*Journal of Discrete Mathematical Sciences & Cryptography*
ISSN 0972-0529 (Print), ISSN 2169-0065 (Online)
Vol. 27 (2024), No. 4, pp. 1357–1365
DOI : 10.47974/JDMSC-1990

# Multilayered authentication for ATM transaction using keystroke dynamics and touch dynamics

Pragya Vaishnav [†]
Linesh Raja *
Poonam Singh [§]
*Department of Computer Applications*
*Manipal University Jaipur*
*Jaipur*
*Rajasthan*
*India*

Ramakrishnan Vairavasamy [‡]
*Tata Consultancy Services*
*Amsterdam*
*Netherlands*

**Abstract**

Genuine person recognition systems are necessary for a system to identify or authorize the identification of a person requesting their services. Ensuring that only authorized users access the provided services is the aim of this proposed system. These systems are susceptible to impersonation attacks in the absence of strong personal recognition methods. Due to its traditional authentication technique (PIN), the ATM has suffered greatly over the years from PIN theft and other related ATM thefts. Therefore, in this paper, we proposed a multilayer (Typing and Touch) based authentication security arrangement to enhance the security and safety for the ATM and its users. The proposed system demonstrates a three-layered design structure. The first layer is the card verification module, which concentrates on the enrolment phase for ATM card. The second layer is the feature extraction and comparing of the typing pattern from the database server. The last layer compares the touch behavior continue till session end with the stored touch data in the database server. During the implementation phase, MySQL server 2010 served as the backend and Java was used for front-end development on Microsoft Windows 10. Based on the False Rejection Rate (FAR), False Acceptance Rate (FAR), and Equal Error Rate (EER) measurements, the application

[†] *E-mail:* pragya.vaishnav23@gmail.com
* *E-mail:* lineshraja@gmail.com (Corresponding Author)
[§] *E-mail:* poonam.singh@jaipur.manipal.edu
[‡] *E-mail:* ramakrishnan21@gmail.com

© Taru Publications

was evaluated. These metrics demonstrate the security and dependability of the suggested system for the authentication and verification of ATM customers.

***Subject Classification:*** *Primary 93A30 Secondary 49K15.*

***Keywords:*** *PIN, Authentication, Security, Verification, ATM, Multilayer, Keystroke dynamics, Touch dynamics.*

## 1. Introduction

Security is one of the most important factors regardless of the time, place, or domain. Improving security is a fundamental duty owed to employees and all governmental and private sectors. Owing to the development of new technologies and the ever-expanding field of information technology, improving security is not only challenging but almost unattainable.

In the modern world, payment methods have advanced from cash to checks to credit and debit cards [1]. An automated teller machine, or ATM, is a device that banks and other financial institutions install that allows users to do tasks including depositing or withdrawing cash, checking their account balance, requesting bank statements, and transferring funds between accounts. Mobile money transactions are available on certain contemporary ATMs. In essence, autonomous banking terminals, or ATMs, are designed to give consumers quicker, more convenient service [1]. The ATM has been regarded as one of the crucial elements of the infrastructure supporting electronic banking among all departments inside a financial institution.

The primary advantage of the ATM is its capacity to serve users and clients around-the-clock, making it a necessary component of daily life. Lately, ATMs' are implemented in many settings such as ticket vending machines, rapid check-in kiosks and self-service petrol stations [2-4]. These days, ATMs are not only located in banks; many schools and companies have also placed them for the convenience of their patrons and to increase revenue.

Most of the users choose readily guessed passwords and PINs, like phone numbers, birthdays, and social security numbers, despite the repeated warnings sent to card users. However, because of this design's shortcomings, a brute force attack or password prediction can be used by an attacker who has the user's card to figure out the user's PIN. One in ten users of a standard four-digit PIN will have the same number [5-8]. Despite all security precautions taken, ATM crimes continue to happen all around

the world. That is why high security in ATM transaction process is much needed. To provide the security ATM transaction process we need to make authentication process very strong and secure.

In this research paper, the author used keystroke dynamics and touch dynamics technologies for multi layered authentication process implemented in the ATM transactions. Keystroke dynamics used during entering the PIN and touch dynamics used whenever user touched the ATM screen.

## 2. Literature Review

Chen Li et al, developed a system called Human Body and Face Detection based Anti-shoulder Attack System on ATM [2] to lessen the risk of a shoulder surfing attack. This system uses AdaBoost-based algorithms and the Gaussian Mixture Model (GMM) method to monitor the face and body of people near ATMs. Shweta Sankhwar & Dhirendra Pandey [3] implemented second step verification, they employed an OTP and a pin number in this way. The user must always use an ATM card with a pin number on it. If the pin is entered correctly, the bank will give the user an OTP to their phone. Author in [4] developed a system in order to stop ATM robberies. The PIC microcontroller serves as an intermediary device in this system, with buzzer, LCD, gas sensor, GSM module, IR sensor, vibration sensor, and Zigbee serving as output devices. When more than one person enters the ATM, a vibration sensor detects the event and sends it to the microcontroller, which then responds by activating the buzzer.

Author proposed different technologies in [9]. The goal of this study is to improve transaction security in the ATM system by utilizing fingerprints. Therefore, the goal of this project is to establish fingerprint verification procedures based on ATM simulators in order to decrease fraud related to ATM use. The LCD display, DC motor, and fingerprint module make up the system. With a GSM module, the system can be expanded. When the GSM module detects the fingerprint of an unauthorized person, it alerts the appropriate authorities [10].

*Proposed System*

The author proposed a developed multilayered authentication system for ATM transaction using keystroke dynamics and touch dynamics to increase the security of ATM transactions. Figure 1 is representing the

flow of developed system. In the proposed system there are three layers to identify user's identity step by steps:

In the first layer user's ATM Reads the chip and magnetic stripe on the card that links the card to confirm the correct bank account. After confirmation the bank account details, system enter in the second layer. In the second layer user's typing behavior confirm the identity of the user using flight time and typing speed. As user enter ATM pin, system collect the keystroke data in the form of flight time and typing speed. If collected keystroke data and pin match with the database server of the bank, then third layer authentication process will start otherwise user will not be able to do transactions. In the third layer user's identity will be check continuously using their touch behavior on the ATM machine. This authentication process will continue till session end. Through every single touch on the ATM machine, User's touch behavior will be check using dwell time and touch size features. As user touch on any option or anywhere on the screen their touch data will be compare with the registered touch data from the database server of the bank. This layer will keep monitor user's identify until session end using touch dynamics technique. At any point of the transaction if user does not find as a genuine user then session will be end and home screen will show.

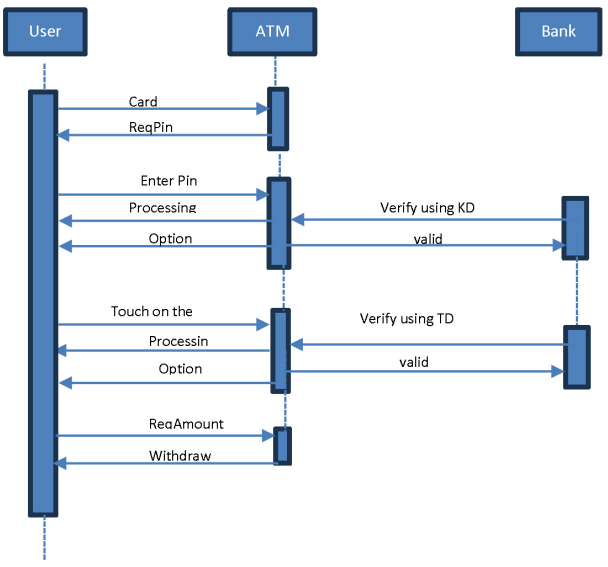


**Figure 1**

**Developed ATM System Working**

Features of the Proposed System

- Typing Speed: - Check typing speed.
- Flight Time: - Time interval between two sequential keys on typing events.
- Dwell Time: - Time interval between finger touch release and finger press on the touch screen.
- Touch Size: -Value of touch area on touch screen.

## 3. Methodology

Methodology is divided into two parts. The first one is for the complete system, and another is for the keystroke and touch data.

### 3.1 *Methodology applied on the system.*

- *Training:* The classifier is trained in this initial stage by creating a statistical model out of the samples that were gathered. This stage involves gathering samples, cleaning them (normalizing and/or treating them for outliers), and creating and storing a template for the user in a database.
- *Data Recollection:* The procedure of collecting data is regarded as the initial and most crucial one. As implied by the name, it involves gathering user biometric samples. Keystroke Dynamics, in this context, refers to the user-generated timing of keystrokes on a ATM keyboard. This process of data gathering is also well-known.
- *Extraction of Relevant Data and Training:* It's time to decide which features can be applied to the data once it has been collected. To ensure the greatest degree of accuracy, keystroke timing features—touch features were also included in this implementation—were applied to a variety of combinations.
- *Classification:* Different methods can be used to compare samples with the data stored in the previously constructed template. These could include anything from straightforward statistical techniques to distance measurements or other classification criteria.
- *Evaluation:* After receiving the classification results from the preceding phases, an action should be taken in this step based on the prior result. The action could be to give access or not if a login procedure is being carried out. On the other hand, a decision

regarding the legitimacy of the user or the sample should be made when dealing with verification or identification. The session will end, for instance, if there were numerous incorrect classifications.

- *Verification:* This stage compares newly obtained samples to those that have been previously stored. Typically, the additional samples receive the same treatment. Before being compared to the template, the identical features are extracted and cleaned.

4.2 *Methodology on Keystroke and Touch Dynamics Data*

- *False* Acceptance Rate (FAR)

  The FAR specifies the proportion of fake user acceptance as an authorized user. When an ATM is authenticated, FAR notifies the user if the authentication is secure or not. If hackers can easily log into the authentication system, the FAR percentage is larger. This invention's FAR value was attained by giving each user a pass-value in order to determine how well the system performed. The formula to determine FAR is:

$$FAR = \left( \frac{\text{Number of wrong acceptances}}{\text{Total number of intruder attempt made}} \right) * 100$$

- *False Rejection Rate (FRR)*

  FRR shows the percentage of error of rejecting a genuine user as a fake user. FRR define about the originality of the system if it is useful or not. If FRR percentage is higher, then genuine user can fail in the authentication system. This invention is achieved FRR value through the pass - value for each user to get the system's performance. To calculate FRR the formula is:

$$FRR = \left( \frac{\text{Number of wrong rejections}}{\text{Total number of genuine attempts made}} \right) * 100$$

- *Equal Error Rate (EER) Analysis*

  EER compares the overall accuracy level of other biometric authentication techniques and displays a number of performance measures. EER is obtained by locating the intersection of two graphs, the first of which is the FRR and the second the FAR. The formula to determine ERR is:

$$ERR = \left( \frac{\text{FRR} + \text{FAR}}{2} \right)$$

The FAR and FRR are used to examine the dataset and determine the EER value; the pass-value, on the other hand, is variable and is ascertained independently for each subject (typing speed and flight time). Only timing feature data is used for analysis.

## 4. Result and Analysis

For the developed system author collected keystroke data from 249 user and touch data from the 55 users and stored it into the database to verify the system's accuracy. Result of FRR, FAR and EER result are given in below table.

**FRR Result**

| FRR | Percentage |
|---|---|
| 249 | 8.718 |

**FAR Result**

| FAR | Percentage |
|---|---|
| 55 | 1.56 |

**EER and Accuracy**

| EER | Percentage | Accuracy in Percentage |
|---|---|---|
| 249 | 5.415 | 96 |

The FAR is 1.56% and the FRR is 8.718%. The system's performance is determined by the proportion of FRR and FRR. It can be taken into consideration if the FRR percentage is high, but it cannot be taken into consideration if the FAR percentage is high because it poses a risk to the system. With an accuracy of 96% and an EER of 5.415%, the system is operating well. As a result, it verifies that the suggested system's accuracy is high and that it is suitable for ATM transaction authentication.

## 5. Conclusion

Currently, it is tedious task for banks to authenticate users in the ATM devices. ATMs typically process data through encryption; however hackers can still access accounts and take out the amount by using covert

hacking tools. The developed multilayered system places more of an emphasis on the user authentication procedure, which allows the ATM to verify the user's identity at any point during the session even after the user enters their pin. This system will stop the unauthorized access because nobody can copy the typing and touch behaviors of the user. Keystroke dynamics and touch dynamics technique is validated by previous research too and fully secure techniques which will improve the security of ATM transactions. In future work will add more layers using face and iris recognition in the ATM transaction process

**References**

[1] Birch, B., and A. Young. "The business and technology history of automated teller machine in the UK, 1967-2005." A Primer Conference Abstracts (2007).

[2] Dahikar, Minakshi S. TumsarePradeep B. "A Review of Security Aspects of Online and ATM Transactions in Banking Domain." (2015).

[3] De Luca, Alexander, Marc Langheinrich, and Heinrich Hussmann. "Towards understanding ATM security: a field study of real world ATM use." Proceedings of the sixth symposium on usable privacy and security (2010).

[4] De Luca, Alexander. Designing usable and secure authentication mechanisms for public spaces. Diss. lmu (2011).

[5] Farooq, Aqeel. "Using LabVIEW to evaluate Hydrogen fuel cell-based systematic vehicular application to promote the green economy." (2022).

[6] Kumar, Ankit, et al. "An enhanced quantum key distribution protocol for security authentication." *Journal of Discrete Mathematical Sciences and Cryptography* 22.4 : 499-507 (2019).

[7] Jebaline, G. Renee, and S. Gomathi. "A novel method to enhance the security of ATM using biometrics." 2015 International Conference on Circuits, Power and Computing Technologies [ICCPCT-2015]. IEEE (2015).

[8] Kumar, Ankit, et al. "An improved quantum key distribution protocol for verification." *Journal of Discrete Mathematical Sciences and Cryptography* 22.4 : 491-498 (2019).

[9] Meduri, Suryaa Pranav, et al. "Design and Smart Automation of Lunar and Martian Habitat using STM32H7 Microcontroller and LabView." 2021 6th International Conference on Inventive Computation Technologies. IEEE (2021).

[10] Padmavathi, M., B. Rajeshkumar, and R. Ganesh Kishore. "Bio-Matric Intelligent ATM System." *International Journal on Future Revolution in Computer Science & Communication Engineering*, ISSN: 2454-4248.

[11] Vaishnav Pragya, Manju Kaushik, and Linesh Raja. "Behavioral biometric authentication on smartphone using keystroke dynamics." *Journal of Discrete Mathematical Sciences & Cryptograph*, ISSN: 0972-0529 (2023).