International Journal of Innovation, Creativity and Change. www.ijicc.net
Volume 6, Issue 8, 2019

E-Banking Fraud Detection: A Short Review

Mostafa A. Ali[a*], Nazimah Hussin[b], Ibtihal A. Abed[c], [a,b,c]Azman Hashim International Business School, University Technology Malaysia, Kuala Lumpur, Malaysia.
Corresponding Author Email: [a]mostafa1988@graduate.utm.my, [b]nazimah@ibs.utm.my, [c]ahmed-1988@graduate.utm.my

E-banking gives customers a lot of satisfaction in terms of getting a better service quality; it also gives banks a competitive advantage over the other players in the sector. However, the security of e-banking has received attention due to the fraudulent behaviour of fraudsters; the absence of adequate e-banking security has kept many people away from the service till today. In this paper, a review of the security challenges associated with e-banking has been presented. Equally, the challenges and characteristics of e-banking fraud have been mirrored. This paper also reviewed different types of fraud and attacks detection systems, as well as some preventive measures in place to secure e-banking services. The different techniques and models used for e-banking security were ranked in this study based on an expert opinion. From the results, "Transaction Monitoring" was identified as the most effective model while the worst models based on the respondent's opinions were "Virtual Keyboards", "Browser Protection", and "Device Identification". This paper is organized into sections; the first section introduced the topic of interest in this paper while the second section presented the background of e-banking. The literature review was presented in the third section while a conclusion was presented in the last section of the paper.

Key words: *E banking, Quality service, Security, Fraud Detection.*

Introduction

The rapid development witnessed in global information infrastructure within the past few decades, especially in the areas of computer and information technology (telecommunications systems and the Internet) has brought electronic commerce development to a global stage. These developments have facilitated the effective interaction between business people and their customers, and with other corporations within and outside their industries (Han and Kim, 2019; Park, 2079). E-commerce is a platform that integrates data management, communications, and security services to ensure an effective exchange of information between business partners, to satisfy customers' needs, and achieve a competitive advantage (Abu-Shanab and Matalqa, 2015). In the banking sector, just like in most business fields, ICT is used to provide customers with value-added services and security (Abu-Shanab and Matalqa, 2015; Diniz et al., 2012). Their e-banking platform ensures effective communication between them and their customers, facilitating the provision of numerous customer-related services. E-banking is also referred to as electronic banking, online banking, or virtual banking, and with the existence of numerous labels in the literature, they all point towards ICT-based banking transactions. E-banking refers to the provision of banking services from anyplace outside the bank premises (Sepehri-Rad al., 2019; Möckel and Abdallah, 2010).

However, as envisaged, e-banking is associated with different challenges which are not only related to bank management, but also to both international and national supervisory and regulatory authorities. The major issue associated with e-banking comes from the increased trans-national transactions on its platform, as well as the heavy dependence on ICT to provide banking services (Abu-Shanab and Matalqa, 2015). The other challenges come from the regularity, legal, operational, reputational, inconvenience, and security perspectives. The major problem facing most financial institutions is how to achieve a safe and secure ICT environment (Alaba et al., 2018) as it determines the security of online banking transactions. With the number of online financial transactions conducted on daily basis globally, bank frauds and cyber-crimes are on the increase as many skilled hackers keep manipulating online banking information systems to hack into private and business accounts. Such threats can come from both within and outside the system, making it necessary that bank administrators must put in place appropriate measures to ensure the confidentiality of their customers' data, as preserve the integrity of the online banking system (Guo et al., 2018).

This paper presents a comprehensive review of the issues associated with the security of e-banking and addresses the importance of ensuring the security of such systems. Furthermore, the common types of frauds encountered on e-banking platforms, as well as the attack prevention and detection systems were reviewed. As earlier stated, this paper is organized in sections; the first section introduced the topic of interest in this paper while the second

section presented the background of e-banking. The literature review was presented in the third section while a conclusion was presented in the last section of the paper.

Background

Understanding of e-banking

E-bank definition

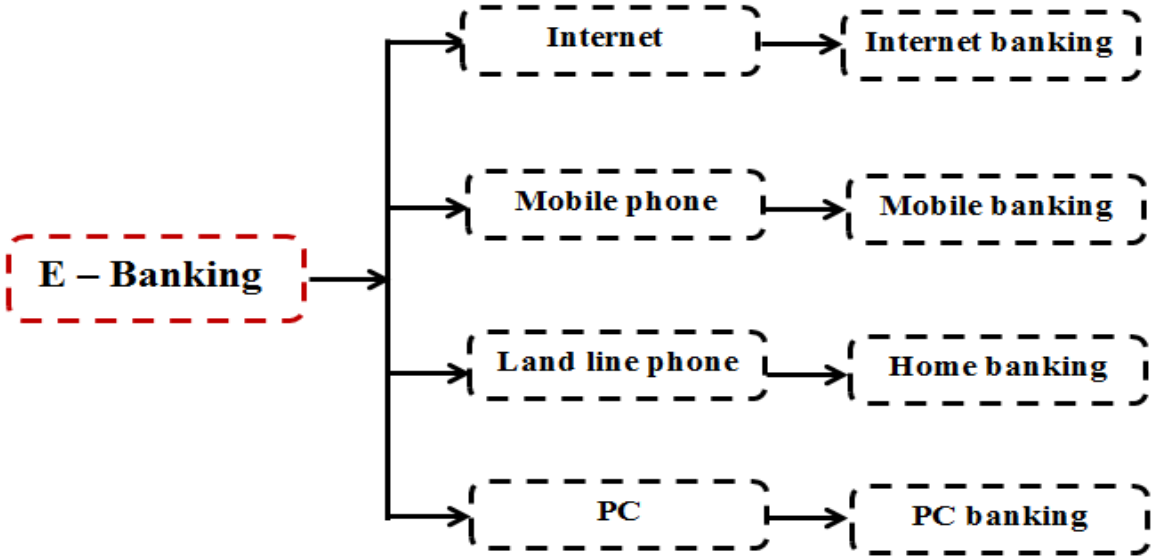
E-banking service is defined as the provision of services via electronic channels (Mu, 2013). Electronic banking or electronic funds transfer is the use of electronic service to transmit money or other services from one account to another over the internet (Shah, 2009). According to Vyas (2009), E-banking is a banking platform that provides services to the customer over the Internet. Electronic banking is an umbrella term for the process by which a customer may perform banking transactions electronically without visiting a brick-and-mortar institution (Drigă and Isac, 2014).

Types of E-Banking Services

According to Drigă and Isac (2014); Chovanová (2006); Wisdom (2012) there are many types of e-banking services:

i. Home banking: It provides customers with information about their personal accounts, giving them access to their banking information and other banking services over the Internet.
ii. PC banking: It is one of the banking services that make it possible for the client to do their transactions using a program.
iii. E-banking service: It is a service that provides customers with their personal banking information at any time.
iv. Mobile banking: It is a device that makes financial services available through a mobile platform. Figure 1. Depicts the E-Banking services.

Fig. 1. E – Banking Services



The various forms of e-banking

According to Elavarasi and Surulivel (2014), there are many forms of e-banking:

i. Automatic Teller Machine (ATM)

An electronic computerized communication gadget that authorizes customers to use IT communication and access their bank accounts and check their accounts without the need for a human bank teller (Hajare et al., 2018).

ii. TeleBanking

Telephone banking is an automated telephone banking service which is convenient and easy to use. The customers can choose any place and time to access their banking information through an interactive voice response system. The benefits of this service are (Mahmood, 2018; Agboola, 1970):

a) Available access at all time.
b) Can review account balances and transactions.
c) Can transmit funds between the linked accounts.
d) Can transfer money to pay for Credit Card account or pay bank loans.
e) Can pay bills.
f) Can organize current and previous statements for savings or payment.

iii. Debit Card

It is a card for "pay now." Debit card transactions make payment directly from the payee to the recipient (Hayashi et al., 2003).

iv. Smart Card

The smart card is a kind of credit card equipped with a microchip which contains all the information about the cardholders' account (Turban and McElroy, 1998).

v. E-cheque

The e-cheque has all the capacity and potential of a paper cheque. It is used in different payments, such as conditional and governmental loans, and it is acceptable in various important fields such as number, coding key, and payer's banking details, the e-cheque works differently from country to country depending on the rules and regulations of each country (Qatawneh et al., 2016).

The services of E-banking

E-banking gives to customers many functions and services in the banking sector; these functions include (Hernando and Nieto, 2017; Mahmood, 2018):

The client can demand their account information, such as the history of their account or the transactions in their account.

i. Balance transfer: The customer can make a transfer to another account in a different country.
ii. Electronic funds transfer: Can make all transfer processes on PC without paper.
iii. Reporting a loss: The customer can report missing accounts or stolen cards to the bank.
iv. Customer account management: The customer can modify his account by changing the password, name of the account, or even demand a new card.

Quality service
Definition

According to Zeithaml et al. (1996); Mahmood (2018), quality service can be defined as a judgment from the customers towards the satisfaction and acceptance of service offered. However, (Kumar et al., 2009) defined quality service as not about the services only, but about the product, time, and the nature of the employee's behaviours towards the client, transmission process, and opinions about the way that the service is performed. So, in our opinion, the quality service is about measuring the product or service satisfaction level from the production to delivery to the customer.

The characteristics of quality service

According to Davis et al. (2009); Newman (2001); Mahmood (2018), the characteristics of quality service are as follows:

i. Intangibility: This is a measure of the relationship between performance and experience.
ii. Heterogeneity: This means that the quality of the service is different from person to person based on performances.
iii. Production and consumption: The quality of a service is a measure of service satisfaction based on the customers' perspective from the production process to the delivery.
iv. Avoidance of price competition: It depends on choosing a strategy that enables competition based on differentiation.
v. Reduction of cost: This focus on quality that prevents errors and reduces maintenance cost.

Factors related to service quality and customers in banks

According to (Zeithaml et al., 1990; Ghimire, 2012; Qadeer, 2014), these are the factors that affect service quality in an institution:

i. Providing a Reliable Service: The bank has to be honest in dealing with customers because reliability is important for customers' satisfaction.
ii. Instilling Confidence in the Customer: Confidence is the responsibility of the bank employees because their behaviour and gentle handling encourage customers to deal with the bank.
iii. Providing physical clues (Intangibles): Such services include after-sales service and product guarantee.
iv. Empathize with the customer: Customers should feel that their needs are important to the organization through the provision of customer's feedbacks on services or products.
v. Responsiveness and Promptness: A quality service means that any request from the customer (delivery or complaint) must be resolved quickly and at a specific time.

Quality service gap

Many problems are encountered when certain services are provided by banks, especially in terms of the quality of service (Taha et al., 2018; Sultana and Rana, 2010). Such problems include:

i. 1. Knowledge gap: This gap happens when the management takes decisions by depending on the information that does not match the needs and expectations of the customers.
ii. Standard gap: This occurs when the service level mismatched the customer's expectation.
iii. Delivery gap: This gap happens when an incompatibility occurs between the service and delivery times.
iv. Internal communication gap: It happens when there is a big difference between the employees who make the product and the delivery time.
v. Perception gap: It is the disagreement between the existing service or product and the customer's expectation.
vi. Illustration gap: It occurs when the service mismatch with the promises to the customers.
vii. Service gap: When the actual services do not match the customers' expectation.

The factors that affect e-banking services

According to Camilleri et al. (2014), the factors that affect e-banking are:

i. Reliability: This is the capability to implement the service with high performance and accuracy.
ii. Responsiveness: Providing services and handling troubles in time.
iii. Communication: The electronic and traditional communication should be clear for the customer and featuring high accuracy and reliability.
iv. Access: It means easy access to the banking and financial information by the customers.
v. Security: It is associated with the safety of transactions process and preventing any unauthorized access to bank accounts and personal information.

Studies related to the security of e-banking

E-banking was first issued as a business model by some of the major banks (such as Citibank and Chase Manhattan) in the 1980s in New York. It was started as a basic set of banking services such as paying bills online and viewing bank statements. However, the platform was expanded to a more sophisticated and comprehensive e-banking service that exist today (Abu-Shanab and Matalqa, 2015; Shannak, 2013). For some time now, e-banking has existed in different forms, such as ATMs and telephone transactions, but recently, it has emerged as a banking platform that grants access to financial transactions to both banks and customers over the Internet. It has also enabled banks to expand internationally, explore new

possibilities, and change their strategic tactics. In this 21st century, the banking industries all over the world have transformed their business ideas and migrated to a new complex and competitive environment (e-platform). A major driver of these substantial changes is ICT. This new technological era has provided banking and financial industries the capability to offer financial services via online platforms to their customers irrespective of their location or time (Tunmibi and Falayi, 2013).

The era of e-banking started in the 1990s when more people gained access to the Internet through a dial-up connection. This technological evolution allowed banks to roll out 24 hours e-banking services to their customers although customers still had reservations concerning e-banking when making serious monetary transactions in those days. Consequently, the banks intensified their efforts toward the development of more security features to protect their online banking platforms. This gave rise to the increase in the acceptability of e-banking by the bank customers in the 2000s, covering most of the banking services (Shannak, 2013).

Various services can be provided via e-banking platforms. Such services include ATMs, credit cards, debit cards, electronic fund transfer (EFT) systems, smart cards, mobile banking, etc. other services can also be provided on e-banking platforms. E-banking platforms have significantly reduced the banks' physical banking costs, especially costs related to information transmission.

E-banking is regarded as an extension of the current physical banks as it involves the retrieval and processing of banking data using computers, as well as initiating direct and remote banking transactions via telecommunication networks. E-banking serves as a platform to addresses most of the customer-related complaints, such as demands for services and other information services (Taha et al., 2019). Different scholars have classified e-banking under e-commerce but placed e-financing under any other form of major financial e-service rendered. E-banking is mainly devoted to telephone banking, Internet banking, and other banking platforms (Chavan, 2013). Although e-banking is the most used term, it is interchangeably used with online banking, virtual banking, phone-banking, cyber-banking, web banking, and remote electronic banking (Shannak, 2013).

Security of e-banking

Several challenges have emerged with the introduction of e-banking, ranging from its acceptance to financial limitations of the new banking system (Usman and Shah, 1970). Several factors have been identified to influence the acceptance of e-banking as a banking platform; such factors include its usefulness, ease of use, trust, social influence, system security, accessibility, cost and time of fund transfer (Mahdi et al. 2019, AbuShanab et al. 2014; Auta, 2010). The most highlighted critical success actor r a successful e-banking

platform is the security of the system since inadequate security will result in potential financial losses, negative media publicity, and punitive measures by regulators. In some research, security is rated as the most crucial issue for online banking services (Auta, 2010; Alaba et al. 2018; Yang et al. 2019).
A study by Jassal and Sehgal (2013) was targeted at unravelling the types of security flaws in online banking platforms that often results in financial losses to both the account holders and financial institutions. The study highlighted the reasons for the security breaches, as well as the involvement of both banks and their customers in enabling unauthorized access online banking networks. On the part of the customers, they often access bank websites through unprotected Web-browsers, thereby, giving chances to the occurrence of cybercrimes. They also pointed out some of the security flaws that could cause financial losses, along with information leakage to unauthorized parties. On the banking websites, security flaws could be in the form of cross-site scripting which usually happens when malicious scripts are injected into a web page by a hacker in a bid to gain access to the website or to pass a command to the database (Jassal and Sehgal, 2013). The other security flaws could be in the form of banking security policies publish online to enhance the users understanding of the security measures in place. Therefore, prospective clients must have a knowledge of the risks that comes with online banking.

The benefits of e-banking and the services that could be provided on its platform have been enumerated by Nigudge and Pathan (2014) when they studied the challenges of e-banking in India. According to the study, legal and security issues are some of the identified issues as evidenced by the lack of legal frameworks, denial of e-documents in courts, increased potential of fraud, and lack of trust. This supported the notion of the importance of strong security measures and business environment advocated by Jassal and Sehgal (2013).

Characteristics of e-banking fraud

Any behaviour by a person that aims at gaining a dishonest advantage over another person is regarded as a fraud (Chakrabarty, 2013). Fraud is any behaviour which by a way of concealment of facts or otherwise, results in an unbalanced gain between two persons. Kovach and Ruggiero (2011) empirically analysed real-world transaction datasets and concluded that several e-banking accounts (including small value transactions) are accessed by a single hacker, with most of the accounts attributable to the increased number of password failures that facilitates fraudulent activities.

Similarly, Wei et al. (2013) investigated online banking frauds in some of the largest banks in Australia and found that most of the banks have the following challenges; i) *Highly imbalanced large dataset*: The high number of daily online transactions on the e-banking

platform and the small number of frauds that occur daily makes fraud detection a tough challenge, ii) *Real-time detection*: The detection of fraud in most online platforms must be done in real time to prevent instant financial losses, iii) *Dynamic fraud behaviour:* Fraudsters keeps changing their tactics in a bid to evade online banking defence systems. There is no single detection system that can defend against the ever-increasing set of online attacks, iv) *Weak forensic evidence:* To understand the nature of fraudulent behaviours, there is a need for some forensic evidence associated with each e-banking transaction, v) *Diverse behaviour patterns of customers*: The users of online banking platforms usually perform various transactions for different purposes in different ways, leading to an increase in the number of genuine transactions which can be simulated by fraudsters, and making it difficult to differentiate fraudulent behaviours from genuine ones.

Types of attacks

Attackers have different aims and objectives, but their major aim is to exploit system vulnerabilities to repeatedly make unauthorized access into a website and cause service denial to the genuine customers (Brar et al. 2012; Davis, 2017; Patel et al. 2017; Agwu, 2018; Weinflash et al. 2018). There are different ways hackers can break into a system, however, the major problems encountered in information systems today are inherent within the computer systems and the setup of the communication networks. Therefore, service providers must protect their networks against different types of online attacks to ensure secure communication over such systems (Taha et al. 2019).

Several studies have strived to categorize online banking attacks into various forms. According to Vrincianu and Popa (2010), the major aims of e-banking security threats are as follows: launch illegitimate use, cause a denial of service, disclose secret information, as well as repudiation. Other studies have classified the common online banking platform attacks (Peotta et al. 2011). For instance, Dalton et al. (2006) suggested a classification of the causes of such attacks into three groups, including legitimate access, device control, and credentials theft. They presented the Attack Tree Model to represent the major efficient attacks and their relationship with each other. This is the simplest and commonly used classification system for online banking system attacks (Peotta et al. 2011).

Various forms of e-banking attacks have been classified by Omariba et al. (2019) to include social engineering attacks, packet sniffers, port scanners, password cracking, denial of service attacks, Trojans, server bugs and superuser exploits. However, Brar et al. (2012) classified attacks into remote, local, and hybrid groups. Remote attacks strive to intercept or redirect a systems' session without modifying the victims' machine. Some of the common types of remote attacks (Brar et al., 2012) include i) *Phishing:* Occurs when an attacker impersonates

a server on a website by setting up a fake version of the targeted website; this website version can contain all the code of the original website. Then, the attacker uses the fake website to send messages to several email accounts to trick the message recipient into visiting the spoofed website and reveal their logon details, ii) *Fishing*: This form of attack is experienced when an attacker contacts his victim and tricks them to reveal secret information using social engineering, iii) *Cloned voice-banking systems:* This is a situation where an attacker clones the voice-banking systems to make them sound like the official systems. This form of attack uses fake e-mails to solicit customer calls to a fake phone number.

Sometimes, local attacks might occur, involving a user opening a real bank website only to observe that the URL in the address bar is not spoofed, and even the secure sockets layer (SSL) padlock might reveal the correct certificate details, but only a fake password request which is not a part of the original website will be of malicious intent. Shoulder surfing is one of the local attacks in which the attacker normally observes the personal identification number (PIN) for a bank card before the actual stealing of the physical card by any means (Brar et al., 2012).

Finally, hybrid attacks are the most powerful form of attack as they combine the features of both local and remote attacks. The attacker is not restricted to only one form of attack. Such attacks involve executing a Trojan on an infected machine by checking all bookmarked pages and replacing important online service addresses with a fake address. It may also involve the modification of the browser settings to ensure it does not display the address bar or overlay the address bar with a fake pop-up window to hide the modified URL from the user. In most cases, the attacker will ensure maximum utilization of the system and could even alter the host files or redirect certain domains to a set IP address (Brar et al., 2012).

Fraud detection

The privacy, secrecy and commercial interests in the banking sector have restricted the number of published work on online fraud detection to just a few. This has made it difficult to develop new fraud detection systems for the banking sector. To complicate the matter, most of the available works in this regard are related only to credit card fraud detection (Kovach and Ruggiero, 2011). In practice, the existing online banking fraud detection methods are rule-based as they involve the generation of rules based on the domain knowledge. As a result, there is usually a high level of false alarm rate in these systems, meaning that the fraud detection rate is low (Wei et al. 2013).

A general fraud detector framework was proposed by Kovach and Ruggiero (2011) with the following main issues:

i. *Device identification:* The access device is identified using a downloadable component that has already been used by the real online banking system. This component is used to generate the access devices' fingerprint which is sent to the bank website as part of every transaction.
ii. *Global behaviour and monitor*: Here, the global behaviour of a user is monitored in a bid to detect fraud. For instance, all the accounts accessed by a user using a single device may be monitored to detect fraud; all login failures over many accounts using a single trial password may also be monitored. For each transaction, the monitor uses counters to verify updated transactions.
iii. *Deferential analysis*: Here, all incoming transaction requests are compared against a set of profiles that typifies the normal usage pattern of a legitimate user. Any significant deviation from the set pattern of a legitimate user indicates a fraud. Differential analysis is often performed using profiles like password failures, payment transaction frequency, and login frequency.
iv. *Global analysis:* This analysis is used to either weaken or strengthen fraud evidence that has already been determined via differential analysis. The probability of this evidence is determined using three lists; Blacklist (contains the fraudulent identities); White list (contains the legitimate identities); and Suspect list (contains unclassified identities).
v. *Suspect list and the exponentially decaying function*: Specific rules are followed to assign devices into one of the three lists before determining the fraud probability. A device placed in the suspect list has an initial value assigned to the fraud probability which is calculated using an exponentially decreasing function with respect to the number of accounts accessed with this device. If a customer reports any of these accounts as a fraud account, the identity of the associated device will be transferred to the blacklist.
vi. *Dempster-Shafer combiner:* This is a mathematical theory of fraud evidence which provides the basis for the combination of different sources of evidence which are estimated by global and differential analysis modules in order to compute a transactions' overall suspicion score.

Fraud detection has been investigated by Wei et al. (2013) in e-banking; the study reported three main types of fraud detection which are credit card fraud detection, telecommunication fraud detection, and computer intrusion detection. Additionally, they developed and implemented an online banking fraud detection system which combines the advantage of mixed features, domain knowledge, multiple data mining methods and multiple layer structure for a systematic solution. The proposed system was evaluated in a major bank where it was proved as effective in detecting fraud in unbalanced datasets. The method also

performed well compared to the other existing fraud detection systems in terms of accuracy and efficiency.

Fraud prevention

Efficient security models which can identify users and authorize transactions are needed in online or e-banking systems to prevent fraud. Currently, the existing models mainly focus on fraud identification rather than its prevention, meaning that actions are often taken after the occurrence of fraud instead having a system in place to prevent it from occurring (Peotta et al. 2011).
Fraud prevention refers to security measures taken to prevent unauthorized access or transactions on an account (Bolton and Hand, 2002). Several security models which are adopted by online banking systems (for the protection of banking users and applications) based on several security layers have been presented by Peotta et al. (2011). They analysed the device security in ten large banks in Brazil and evaluated the security models used by each bank against the most and least used models. Table 1 presents the results of the evaluated models. Similarly, Brar et al (2012) presented some options for fraud prevention which have similarities with the models presented by Peotta et al. (2011). They suggested that online banking security should not solely depend on the security on the end user (the users' PC). Table 2 presents the discussed methods.

Online banks have spent many efforts in ensuring the security of customers' financial information. A five-step methodology that will ensure a secured banking environment has been developed to protect users against external threats. These steps are sequentially executed thus: First, the user must enter the bank-provided access number (ID); second, the user is requested to enter a valid password. The third and fourth steps require the user to respond to a set of personalized questions. Finally, a previously marked image must be identified by the user. Upon the completion of these five steps, the user can have access to the banking system (French, 1970).

In addition to the methods used for fraud prevention in online platforms, many national regulators have already strengthened their regulations to improve the safety of their domestic banking systems, achieve public trust, and protect customer rights. Some of the policies that can ensure a safe and secure online banking platform include licensing, individuals' identity verification, capacity planning, legalization, harmonization, adaptation, and integration (Bahl, 2012).

Table 1: The commonly used security models in internet banking (Peotta et al. 2011)

Model	Description
Virtual keyboards	They capture the typed information on a device using Java and software-based cryptography with the aim of thwarting an efficient use of key loggers.
One-time password cards	Serves as an added authentication level; they are less expensive for dynamic passwords generation.
Browser protection	The users' browser is protected against known malware by monitoring the allocated browser memory.
Digital certificates	Here, Public Key Infrastructure (PKI) and a Certificate Authority (CA) are used to protect the system and the users.
One-time password tokens	These devices are used to dynamically change passwords (serves as a second authentication factor).
Device identification	This is applied together with device registering but can be used alone. It depends on the physical characteristics of the users' device.
Positive identification	This requires some user information which is only known to the user.
Pass-phrase	This technique depends on the information held by the user during money transactions.
Device registering	With this system, previously known and registered devices are restricted from accessing the banking system.
CAPTCHA	This system provides automatic attacks against ineffective authenticated online sessions.
Short message service (SMS)	Notifies users via messages about transactions that require their authorization.
Transaction monitoring	Involves fraud pattern identification using various approaches such as transaction history analysis and Artificial Intelligence.

Table 2: Methods for fraud prevention (Brar et al., 2012)

Method	Description
SMS challenge code	This is used to ensure a user logs on to his valid mobile phones by receiving activation code in the registered mobiles numbers associated with their bank account. Such temporary passwords are generated by the bank and sent as an SMS to the user's mobile phone number. The code is then used by the user to access his account.
Image verification	This method is based on a shared secret (image or verification phrase) between a user and the bank. Upon logging into a banking system with a username, the device ID is sent to the user with this username and delivered via an encrypted cookie that is stored on the user's device. Then, the system determines if the device ID matches with the username stored in the system before directing the user to the login page where a secret image/phrase will be verified before accessing the system.
Dynamic security skins (DSS)	Here, the user is meant to choose an image (contains sensitive information prompts) which will be overlaid on web forms. This image is equipped with a virtual hash and tied to the secured SSL session. This makes it impossible for attackers to spoof a pop-up that is similar to password requests.
PKI-based software solution	With the Public Key Infrastructure (PKI), both the user and the server can be authenticated. This form of authentication would eliminate 'Man in the Middle' attack.
PKI-based hardware token	Security against Trojans which can steal PIN codes and private keys from a PKI-based software token is ensured in this system using tamper-resistant key storage. The certificates and key pairs are pre-generated and saved on a tamper-proof smartcard. The PIN code on the external keypad is used to unlock the key vault in the smartcard to prevent key logger.

Conclusion

Today's' business environment (including the e-banking industry) has benefited immensely from the exponential growth of the Internet. E-banking revolutionized the banking business through the provision of many customer-related benefits and new business platforms for banks. However, it came with a price, mainly in terms of banking risks, challenges, and security issues. To protect against various forms of frauds, the security aspect must be considered at all levels of financial organizations. Many researchers have proposed several methods for fraud prevention and detection; some of these methods are effective in

improving fraud detection and prevention accuracy while the others are not. However, there is no current single method that will be efficient in the detection and prevention of all kinds of attacks on e-banking platforms.

REFERENCES

Abu-Shanab, E. & Matalqa, S. (2015). Security and fraud issues of e-banking. International Journal of Computer Networks and Applications, 2(4): 179-188.

AbuShanab, E., Pearson, J. M. & Setterstrom, A. J. (2010). Internet banking and customers' acceptance in Jordan: the unified model's perspective. Communications of the Association for information systems, 26(1): 23.

Agboola, A. (1970). Electronic payment systems and tele-banking services in Nigeria. The Journal of Internet Banking and Commerce, 11(3): 1-7.

Agwu, E. (2018). The role of e-banking on operational efficiency of banks in Nigeria.

Alaba, F. A., Hakak, S., Khan, F. A., Adewale, S. H., Rahmawati, S., Patma, T. S. & Herawan, T. (2018). Model-based testing for network security protocol for e-banking application. In Information Systems Design and Intelligent Applications (pp. 740-751). Springer, Singapore.

Alaba, F. A., Hakak, S., Khan, F. A., Adewale, S. H., Rahmawati, S., Patma, T. S. & Herawan, T. (2018). Model-based testing for network security protocol for e-banking application. In Information Systems Design and Intelligent Applications (pp. 740-751). Springer, Singapore.

Auta, E. (2010). E-banking in developing economy: Empirical evidence from Nigeria. Journal of Applied Quantitative Methods, 5(2): 212 – 222.

Bahl, S. (2012). E-banking: Challenges & policy implications. Proceedings of 'I-Society.

Bolton, R. J. & Hand, D. J. (2002). Statistical fraud detection: A review. Statistical Science, 235-249.

Brar, T. P. S., Sharma, D. & Khurmi, S. S. (2012). Vulnerabilities in e-banking: A study of various security aspects in e-banking. International Journal of Computing & Business Research, 6: 127-132.

Camilleri, Silvio J. & Others. (2014). Service quality and e- banking serviceperception of maltese retail bank customers.

Chakrabarty, K. C. (2013). Fraud in the banking sector—causes, concerns and cures. In National Conference on Financial Fraud organised by ASSOCHAM, New Delhi, 26.

Chavan, J. (2013). Internet banking-Benefits and challenges in an emerging economy. International Journal of Research in Business Management, 1(1): 19-26.

Chovanová, A. (2006). Forms of electronic banking. Available from: http://www.nbs.sk.

Dalton, G. C., Mills, R. F., Colombi, J. M. & Raines, R. A. (2006). Analyzing attack trees using generalized stochastic petri nets. In Information Assurance Workshop. pp: 116-123.

Davis, B. E. (2017). U.S. Patent No. 9,800,550. Washington, DC: U.S. Patent and Trademark Office.

Davis, P., Lu, V. & Crouch, R. (2009). Importance of service quality across different services types: An exploratory study of Australian and Chinese consumers.

Diniz, E., Birochi, R. & Pozzebon, M. (2012). Triggers and barriers to financial inclusion: The use of ICT-based branchless banking in an Amazon county. Electronic Commerce Research and Applications, 11(5): 484-494.

Drigă, I. & Isac, C. (2014). E-banking services–features, challenges and benefits. Annals of the University of Petroşani, Economics, 14(1): 41-50.

Elavarasi, M. R. & Surulivel, S. T. (2014). Customer awareness and preference towards e-banking services of banks (A Study of SBI). International Research Journal of Business and Management–IRJBM (ISSN 2322-083X).

French, A. M. (1970). A case study on e-banking security Ã¢ Â Â when security becomes too sophisticated for the user to access their information. The Journal of Internet Banking and Commerce, 17(2): 1-15.

Ghimire, A. J. (2012). Service quality and customer satisfaction in the restaurant business: Case study-Sagarmatha Nepalese Restaurant in Vantaa.

Guo, C., Wang, H., Dai, H. N., Cheng, S. & Wang, T. (2018). Fraud risk monitoring system for e-banking transactions. In 2018 IEEE 16th Intl Conf on Dependable, Autonomic and Secure Computing, 16th Intl Conf on Pervasive Intelligence and Computing, 4th Intl Conf on Big Data Intelligence and Computing and Cyber Science and Technology Congress (DASC/PiCom/DataCom/CyberSciTech)(pp. 100-105). IEEE.

Hajare, U., Mahajan, R., Jadhav, S., Pingale, N. & Salunke, S. (2018). Efficient cash withdrawal from ATM machine using mobile banking.

Han, J. H. & Kim, H. M. (2019). The role of information technology use for increasing consumer informedness in cross-border electronic commerce: An empirical study. Electronic Commerce Research and Applications, 100826.

Hayashi, R., Miyawaki, Y., Maeda, T. & Tachi, S. (2003). Unconscious adaptation: A new illusion of depth induced by stimulus features without depth. Vision Research, 43(26): 2773-2782.

Hernando, I. & Nieto, M. J. (2007). Is the internet delivery channel changing banks' performance? The case of Spanish banks. Journal of Banking & Finance, 31(4): 1083-1099.

Jassal, R. K. & Sehgal, R. K. (2013). Online banking security flaws: A study. International Journal of Advanced Research in Computer Science and Software Engineering, 3(8): 1016-1021.

Kovach, S. & Ruggiero, W. V. (2011). Online banking fraud detection based on local and global behaviour. In Proc. of the Fifth International Conference on Digital Society, Guadeloupe, France (pp. 166-171).

Kumar, M., Tat Kee, F. & Taap Manshor, A. (2009). Determining the relative importance of critical factors in delivering service quality of banks: an application of dominance analysis in SERVQUAL model. Managing Service Quality: An International Journal, 19(2): 211-228.

Mahdi, Mohammed Hashim, et al. (2019). Improvement of image steganography scheme based on LSB value with two control random parameters and multi-level encryption. IOP Conference Series: Materials Science and Engineering, 518(5). IOP Publishing.

Mahmood, Y. N. (2018). The impact of quality service factors on banking service sector case study in Erbil banks. Tikrit Journal for Administration & Economics Sciences, 2(42 part 2): 1-11.

Möckel, C. & Abdallah, A. E. (2010). Threat modeling approaches and tools for securing architectural designs of an e-banking application. In Information Assurance and Security (IAS), 2010 Sixth International Conference on. IEEE pp: 149-154.

Mu, Y. (2003). E-banking: Status, trends, challenges and policy implications.

Newman, K. (2001). Interrogating SERVQUAL: A critical assessment of service quality measurement in a high street retail bank. International Journal of Bank Marketing, 19(3): 126-139.

Nigudge, S. & Pathan, M. (2014). E-banking: Services, importance in business, advantages, challenges and adoption in India. Asian Journal of Management Sciences, 2(3): 190-192.

Park, Y. (2019). Recommender technologies and emerging applications. In Advanced Methodologies and Technologies in Network Architecture, Mobile Computing, and Data Analytics. IGI Global. pp: 458-470.

Patel, P., Patel, R., Patel, V. & Pathrabe, T. (2017). Survey of privacy and security issues in spice world e-commerce website. International Journal for Innovative Research in Science & Technology, 19-23.

Peotta, L., Holtz, M. D., David, B. M., Deus, F. G. & De Sousa, R. T. (2011). A formal classification of internet banking attacks and vulnerabilities. International Journal of Computer Science & Information Technology, 3(1): 186-197.

Qadeer, S. (2014). Service quality & customer satisfaction: A case study in banking sector.

Qatawneh, A. M., Aldhmour, F. M. & Aldmour, L. T. (2016). the impact of applying the electronic cheque clearing system on employees' satisfaction in accounting departments' of Jordanian Islamic banks. International Business Research, 9(2): 137.

Sepehri-Rad, A., Sadjadi, S. & Sadi-Nezhad, S. (2019). An application of DEMATEL for transaction authentication in online banking. International Journal of Data and Network Science, 3(2): 71-76.

Shah, M. (2009). E-banking management: Issues, solutions, and strategies: Issues, solutions, and strategies. IGI Global.

Shannak, R. O. (2013). Key issues in e-banking strengths and weaknesses: The case of two Jordanian banks. European Scientific Journal, ESJ, 9(7).

Sultana, S. & Rana, S. (2010). Service quality: (Service Gap Analysis) A case study-" Komvux".

Taha, M. S., et al. (2018). Wireless body area network revisited. International Journal of Engineering & Technology, 7(4): 3494-3504.

Taha, M. S., et al. (2019). Combination of steganography and cryptography: a short survey. IOP Conference Series: Materials Science and Engineering, 518(5). IOP Publishing.

Tunmibi, S. & Falayi, E. (2013). IT security and e-banking in Nigeria. Greener Journal of Internet, Information & Communication System, 1(3): 61-65.

Turban, E. & McElroy, D. (1998). Using smart cards in electronic commerce. In System Sciences, 1998., Proceedings of the Thirty-First Hawaii International Conference on. IEEE, 4: 62-69.

Usman, A. K. & Shah, M. H. (1970). Critical success factors for preventing e-banking fraud. The Journal of Internet Banking and Commerce, 18(2): 1-14.

Vrancianu, M. & Popa, L. A. (2010). Considerations regarding the security and protection of e-banking services consumers' interests. The Amfiteatru Economic Journal, 12(28): 388-403.

Vyas, C. (2009). Mobile banking in India - perception and statistics. Vital Analytics. Available from: http://www.telecomindiaonline.com.

Wei, W., Li, J., Cao, L., Ou, Y. & Chen, J. (2013). Effective detection of sophisticated online banking fraud on extremely imbalanced data. World Wide Web, 16(4): 449-475.

Weinflash, L.E., Janis, E. S. & Jinghong, Q. (2018). System and method for detecting fraudulent account access and transfers. U.S. Patent Application 15/826,229, filed March 22, 2018.

Wisdom, K. (2012). The impact of electornic banking on service delivery to customers of Ghana commercial bank limited. Available from: http://ir.knust.edu.gh.

Yang, L., Elisa, N. & Eliot, N. (2019). Privacy and security aspects of E-government in smart cities. In Smart Cities Cybersecurity and Privacy. Elsevier. pp: 89-102.

Zeithaml, V. A., Berry, L. L. & Parasuraman, A. (1996). The behavioral consequences of service quality. The Journal of Marketing, 31-46.

Zeithaml, V. A., Parasuraman, A., Berry, L. L. & Berry, L. L. (1990). Delivering quality service: Balancing customer perceptions and expectations. Simon and Schuster.