INTERNATIONAL JOURNAL OF SOFTWARE ENGINEERING AND COMPUTER SYSTEMS
E-ISSN: 2180-0650
VOLUME 10, ISSUE 1, 2024, pp. 32 – 39
DOI: https://doi.org/10.15282/ijsecs.10.1.2024.3.0121

RESEARCH ARTICLE

Hybrid Biometric Authentication for Automatic Teller Machine

Steven R. Arokiasamy[1], Md Raihanul Islam Tomal[1], Kohbalan Moorthy[1,*] Kauthar Mohd Daud[2]

[1]Faculty of Computing, Universiti Malaysia Pahang Al-Sultan Abdullah, Pekan, 26600 Pahang, Malaysia.
[2]Faculty of Information Science & Technology, Universiti Kebangsaan Malaysia, 43600 Bangi Selangor, Malaysia.

ABSTRACT - Automated Teller Machines (ATMs) are a crucial part of modern life, providing users with the ability to conduct basic banking transactions electronically without the need for bank representatives. These machines are ubiquitous, particularly in developed countries, and their usage is expanding rapidly across the globe. However, this widespread adoption has highlighted significant security concerns for general users. Traditional security measures, such as Personal Identification Numbers (PINs), are increasingly proving insufficient due to issues like card theft, ATM scams, and other security breaches. To address these vulnerabilities, biometrics-based authentication is emerging as a promising alternative. Unlike traditional password or PIN-based methods, biometric authentication uses unique physical characteristics, such as fingerprints, to verify identity. This method offers a higher level of security by making it significantly harder for unauthorized users to access accounts. In this research, we introduce a hybrid biometric authentication system for ATMs, focusing on fingerprint recognition. Our prototype aims to enhance transaction security and provide a more user-friendly experience. By integrating biometric strategies with ATMs for single verification, we aim to reduce the risks associated with PIN-based authentication and improve overall security. This approach not only addresses existing vulnerabilities but also sets the stage for more secure and reliable ATM transactions in the future.

ARTICLE HISTORY
Received : 20 September 2022
Revised : 14 August 2024
Accepted : 27 August 2024
Published : 5 September 2024

KEYWORDS
Biometric
Fingerprint Authentication
Automatic Teller Machine
Security
Banking System

1.0 INTRODUCTION

Automated Teller Machines (ATMs) are essential to contemporary banking, providing customers with 24/7 access to a wide range of financial services. Introduced in the 1960s, ATMs revolutionised the banking industry by enabling users to perform transactions such as cash withdrawals, deposits, fund transfers, and account inquiries without visiting a bank branch. This convenience has made ATMs ubiquitous, especially in developed countries, and their usage is rapidly spreading to emerging markets.

The proliferation of ATMs has not only increased accessibility to banking services but also posed significant security challenges. Issues like card skimming, PIN theft, and ATM fraud have underscored the need for robust security measures. Traditional security methods, primarily reliant on Personal Identification Numbers (PINs), are proving inadequate in preventing unauthorized access and fraudulent activities. As a result, the banking industry is increasingly turning to advanced technologies, such as biometric authentication, to enhance the security and reliability of ATM transactions.

Automated Teller Machines (ATMs) have brought new insights to customers and banks with the growth of telecommunication industries and personal computers. The idea is to use a plastic card equipped with an intelligent chip that holds encrypted information of customers' data and enables the customer to withdraw from any ATM [1]. This technology has provided convenience to customers.

However, security issues have become a concern among users, such as identity theft, fraud operations, and others. To date, Personal Identification Numbers (PINs) are the only authentication protocol in ATMs. In a PIN-based system, the ATM system does not authenticate the identity of the authorized cardholder because the password or PIN is only known to the cardholder [2]. In other words, any individual can withdraw from the ATMs regardless of the user's identity, provided the user inserts the correct PIN.

Therefore, personal identification based on biometrics has been introduced in information security domains. Biometrics is a technology that uses individual unique physical and behavioural characteristics such as fingerprint, iris, hand recognition, face recognition, and others, intending to strengthen the security of the data [3-4]. Biometrics offers more advantages over standard and current procedures. For instance, the card or passwords can be stolen, lost, copied, or hacked by third-party individuals and others.

***CORRESPONDING AUTHOR | K. Moorthy** | ✉ kohbalan@umpsa.edu.my

Biometric identifiers offer favourable conditions over standard and current procedures when it comes to security. Tokens, for instance, appealing stripe cards, smart cards, and passwords, can be stolen, lost, copied, or left behind; passwords can be shared, disregarded, hacked, or by chance observed by a third-party individual. A biometric structure offers two critical features, first physical proof and confirmation through fingerprint. Therefore, this article concentrates on perceiving and affirming a client by one-of-a-kind unique mark acknowledgement for improved security.

The problem arises because bank account passwords can be hacked by shoulder surfing, ATM PIN cracking [5], and card skimming methods, allowing criminals to take all money within the briefest time and bring significant losses to the clients. Besides that, traditional ATM systems accept only the PIN code, which leads to a third party accessing the account very easily and withdrawing money without the client's permission. The client must remember the passwords and carry the cards to access the current ATM system. If the client accidentally loses their card, then this will lead to the third party stealing the money from the client's account [6].

This article aims to implement a hybrid biometric authentication in the ATM system to securely let the client access the bank account. The proposed hybrid biometric authentication for automatic teller machines is a working prototype based on fingerprint recognition. The organization of the paper is as follows: In the next section, related works on ATMs are presented. In Section 3, the proposed system design of this research is explained. The implementation of the proposed biometric authentication for ATMs is presented in Section 3 as well. Finally, Section 4 is the conclusion and the discussion of future works.

2.0 RELATED WORKS

We have studied several research based on ATM, and some of them are very logical to introduce in this research for our research enhancement. In this research [7], the author tried to secure the ATMs through mobile applications and IOT-based; ATMs are frequently targeted for fraud, primarily through attacks on the 4-digit PIN used for authentication. Common threats include shoulder surfing and filming attacks. To counter these vulnerabilities, a proposed ATM design employs a cardless IoT architecture, enhancing security with a two-level framework. It utilizes penetration testing, session key techniques, and modified black-white methods for secure PIN entry. An Android app facilitates transactions, and the hash function ensures secure PIN transmission across open channels.

This study [8] explores advancements in computer vision for ATM security, proposing a comprehensive solution using facial recognition to enhance privacy and security. The system captures real-time images during transactions, matching faces with stored ATM card owner data, effectively turning the face into a password. This method mitigates fraud risks from card theft and duplication. Additionally, the study reviews machine learning applications in computer vision and their implementation on embedded hardware. This survey [9] shows that ATMs have evolved from simple cash dispensers to complex banking machines, necessitating a focus on interface usability and security. Studies emphasise the importance of both aspects in user interactions with ATMs. A systematic literature review identified 160 metrics in 13 categories for assessing Internet Banking security and usability.

Future research aims to evaluate the applicability of these metrics to ATM interfaces, enhancing their overall usability and security. Modern operations requiring personal information protection, such as accessing bank accounts via ATMs, face challenges due to outdated identification methods like ID cards and signatures [10]. To enhance security and usability, biometric technologies, particularly fingerprint scanners, are increasingly used. This system involves storing fingerprint data in a bank's database, allowing users to securely authenticate and conduct transactions. If the fingerprint does not match, the transaction is cancelled, preventing financial losses from criminal activities. Cardholders face security issues at POS terminals, such as ATM card theft, forgotten PINs, and cardholder verification. This study [13] introduces a biometric iris scan to enhance security. The developed system, using iris recognition, significantly reduces cardholder fraud, as demonstrated by experimental results.

The advancement of information technology has led to automated banking systems [14] like ATMs, reducing the need for manual transactions. However, security concerns arise. This study proposes a hybrid authentication system combining graphical pattern passwords and PINs, enhancing ATM transaction security without requiring additional hardware. This study [15] aims to aid visually impaired individuals in using ATMs. Utilizing Raspberry Pi and biometric IVRS systems, the research found ratified ATMs to outperform smart ATMs. Statistical analysis showed a significant difference ($p=0.878$, $p>0.05$), highlighting the effectiveness of this method for safe money withdrawal for visually impaired and other disabled individuals.

Finger examination is different compared to other biometric advancements. A finger-examine or biometric fingerprint requires more specific physiological qualities than the distinctive mark, such as the iris and retina. However, the application of biometric fingerprints is limited due to the innovation of automated identification which is still new. Biometric information is partitioned and identifiable from individual data. The advantage of biometrics is it is not reproducible as everyone has distinctive features and characteristics. Therefore, the biometric layouts cannot be figured out, and the data cannot be stolen. Table 1 shows a brief review of three existing ATM systems.

Table 1. Review of Existing ATM System

Type	Technology	Input Method	Strength	Weakness
Automatic Teller Machine using Smart Card	Pin Number Card	Smart card and password	Convenient to ATM clients 24 hours service The client does not have to carry a large amount of cash.	Card skimmer Shoulder surfing ATM card cloning fraud Pin Crack.
Cashless Withdrawal	Tac number Near-Field Communication QR code	Special Id and online login	High technology Convenient.	Withdrawal limit is not sufficient. Other than the client can withdraw if know the security feature. Clients with the same number can only do a couple of transactions per day.
Talking ATM	Card, password, Audio jack	Card Password Audio Jack (Hands-free)	Blind or vision issue client can use ATM Secure with Password and password	Shoulder skimmed Clone card.

The Automatic Teller Machine (ATM) is a programmed money machine (ABM) that enables clients to finish essential exchanges such as account trades with no assistance from bank agents. The customers get to their records through a plastic card encoded with customer information on an alluring strip. The strip contains a recognizing confirmation code that is transmitted to the bank's central PC by modem. Another ATM system is the talking ATM was first introduced by the Royal Bank of Canada in Ottawa, Ontario, in the year 1997. Talking ATMs are designed specifically for persons who cannot read the ATM by providing audible instructions via pre-recorded or text-to-speech synthesis.

Meanwhile, cardless withdrawal is an ATM system that allows customers to perform trade exchanges with the individual-to-particular store immediately without swiping or inserting the card into a card reader. For example, Maybank allows its clients to do trade exchanges with any adaptable Malaysian number. Once the deal is successful, the recipient will get a transaction ID, while the sender will receive a password. This kind of ATM system is convenient due to less contact considering the current pandemic situation and security. It adds more verification layers such as biometrics, verification codes, and QR codes.

Based on previous works comparison, this article proposes a hybrid biometric authentication for automatic teller machines as a working prototype based on fingerprint recognition. The idea is to redesign an ATM login using fingerprint authentication [11]. Fingerprint authentication is the most refined input type for ATM systems because fingerprints are more secure and easy to implement than other input types [3, 12]. Furthermore, this approach will reduce ATM-related fraud or crime rates as security is improved through biometric implementation.

3.0 ATM FINGERPRINT-BASED AUTHENTICATION SYSTEM

Ever since the discovery of fingerprints, the domain of science surrounding the facts of fingerprints has been progressing rapidly. Dactylography, which is the study of fingerprints, has led to the realization of much higher security methods, that is the biometric authentication system which utilizes the uniqueness of every fingerprint as each fingerprint is different from one another. Today, Automated Teller Machines has also implemented this biometric authentication system by exploiting the individualism of each fingerprint, allowing the ATM system to recognize the user, thus providing a much safer transaction and a better user experience than the older version of ATM that uses a debit card. Figure 1 shows a typical ATM system model.

Figure 1 depicts a typical ATM used worldwide. For enhanced security, we propose a model that incorporates biometric authentication through fingerprint recognition. Currently, integrating a fingerprint sensor for authentication is both feasible and advantageous. In Figure 2, we present an overview of our proposed model for the reader's convenience. The red-marked area highlights the primary modification in our model compared to the traditional ATM setup.

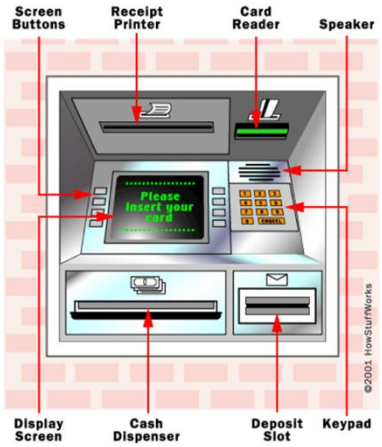

Figure 1. Typical ATM

According to our proposed model, the user must first insert their ATM card and select their preferred language. In Malaysia, available languages include English, Malay, Chinese, and others. The subsequent authentication process is our main focus. Traditional models rely solely on PINs for security; however, we propose adding biometric verification. As illustrated in Figure 2, our model incorporates a verification section post-authentication, ensuring transaction security via

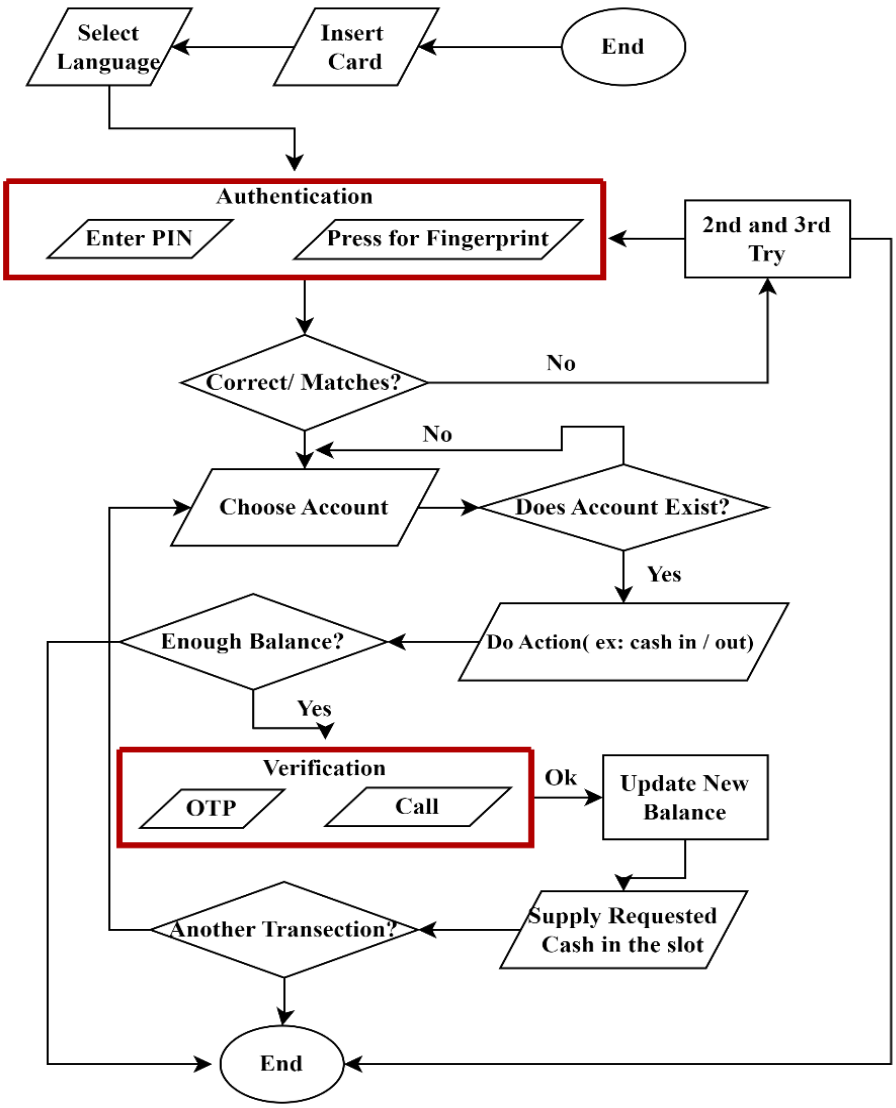

Figure 2. Flowchart of our proposed model.

SMS, OTP, or phone call, based on company and user preferences. By following these steps, users can successfully withdraw money from the ATM, making it a user-friendly and secure method in line with modern technology. For reader convenience, we demonstrate a graphical representation of our proposed ATM in Figure 3.

4.0 PROTOTYPE SETUP

The basic setup for this prototype includes a desktop computer or a laptop running Microsoft Windows operating system that can execute the .exe program developed using Microsoft Visual Studio. Then a fingerprint reader is required to access and read the fingerprint of the user. The fingerprint reader used in this prototype is the URU4500 Digital Persona Biometric Reader which is attached to the desktop computer or laptop. The system developed has two main interfaces, which are the Bank Interface and the Customer Interface.

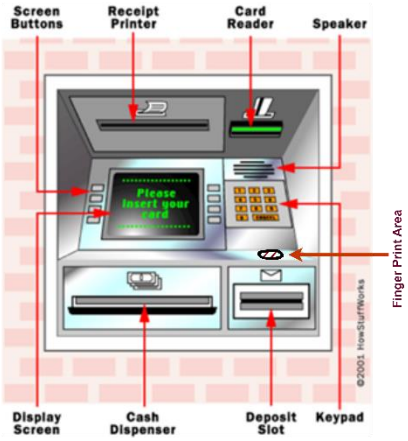

Figure 3: Proposed ATM

5.0 BANK INTERFACE

In this interface, the admin will need to log into the system with the username and password to proceed with the customer information registration and fingerprint authentication setup. Then, the admin will be able to input all the required information for the registration of the customer fingerprint with the following information: Customer Name, Customer ID, Contact Number, and the remaining information will be automatically retrieved based on the input of the customer's existing account number. The interface also allows the registration of new customers which will be linked back to the Bank's existing system. This interface only focuses on the registration of the customer fingerprint to the existing bank account.

Next, the admin can proceed with the fingerprint registration for the selected customer by first performing the read, where the customer must place her/his finger on the URU4500 Digital Persona Biometric Reader for reading and recognition of the fingerprint. Then the admin can save and store the registered finger in the system database followed by a verification where the customer is required to place her/his finger again for testing of the authentication. Once this process is settled, the ATM will be able to authenticate the customer's fingerprint for ATM transactions as intended.

The main source for fingerprint authentication and verification is developed as shown in Figure 4 below.

```
Imports System.Data.SqlClient
Imports DPFP
Public Class Verify
    Private WithEvents verifyControl As DPFP.Gui.Verification.VerificationControl
    Private matcher As DPFP.Verification.Verification
    Private matchResult As DPFP.Verification.Verification.Result
    Private allReaderSerial As String = "00000000-0000-0000-0000-000000000000"
    Public template As DPFP.Template
    Private userTemplateColumn As String = "Template"
    Private userIDColumn As String = "ID"
    Dim bytes As Byte()
    Private Sub CreateDPControl(ByRef control As DPFP.Gui.Verification.VerificationControl)
        Try
            control = New DPFP.Gui.Verification.VerificationControl()
            control.AutoSizeMode = Windows.Forms.AutoSizeMode.GrowAndShrink
            control.Name = "verifyControl"
            control.Location = New System.Drawing.Point(650, 250)
            control.ReaderSerialNumber = "00000000-0000-0000-0000-000000000000"
            control.Visible = True
            control.Enabled = True

            control.BringToFront()
            Me.Controls.Add(control)
        Catch ex As Exception
            MessageBox.Show("exception")
        End Try
    End Sub



            Private Function ConnectString() As String
                Dim connectionString As String
                connectionString = ("Data Source=.\SQLEXPRESS;AttachDbFilename=C:\Users\Admin\Desktop\New
                folder\DigitalPersona\DigitalPersona\One Touch SDK\.NET\Samples\Visual Studio 2005\VBNET\UI
                Support\test.mdf;Integrated Security=True;User Instance=True")
                Return connectionString
            End Function
            Private Sub VerifyBiometric_Load(ByVal sender As System.Object, ByVal e As System.EventArgs)
        Handles MyBase.Load
                matcher = New Verification.Verification()
                matchResult = New Verification.Verification.Result
                CreateDPControl(verifyControl)
            End Sub
            Private Sub verifyControl_OnComplete(ByVal Control As Object, ByVal FeatureSet As
             DPFP.FeatureSet, ByRef EventHandlerStatus As DPFP.Gui.EventHandlerStatus) Handles
             verifyControl.OnComplete
                Dim dataSet As DataSet = New DataSet()
                Dim adapter As SqlDataAdapter = New SqlDataAdapter()
                Dim sqlCommand As SqlCommand = New SqlCommand()
                Dim ctr = 0
                Try
                    Dim max As Integer = 0
                    Dim cn As New SqlConnection(ConnectString())
                    cn.Open()
                    sqlCommand.CommandText = "Select MyBinaryData from tbStoreFile"
                    sqlCommand.CommandType = CommandType.Text
                    sqlCommand.Connection = cn
                    Dim lrd As SqlDataReader = sqlCommand.ExecuteReader()
                    Dim usr = 0
                    While lrd.Read()
                        usr = lrd("MyBinaryData")
                    End While
                    bytes = Nothing
                    bytes = usr
                    template = New DPFP.Template()
                    template.DeSerialize(usr)
                    'Perform match
                    matcher.Verify(FeatureSet, template, matchResult)
                    If matchResult.Verified Then
                        My.Computer.Audio.Play("C:\Users\Admin\Desktop\New
                        folder\DigitalPersona\pic\tingpopup.wav")
                        EventHandlerStatus = Gui.EventHandlerStatus.Success

                        Me.Hide()

                        MainMenu.Show()
                    Else
                        EventHandlerStatus = Gui.EventHandlerStatus.Failure
                        MsgBox("Please Try Again!")
                    End If
                Finally
                End Try
            End Sub
            Private Sub Form1_Load(ByVal sender As Object, ByVal e As EventArgs) Handles MyBase.Load
            End Sub
        End Class
```

Figure 4. Fingerprint verification module.

6.0 CUSTOMER INTERFACE

In this interface, the user is presented with the welcome screen where the customer is not required to insert the ATM card but instead just place the fingerprint on the fingerprint reader provided in this prototype. The customer's finger will be automatically authenticated for the transaction's menu. If the authentication fails, the customer will be prompted with an error message and will not be able to proceed with the ATM transactions as intended by the Bank.

In the transaction menu, the customer will be able to perform all the allowed transactions as intended by the Bank, such as Cash Withdrawals, Balance inquiries, and Other Transactions that are authorized. Other transaction access will depend on the specific Bank setup and display accordingly. The basic customer interface is presented in this prototype to show the functionality and execution of fingerprint authentication as intended.

7.0 CONCLUSIONS

The implementation of hybrid biometric authentication for ATMs, specifically through fingerprint recognition, significantly enhances the security system beyond the standard versions currently in use. This advancement is expected to reduce fraud cases substantially and security issues related to client data and access. However, the development of this prototype presented considerable challenges due to the lack of existing resources and references, necessitating a build-from-scratch approach. The most formidable obstacle was the integration and communication between the hardware and software components essential for the prototype's functionality. Despite these challenges, the increasing use of fingerprint authentication in various applications today indicates the feasibility of integrating this technology into ATMs soon. As we progress towards a more secure world, implementing such advanced biometric systems will be a pivotal step in safeguarding user transactions and enhancing the overall security framework of banking systems. This initiative not only promises a higher level of security but also aligns with the global trend towards more sophisticated and user-friendly authentication methods, ensuring a safer and more reliable banking experience for all users.

ACKNOWLEDGEMENTS

The authors would like to thank the Ministry of Higher Education Malaysia for providing financial support under Universiti Malaysia Pahang Al-Sultan Abdullah for laboratory facilities as well as additional financial support under Internal Research grant RDU2303103.

AUTHORS CONTRIBUTION

System development was done by S. R. Arokiasamy and manuscript preparation was equally contributed by the authors.

REFERENCES

[1] A.M.S.E. Saad, "A Systematical Review Study to Investigate the Use of Biometric Security Techniques in Automatic Teller Machines: Insight from the Past 15 Years," In 2019 1st International Informatics and Software Engineering Conference (UBMYK)., pp. 1-4, 2019.

[2] A. Lasisi, A.A. Ajisafe, "Development of Stripe Biometric Based Fingerprint Authentications Systems in Automated Teller Machines," In 2nd International Conference on Advances in Computational Tools for Engineering Applications (ACTEA)., pp. 172-175, 2012.

[3] A.K. Jain, A. Ross, S. Prabhakar, "An introduction to biometric recognition," IEEE Transactions on circuits and systems for video technology., vol. 14, no. 1, pp. 4-20, 2004.

[4] M. Karnan, M. Akila, N. Krishnaraj, "Biometric personal authentication using keystroke dynamics: A review," Applied soft computing, vol. 11, no. 2, pp. 1565-1573, 2011.

[5] M. Mannan, V. Oorschot, "PC: Weighing down the unbearable lightness of PIN cracking," In International Conference on Financial Cryptography and Data Security. Springer, Berlin, 2008.

[6] L. O'Gorman, "Comparing passwords, tokens, and biometrics for user authentication," Proceedings of the IEEE, vol. 91, no. 12, pp. 2021-2040, 2003.

[7] Pradeep, D., et al. "Security Enhancement for ATM Machine Using Mobile Application and IoT Technology." 2024 5th International Conference on Intelligent Communication Technologies and Virtual Mobile Networks (ICICV). IEEE, 2024.

[8] Kalmani, Shailaja. "Application of Computer Vision for Multi-Layered Security to ATM Machine using Deep Learning Concept." 2022 International Conference on Applied Artificial Intelligence and Computing (ICAAIC). IEEE, 2022.

[9] Falconi, Fiorella, et al. "A systematic literature review about quantitative metrics to evaluate usability and security of ATM interfaces." Design, User Experience, and Usability. Case Studies in Public and Personal Interactive

Systems: 9th International Conference, DUXU 2020, Held as Part of the 22nd HCI International Conference, HCII 2020, Copenhagen, Denmark, July 19–24, 2020, Proceedings, Part III 22. Springer International Publishing, 2020.

[10] Narsaiah, M. N., et al. "Fingerprint Recognition for Future ATM Security." E3S Web of Conferences. Vol. 430. EDP Sciences, 2023.

[11] H. Miki, K. Hirano, K. Suzuki, M. Nomura, "Another type of talking ATM: ATM with tactile symbols for visually impaired users," In Proc. of HCI international, 2005.

[12] S. Prabhakar, S. Pankanti, A. K. Jain, "Biometric recognition: Security and privacy concerns," IEEE security & privacy, vol. 1, no. 2, pp. 33-42, 2003.

[13] Abikoye, Oluwakemi Christiana, Ganiyat K. Afolabi, and Taye Oladele Aro. "Biometric-based point-of-sale authentication system." International Journal of Software Engineering and Computer Systems 5.1 (2019): 36-51.

[14] Mridha, M. F., Jahir Ibna Rafiq, and Wahid Uz Zaman. "Two-Dimensional Hybrid Authentication for ATM Transactions." Advances in Data and Information Sciences: Proceedings of ICDIS 2019. Springer Singapore, 2020.

[15] Madhuvani, V., A. S. Vickram, and P. R. Yaashikaa. "The ratified biometric automatic teller machine for visually impaired availing IVRS technology in comparison with smart ATM." AIP Conference Proceedings. Vol. 2853. No. 1. AIP Publishing, 2024.