

BANK DATA SECURITY: DEVELOPMENT OF AN ENHANCED FAMG CRYPTOGRAPHY MODEL

¹Oyewo D. T., ¹Adeola O. O., ¹Ayomitan A. O., ²Benson-Iyare J. C., ¹Kilani S.
+Department of Computer Science, Oyo State College of Agriculture and Technology, Nigeria
#Computer Science Department, Federal Polytechnic Idah, Nigeria
Correspondence: dammyoyewo@gmail.com, +2347033278662

Abstract

As a result of the various gains offered by the Internet, businesses have become more open to supporting Internet-powered initiatives such as customer care, e-commerce and web enabled financial transaction such as online banking. However, the online banking system presents a challenge whereby cryptanalysts take advantage of the general accessibility features of the internet network to carry out fraudulent acts and perform unauthorized financial transaction, thereby victimizing or probably defrauding the internet banking users. In this study, we proposed an enhanced 'FAMG cryptography model' for encrypting and decrypting online banking information in such a way that only authorized users with the required public key would be permitted to view customer record. The model is an ensemble of Playfair cipher and Caesar cipher algorithms. The dual algorithms cascades into each other for the purpose of encryption and decryption of banking operations. The novel model was converted into machine executable code using C# programming language. The result showed that the model has the capacity of encrypting customer data as soon as it arrives on the web application from the hawk eyes of web application system intruders and hackers. The ensemble model provides better data security than the constituent traditional algorithms because of the improved complexities it offers. This model is expected to promote confidence on the integrity of data provided/available on the bank websites or on any other platform where banking details will be required.

Keywords: Cryptography; online banking; data security; encryption; decryption

1. Introduction

There is no doubt about the fact that Information technology advancement is a tool for economic development, and its impact in the financial and banking sector which has permitted customers performing desired wireless banking operations over the internet is indeed immense. Online banking, also known as internet banking, e-banking or virtual banking, is an electronic payment system that enables customers of a bank or other financial institution to conduct a range of financial transactions efficiently and speedily through the financial institution's website (Frankfield, 2022). With online banking, customers are not required to visit a bank branch to complete most of their basic banking transactions. (Alamgir, 2020) confirmed that online banking is a vital instrument for delivering banking service to customer and service provider in shortest possible time, ensuring affordability and usability.

Customers have an opportunity to monitor their accounts closely, allowing them to keep their accounts safe to an extent. Around-the-clock access to banking information provides early detection of fraudulent

activity; thereby acting as a guardrail against financial damage or loss.

As a result of the various gains presented by the internet, businesses have become more open to supporting Internet-powered initiatives such as customer care, e-commerce, extranet collaboration and web enabled financial transaction such as online banking. However, all these services are prone to intruders and unauthorized users taking advantage of the general accessibility features of the internet network to carry out fraudulent acts and perform unauthorized financial transaction, victimizing and defrauding the internet banking users. Hence the need for this study.

An insight to ascertain the existing security features into banks such as First bank of Nigeria, Stanbic IBTC and United Bank for Africa (all in Nigeria), revealed that the existing applications were unable to stop offline credential attacks (Sarjiyus, 2021). Internet insecurity is one of the leading issues among online banking customer across the world with high level threats, lack of trust and fear of loss (Qais, 2021). (Anshita 2020) believes we live in an era where data security is of global concern due to high rate of information theft and

impersonation over the internet, he therefore proposed biometric impressions and digital signatures to make transaction seamless by bank's customer.

Cryptography is a technique to make data information in disarray to confuse unauthorized persons or attackers from accessing the data. Cybersecurity is aimed at protecting the 'good' parties, who use computer system and network legitimately, from damages due to misbehaving entities, to whom we usually refer as attackers or adversaries). Therefore, introducing Cryptography into the conventional authentication and authorization mode of the online banking system will be a success (Amir, 2022). Also appalls the conventional verification and two-factor authentication of plain online banking system data, describing them to be inadequate for preventing cyber attacks especially in systems that involve finance and therefore recommends a hash-based (cryptography) multi-server authentication scheme in conjunction with a smart card.

Although online banking security is continually improving but accounts of customers are still vulnerable and intrusion has always been a major challenge to online banking. Intrusion detection is the process of monitoring the events occurring in a computer system or network and analyzing them for signs of intrusions defined as attempts to compromise the confidentiality, integrity, availability, or to bypass the security mechanisms of a computer or network has been a practice in curbing security threat to online banking (Nigel, 2005). Intrusion Detection Systems (IDSs) are software or hardware products that automate this monitoring and analysis process. Intrusion detection allows organizations such as the banks to protect their systems from the threats that come with increasing network connectivity and reliance on information systems. With the high usage of Internet in our day today life, security of network has become the key foundation to all web applications, like online banking, online retail sales, etc.

(Waleed, 2020) showed that new model of storing user password can go a long way in curbing the security challenge of internet banking, this work provided a deep motivation for our study in hashing content of the bank applications and websites. Cryptography is one of the major means of protecting information through the use of hash codes, so that only those for whom the information is intended can read and process it with the use of appropriate keys. In computer science, cryptography refers to secure information and communication techniques derived from mathematical concepts and a set of rule-based calculations called algorithms, to transform messages in ways that are hard to decipher. These deterministic algorithms are used for cryptographic key generation, digital signing, verification to protect data privacy,

web browsing on the internet and confidential communications such as credit card transactions and email. There are numerous cryptographic algorithm but this research tends to combine the playfair cypher algorithm and the ceaser cipher to ensure optimum security.

The aim of this research is to design and implement an enhanced FAMG cryptography model for online banking system security. The objectives are:

1. To formulate an algorithm for the proposed ensemble model
2. To design UML models for the formulated algorithm
3. To translate the model into a program code
4. To plug the program code in (3) above into a web application to test the suitability of the model in a real life scenario.

2. Materials and Methods

Adopted Cryptography Algorithm

1. Playfair Cipher: The Playfair cipher was the first practical digraph substitution cipher. The scheme was invented in 1854 by Charles Wheatstone but was named after Lord Playfair who promoted the use of the cipher. In playfair cipher unlike traditional cipher we encrypt a pair of alphabets(digraphs) instead of a single alphabet. The playfair algorithm consists of 2 steps:

Generate the key Square (5×5): The key square is a 5×5 grid of alphabets that acts as the key for encrypting the plaintext. Each of the 25 alphabets must be unique and one letter of the alphabet (usually J) is omitted from the table (as the table can hold only 25 alphabets). If the plaintext contains J, then it is replaced by I. The initial alphabets in the key square are the unique alphabets of the key in the order in which they appear followed by the remaining letters of the alphabet in order.

A	T	H	E	N
S	B	C	D	F
G	I/J	K	L	M
O	P	Q	R	U
V	W	X	Y	Z

Fig 1.0 5x5 square sample

To determine the cipher (encryption) text,

5. A 5 by 5 key-matrix or key-table is built and filled with the letters of alphabets, as shown in fig 1.1 above
6. The first row (left to right) is filled with the letters of the given keyword. In this case "ATHENS". If the keyword has duplicate letters (if any), they are avoided. It means a letter will be considered only once. After that,
7. The remaining letters in the alphabetical order are filled orderly as shown in fig 1.1 above

Algorithm to encrypt the plain text: The plaintext is split into pairs of two letters (digraphs) and the following rules is or are applied:

1. **If both the letters are in the same column:** Take the letter below each one (going back to the top if at the bottom). If there is no letter below, then the first letter in the column is considered. From the generated grid in fig 1.1 above, "AS" will produce "SG"; "GV" will produce "OA"

2. **If both the letters are in the same row:** Take the letter to the right of each one (going back to the leftmost if at the rightmost position). If there is no letter to the right, then the first letter of the same row is considered as the right letter. From the generated matrix in fig 1.1, "AT" will produce "TH"; "WZ" will produce "XV" and "OP" will produce "PQ"
3. **If neither of the above rules is true:** A rectangle is formed with the two letters and the letters on the horizontal opposite corner of the rectangle is taken. In this case, a 3*3 matrix is selected from a 5*5 matrix such that pair of letters appear in the 3*3 matrix. Since they occupy two opposite corners of a square within the matrix. The other corner will be a cipher for the given digraph. From the generated matrix, to encipher "CU", a 3x3 matrix is selected from the 5x5 matrix having the letters at each end as shown in fig 1.2 below

A	T	H	E	N
S	B	C	D	F
G	I/J	K	L	M
O	P	Q	R	U
V	W	X	Y	Z

Fig 1.2: 5x5 grid containing 3x3 grid for letters "CU"
Thus, from the figure above, "CU" will produce "FQ"

2. Ceaser Cipher: The Caesar Cipher technique is one of the earliest and simplest method of encryption technique. It's simply a type of substitution cipher, i.e., each letter of a given text is replaced by a letter some fixed number of positions down the alphabet. For example, with a shift of 1, A would be replaced by B, B would become C, and so on. The method is apparently named after Julius Caesar, who apparently

used it to communicate with his officials. Thus to cipher a given text we need an integer value, known as shift which indicates the number of position each letter of the text has been moved down. The encryption can be represented using modular arithmetic by first transforming the letters into numbers, according to the scheme, A = 0, B = 1..., Z = 25 as shown in Table 1.1 below.

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
00	01	02	03	04	05	06	07	08	09	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

Table 1.1 Alphabets and their respective number chart

Encryption of a letter by a shift n can be described mathematically as.

$$E_n(x) = (x + n) \bmod 26 \text{ (encryption phase with shift } n)$$

$$D_n(x) = (x - n) \bmod 26 \text{ (decryption with shift } n)$$

From the alphabet and number chart and applying the Ceaser cipher mathematical formula with a shifting key 3; the encryption of "ABC" will produce "DEF" as shown in the table 1.2 below

Plaintext: A → 0	$E_n: (0 + 3) \bmod 26 = 3$	Ciphertext: 3 → D
Plaintext: B → 1	$E_n: (1 + 3) \bmod 26 = 4$	Ciphertext: 3 → E
Plaintext: C → 2	$E_n: (2 + 3) \bmod 26 = 5$	Ciphertext: 3 → F

Table 1.2: Ceaser Cipher for ABC with shift key of 3

Conceptual Framework of FAMG Cryptography Model

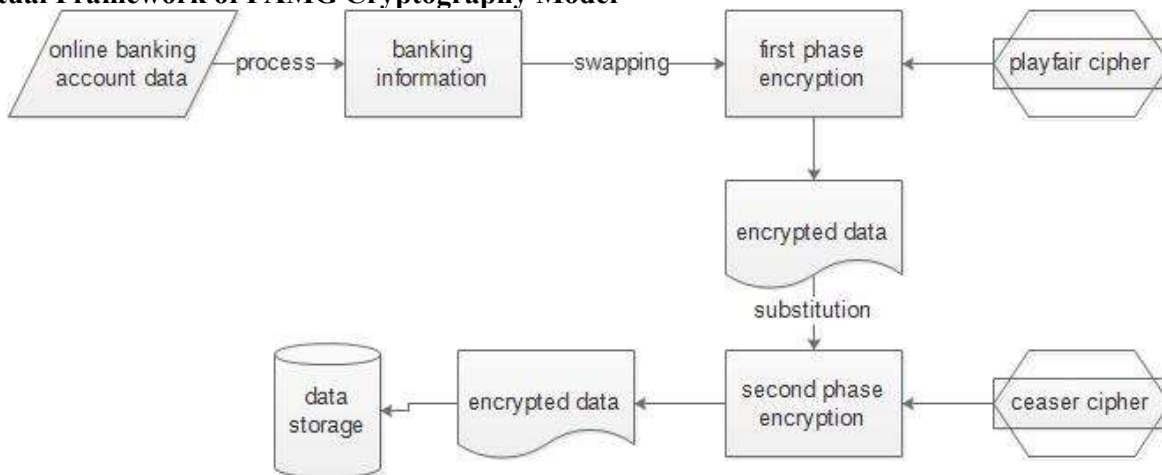


Fig 1.2 conceptual framework for FAMG cryptography model

The conceptual framework is one of the representation techniques of a set of concepts, systems, layers; including their principles, elements, and components. Architectural diagrams break down complex systems and processes into layers. Conceptual framework for the proposed system is represented in fig 1.2 account data is processed into a financial information which

undergoes the first encryption phase of the model using playfair cipher algorithm to perform character substitution and obtain the first encrypted data. The first encrypted data is going to the second phase of the encryption of the model where ceaser cipher algorithm is used to perform a letter swapping to obtain a more sophisticated cipher text.

The Proposed FAMG Cryptography Model

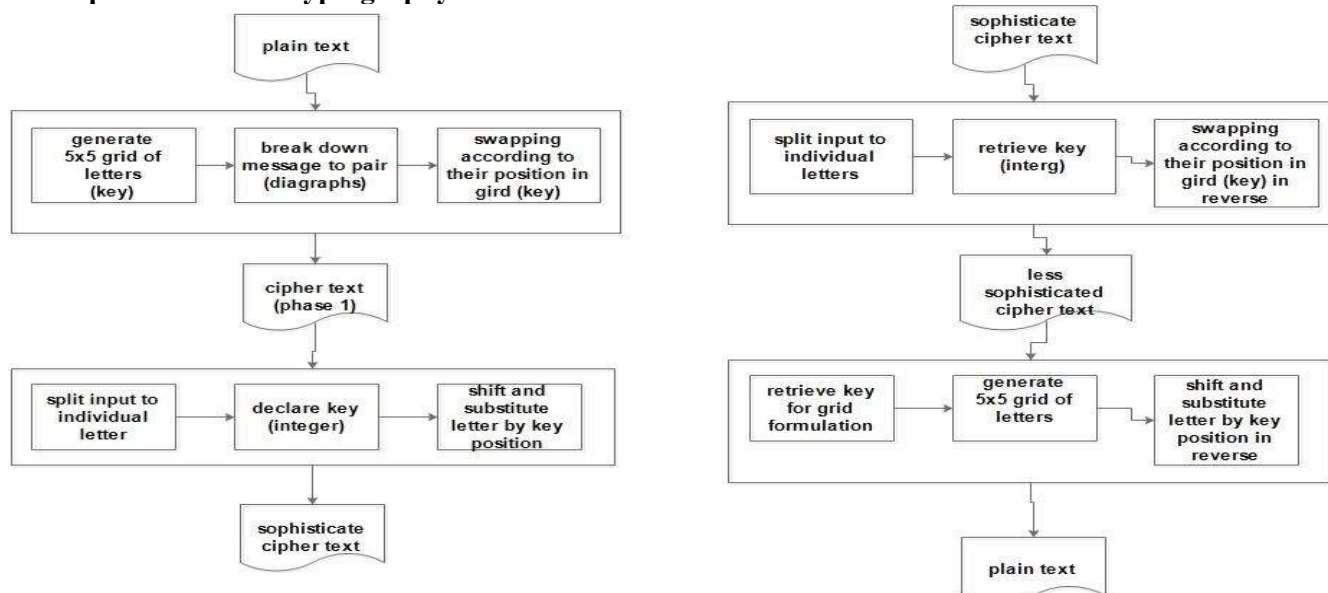


Fig 1.3 the proposed FAMG cryptography model

The mark model cryptography merges two cryptographic model to get a more sophisticated cipher text which is believed that, it will make intrusion difficult. The first phase of the encryption process make use of the playfair cipher model. This phase receives a plan text, generate a 5x5 grid of letters which act as the encryption key, break down the message into pairs called diagraph. The diagraph (pairs of letter) are swapped using the key to generate the cipher text for the diagraphs. The process continue until all pairs of letter in the play text has been encrypted. The encrypted text from phase one is passed to the phase two of the encryption model which uses ceaser model to create more sophisticated cipher text. The input is split into individual letters, an integer is generated and letter substitution is performed on all the individual letter using the key as the shift length. The reverse is the case for decryption, the ceaser cipher is used firstly to generate the playfair cipher text which is further decrypted using playfair model to get the plain text.

Application Flowchart

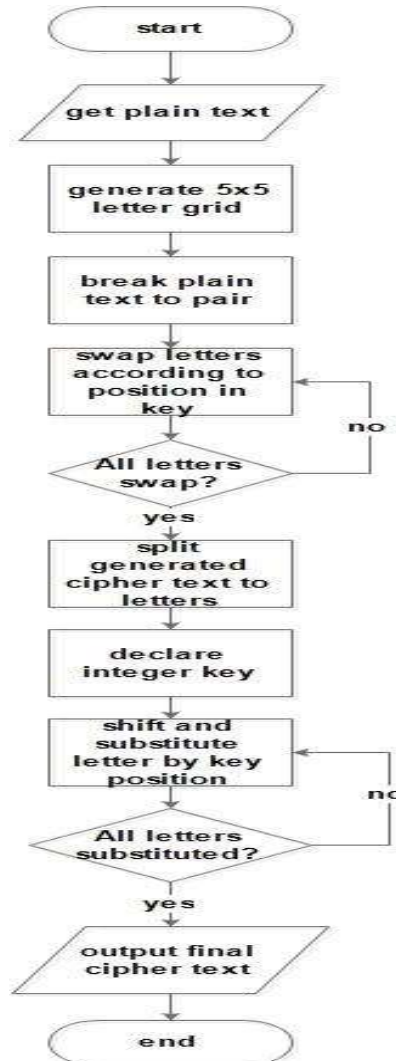


Fig 1.4 Application flowchart

4. Result and discussion

The proposed model is built with the benefit of an object-oriented approach. The system seeks to build a computational model to solve intrusion problems associated with the online banking system. The flow of data in the proposed system is in such a way that user can only access the application using web browser, login or register as new user to perform desire task. The proposed system adopts and integrate Playfair cipher algorithm and Ceaser cipher algorithm. The playfair algorithm is first use to encrypt banking

information, generating a Playfair cipher text, the playfair cipher text is further encrypted using the ceaser algorithm to generate a more sophisticated cipher text that will be difficult to decrypt whenever intrusion occurs.

To test and validate the developed model, an online banking system was mimicked that will allow customer create online banking system information linked to mimicked bank account. Fig 1.5 shows the mimicked online banking system.

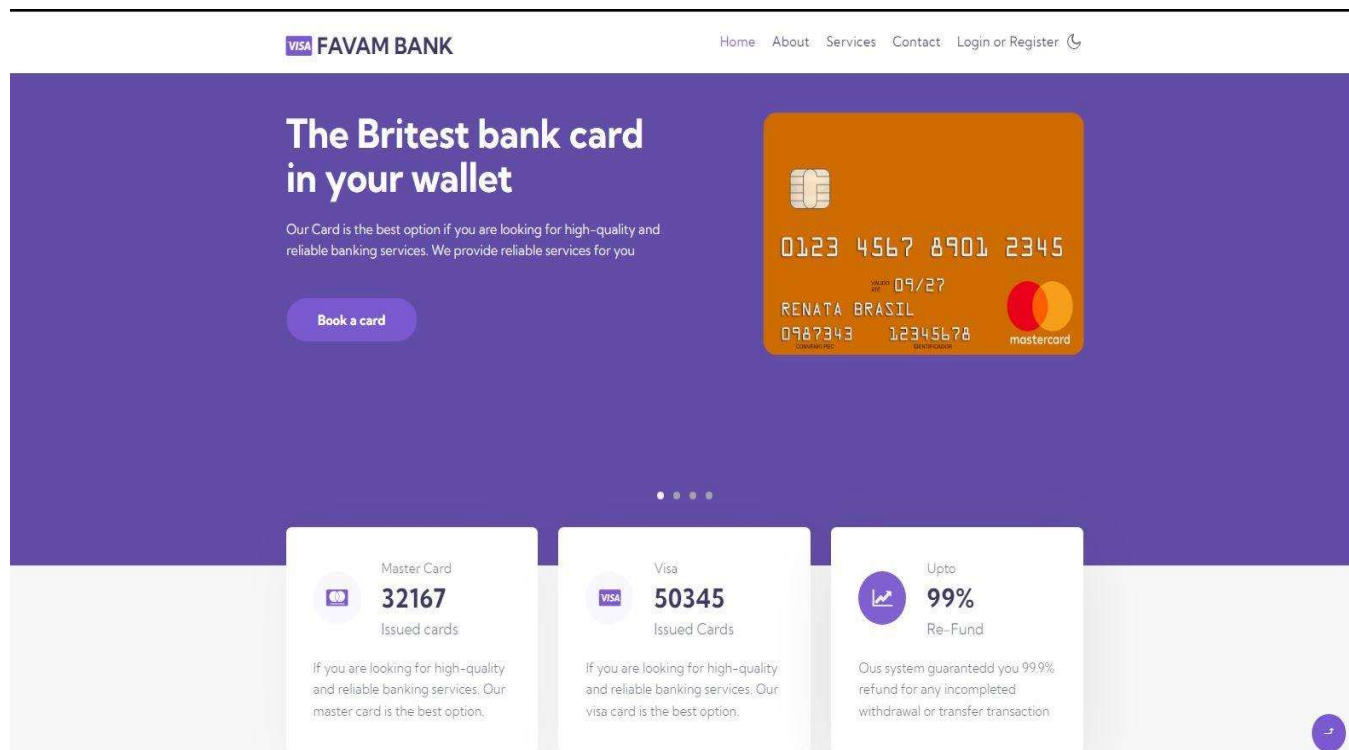


Fig 1.5 online banking home page

The online banking homepage in fig 1.5 is the starting point of the mimicked online banking application, it gave a brief introduction of the bank and provides navigation links, linking the user to other module within the online banking space.

Customer Information

Surname

Firstname

Othername

Email

Phone

State of Origin

LGA

Contact Address

Residential Address

Account Type

Savings Account

Current Account

Fig 1.6

Fig 1.6 shows a mimicked form of online banking users information. Users are to provide the above information so as to have a mimicked bank account and online banking profile which enables them to perform basic banking operation. The FAMG model

takes on the provided information and perform encryption process to obtain a sophisticated cipher text that will be stored in the database and can't not be easily read by cryptanalysts. Fig 1.7 below shows shot of the saved customer information.

	Phone	Surname	FirstName	OtherNames	AccountNum...	AccountType	CardType	RequestType	PickUpType	PickUpLocation	DeliveryLocati...	PasswordHash
▶	sdtttdkdgj	vjtceukqsZ	eisigzvY	Efxft	ikikuqqiuq	tezjinaS	NULL	NULL	NULL	NULL	NULL	\$2a\$13\$bSfBrt8...
	nduonfdsiusC	vjtceukqsZ	eisigzvY	eisigzvY	NULL	hmnixvB	NULL	NULL	NULL	NULL	NULL	\$2a\$13\$ya.rm1X...
	NULL	NULL	NULL	NULL	admin	NULL	NULL	NULL	NULL	NULL	NULL	\$2a\$13\$9MfOz...
◊	NULL	NULL	NULL	NULL	NULL	NULL	NULL	NULL	NULL	NULL	NULL	NULL

Fig 1.7 image showing encryption result of FAMG model

The FAMG model uses the combination of Playfair cipher and Caesar cipher to encrypt the online banking information such that only authorized and authenticated user with generated key can have the information decrypted for human understanding. Fig

1.7 shows encrypted online banking customer information. The model uses the Playfair cipher to encrypt the information, the encrypted data is encrypted using the Caesar cipher model to obtain a more complicated cipher text.

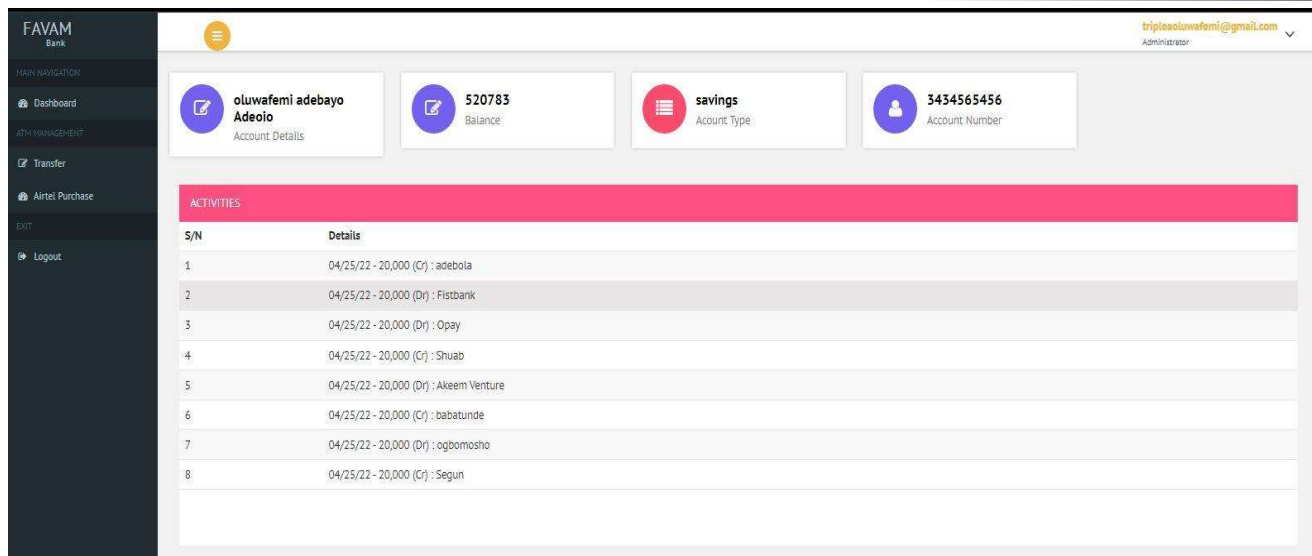


Fig 1.8 authorized user dashboard

The online banking dashboard allow authenticated and authorized user performed financial transaction against their account balance. The information show to the customer have been decrypted using the key assigned to them during authentication and have been organized to its minimum simplicity.

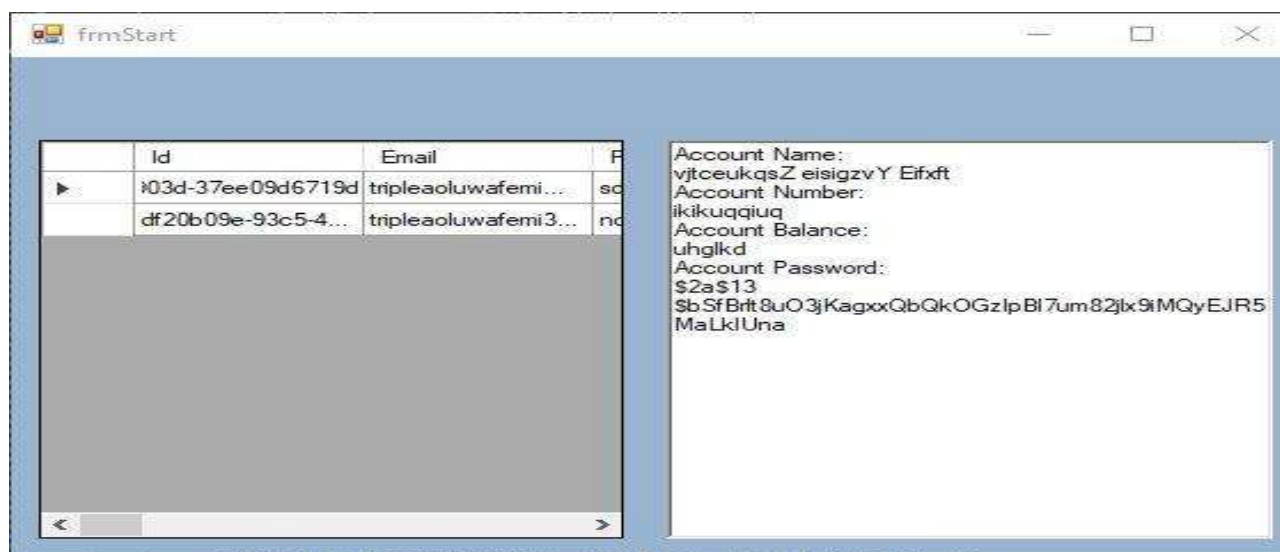


Fig 1.9 SQL injection/penetration

To test the efficiency of the proposed model, and SQL injection application was designed. The application attempt to retrieve the online banking customers' information through intrusion using SQL injection. Fig 1.9 shows the result from the intrusion which is human unreadable and encrypted.

5. Conclusion

Online banking is a kind of banking operation that take place over the internet without the customer visiting the bank physically. Online banking has been employed recently to ease banking stress and control crowding in the banking premises. In this research, we discover various challenging facing the online

banking system in which intrusion ranked highest. In view of this, we proposed a FAMG cryptography model which combines playfair cipher and ceaser cipher to produce a complicated cipher text. C# programming language is used for mimicking of an online banking system where the proposed model was implemented. Models have been developed, algorithm has been formulated and being translated to machine readable code. The efficiency of the model to encrypt and decrypt in good time considers it to be good for the identified problem and the encryption cannot easily be decrypted because it complicated and uses more computing power than can be imagined by the cryptanalysts.

References

- Ahmed, Alim Al Ayub; Paruchuri, Harish; Vadlamudi, Siddhartha; Ganapathy, Apoorva. Cryptography in Financial Markets: Potential Channels for Future Financial Stability. *Academy of Accounting and Financial Studies Journal*; Arden 25(4), 1-9.
- Alamgir H., Yukon B., Najmul H. and, Md Farijul I. (2020). Perception and prediction of intention to use online banking systems: An empirical study using extended TAM. *International Journal of Research in Business and Social Science*, VOL 9NO 1ISSN: 2147-4478
- Ali, M., Kalwar, M., and Khan, M. (2021). Challenges for Online Banking in Customers' Perspective: A Review. 2021.
- Amir H. (2022). Applied Introduction to Cryptography into the conventional authentication and authorization mode for the online banking
- Anish, K. (2016). Attack Development for Intrusion Detection Evaluation. Submitted to the Department of Electrical Engineering and Computer Science in partial fulfillment of the requirements for the degree of Bachelor of Science in Computer Science and Engineering and Masters of Engineering in Electronic Engineering and Computer Science at the Massachusetts Institute of Technology.
- Anshita (2020) Proposal biometric impression and digital signatures to make transaction by bank customers, <https://scholars.google.com>
- Arafat, H. (2001). A new Model for Monitoring Intrusion based on Petri Nets. Information.
- Damien, H. and Mathew, W. (2010). Security for Internet banking: a framework. *Logistics Information Management* 16(1): 64-73
- Debar, Hervé. (2021). An Introduction to Intrusion-Detection Systems.
- Dhananjay, D. (2021) Introduction to Cryptography Indian Institute of Information Technology, Lucknow ddey@iiitl.ac.in January 18, 2021
- Frankenfield (2022) What is Online Banking? Definition and How It Works, Updated March 24, 2022, www.investopedia.com, accessed August 12, 2022
- Gaikwad, S., Kunal, T. and Vaishali, B. (2021). Anomaly Based Intrusion Detection System Using Artificial Neural Network and fuzzy clustering., *International Journal of Engineering Research & Technology (IJERT)*, ISSN: 2278-0181.
- Halimaa, A. and Sundarakantham, K. (2020) "Machine Learning Based Intrusion Detection System," 2020 3rd International Conference on Trends in Electronics and Informatics (ICOEI), 2020, pp. 916-920, doi: 10.1109/ICOEI.2019.8862784.
- Joseph, S., Tommy, G. (2003). Intrusion detection: methods and systems. Part II. <http://www.emeraldinsight.com/0968-5227.htm>
- Kishore, R. and Chauhan, A. (2020). Intrusion Detection System a Need," 2020 IEEE International Conference for Innovation in Technology (INOCON), 2020, pp. 1-7, doi: 10.1109/INOCON50539.2020.9298398.
- Lakshmi P. and Ramesh, A. (2020). Secure Internet Banking Authentication. *Journal of Engineering Science*, Vol 11, Issue 2, FEB /2020, ISSN NO:0377-9254
- Mechanisms, Human Vulnerabilities and Attack Methods. *IEEE Access*, vol. 9, pp. 11895-11910, 2021, doi: 10.1109/ACCESS.2021.3051633.
- Mehmood A., Muhammad A. K., and Muhammad A. K. (2021). Challenges for Online Banking in Customers' Perspective: A Review. *International Journal of Business Education and Management Studies*, Vol.5. Issue 1.
- Nigel P. Smart (2005) Information Security and Cryptography University of Bristol, UK ISSN 1619-7100 ISSN 2197-845X (electronic) ISBN 978-3-319-21935-6 ISBN 978-3-319-21936-3 (eBook) DOI 10.1007/978-3-319-21936-3
- Omega. S, Baha, E. Garba, J. (2021). Enhanced Security Framework for Internet Banking Services. *Journal of Information Technology and Computing*, Volume 2, Issue 1: 9–29
- Qais (2021) Internet insecurity is one of the leading issues among online banking customer across the world with high level threats <https://researchgate.net>
- Sarjiyus (2021) An insight to ascertain the existing security features into banks, [https:// www.investopedia.com](https://www.investopedia.com)
- Sodiya, A and Akinwale, A. (2004). A new two - tiered strategy to intrusion detection. *Information Management and Computer Security*. Pp 27-44.
- Tsai, C. H. and Su, P. C. (2021). The application of multi-server authentication scheme in internet banking transaction environments. *Inf Syst E-Bus Manage* 19, 77–105 (2021).
- Waleed A., Hammood, R. A. and Omar A. H. (2020). A Review of User Authentication Model for Online Banking System based on Mobile IMEI Number. *IOP Conference Series: Materials Science and Engineering*