Asian Journal of Research in Computer Science

5(3): 7-20, 2020; Article no.AJRCOS.56340
ISSN: 2581-8260

Design and Implementation of Cost Effective Multi-factor Authentication Framework for ATM Systems

Nuku Atta Kordzo Abiew[1*], Maxwell Dorgbefu Jnr.[2] and Samuel Osei Banning[1]

[1]Faculty of Computing and Information Systems, GTUC, Ghana.
[2]Department of Information Technology Education, UEW, Ghana.

Authors' contributions

This work was carried out with a solid collaboration among all authors. Author NAKA worked on the system design, coded the system and performed the experiments. Author MDJ managed the literature searches, developed the threat model, validated the system design and wrote the first draft. Author SOB run the experiments and managed the analyses of the findings. All authors read and approved the final manuscript.

Article Information

DOI: 10.9734/AJRCOS/2020/v5i330135
Editor(s):
(1) Dr. R. Gayathri, Anna University, India.
Reviewers:
(1) Ding Wang, Peking University, China.
(2) Irena Ilieva Jekova, Bulgarian Academy of Sciences, Bulgaria.
Complete Peer review History: http://www.sdiarticle4.com/review-history/56340

Original Research Article

Received 14 February 2020
Accepted 20 April 2020
Published 27 April 2020

ABSTRACT

Banks and financial institutions all over the world have adopted and continue to adopt Automated Teller Machine (ATM) systems into their transactions to extend banking hours, and also provide convenience for their customers. ATM systems are networked computerized systems, and as the case is in these systems, their security must be given the highest priority. Among the many strategies for ensuring secured networked systems, authentication is very important. Authentication is the process of verifying the identity of a user or a process that attempts to access information resources from a system. Good authentication methods and schemes are one of the best standard ways of implementing security on computerized systems. The importance of selecting an environment appropriate authentication method is perhaps the most crucial decision in designing secure systems. Authentication protocols are capable of simply authenticating the connecting party or authenticating the connecting party as well as authenticating itself to the connecting party. The verification process is usually based on authentication factors like facts, characteristics, behaviors, or knowledge known only to both the claimant and the verifier. Based on these authentication factors, authentication is classified into knowledge-based (KBA), token-based (TBA) and

**Corresponding author: E-mail: akordzo@gtuc.edu.gh;*

biometrics-based (BBA) authentications. In this paper, we designed and implemented a hybrid and secure cost-effective authentication framework for ATM systems based on the strengths of the three main authentication classifications.

Keywords: Authentication; biometrics; claimant; knowledge-based; token-based; verifier.

1. INTRODUCTION

The Enfield Town branch in North London, United Kingdom of the Barclays Bank, is recorded in history to have introduced the first ATM on June 27, 1967. Two years later on September 02, 1969 the Chemical Bank also installed the first ATM in the United States at its branch in Rockville Centre, New York. These two remarkable developments in retail banking has transformed the face of banking to date with numerous gains to both the banks and their customers. An automated teller machine (ATM) is an electronic telecommunications device that enables customers of financial institutions to perform financial transactions, such as cash withdrawals, deposits, transfer funds, or obtaining account information, at any time and without the need for direct interaction with bank staff [1]. ATMs are means of extending banking hours and also providing convenience to bank customers.

Since the inception and adoption of ATMs, these systems have evolved over the years. As in all networked computerized systems, these systems require a great deal of security for their continuous function. Hackers over the years have launched numerous attacks on ATM systems. These attacks are usually categorized into card skimming, card trapping, transaction reversal fraud, cash trapping, physical attacks, and logical attacks. Many of the financial institutions that were victims of these attacks due to one vulnerability or the other in the ATM systems have suffered a great deal of financial loss in these attacks. The motives of these attackers are largely to steal funds of legitimate owners of bank accounts they compromise.

Many studies have shown that most of the attacks are largely due to security lapses on the part of the account owners. Key among these lapses are easy to guess personal Identification numbers (PINs), writing down of PINs, asking for help during transactions from strangers who lurk around ATMs, and unnecessary exposure of ATM cards. The presence of these lapses demands that the authentication processes are strengthened in ATM systems.

Authentication in ATM systems has been largely a two-factor thing. Thus token based authentication (TBA); this is authentication based on what you have or possess, and knowledge based authentication (KBA); authentication based on what you know. But over the years, the third mechanism has emerged and has been implemented; the biometric based authentication (BBA); authentication based on what you are. Biometric authentication ranges from iris scan, hand geometry, gait, and keystroke dynamics.

Many studies have moved from the two-factor authentication to a three-factor authentication. The researchers in these areas have designed and implemented novel frameworks for ATM systems authentication thereby improving upon the overall security of these systems. Many of these studies are detailed in the related works section of this paper. Although these studies have proposed, designed and implemented these multifactor authentication systems, we found out that, the cost element in implementing these systems was not considered.

There's no arguing that PIN based authentication are less reliable in protecting financial data and identities. Their management and protection are increasingly problematic, and malicious actors have countless ways to steal them, break them, reset them, or get past them. It is also worth noting that, PIN based authentication schemes gives a smaller window to attackers to guess. In the work of Wang et al. [2], the authors elaborated on the characteristics, distribution and security of human-chosen PINs. PIN-based authentication attacks threaten the security of Internet banking operations and demoralize the users. To strengthen these authentication schemes, several strategies are exercised. Two factor authentications involving a PIN is a commonly used approach. But PINs are vulnerable to attacks during the PIN entry stage. Even though there are several secured PIN entry models proposed, our scheme is cost effective and offers superior security and good usability because of its hybrid nature, because PINs alone are not enough for full-proof authentication schemes for ATM systems.

In this paper, we design and implement a hybrid, secure and cost effective authentication

framework for ATM systems based on the strengths of the three main authentication classifications; thus PIN, card and keystroke dynamics.

1.1 Threat Model

According to Wang et al. [3], in the conventional password authenticated key exchange (PAKE) protocols the attacker A is generally assumed to be able to eavesdrop, block, alter or insert messages exchanged between the communicating parties, i.e., in full control of the communication channel. Effective evaluation of authentication frameworks need a clearly defined adversarial or threat models. In the work of Roy et al. [4] the authors adopt the widely-used Dolev-Yao threat model because of the nature of their scheme. Threat models must specify the goal, assumptions and capabilities of adversaries. Following the existing works in [5,6,7], we describe the threat model of our framework subsequently. We assume the goal of the adversary in this framework is to obtain user authentication information such as password, and ATM PINs, and maliciously perform banking transactions on an ATM system. Based on the goal of the adversary, we chose the following attacks to represent the capabilities of the adversary for our multi-factor authentication scheme for ATM systems.

1. Shoulder Surfing
2. Recording user information
3. Social engineering
4. Password guessing and Brute-force
5. Dictionary attacks

The remainder of the paper is organized as follows: literature review section carefully reviews related works in multi-factor authentication. In the system design and methodology section, we describe the design strategy and algorithms used in the design and implementation of the framework. The analysis of findings section discusses the analysis, empirical evidence and implementation of the algorithms presented. Finally, the paper is concluded in the conclusion and recommendations section.

2. LITERATURE REVIEW

The need for implementing multi-factor authentication in today's complicated and distributed Information Systems (IS) cannot be over emphasized. Our daily lives depend on computer systems many of which we use to create, as well as use data and information. Many of the information resources we rely on in the cyber space are very sensitive in nature, and useful to the survival of the 21st century business enterprises, and institutions. Multi-factor authentication systems, rely on more than a single means or factor in granting users access to their information resources in the cyber space.

According to [8], Multi-factor authentication (MFA) is a security system that requires more than one method of authentication from independent categories of credentials to verify the user's identity for a login or other transactions. MFA combines two or more independent credentials: what the user knows (such as password), what the user has (such as security_token) and what the user is (such as biometric verification). MFA is variously referred to as Two-factor authentication (2FA) or three-factor authentication (3FA). The goal of MFA is to create a layered defense and make it more difficult for an unauthorized person to access a target such as a physical location, computing device, network or database. If one factor is compromised or broken, the attacker still has at least one more barrier to breach before successfully breaking into the target.

Multifactor authentication is used to determine the right of an individual to access a physical facility or to access data within an information system. There are many commonly used authentication methods available, but individually, any of these methods have their limitations or might be easily affected by the environment in which they are implemented. In order to make a better and robust authentication, there is the need to combine all these methods to achieve higher authentication scheme to counter the weaknesses of the single-factor mechanisms. This is implemented by adding extra authentication factors to the process of authenticating a user into a system, as shown in Fig. 1. For instance, an online banking application requests the customer to enter the bank card number. After the application verifies the card number (i.e., a unique number identifies the customer record in the bank database), the customer is asked to enter a secret answer to one of the questions this customer has previously answered at enrolment time. If the customer answers correctly, the application finally requests a password to allow the customer access to his or her account. In terms of security, multi-factor authentication offers better protection against several attacks such as guessing, brute-

force, and phishing. However, the one channel used in this mechanism is the weakest part because, if the channel is compromised, all factors exchanged between the end-user and the system can be compromised accordingly.

Keystroke dynamics is a behavioral biometric characteristic based on the assumption that different people type in a unique manner. Neurophysiologic factors make written signatures distinctive as per person. These factors are also expected to make typing characteristics unique as per person. The idea behind keystroke dynamics authentication appeared in the twentieth century when telegraph operators could authenticate each other based on their distinctive patterns when keying messages on telegraph lines. Keystroke dynamics is also known variously as keyboard dynamics, keystroke analysis, typing biometrics and typing rhythms [9].

As posited in [9], although physiological biometrics is considered to be more robust and secure, they are expensive to use because specialized hardware components are required for feature detection, extraction, and verification. On the other hand, behavioral characteristics are cheaper than physiological characteristics because additional hardware is not required. Thus behavioral characteristics are easy to reveal but hard to forge. Because of the variability over time, most of the biometric systems need to be designed to be more dynamic and accept some degree of instability.

Keystroke rhythm is a good sign of identity. Moreover, unlike other biometric systems which may be expensive to implement, keystroke dynamics is almost free - the only hardware required is the keyboard; which is already an integral part of most ATM systems [10].

2.1 ATM Authentication

An Automated Teller Machine (ATM) is a computerized system that allows users to perform basic banking functions when a valid bank card is inserted without the need for a bank representative's assistance. The commonest use of ATMs is for cash withdrawals despite the many other functions such as cash deposit. ATMs are kind of representation of some bank processes to the customer outside the banking hall and banking hours. The reliance of the 21st century bank customers on ATM services requires that these machines are secured, thereby protecting them from unauthorized access. A number of works have been done by researchers in ATM authentication over the years. In this section of our paper we review works related to our study. In [11], the authors outlined the main methods used for unauthorized drawing of funds from ATMs by fraudsters. These methods keep evolving as these authorized people keep changing their strategies.

In [12] the author proposed a three-factor authentication mechanism for ATM systems. The third factor in addition to password or PIN (something you know), ATM card (something you have) in their study is fingerprint (something unique about you). This work however requires extra hardware for its implementation there by incurring extra cost.

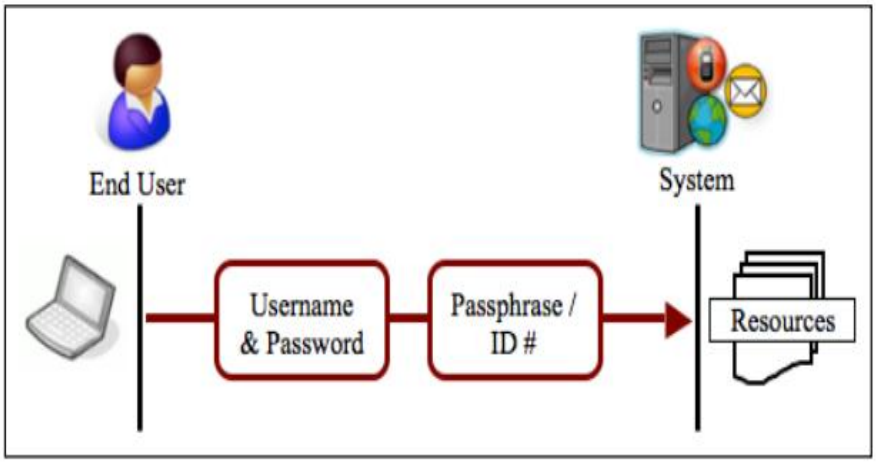

Fig. 1. Multi-factor authentication mechanism

In [13], an enhanced security for ATM machine with One-Time Password (OTP) and facial recognition features was proposed to enhance ATM security. The OTP was used for the enrichment of security of accounts and privacy of ATM users. The face recognition technology proposed in their system was to cater for the biometric authentication bit of their multi-factor authentication system. The researchers however, concluded that, there are some little flaws associated with the face recognition technique, thus the failure to detect a face when aging faces, beard, caps and glasses [13]. In addition to their own identified little flaw in the system, cost is also of concern as extra hardware component(s) are required for the full implementation of their system. ATM Transaction Security System Using Biometric Palm Print Recognition and Transaction Confirmation System was proposed by [14] (Sanjay, et al. 2014), the researchers acknowledged that, the PIN authentication system only, as used in most ATM machines is not secured. Hence, they sort to enhance the security system by introducing palm print recognition authentication as better and further mode of ensuring security at the ATM.

The inclusion of fingerprint reader in the work of [15] on improving security levels in ATM using multifactor authentication also raises the issue of extra cost element in implementing their proposed system.

The authors in [16] proposed fingerprint and PIN (the usual 4-digit long password) authentication mechanisms for enhancing security at ATM systems. The authors also ensured secured communication link between the client machines and the bank server by using an optimized energy efficient AES processor based on AES algorithm. By using biometric and cryptographic techniques their system improved security level at ATMs. The study of [16] however focused only on combining biometric system with the password-based authentication to improve security level at ATMS without considering the cost of extra hardware component; the added fingerprint readers just as the case is in most of the works reviewed in this study.

Inasmuch as these novel studies have designed and implemented systems for multi-factor authentication for ATM systems, their studies however did not take the extra hardware components leading to extra cost factor into consideration for implementing these systems. Our study therefore proposes a cost effective multi-factor authentication system using what the user has (ATM card), what the user knows (ATM PIN), and what the user is; in this case behavioral biometric: Keystroke dynamics. From the review of related works above, it is established that most of the works done in multifactor authentication for ATM systems did not take cost factor into consideration. The main focus is on providing secured system for effective ATM transactions without recourse to cost elements. This paper proposes a cost effective multifactor authentication (card, PIN, and keystrokes) framework for ATM systems.

3. SYSTEM DESIGN AND METHODOLOGY

Our proposed framework is a robust security system that can work in a real time environment. Recent works in user authentication in the financial organizations accepts biometrics as the most secure and confidential way of authentication in these organizations as this mechanism relies on some unique characteristics of every individual.

According to Monrose and Rubin [10] “Keystroke dynamics is the process of analyzing the way a user types at a terminal by monitoring the keyboard inputs thousands of times per second in an attempt to identify users based on habitual typing rhythm patterns”. It is considered as a strong behavioral biometric based authentication system. Moreover, unlike other biometric systems, which may be expensive to implement, keystroke dynamics is almost free as the only hardware required is the keyboard. ATM authentication using PIN-based entry is highly susceptible to shoulder- surfing or observation attacks.

In this paper, we implement a low cost Multifactor Authentication Framework for ATM using KBA, TBA and BBA approaches. In our system, we propose the Secure-PIN- Authentication, OTP-based authentication service for ATMs using keystrokes dynamics. Our proposed system has a significant benefit on the existing architecture adopted by the various banks since it will not require any additional hardware. The proposed system involved two stages of operations, namely registration (sign up) stage and transaction stage.

3.1 The User Registration Module

Fig. 2 shows the conceptual framework for the registration module of the proposed inexpensive

multifactor authentication scheme for ATMs. This module makes use of the three authentication schemes: TBA (something the user has), KBA (something the user knows) and BBA (something the user is).

Currently, authentication of ATM is being achieved through the use of two means of authentication, that is, through the use of a physical token such as a card and a memorized security PIN. When the confidentiality of information is particularly needful, the use of two-factor authentication may not guarantee enough protection. A stronger means of authentication, something that is more difficult to compromise and inexpensive is necessary. This is what we hope to achieve with the proposed system.

Our proposed system added an inexpensive methodology for implementing an additional layer of security to the authentication process by extracting keystrokes as the user types the PIN. The predefined processes include the training and extraction of keystrokes of users. Typing Pattern Recognition or Keystroke Dynamics is not what you type, but how you type.

During the learning stage, users are allowed to learn their typing rhythm for ten (10) consecutive times. The rhythm at each cycle is stored and a matched score is computed. In computing the matched score for each training section, the frequency or the occurrence of each of the typing rhythm or pattern is computed. The matched score is then computed as the proportion of the frequency to the total trial in our case, 10. The Matched Score (MS) is mathematically computed as.

$$MS = \frac{f}{T} * 100 \quad (1)$$

Where *f* refers to the frequency value and *T* is the total number of training in a cycle. The highest and unique MS value is then stored as the accepted rhythm of the user. In a situation where two or more MS values are the highest, the user is given the opportunity to go through the learning process all over again since for lack of uniqueness in the typing pattern or rhythm of the user.

Keystroke dynamics typically includes the analysis of characteristics such as duration of a key press or group of keys and the latency between consecutive keys i.e. time elapsed from one key to a subsequent key. During typing of the PIN, the ATM is used to record the time at which the key is pressed (dwell time) and how long the key is pressed. The time elapsed from one key to a subsequent key known as the latency is also measured. The time measured between key up and the key down is called Flight time.

Therefore, from the timing data acquired, we extract three timing features, namely:

i. Press-to-Press (PP),
ii. Release-to-Release (RR) and
iii. Release-to-Press (RP).

3.2 The User Verification Module

The user verification module ensures the user input corresponds to the claimed identity. The way of capturing these inputs greatly depends on the kind of keystroke dynamics system used (e.g., for static authentication, the user must type its login and password). While the features are extracted from the raw biometric sample (same procedure than during the enrollment), they are compared to the model of the claimed user. Usually, the verification module (a predicate method) returns a comparison score of the typed rhythm against the stored rhythm. If this score is 1 (or true), then the user is authenticated, otherwise the user is rejected.

The user verification of the proposed systems consists of two authentication stages. The first stage is devoted to measuring the typing speed of the users' chosen passwords. The second stage is the authentication stage. After extensive training with password typing, the user enters his/her password for each login session. The typing speed is calculated and compared to the password and its related typing rhythm or speed stored in the database. The difference between the actual trained typing rhythm or the value stored in the database and the current typing rhythm of the login user is compared, if the compared password or PIN and the typing rhythms are the same, the user is authenticated, otherwise the user is rejected.

Fig. 3 shows the flowchart for the PIN and keystrokes rhythm verification component for verifying authenticity of a user. A user who is already enrolled and trained already enrolled and registered onto the proposed system, will have to go through the verification process as presented in Fig. 3.

Fig. 4 to Fig. 9 show sample user interfaces of the proposed system.

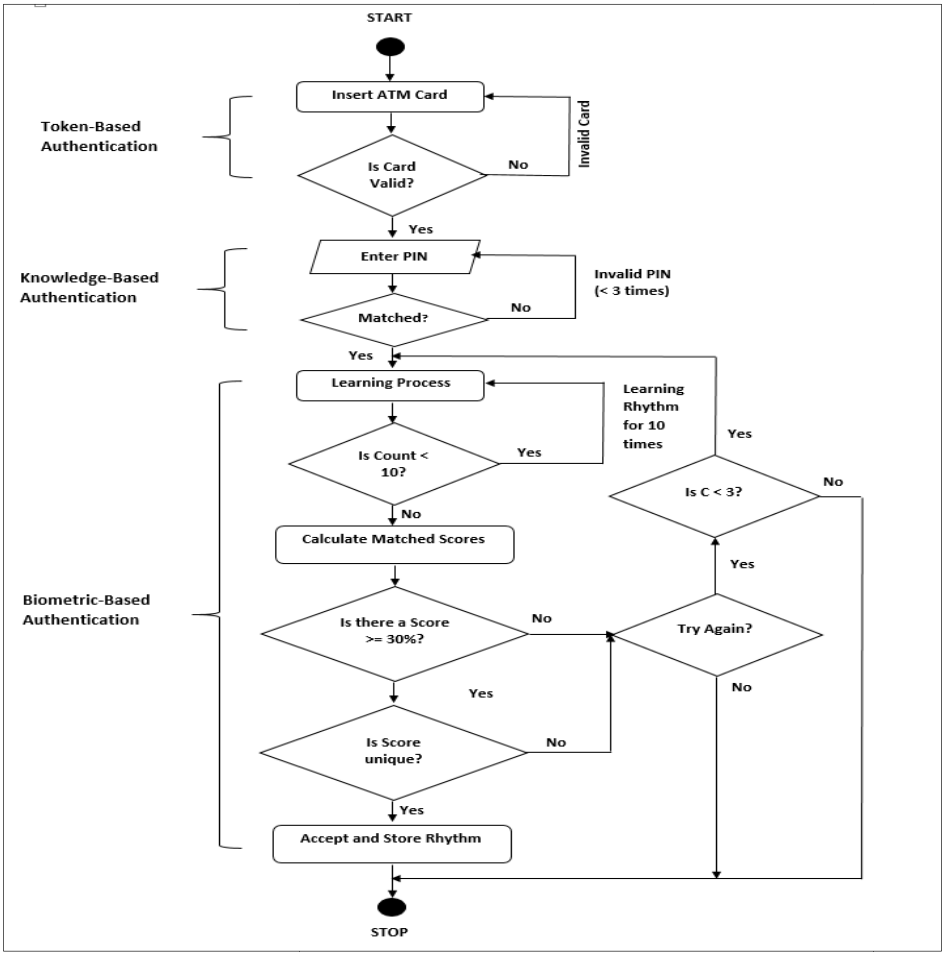

Fig. 2. Conceptual design for user registration

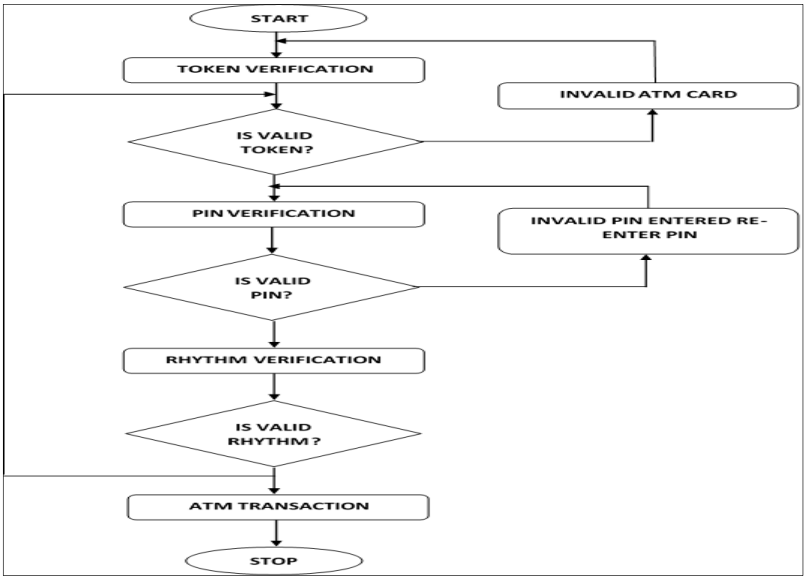

Fig. 3. Conceptual design for user verification

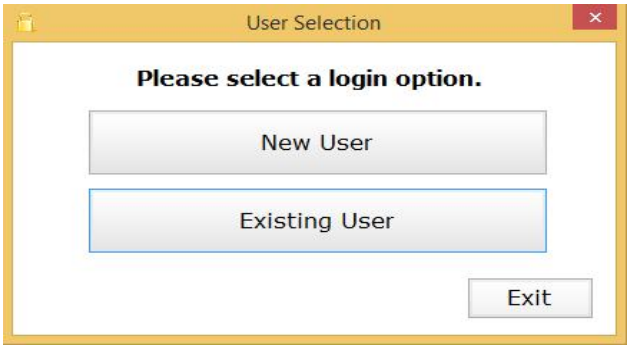

Fig. 4. User selection

Fig. 5. New user registration

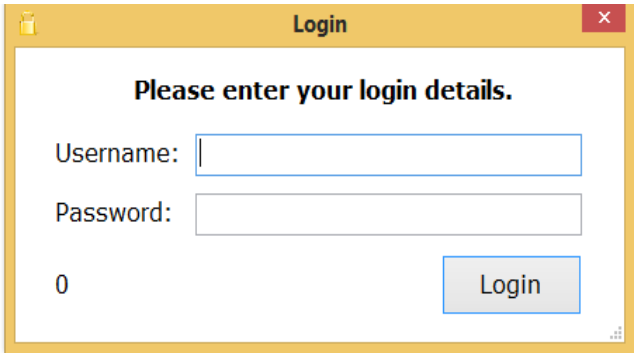

Fig. 6. User login form

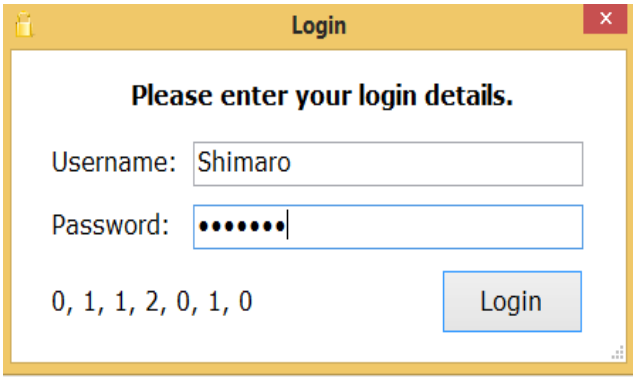

Fig. 7. User login form (showing rhythm)

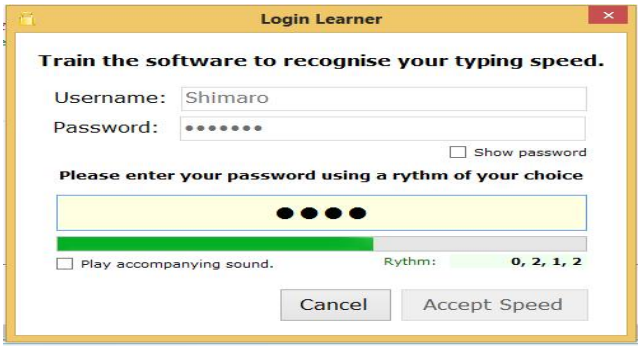

Fig. 8. Login learner

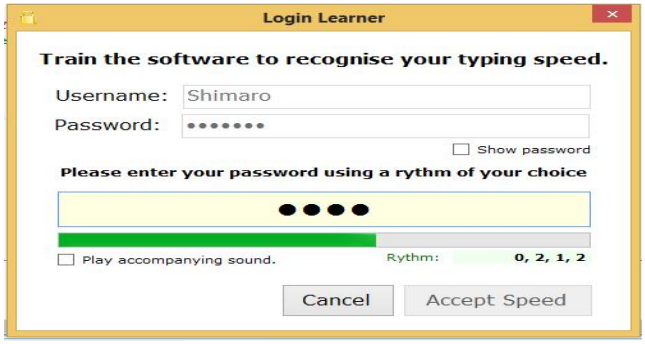

Fig. 9. Login learner (training stage)

4. ANALYSIS OF FINDINGS

After successful implementation of the proposed framework, the system was tested against the following attacks as indicated in our threat model:

1. Shoulder Surfing
2. Recording of user information
3. Social engineering
4. Password guessing and Brute-force
5. Dictionary attacks

4.1 Shoulder Surfing

Shoulder surfing is the practice of spying on users in order to obtain their personal identification number or password. Shoulder surfing is using direct observation techniques, such as looking over someone's shoulder, to get information. Shoulder surfing is an effective way of getting information in crowded places because it's relatively easy to stand next to someone and watch as they fill out a form, enter a PIN number at an ATM machine, or use a calling card at a public pay phone. Shoulder surfing can also be done at long distances with the aid of binoculars or other vision-enhancing devices such as CCTV camera. To prevent shoulder surfing, experts recommend that users shield paperwork or their keypad from view by using their body or cupping their hands. However, these approaches have not effectively prevented shoulder surfing. In [17] there is a detailed work on shoulder surfing as an attack vector that is a real threat to most authentication schemes. The authors explained the serious nature of this attack vector from different dimensions, and pointed out how most user authentication schemes take this attack for granted.

The Shoulder Surfing attack was tested using 100 users. From Table 1, it can be seen that, 0% of the attackers were successful, meaning none of the attackers was able to log in to the system though the attackers were able to capture the password successfully, they were not able to capture the pattern. They failed because they could not get the pattern and the sequences correctly.

4.2 Recording of User Information

Spywares are software that can record information about users during authentication. The use of Internet increases the chance of spywares attacks, which records users typing. Keystroke dynamics is not just about user name and password alone, it also focuses on the

sequences and patterns of typing on the keyboard. These measures make recording of user information difficult for spywares.

Spyware application such as Trojan virus was installed on the twenty-five user computers, with the aim of recording their authentication information. During the first experiment (Experiment 1) none of the user records were captured by the spyware virus. Three other experiments (Experiments 2, 3 and 4) were conducted with three different groups consisting of twenty-five users each. The spyware application was again installed on all the user computers with the same aim of recording their authentication information. None of the users' records were captured by the spyware. It is observed from Table 2 that, testing the recording of user information attack technique against keystroke dynamics authentication of the framework has a 100% failure rate.

4.3 Social Engineering

Social engineering is an attack vector that relies heavily on human interaction and often involves manipulating people into breaking normal security procedures and best practices in order to gain access to systems, networks or physical locations, or for financial gain. Social engineering according to [18] is the practice of obtaining confidential information by the manipulation of legitimate users. Because of social bonding at organizations, people entrust their password to friends. Others are able to trick people to give their passwords through telephone calls and other forms of conversations. Requesting for user credentials and posing to be the legit operators were not possible.

On the first experiment all the twenty-five intruders used impersonation type of social engineering attack on users, by calling and sending emails to trick them to give out their credentials. Although the intruders were successful in getting some passwords from the users, they were not able to type according to the pattern known to the system. The intruders were unable to gain access to account information using the actual users' credentials obtained via social engineering. To further ascertain the effectiveness of the proposed system against social engineering, three other experiments were conducted. The user group deployed in Experiment 1 was changed and new groups were introduced for each of the experiments. The results from Experiment 2, 3 and 4, confirmed that even though the intruders were able to guess the users' passwords, it was very difficult for the intruders to login as a result of the difference in their respective typing rhythm. Testing keystroke dynamics against social engineering attack has a success rate of 0%. Nevertheless, the associated breakthrough tends to be low.

4.4 Password Guessing and Brute-force

With brute-force attacks, impostors use several conceivable character groupings to break the system, and the extra difficult a login credential is, the further protected it is from brute-force attacks [18]. To best protect a system against brute-force attacks, one must have a lengthier password. Brute-force attacks are extended forms of password guessing. In both cases, attacker tries as much as possible to formulate passwords purported to represent the users' login credentials, to gain access into systems as a legitimate user. The length associated with keystroke dynamics is fairly good and almost unbearable for brute-force attacks. The unique password typing rhythm that keystroke dynamics provide makes password guessing a low threat to our framework. The invader or application should habitually produce keystroke designs and emulate human input. The use of keystroke dynamics as a two-factor verification mechanism prevents intruders from overriding users' security and safety schemes.

Brute-Force and Dictionary Attack programs were installed on twenty-five user computers to automatically search for users keystroke dynamics pattern passwords. Table 4 shows the experimental results for tested password guessing and Brute-Force attacks. The results of the four experiments conducted involving 100 users, show that none of the twenty-five intruder programs for each experiment was able to capture the keystroke dynamics pattern with the passwords.

In password guessing and brute force attacks, 0% was successful against the keystroke dynamics authentication of our framework. The attacker or program needs automated keystroke generation pattern and imitate the human input which is difficult to achieve. When the dynamics are used as two factor mechanism, it becomes more or less impossible to hack, thus making the keystroke dynamics more secure and cost effective.

Table 1. Shoulder surfing experiment

Experiment	Users	Success	Failure	Remarks
Experiment 1	25	0	25	Excellent Authentication
Experiment 2	25	0	25	Excellent Authentication
Experiment 3	25	0	25	Excellent Authentication
Experiment 4	25	0	25	Excellent Authentication

In experiment 1, twenty-five (25) users were selected randomly

Table 2. User information recording by spyware experiment

Experiment	Users	Success	Failure	Remarks
Experiment 1	25	0	25	Excellent Authentication
Experiment 2	25	0	25	Excellent Authentication
Experiment 3	25	0	25	Excellent Authentication
Experiment 4	25	0	25	Excellent Authentication

Table 3. Social engineering attack experiment

Experiment	Users	Success	Failure	Remarks
Experiment 1	25	0	25	Excellent Authentication
Experiment 2	25	0	25	Excellent Authentication
Experiment 3	25	0	25	Excellent Authentication
Experiment 4	25	0	25	Excellent Authentication

Table 4. Summary of the results of tested attack for guessing and brute-force

Experiment	Users	Success	Failure	Remarks
Experiment 1	25	0	25	Excellent Authentication
Experiment 2	25	0	25	Excellent Authentication
Experiment 3	25	0	25	Excellent Authentication
Experiment 4	25	0	25	Excellent Authentication

4.5 Dictionary Attacks

In dictionary attacks, the attacker utilizes a wordlist with the hopes that the user's password is a commonly used word (or a password seen in previous sites). Dictionary attacks are optimal for passwords that are based on a simple word (e.g. 'cowboys' or 'longhorns'). Wordlists aren't restricted to English words; they often also include common passwords (e.g. 'password,' 'letmein,' or 'iloveyou,' or '123456'). But modern systems restrict their users from such simple passwords, requiring users to come up with strong passwords that would hopefully not be found in a wordlist. However as stated earlier, ATM systems cannot impose such restriction since PINs are numeric and are commonly a 4-digits or 6-digits. A 4-digit PIN has only 10000 combination of digits thereby making ATM PIN more vulnerable to dictionary attacks. The length of time required to crack a four-digit ATM PIN might be under a minute. The use of keystroke dynamics as an additional level of authentication scheme is one of the best practices to defend against dictionary attacks on ATM systems.

Dictionary attacks involve overcoming system authentications through a pass phrase against its database of possibilities [13]. As opposed to brute-force attacks, when all attempts proof futile, it then tries possible attempts likely to succeed and thus relying on words from the dictionary. In this case, dictionary attacks have also been noted where users download software from the Internet to carry out these attacks. As for dictionary attack, it was impractical and barely impossible to carry it out against keystroke dynamics authentication mechanism.

5. CONCLUSION AND RECOMMENDATIONS

Authentication mechanism provides the basis for access control in order to ensure the security of information resources. Relying on the traditional text based password method to authenticate

users is not effective anymore due to its numerous vulnerabilities. Many alternative solutions such as the use of multi-level authentication, graphical password or biometric password have been suggested in the last few decades. Keystroke dynamics is a low cost biometric solution as it does not require any special hardware. The assumption behind keystroke dynamics is that typing rhythm is unique for any individual. In this study, a simple and secure authentication scheme has been produced by adding this biometric feature with the existing ID/password method for authentication at Automated Teller Machines.

The main aim is to authenticate users based on the combination of habitual patterns of their typing rhythm and the text password. There are mainly two phases in the policy that a user has to go through to be authenticated which are the registration phase and log-in phase. In registration phase, the major functions are data capture, feature extraction and the learning step. Keystroke dynamics features are extracted by analyzing the timing information of the key down/hold/up events. The proposed system stores the keystroke times in correspondence to the user's other credential details like username, and password in a database.

Login phase takes place whenever a user needs to access the system. The login phase realizes the identification, data capture and feature extraction for comparison purpose. Correct username and password does not ensure authentication of a user because an illegitimate user having the knowledge of a correct username and password combination may access the account as well. So the parallel typing verification is the main concern of this study. Microsoft Visual C Sharp(C#) have been used as the primary language for coding and implementing the proposed system since it contains in-built functions for reading keyboard events. The method is quite simple since it is based on statistical approach and provides interesting results with more than 95% accuracy.

The future of biometric technologies usage in the banking sector is a promising area. This paper places an emphasis on the importance of using keystroke dynamics as inexpensive approach for adding additional layer of security to ATMs. The framework is cost effective, compatible and can be easily integrated into existing hardware devices (ATM) used by banks.

Keystroke Dynamics is a two factor security biometric security, hence, for a successful login, firstly password should be known and secondly, typing rhythm should match. Keystroke dynamics is a lesser-known biometric technology that has potential to authenticate a user with relatively good accuracy. Experiments have proved that accuracy is constantly being improved and software based systems can be as effective as expensive and cumbersome hardware solutions [19]. However, the procedure required for authentication make it unsuitable for use as a primary method of authentication for e-banking security. Nevertheless, the qualities of this behavioral biometric give indication that it will be suitable as a secondary or tertiary security measure for banks. Its ease of implementation, potential low cost of ownership and user-friendliness makes it an ideal candidate for inclusion into the banking security family. Beyond e-banking fraud prevention, this technology has the potential to play a key role in fraud detection by offering investigative features. For example, it can assist in tracing internal fraud in banks by identifying possible culprits even where bank staff may have used shared administrative passwords or their colleague's credentials to access banks systems.

It has been argued that single factor authentication is no longer sufficient and that multifactor authentication is required to address online banking security cybercrime [20]. Given the numerous advantages of keystroke dynamics, it is advisable that banks across the globe adopt keystroke dynamics as a secondary authentication method in order to add an additional level of security. However, the rate of this adoption has been relatively slow. Keystroke dynamic technology can conveniently and efficiently authenticate people [21] making it suitable for improving security across e-banking infrastructure. Provided the challenges presented in this paper are addressed, and positive feedback is received from banks that have already introduced the technology into their e-banking security portfolio, we can certainly expect its role in e-banking security to grow.

COMPETING INTERESTS

Authors have declared that no competing interests exist.

REFERENCES

1. Automated teller machine - Wikipedia. [Online].

Available:https://en.wikipedia.org/wiki/Automated_teller_machine
[Accessed: 10-Mar-2020]

2. Wang D, Gu Q, Huang X, Wang P. Understanding human-chosen PINs: Characteristics, distribution and security. ASIA CCS 2017 - Proc. 2017 ACM Asia Conf. Comput. Commun. Secur., No. 2017;372–385.
DOI: 10.1145/3052973.3053031
3. Wang D, Wang P. Two birds with one stone: Two-factor authentication with security beyond conventional bound. IEEE Trans. Dependable Secur. Comput. 2018;15(4):708–722.
DOI: 10.1109/TDSC.2016.2605087
4. Roy S, Das AK, Chatterjee S, Kumar N, Chattopadhyay S, Rodrigues JJPC. Provably secure fine-grained data access control over multiple cloud servers in mobile cloud computing based healthcare applications. IEEE Trans. Ind. Informatics. 2019;15(1):457–468.
DOI: 10.1109/TII.2018.2824815
5. Wang D, Li W, Wang P. Measuring two-factor authentication schemes for real-time data access in industrial wireless sensor networks. IEEE Trans. Ind. Informatics. 2018;14(9):4081–4092.
DOI: 10.1109/TII.2018.2834351
6. Wang D, He D, Wang P, Chu CH. Anonymous two-factor authentication in distributed systems: Certain goals are beyond attainment. IEEE Trans. Dependable Secur. Comput. 2015;12(4): 428–442.
DOI: 10.1109/TDSC.2014.2355850
7. Madhusudhan R, Mittal RC. Dynamic ID-based remote user password authentication schemes using smart cards: A review. J. Netw. Comput. Appl. 2012;35(4):1235–1248.
DOI: 10.1016/j.jnca.2012.01.007
8. What is multifactor authentication (MFA)_ - Definition from WhatIs.pdf. [Online].
Available:https://searchsecurity.techtarget.com/definition/multifactor-authentication-MFA
[Accessed: 25-Nov-2019]
9. Patil AL, Renke RA. Keystroke dynamics for user authentication and identification by using typing rhythm. Int. J. Comput. Appl. 2016;144(9):27–33.
DOI: 10.5120/ijca2016910432
10. Monrose F, Rubin AD. Keystroke dynamics as a biometric for authentication. Futur. Gener. Comput. Syst. 2000;16(4):351–359.
DOI: 10.1016/S0167-739X(99)00059-X
11. Partha Pratim Ghosh, Sabyasachi Pattnaik. Multi-factor authentication in relation to secured payment systems in Atm's. Int. J. Comput. Networking, Wirel. Mob. Commun. 2012;2(2):1–20.
12. Oruh JN. Three-factor authentication for automated teller machine system. 2014;4(6):160–166.
13. Karovaliya M, Karedia S, Oza S, Kalbande DR. Enhanced security for ATM machine with OTP and facial recognition features. Procedia Comput. Sci. 2015;45(C):390–396.
DOI: 10.1016/j.procs.2015.03.166
14. Ghodke SS, Kolhe H, Chaudhari S, et al. ATM transaction security system using biometric palm print recognition. IOSR J. Electron. Commun. Eng. 2014;9(5):06–11.
DOI: 10.9790/2834-09510611
15. Twum F, Nti K, Asante M. Improving security levels in Automatic Teller Machines (ATM) using multifactor authentication. Int. J. Sci. Eng. Appl. 2016;5(3):126–134.
DOI: 10.7753/ijsea0503.1003
16. Madara J, Okeyo G, Kimwele M. A fingerprint & pin authentication to enhance security at the automatic teller machines. Int. J. Sci. Eng. Res. 2017;8(4):380–387.
17. Bošnjak L, Brumen B. Shoulder surfing: From an experimental study to a comparative framework. Int. J. Hum. Comput. Stud. 2019;130:1–20.
DOI: 10.1016/j.ijhcs.2019.04.003
18. Shanmugapriya D, Padmavathi G. A survey of biometric keystroke dynamics: Approaches, security and challenges. 2009;5(1):115–119.
19. Revett K, De Magalhães ST, Santos HMD. Enhancing login security through the use of keystroke input dynamics. Lect. Notes Comput. Sci. (including Subser. Lect. Notes Artif. Intell. Lect. Notes Bioinformatics), LNCS. 2006;3832:661–667.
DOI: 10.1007/11608288_88
20. Blum D. Authentication_ Where's the magic factor_ _ Network World-Daniel Blum 2006.pdf. [Online].

Available:https://www.networkworld.com/article/2310935/authentication--where-s-the-magic-factor-.html%0A
[Accessed: 18-Feb-2020]

21. Boechat GC, Ferreira JC, Carvalho Filho ECB. Using the keystrokes dynamic for systems of personal security. Proc. World Acad. Sci. Eng. Technol. 2006;18:200–205.

Peer-review history:
The peer review history for this paper can be accessed here:
http://www.sdiarticle4.com/review-history/56340