Holistic Exploration of Gaps vis-à-vis Artificial Intelligence in Automated Teller Machine and Internet Banking

Adekunle Y. A.
Computer Science Department
Babcock University, Ilisan-Remo, Ogun State, Nigeria

Akinola Kayode E.
Computer Science Department
Babcock University, Ilisan-Remo, Ogun State, Nigeria

Okolie S. O.
Computer Science Department
Babcock University, Ilisan-Remo, Ogun State, Nigeria

Adebayo A. O.
Computer Science Department
Babcock University, Ilisan-Remo, Ogun State, Nigeria

Ebiesuwa S.
Computer Science Department
Babcock University, Ilisan-Remo, Ogun State, Nigeria

Ehiwe D. D.
Computer Science Department
Babcock University, Ilisan-Remo, Ogun State, Nigeria

ABSTRACT

Artificial Intelligence (AI) is a computer science discipline that seeks to create intelligent software and hardware that can replicate our critical mental faculties in order to work and react like humans. Key applications of AI include speech recognition, language translation, visual perception, learning, reasoning, inference, strategizing, planning, decision making, and intuition. Automated Teller Machine (ATM) is a system that is in place to provide the users with instant cash; this system rides on the technology of AI. But the system functions with a single tier of security - called the Personal Identification Number (PIN). The ATM is an electronic telecommunication device that allows the financial institutions customers to directly use a secure method of communication to access their bank accounts. It is a self-service banking terminal that accepts deposits and dispenses cash at a lightning speed. Any ATM installed operates while the card is inserted into the machine. However, as man begins to realize the gains brought about by this machine to supplement human tellers, little did one know that the joy shall be short lived by the various sharp practices leading to financial losses. As banks are losing, so are the customers. News Media are filled with various forms of complaints on how users are losing money to fraudsters. Some have vowed never to come near usage of various cards – debit, credit or prepaid – local or international. The problem may even go as deep as engaging in legal battle between banks and their customers.

This paper presents various gaps in authentication methods used in ATM transaction and their vulnerabilities and proffer robust authentication method to curb fraudulent activities in ATM. Hence, the need to find a lasting solution to ATM fraud is the main thrust of this paper.

Keywords

ATM, Artificial Intelligence (AI), Iris Recognition, Fraudster, Gaps, Internet Banking (IB)

1. INTRODUCTION

1.1 What is Artificial Intelligence (AI)?

Artificial Intelligence (AI) can be defined as a branch of computer science that aims to create intelligent machines. Also, it refers to the development of machines or systems that can perform complex tasks normally considered to require ‘intelligence’ and thus thought to be the preserve of humans. Broadly speaking, a computer system that can sense, comprehend, act and learn. In other words, a system that can perceive the world around it, analyze and understand the information it receives, take actions based on that understanding, and improve its own performance by learning from what happened. In other words, by enabling machines to interact more naturally – with their environment, with people and with data – the technology can extend the capabilities of both humans and machines far beyond what each can do on their own.

Machine learning is a core part of AI. It uses data to train algorithms and give computer systems the ability to "learn" (i.e. progressively improve performance on a specific task) with data, without being explicitly programmed.

Deep learning is the most advanced type of machine learning. In recent years, the availability of large amount of data (“big data”) and the leap forward in computing power have paved the way towards unprecedented levels of performance, allowing for new levels of automation.

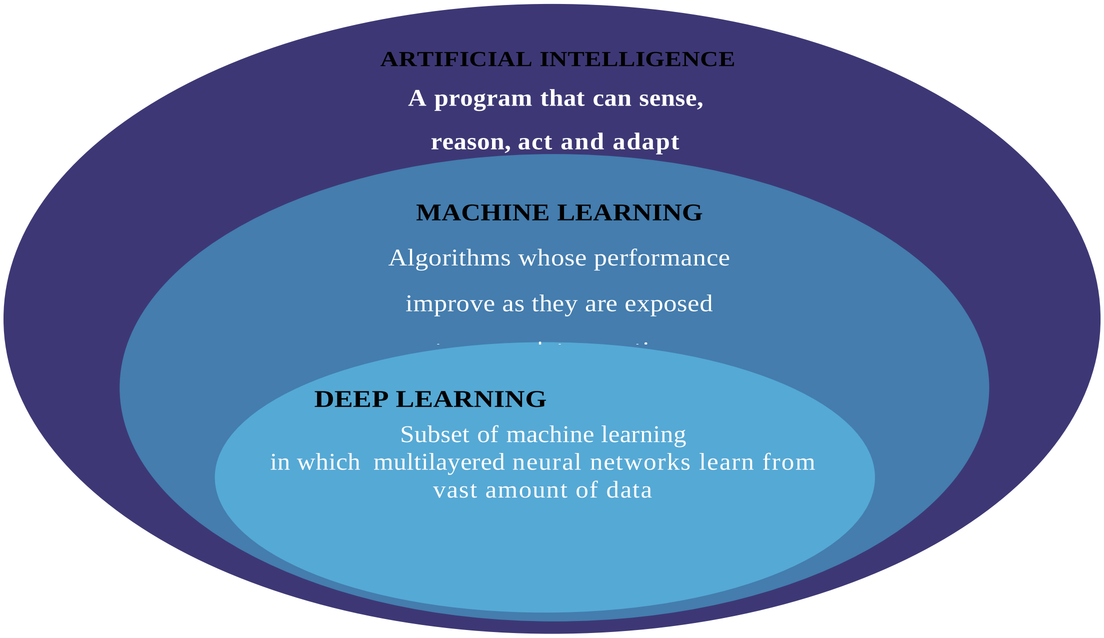
ARTIFICIAL INTELLIGENCE
A program that can sense,
reason, act and adapt
MACHINE LEARNING
Algorithms whose performance
improve as they are exposed
DEEP LEARNING
Subset of machine learning
in which multilayered neural networks learn from
vast amount of data

Figure 1. Artificial Intelligence, Machine Learning and Deep Learning

This work focuses at analyzing and exploring gaps vis-à-vis artificial intelligence in ATM and IB transactions.

From the definition of AI - A computer system that can sense, comprehend, act and learn. In other words, a system that can perceive the world around it, analyze and understand the information it receives, take actions based on that understanding, and improve its own performance by learning from what happened.

Automated Teller Machine (ATM) is a system that is in place to provide the users with instant cash; this system rides on the technology of AI. But the system functions with a single tier of security - called the Personal Identification Number (PIN). The ATM is an electronic telecommunication device that allows the financial institutions customers to directly use a secure method of communication to access their bank accounts. It is a self-service banking terminal that accepts deposits and dispenses cash at lightning speed. Any ATM machine installed operates while the card is inserted into the machine.

The primary step of the functioning is the insertion of the ATM Card into the system. This process is followed by the phase that requests for the PIN of the ATM card inserted. PIN is generally four digits that are kept in secrecy by the user. This PIN entry determines the transaction to continue or abandon. Also the three times wrong entry of a PIN would lead to the blocking of the ATM card in sensing a possible fraudulent transaction. Once the ATM PIN number is successfully validated, the user is given options regarding the financial services to be performed. Once selection of a particular financial service is made, the service is rendered by the ATM and the transaction is said to have come to an end.

1.2 Statement of Problem

In the existing system, there is this lack of the complete authentication phenomenon in the ATM terminal. Any individual is not completely authenticated before they are allowed to perform the transactions in their ATM terminal. Their authenticity is only determined with the PIN they enter in the terminal. The true verification of customer's identity with any other available means is the thrust of this write up; while the focus of this study is to analyze and explore gaps vis-à-vis artificial intelligence models in ATM and internet banking with a view to propose robust authentication method.

1.3 Aim and Objectives

The aim of this study is to propose a robust authentication mode of operation using Iris recognition as a means of authenticating users during ATM transaction to solve the present security challenge faced in the use of ATM.

The study sets out to achieve the following specific objectives:

1. Examine the characteristics of existing embedded artificial intelligence (AI) models in automated teller machine and internet banking transaction.

2. Identifies gaps in the existing embedded artificial intelligence (AI) models in automated teller machine and internet banking transaction.

3. Propose robust artificial intelligence authentication models in ATM and IB transaction.

1.4 Existing Model of Authentication in ATM

In the existing system, the major sequential operations that are currently involved in the ATM services are as follows:

1. Inserting the ATM card in the respective ATM Terminal.
2. Entry of the secret Personal Identification Number (PIN) with respect to the ATM card by the card holder.
3. Transaction selection (Financial aspects like balance enquiry, withdrawal, deposits).
4. Completion of the transaction and termination of the session.

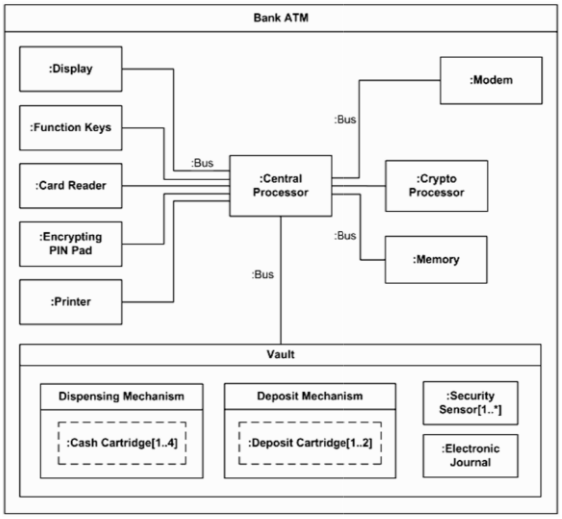

Figure 2. Internal Architecture of ATM (Source: Navneet, 2011)

1.4.1 Flaws in the existing ATM authentication model

Identity Theft or Impersonation - is the major challenge and upon which all other ATM fraud revolves.

1. Eavesdropping

The ATM card or PIN of a user can be spied upon and can be accessed easily by obtaining the card by faulty means. This can lead to some serious consequences.

2. Spoofing

There is a possibility that, when a user enters the PIN during the transaction process, a hacker fakes as the authorized site and prompts the user to re-enter PIN due to a system error. When a user complies with the instruction the hacker stores the data and uses it for his future peccadillo intentions.

2. REVIEW OF EXISTING EMBEDDED AI MODELS IN ATM AND INTERNET BANKING TRANSACTIONS.

Ibidapo et al., (2010) introduced the finger print recognition as a form of AI model into ATM for authentication. The customer would insert an ATM card, PIN number and enroll his or her fingerprint into the fingerprint device or reader adapter into the system. After which the fingerprint database compares the live sample provided by the customer with the template in the database. On confirmation that the information provided is true, that customer is granted access to the ATM system. However, the system was not fully deployed to ascertain flaws that may emanate from its usage in ATM transaction.

Scotiabank (2010) presented a software token that is stored on the computing devices such as laptop, android phones and so on as a second authentication factor. Like the hardware token, a user accesses the software token from the device where it is installed after supplying the PIN and password, it generate a set of digits to be used as a second factor authentication. However, as reliable as the device is, an outright theft of loss can lead to fraud.

Oko and Oruh (2012) developed an ATM based fingerprint and token verification as an embedded AI model. The customer incorporate fingerprint into the bank’s database during registration. Verification is conducted during ATM transaction with hardware token. The set back in this solution was that, the system developed did not have matching algorithm. Hence, high false rejection rate (FRR).

Krisbruner (2013) emphasized the relevance of voice recognition and PIN as an AI instrument for authentication in mobile banking transaction. The solution employed voice recognition as second level authentication in addition to PIN before accessing mobile banking transaction. The customer would be required to speak a word or phrase which will be recorded for subsequent use. However, the solution has high false rejection rate (FRR) may be due to the fact that the customer has cough or crack in their voice.

Jimoh and Babatunde (2014) developed prototype of an enhanced ATM using short message service (SMS) in addition to the existing four digital PIN and card as a means of authentication. For Withdrawal Operation, if the amount to be withdrawn is greater than #5,000, the ATM automatically generates a four digit random code, stores the code as the authentication code and send to the phone number corresponding to the account number. However, if the amount to be withdrawn is less than #5,000, the machine dispenses cash immediately. The solution only considered a minimum withdrawal amount and network failure or fluctuation can truncate the transaction process.

Sirapat and Boonkrong (2015) introduced image drawing, password and username as an embedded AI model during in internet banking transaction. Combining the use of username and password, users are allowed to draw any image of their choice as a means of authentication. This makes it different from other existing image authentication mechanisms which force users to choose pre-defined images. The solution has some advantage over the existingPIN and password. Nevertheless, during the implementation failure to login was observed and the system was two seconds longer than the existing system.Frimpong, Kofi and Michael (2016) implemented multi factor authentication method using finger print scanner. Microsoft visual studio 2010 (C#) was used to develop the front end while Microsoft structured query language server 2008 was used to design the back end and finger print scanner a Grfinger software development kit (SDK) was employed in the implementation. The system has an overall efficiency of 94%, FAR 4%, FRR 2% and TER 6%.

Ankit and Neelu (2017) proposed multi factor fraud reduction in ATM using voice recognition and encrypted PIN. The system consists of training the database of an authorized person. The real voice input through the use of microphone will then be compared. The comparing process is carried out by feature extraction and feature matching with that of the stored samples of authorized person in the database. The draw back in this proposed system was that; the system was not built as an enhancement of the existing system.

Jayakumar et al., (2017) proposed multi factor authentication model using smartcard, short message service, iris and finger print of the customer. The smartcard would be inserted into the ATM, then the machine would request for the PIN , scan the iris and recognize finger print before allowing the legitimate owner of account to withdraw money. If somebody tries to break the ATM an alert message is sent to the nearest police station and the ATM shutter is automatically closed. The draw back in this proposed system was that; the system was not built as an enhancement of the existing system.

2.1 Summary and Proposed Authentication Model

Consequently, looking at the various gaps in the existing AI models, this study proposes integrating biometrics (Iris Recognition) AI model; as a means of identifying and authenticating account owners at the Automated Teller Machines and IB transactions as this will give the needed and much expected solution to the problem of illegal transactions (Awodele and Akanni, 2012).

3. BIOMETRIC TECHNOLOGY

Biometric technology deals with recognizing the identity of individuals based on their unique physical or behavioral characteristics. Physical characteristics such as fingerprint, palm print, hand geometry and iris patterns or behavioral characteristics such as typing pattern and hand-written signature present unique information about a person and can be used in authentication applications (Jain and Anil, 2008; Jain and Hong, 2000).

3.1 Biometrics Comparison

Table 3.1.Comparison of Biometric Technologies

Biometrics	Cost	Accuracy	Performance	Flaws	Stability
Iris	Medium	High	High	Lighting	High
Retina	Medium	High	High	Glasses	High
Face	Medium	Medium	Medium	Beard, glasses, age	Medium
Fingerprint	Low	Medium	Medium	Dirt, dryness	High

4. CONCLUSION AND RECOMMENDATION

This study review and explore various gaps vis-à-vis artificial intelligence (AI) in automated teller machine (ATM) and internet banking (IB) and proposes a robust authentication model in ATM and IB transactions through the use of Iris recognition, PIN and smartcard.

5. REFERENCES

[1] Ankit, S. and Neelu, J. (2017). Fraud Reduction in ATM Machines using Voice Recognition- A Review. International Journal of Innovative Research in Science, Engineering and Technology(ijirset), 6(5), 7525-7530.

[2] Awodele, O. and Akanni, A. (2012). Combating automated teller machine frauds through biometrics. International Journal of Emerging Technology and Advanced Engineering, 2(11), 441 -444.

[3] Frimpong, T., Kofi, N., and Michael, A. (2016). Improving Security Levels In Automatic Teller Machines (ATM) Using Multifactor Authentication. International Journal of Science and Engineering Applications. 5(3), 126-134.

[4] Ibidapo, O. A., Omogbadegun, Z. O, and Oyelami, O.M. (2010). Towards Designing a Biometric Measure for Enhancing ATM Security in Nigeria E-Banking System. International Journal of Electrical and Computer Sciences IJECS-IJENS. 10 (6). 63-68.

[5] Jayakumar, S., Alamelu, Radhika , Ramya , Dharani and Senthil J., (2017). Enhanced way of Securing Automated Teller Machine to track the mis-users using secure monitor tracking analysis. IOP Conf.

Ser.: Mater. Sci. Eng. 263 042032. doi:10.1088/1757-899X/263/4/042032.

[6] Jimoh, R.G. and Babatunde, A. N. (2014). Enhanced Automated Teller Machine using Short Message Service authentication verification. World Academy of Science, Engineering and Technology. International Journal of Computer, Information Science and Engineering. 8(1). 14-17.

[7] Muhammad, B.L., Alhassan M.E. and Ganiyu, S.O. (2015). An Enhanced ATM Security System using Second-Level Authentication. International Journal of Computer Applications. 111(5). 8-15.

[8] Navneet S. (2011). Vulnerability and security issues in Auto teller machine transactions . National Conference on Secure Data Communication and networks, 978-81-7906-273-9

[9] Oko, S. and Oruh, J. (2012): Enhanced ATM security system using biometrics. IJCSI International Journal of Computer Science Issues. 9(5). 352-357.

[10] Scotiabank (2010). Mobile Banking Security and Privacy. www.scotiabank.com.

[11] Supakit, M. and Sirapat, B.(2015). Improving Security with Two-factor Authentication Using Image. KMUTNB Int J Appl Sci Technol. 8(1), 33-43.