International Digital Organization for Scientific Research ISSN: 2579-079X
IDOSR JOURNAL OF SCIENCE AND TECHNOLOGY 6(1):1 -10, 2021

Design and Implementation of Online System for Quality Assurance in Nigeria Forex

Onwuka U. Paulinus, Onyesolu O. Moses, and Okeugo V. Chibuike

Department of Computer Science, Faculty of Physical Sciences Nnamdi Azikiwe University, Awka.onwukauchepaul@gmail.com, mo.onyesolu@unizik.edu, okeugo.victor.c@gmail.com

ABSTRACT

Over the years the activities of Bureau De Change (BDC) operators in the Nigerian economy have been on without quality assurance. The country's forex allocations to BDC, subsequent renditions and monitoring have loopholes, hence, a great need for efficient system to control the activities. The areas of interest that need attention are the profit margin, identification of customers, verification of documents and bi-monthly authorized period of transaction by each customer. This work developed and implemented an online system for monitoring and verification of forex transactions by BDC operators. This will make the monitoring easy for the regulator (the Central Bank of Nigeria). To achieve this, Agile Development Methodology was adopted alongside Object Oriented Analysis for modelling the object interactions. The system was designed and implemented using Ruby and Sinatra programming environments in model-view-controller (MVC) framework with PostgreSQL Server acting as the Database Management System (DBMS). The result of the system is an online system for monitoring and verification of forex transactions hosted on a private Heroku cloud. In the system, transaction requests can be made and completed at the convenience of the customers' homes and offices. BDC operators can send returns at the convenience of their offices. The system makes available all the information needed as regards to daily, weekly, and monthly transactions.
Keywords: Online System, Quality Assurance, Forex

INTRODUCTION

During the past decade, Information and Communication Technology (ICT), has penetrated almost all areas of lives. In major economies of the world, ICT has been proven to be one of the vehicles that drive national development, both economically, educationally, in governance, in health, and other key sector areas. Information and communication technologies are radically changing the way of business. These changes and development resulted in new delivery of channels for banking products and services such as Automated Teller Machines (ATMs), Telephone Banking, PC-Banking, and Electronic Funds Transfer at Point of Sale (EFTPoS). Many banks are making huge investments in technology to maintain and develop their infrastructure. Not only do they provide new electronic information-based services, but also to manage their risk positions and pricing [1]. The industry depends heavily on the use of different Information Technology (IT) techniques in delivering quality service to customers. With the introduction of mobile and internet banking, it is easier to carryout secure bank transactions within the comfort of their homes and offices.

The foreign exchange market (also known as Forex, FX, or currency market) is a global decentralized or over-the-counter (OTC) market for the trading of currencies. This includes all aspects of buying, selling and exchanging currencies at current or determined prices. In terms of trading volume, it is

by far the largest market in the world, followed by the Credit market. The main participants in this market are the larger international banks. Financial centers around the world function as anchors of trading between a wide range of multiple types of buyers and sellers around the clock, with the exception of weekends. Since currencies are always traded in pairs, the foreign exchange market does not set a currency's absolute value but rather determines its relative value by setting the market price of one currency if paid for with another [2].

The foreign exchange market works through financial institutions, and operates on several levels. Behind the scenes, banks turn to a smaller number of financial firms known as dealers, who are involved in large quantities of foreign exchange trading. Most foreign exchange dealers are banks, so this behind-the-scenes market is sometimes called the interbank market (although a few insurance companies and other kinds of financial firms are involved). Trades between foreign exchange dealers can be very large, involving hundreds of millions of dollars. Because of the sovereignty issue when involving two currencies, Forex has little (if any) supervisory entity regulating its actions. Under the regulation of the Central Bank of Nigeria (CBN), the forex market remains indebted to the different implementation of information technology and tools for adequate monitoring and supervision.

LITERATURE REVIEW

[3] developed a robust identity management system and opined that the system will bring improvements in security, reduce cost and improve service levels. This research also highlighted that identity management in the public domain also requires strong authentication, noting that instead of simply relying on traditional password-based technology, two-factor authentication technologies is safer, efficient, and more reliable.

[4] identified benefit from various Decision Support Systems (DSS), and introduced a range of examples from the literature. These examples were organized according to the driving technological architecture of the DSS. Benefits may impact a decision or the decision making process. Some techniques for assessing the benefits of a particular DSS were also surveyed.

[5] proposed a prototype of a Decision Support System (DSS) for providing the knowledge for optimizing the newly adopted e-verification strategy in financial institutions. They suggested that if a financial technology organization adopts e-verification and identity as a new strategy, it should undertake a preliminary evaluation to determine the percentage of success and areas of weakness of this strategy. If this evaluation is done manually, it would not been easy task to do, and would not provide knowledge about all pit fall symptoms. The proposed DSS is based on exploration (mining) of knowledge from large amounts of data yielded from operating the institution to its business. This knowledge can be used to guide and optimize any new business strategy implemented by the institution. The proposed DSS involves Database engine, Data Mining engine, and Artificial Intelligence engine. Therefore, all these engines work together in order to extract the knowledge necessary to improve the effectiveness of any strategy.

[6] in their study show that the role of management information systems is described and analyzed in light of its capability for decision making. Good management of information systems leads to good decision making in business. In the same way, poor management leads to poor decision making. It is based on this foundational concept that this paper is going to circumspectly analyze the roles of management systems in decision making.

Internet is significant for redefining and reshaping the various concepts in all spheres of life [7]. To acquire ease, swiftness and downsizing, ICT banking has a forceful edge over the competitors, homogenize qualitative services, swell market share, and on the whole, to get better eminence, ICT has become an

appropriate pedestal for banking sector. ICT is helpful to the central banking regulatory authorities, foreign exchange markets and the various stakeholders in international currency exchange trade.

Internet banking is one of the latest technological wonders in the recent past involving use of ICT for delivery of banking products and services [8]. ICT banking is changing the banking industry and is having the major effects on banking relationships. Banking is now no longer confined to the branches where one has to approach the branch in person. [9] suggest that ICT Banking adoption is a complex and multifaceted process and a joint consideration of customers' personal, social, psychological, utilitarian and behavioral aspects is more important than adoption itself and will ultimately result in the intended behaviour. [10] in their research say that customers are encouraged to utilize ICT banking as first priority. Increasing the customer's arousal by ICT advertisements to use ICT banking creates a positive attitude toward bank's brand, which in-turn is the key factors in ICT banking effectiveness.

[11] research states that ICT banking needs, compatibility, convenience, and communication on customer adaptation. In the context of private commercial banks in order to attract more users to ICT banking, it is not going to be enough only to introduce an ICT banking system, but they need to develop the belief of usefulness of the system among their users. The importance of ICT banking needs and the ease of using it should be acknowledged by demonstration on trial basis. [12] in their research found that younger consumers are more likely to adopt ICT banking. The study states that consumers in the age group below 25 years old are the major contributor to ICT banking.

[13] stated in their study that the main purpose was to extend the technology acceptance model (TAM) in the context of ICT banking adoption in India under security and privacy threat. The researchers incorporated various inhibitors of ICT banking which restrict the use of ICT banking adoption under "perceived risk", and also considered the role of the bank website as a key determinant of perceived risk and of perceived ease of use in the context of ICT banking services. The work revealed that perceived risk has a negative impact on behavioral intention of ICT banking adoption and trust has a negative impact on perceived risk. A well-designed web site was also found to be helpful in facilitating easier use and also minimizing perceived risk concerns regarding ICT banking usage. [14] identified the challenges of using e-banking in different aspects of continuous improvement. The study concluded that in the use of ICT banking, process development is the most important area of continuous improvement.

[15] conducted a study to help banks mitigate the key cause of profit reduction in ICT banking industry which is an insufficient understanding of customer behavior and preference by recommending effective strategies to help banks retain existing ICT banking customers. [16] stated that ICT banking adoption has a positive impact on the level of profits, deposits and loans per branch. As operational activities are now provided via ICT branches, ICT banking facilitates banking activities in branches that require more human input. They also find that ICT banking adoption has a negative impact on bank profitability.

[17] found that personal capacity is an important determinant of ICT banking. Use of it in a standard, non-sequential approach has no significant effect when the model is sequential. Results suggest that policy makers should emphasize useful attributes of ICT banking when attempting to increase its usage by people who already use the ICT.

[18] stated in their work that within information systems, accountability can be accomplished by identifying and authenticating users of the system with a user identity (user-ID). This user-ID should uniquely identify a single individual, such that subsequent tracing of the user's activities on the system is possible should an incident occur or if a violation of the IT security policy is

detected. Shared or group user-IDs should be prohibited unless it is unavoidable due to specific business needs.

[19] is of the opinion that the signaling theory is another strategy that can be used in identity deception prevention. Signaling theory posits that there are assessment signals (evidence that are hard to fake such as a government identification) and conventional signals (evidence easier to fake such as marital status on one's social networking profile). There is prevalence on the Internet for conventional signals and having the mindset that a conventional signal is sufficient to verify one's identity could lead to erroneous conclusions. Instead, we suggest that users should be empowered to know the difference between these two types of signals and rely on additional evidence (preferably assessment signals).

Early Internet banking applications have been using this authentication mechanism [20]. Increasing identity theft incidents such as phishing have prompted institutions to use more advanced authentication mechanisms to identify their users. Passwords are still the most common authentication method. To reduce the possibility of passwords being compromised using brute-force attacks, consecutive unsuccessful log-in trials should be controlled. This can be accomplished by disabling an account after a limited number of unsuccessful log-ins. Alternatively, a mechanism of increasing the time delay between each consecutive login attempt could be considered as a way of preventing password guessing activities. A strong password policy and frequent password changes should be enforced to deter password attacks. Additional authentication methods, such as biometrics or two-factor authentication, could also be considered to strengthen the authentication process. Functions requiring another level of authorization should be implemented using re-authentication. In addition, idle logged-on sessions should be timed-out after a set period to prevent attackers from stealing idle session information.

Another type of non-verbal user activity to use for deception detection online based services is the social context (e.g., employment history or social connections of individuals which can be used as evidence of a user's identity) [21]. The study has demonstrated that the accuracy of deception detection increases when a user's social context features are included in the detection analysis

Review and Knowledge Gap

The inherent design of many online systems allow people to freely create new identities by registering new accounts. This accounts for noticeable gaps of identity forgery. Even if mechanisms for detection were placed into these systems, the computational load incurred by detection mechanisms along with having users creating new accounts with limited verification (usually just email verification) will make detection an infeasible strategy. This opens the door for this work to focus on a unified identity system that is the same for all users across the entire system. Incorporating security features along with such measures will not only increase the difficulty for deceivers but also reduce the impact of identity deception to other users.

a. Discretionary Access Control (DAC): in this mechanism, users own the objects under their control, and the granting and revoking of access control privileges are left to the discretion of individual users.
b. Mandatory Access Control (MAC): it is a means of restricting access to objects based on the sensitivity of the information contained in the objects, along with formal authorization of subjects to access information of such sensitivity.
c. Role-based access control (RBAC): it is an authorization mechanism in which access decisions are based on the roles that individual users have as part of an organization.

When assigning access rights to an entity, the principles of least privilege and separation of duties are strongly recommended. The principle of least privilege recommends that the least amount of privileges necessary to perform one's task should be granted to an entity. The principle of segregation of duties suggests that critical functions are divided into steps among different individuals to prevent a single individual from subverting a critical process.

Identity Deception in Online Based Services

Online identity deception is the deliberate concealment or altering of a sender's true identity in order to convey that false belief to a receiver while a receiver does not anticipate identity tampering by the sender [22]. In addition, for deception to take place, an individual should not be expecting that all or part of the information in a message will be concealed or altered [23]. Some of the objectives behind deception include instrumental (goal-driven), relational (relationship-driven), or identity (e.g. protecting one's reputation) [24].

There are three types of identity deception [25]:

a. Identity Concealment
b. Identity Theft
c. Identity Forgery

Identity Concealment as shown in Figure 2.1 occurs when part of the identity information is omitted or altered. **Identity Theft** occurs when a person's identity is stolen. **Identity forgery** occurs when a new person is created along with a new history record.

A personal identity usually consists of an attributed identity such as name or place of birth, a biometric identity such as finger prints and a biographical identity such as criminal record or credit history [26]. In addition to personal identity, a person's identity also contains a social identity (e.g., Social relations), [27].

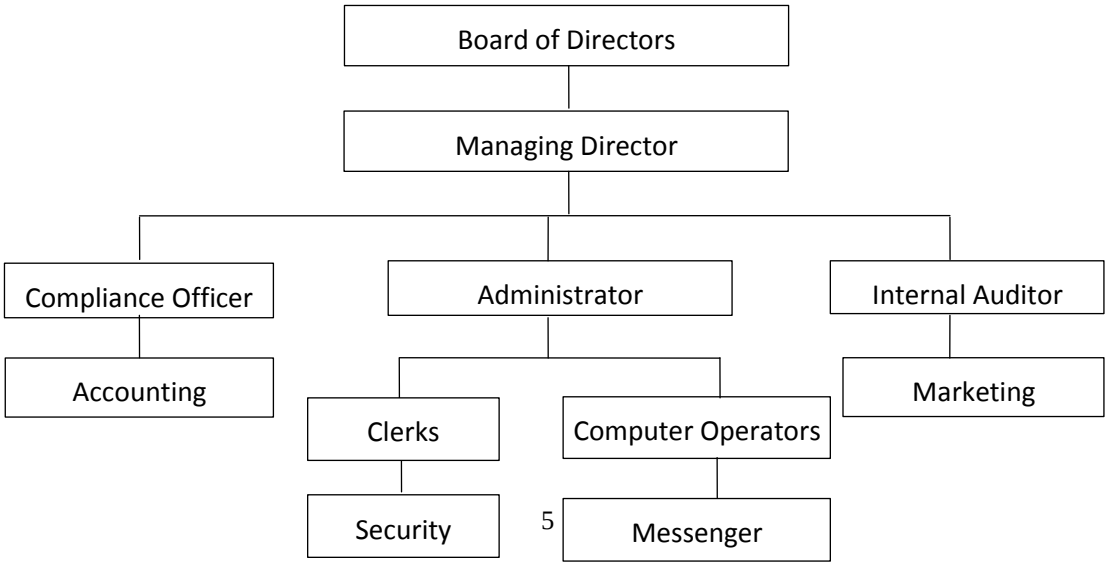
Methodology Adopted

The methodology adopted for this work is the Object Oriented Analysis and Design Methodology (OOADM). This methodology was adopted because of its unique process of analyzing a problem and hence enhances the deduction of the project's requirement that is determining what the system is supposed to do. With this methodology, a problem can be analyzed with an approach also developed in solving such problem.

The Organization and Its Environment

The study environment is a licensed BDC operator called Golden Gate Bureau De Change Ltd. Golden Gate Bureau De Change was founded in 2013 with headquarters office at 455 City Mart Plaza Nnebisi Road Asaba, Delta State. The company size is about 10-20 employees.

Figure1: Shows the organizational structure of the organization.



Use Case Diagram

A use case diagram portrays the different types of users of a system and the various ways that they interact with the system. [6] is the use case diagram for the proposed system.

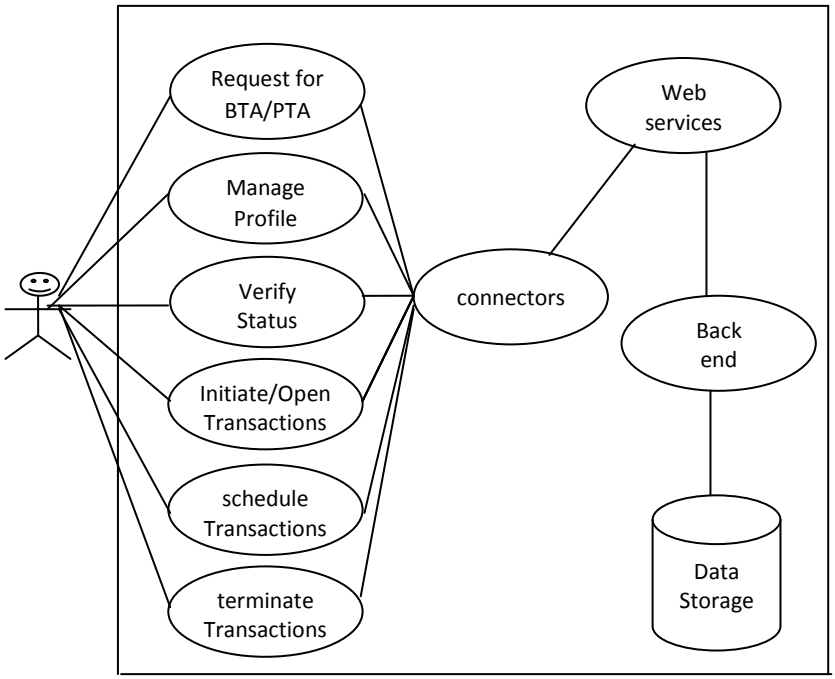


Fig.2.Database Design and Structure

An Object Relational Mapper (ORM) known as Active Record was used for interaction with the database. The database is used for storing the necessary customer data, transaction history, as well as suspicious transactions. The database specification for this system is represented as tables shown in Tables 1.0 and 1.1

Table 1.0 Transactions Table

Field name	Data type	Size	Constraint
Transaction ID	Int	08	Primary key
Description	Varchar	20	
Transaction Type	Varchar	30	
Transaction Status	Varchar	20	
Created By	Varchar	15	
Timestamp	Date/Time	08	
Token Verification	Varchar	08	
Approved By	Varchar	12	

Table 2 Login Table

Field name	Data type	Size	Constraint
ID	Int	08	Primary key
Username	Varchar	20	
Password	Varchar	30	
Login Status	Varchar	05	

System Implementation

These are the hardware and software requirements as well as the environment in which this new system can be operated. These are necessities for proper and effective implementation of the new system.

Hardware Requirements

The following hardware are required for the efficient working of the system:

1. Minimum of 120GB of HDD
2. Minimum of 1GB of RAM
3. Minimum of 1.6.0GHz processor speed
4. CD ROM or external USB drive or any other removable media
5. Internet enabled device such as USB modem, Ethernet cable, LAN, WLAN adapters

Software Requirements/ User Interface

The following software is needed for adequate implementation of the new system:

1. Windows XP /7/8/8.1/10 or MAC , or Linux
2. Apache Web Server
3. Internet Explorer any other web browser (Firefox, Google Chrome) 4.Unix or Windows server operating system

The customer purchase form. This is where the customer inputs the required information which allows him to place an order request form a BDC.

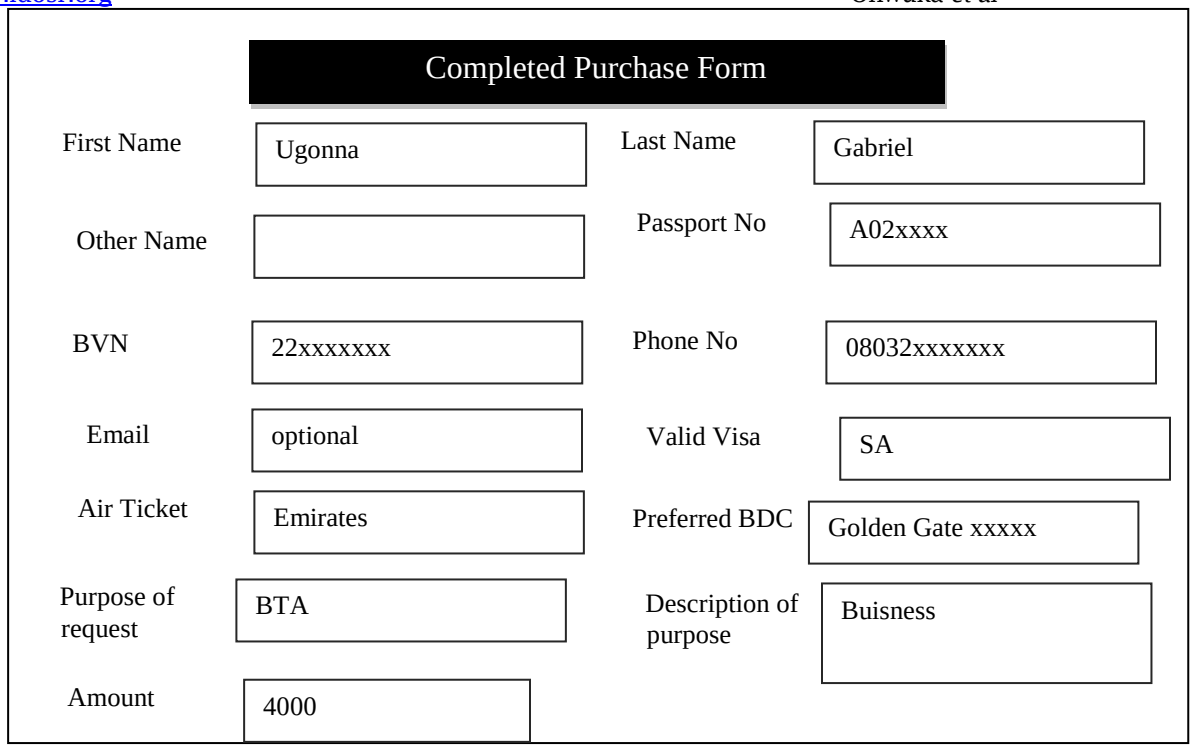


Fig. 3: Completed Purchase Order

CONCLUSION

This work describes the modeling and development of a semi real-time online monitoring and verification system. This system will improve upon the traditional approach of verification of FX transactions between BDC operators and customers. The implementation of the system will bridge security gaps, optimize authenticity of FX transactions, and eliminate opportunities for defrauding customers. More so, using a central database will ensure data integrity and provide a platform for reporting and evaluation. The stated objectives of the work were achieved. Some challenges encountered were strict restrictions on classified information, limited access to the internal processes of FX regulatory bodies, and steep budget for the full scale implementation.

REFERENCES

1. Abu-Naser, Ganguly, A. R. & Gupta, A. Data mining and decision support for business and science: Encyclopedia of Data Warehousing and Mining". J. Wang Ed. Idea Group.
2. Allen, R., & Slender, A.N. (2012). Introduction to Information and Information Management System, Belmont: Hawkins Press.
3. Al-Weshah, G. A. (2013). The role of ICT banking in continuous improvement areas: quantitative evidence from Jordanian banks. International Journal of Business Performance Management, 14(2), 181-196.
4. Buller D. B. & Burgoon, J. K. (2015). Interpersonal Deception Theory, Commun. Theory, 6(3), 203–242.
5. Cornford, T. & Shaikh, M. (2013). Introduction to information Systems, London, UK: University of London
6. Donald, H.S. (2000). Computer Implication for Information Management, New York:
7. McGraw- Hill.

8. Ekman, P. (2015). Deception, Lying, and Demeanor in States of Mind, American and PostSoviet Perspectives on Contemporary Issues in Psychology, D. F. Halpern and A. E. Voiskounsky, (Eds.), Oxford, UK: Oxford University Press..
9. Elkins, A., Zafeiriou, S., Pantic, M. & Burgoon, J. (2014). Unobtrusive Deception Detection,
10. In The Oxford Handbook of Affective Computing, R. Calvo, S. K. D'Mello, J. Gratch, and A. Kappas, (Eds.) Oxford, UK: Oxford University Press.
11. Jahangir, N. and Parvez, N. (2012). Factors determining customer adaptation to ICT banking in the context of private commercial banks of Bangladesh, Business Perspectives & Research, Jul-Dec, 25-36.
12. Kesharwani, A. & Bisht, S. S. (2012). The impact of trust and perceived risk on ICT banking adoption in India: An extension of technology acceptance model. International Journal of Bank Marketing. 30(4), 303-322.
13. Lane, H. (2013). Data Processing and Management Information Systems (2nd ed.), London: MacDonald and Evans Ltd.
14. Li, H., Bond Jr, C. & Robinson, M. (2014). The evolution of deception, J. Nonverbal Behav., 12(4), 295–307.
15. Martin, J. (2014). Telecommunications and the Computer (3rd ed.), Englewood Cliffs, NJ: Prentice-Hall.
16. Moghadam, B. A., Behboudi, M. & Jafari, F. (2012). Does ICT advertising affect the ICT banking effectiveness? A three dimensional model for Iran, Journal of ICT Banking & Commerce, 17(3), 1-16.
17. Munusamy, J., De Run, E.C., Chelliah, S. & Annamalah, S. (2012). Adoption of retail ICT Banking: A study of demographic factors, Journal of ICT Banking & Commerce. 17(3), 1-14.
18. Onay, C. & Ozsoz, E. (2013). The Impact of ICT-Banking on brick and mortar branches: The case of Turkey, Journal of Financial Services Research, 44(2), 187-204.
19. Park, T., Pavlidis, I. & Levine, J. (2012). Thermal facial screening for deception detection, Prcceedings of the Second Joint EMBSEIMES Conference 2012, 1143–1144.
20. Patsiotis, A.G., Webber, D. J. & Hughes, T. (2013). ICT shopping and ICT banking in sequence:
21. An explanatory case study, Journal of Financial Services Marketing. 18(4), 285-300.
22. Pick and Weatherholt (2013). A Brief History of Decision Support Systems. DssResources.com.
23. Qin, T., Burgoon, J. K. & Nunamaker, J. F. (2004). An exploratory study on promising cues in deception detection and application of decision tree, Proceedings of the 37th Annual Hawaii International Conference of System Science, 2004.
24. Saranya. J., Anitha, K. &.Vasantha, S. (2014). An empirical study on role of ICT in banking Sector 15(2), 2321-3124.
25. Sharma, S. & Singh, R. (2011). Factors influencing ICT banking: An empirical investigation. IUP Journal of Bank Management, 10(4), 71-80.
26. Solanki, Virender Singh. Impact of ICT Banking on Customer Services: An empirical study. BVIMR Management Edge. 2011, Vol. 4 Issue 1, pp. 50-56.
27. Wang, G. A., Chen, H., Xu, J. J. & Atabakhsh, H. (2014). Automatically detecting criminal identity deception: an adaptive detection algorithm," IEEE Trans. Syst. Man Cybern. Part A Syst. Humans, 36(5), 988–999.
28. Wood, P. (2015). Implementing identity management security - an

ethical hacker's view, Network Security, 20(9), 12-15.

30. Yousafzai, S. (2012). A literature review of theoretical models of ICT banking adoption at the individual level. Journal of Financial Services Marketing, 17(3), 215-226.
31. Yuen, Y. Y. (2013). Gender and age effect on acceptance of ICT Banking: Cultural comparison between United States and Malaysia, International Journal of Business & Management. 8 (18), 1-11.
32. Zahavi, A. (2014). The Fallacy of Conventional Signalling, Philos. Trans. R. Soc. London. Ser. B Biol. Sci., 340 (1292), 227–230.