ® Omega S.. All Rights Reserved.

Fig. 8. Account summary page

Consider Fig. 7, which is the Transaction page was obtained as a result of the successful decryption of the initial account-bound CHALLENGE by bank's server to match the one in the encrypted RESPONSE.

Clearly, it can however be deduced from Fig. 7 that all the steps taken (from entering customer account number to RESPONSE string generation) aimed at making customers data at the transaction page secured. At the transaction page therefore, a high level of authenticity, confidentiality, integrity and nonrepudiation is thus maintained in accordance with assertion of [16] who stated that any Internet banking system must provide authentication, confidentiality integrity and nonrepudiation.

Furthermore, Fig. 8 which is the Account summary table, was obtained by selecting and clicking the account summary option in the transaction page menu. The account summary displays the result of transaction (for instance money transfer) carried out by the customer. It displays the account number, name of the customer, phone number, amount transferred, the day and date of such transfer including the time the transaction was carried out. The result in Fig. 8 is in accordance with the assertion of [34] who stated that every transaction made in a secure environment is traceable and verifiable, and so, cannot in any way be denied by either of the parties involved.

In addition to authentication and nonrepudiation, confidentiality and integrity have been built up in the research. The environment has thus been shown to counter all forms of credential-stealing and Channel-breaking attacks.

4. CONCLUSION

Implementing the tripartite security model of this research serves to offer safe and secure e-banking platform in which case, transactions are secured from all forms of threats and malicious attacks moreover, the use of steganographic mechanisms further consolidates security of data on transit within the network. Finally, the use of hard token public key infrastructure (PKI) offline card readers to provide mutual authentication ensures that only qualified persons can access the system. The use of smart card however, pre-stores and encrypts customer credentials to generate the RESPONSE string which prevents credentials stealing attacks and man-in-the browser attacks since credentials are not directly entered into the web browser, but are entered only in an encrypted form (the response string, and transits as a stego-image within the network).

4.1 Contribution to Knowledge

Students on research in the area of information security and building security for Internet banking systems can review the study and expand further on it. The results of this study will enable banks to critically assess their services, their competitor service, determine the extent of matching key factors in Internet customer expectations and identify areas and means for possible improvements.

COMPETING INTERESTS

Authors have declared that no competing interests exist.

REFERENCES

1. YeeLoong Chong A, Ooi K, Lin B, Tan B. Online banking adoption: An empirical analysis. International Journal of Bank Marketing. 2010;28(4):267–287.
2. David C. Chou, Amy Y. Chou. A guide to internet revolution in banking, the E-Commerce revolution. Information System Management. 2000;17:1-7. [10]Whitten
3. Lichtenstein, S. and Williamson, K. Understanding consumer adoption of internet banking: An interpretive study in the australian banking context. Journal of Electronic Commerce Research. 2006; 7(2):50–66.
4. Jolly V. The influence of internet banking on the efficiency and cost savings for banks' customers. International Journal of Social Sciences and Management. 2016;3: 163-170.
5. Safeena R. Customer perspectives on E-business value: Case study on Internet banking. Journal of Internet Banking and Commerce. 2010;15:1-17.
6. Sharma S. A detail comparative study on e-banking VS traditional banking. International Journal of Advanced Research. 2016;2:302-307.
7. Konoth RK, van der Veen V, Bos H. How anywhere computing just killed your phone-based two-factor authentication. In Proceedings of the 20th International Conference on Financial Cryptography and Data Security; 2016.
8. Razak LT. The effect of security and privacy perceptions on customers' trust to accept internet banking services: An extension of Mohammed TAM Al-Sharaf A, Ruzaini A, Arsha Emad Abu-Shanab, Nabil Elayah. Faculty of Computer Systems and Software Engineering, UMP; 2016.
9. Vaciago G, Ramalho DS. Online searches and online surveillance: The use of t9 rojans and other types of malware as means of obtaining evidence in okcriminal proceedings, Digital Evidence & Elec. Signature L. Rev. 2016;13:88.
10. Chiu CL, Chiu JL, Mansumitrchai S. Privacy, security, infrastructure and cost issues in internet banking in the Philippines: Initial trust formation, International Journal of Financial Services Management. 2016;8:240-271.
11. Balk R, Yap BK, Loh C, Wong HD. To trust or not to trust: The consumer's dilemma with e-banking. Journal of Internet Business. 2009;6:1-27.
12. Leukfeldt ER, Kleemans ER, Stol WP. Cybercriminal networks, social ties and online forums: Social ties versus digital ties within phishing and malware networks. British Journal of Criminology. 2016;9.
13. Arachchilage NAG, Love S, Beznosov K. Phishing threat avoidance behaviour: An empirical investigation. Computers in Human Behavior. 2016;60:185-197.
14. Alsayed AO, Balgrami A. E-banking security: Internet hacking, phishing attacks, analysis and prevention of fraudulent activities. International Journal of Emerging Technology and Advanced Engineering. 2017;1(7):109-112.
15. Hiltgen A, Zurich TK, Weigold T. Secure internet banking authentication. IEEE Journal of Security & Privacy. 2006;4(2): 21–29
16. Devadiga D, Jain H, Kothari H, Sankhe S. E-banking security using cryptography, steganography and data mining. International Journal of Computer Applications. 2017;164(9):26-28.
17. Ruman K, Phaneendra. Implementation of methods for transaction in secure online banking. International Journal of Technical Research and Applications. 2015;3(4):41-42.
18. Khrais LT. Highlighting the vulnerabilities of online banking system. Journal of Internet Banking and Commerce. 2015;20(3):1-4.
19. Kaur N. A survey on online banking system attacks and its counter measures. International Journal of Computer Science and Network Security. 2015;15(3):57–60.
20. Mohammed SK, Siba SM, Sreek U. Service quality evaluation in Internet banking: An empirical study in India, International Journal of Indian Culture and Business Management. 2009;2(1):27-31.

21. Gonzalez ME. An alternative approach in service quality: An e-banking case study. Quality Management. 2008;15:41-48.
22. Maholtra P, Singh B. Determinants of Internet banking adoption by banks in India. Journal of Emerald Internet Research. 2007;17(3):323-339.
23. Peotta, Holtz B, David D. A formal classifycation of internet banking attacks and vulnerabilities. International Journal of Computer Science & Information Technology. 2011;3(1):186-197.
24. Laukkanen P, Sinkkonen S, Laukkanen T. Consumer resistance to internet banking: Postponers, opponents and rejectors. International Journal of Bank Marketing. 2008;26(6):440–455.
25. Jassal RK, Sehgal RK. Online banking security flaws: A study. International Journal of Advanced Research in Computer Science and Software Engineering. 2013;3(8):1016-1021.
26. Karapanos N, Capkun S. On the effective prevention of TLS man-in-the-middle attacks in web applications. USENIX Security Symposium. USENIX Association. 2016;23:671-686. Cain C. Analysing on man in the browser attack. SANS Intitute InfoSec Reading Room. 2014;1-23.
27. Eriksson M. An example of a man-in-the-middle attack against server authenticated SSL-sessions. International Conference on Applied Cryptography and Network Security; 2003.
28. Whitten A, Tygar JD. Why Johnny can't encrypt: A usability evaluation of PGP 5.0. Usenix Security; 1999.
29. Cain C. Analysing on man in the browser attack. SANS Institute Info Sec Reading Room. 2014;1-23.
30. Mahmadi FN, Zaaba ZF, Osman A. Computer security issues in online banking: An assessment from the context of usable security. International Engineering Research and Innovations Symposium. 2016;2-3.
31. Kuppuswamy P. Enrichment of security through cryptographic public key algorithm based on block cipher. 2011;2(3). [ISSN : 0976-5166]
32. Srivastava SS, Gupta N. A novel approach to security using extended Playfair cipher. International Journal of Computer Applications. 2011;20(6).
33. Alshehri S, Radziszowski S, Raj RK. Designing a secure cloud-based EHR system using ciphertext-policy attribute-based encryption. ACM Digital Library. IJCS; 2011.
34. Lasheng Y, Mukwande P. Three-tier security model for e-business. Proceedings of the Second Symposium International Computer Science and Computational Technology (ISCSCT). 2009;114-119.

Peer-review history:
The peer review history for this paper can be accessed here:
http://www.sdiarticle3.com/review-history/47953