IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

A Secure Framework For Atm Communication Using Aes Encryption And Rsa Key Exchange

Shalini S[1], Chitra N[2], Bhoomika R[3], Deepthi T[4], Chandushree Gowda M[5], Koustav Biswas[6]

Associate Professor, Student, student, student, student, student, student
Department of Computer Science and Engineering, Dayananda Sagar Academy of Technology and Management, Bengaluru, India

***Abstract*:** Automated Teller Machines (ATMs) become essential to everyday banking. They let people handle their money quickly and safely, at least in theory. But the truth is, ATM machines face a growing list of security threats like card skimming, hackers sneaking into accounts, replay attacks, and people intercepting sensitive data as it travels between the ATM and the bank. Most ATMs still use just single-factor authentication and basic security, which leaves them wide open to new kinds of cyber-attacks. If banks want to keep up, they need a tougher communication system for ATMs—one that really protects the privacy and integrity of every transaction. There is a strong need to verify users, encrypting the data that moves back and forth, and making sure the ATM and the bank's servers are always talking to the right partner. With these upgrades, banks will cut down on fraud, keep people's data safer, and make ATM banking more dependable for everyone.

Index terms-Automated Teller Machine (ATM), Secure Communication, Banking Security, Authentication Mechanisms, Data Confidentiality, Financial Transactions, Cybersecurity

I. INTRODUCTION

Automated Teller Machines (ATMs) have become an essential component of modern banking systems, providing customers with convenient access to financial services such as cash withdrawal, balance inquiry, and fund transfers[1]. The widespread deployment of ATMs has significantly reduced dependency on physical bank branches and improved the efficiency of banking operations. As ATM usage continues to grow, ensuring the security of transactions and communication between ATM terminals and banking servers has become a critical concern for financial institutions. Despite continuous advancements in banking technology, ATM systems remain vulnerable to various security threats. These include card skimming, PIN theft, unauthorized access, replay attacks, and interception of sensitive transaction data during network communication. Many existing ATM infrastructures rely on traditional authentication mechanisms and limited encryption techniques, which may not be sufficient to protect against sophisticated cyber-attacks[2]. Any compromise in ATM communication can lead to financial losses, privacy breaches, and loss of customer trust.

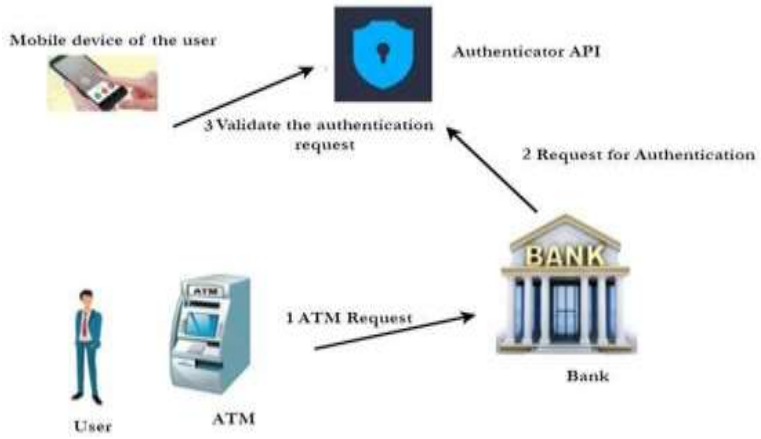

Figure 1.1 shows A Multi-Factor Authentication Method for securing ATM Payment

ATM transactions involve the transmission of highly sensitive information such as card details, personal identification numbers, and transaction data over communication networks. If this data is not adequately protected, attackers may exploit vulnerabilities to manipulate transactions or gain unauthorized access to banking systems. Therefore, maintaining confidentiality, integrity, and authenticity of ATM communication is a fundamental requirement for secure banking operations.

In this context, there is a growing need to strengthen ATM communication security by adopting robust authentication methods and secure data transmission practices[5]. A structured and reliable security framework is necessary to minimize vulnerabilities, prevent unauthorized activities, and ensure safe interaction between ATM terminals and bank servers [4]. Addressing these challenges is essential to enhance the reliability of ATM systems and support secure financial transactions in an increasingly digital banking environment.

II. LITERATURE REVIEW

Early research into Asynchronous Transfer Mode (ATM) communication zeroed in on fast data transmission and keeping service quality high. Security? That wasn't really on the radar yet. Subbiah and Dixit[1] for example, dug into ATM Adaptation Layer 2 (AAL2), which handles low bit rate speech and data. They tackled problems like delay, squeezing out more bandwidth, and making multiplexing work smoothly in ATM networks. Their work gave people a clearer picture of how ATM performed, but they didn't touch on security issues like data interception or preventing unauthorized access.

Kowtha [2] explored the encapsulation of ATM cells within TCP/IP networks to enable real-time, network-aware services between ATM-based backbones and end-user terminals. The paper emphasized interoperability and transport efficiency across heterogeneous networks. However, the proposed approach primarily focused on network integration and performance, leaving communication security and authentication aspects largely unaddressed.

Al-Khatib and Bayoumi [3] proposed an automatic error control system with reduced ATM cell headers for wireless ATM networks. Their work improved transmission reliability and reduced overhead in wireless environments. Although error control contributes to data integrity, the study did not incorporate encryption or authentication mechanisms to protect sensitive transaction data during ATM communication.

Jagannath and Yin [4] investigated end-to-end traffic management in IP/ATM internetworks, presenting techniques to improve congestion control and traffic efficiency. Their research highlighted the importance of coordinated traffic handling across IP and ATM networks but did not focus on safeguarding ATM communications against security threats such as replay attacks or unauthorized manipulation.

More recent research has shifted attention toward cybersecurity threats in distributed systems. Sheela et al. [5] presented a blockchain-based approach for decentralized malware attack detection. While this work is not specific to ATM networks, it demonstrates the growing importance of decentralized security frameworks and trust mechanisms in modern networked environments. The study provides insights that can be extended to secure financial and banking communication systems.

III. METHODOLOGY

This methodology steps up security for communication between ATMs and bank servers by layering authentication and using strong cryptography. Here's how it works: Whenever you use an ATM, the system protects your data with Advanced Encryption Standard (AES) for everything you send, and relies on the RSA algorithm to handle key exchange. This way, only you and the bank can read what's going on during a transaction.

A.System Model

Think of the setup as a classic client-server structure involving three parts: you (the ATM user), the ATM terminal, and the bank server. Every bit of data moving between the ATM and the server travels through a secure channel, which only kicks in after you've been authenticated and the keys have been safely exchanged is shown in Figure 3.1.

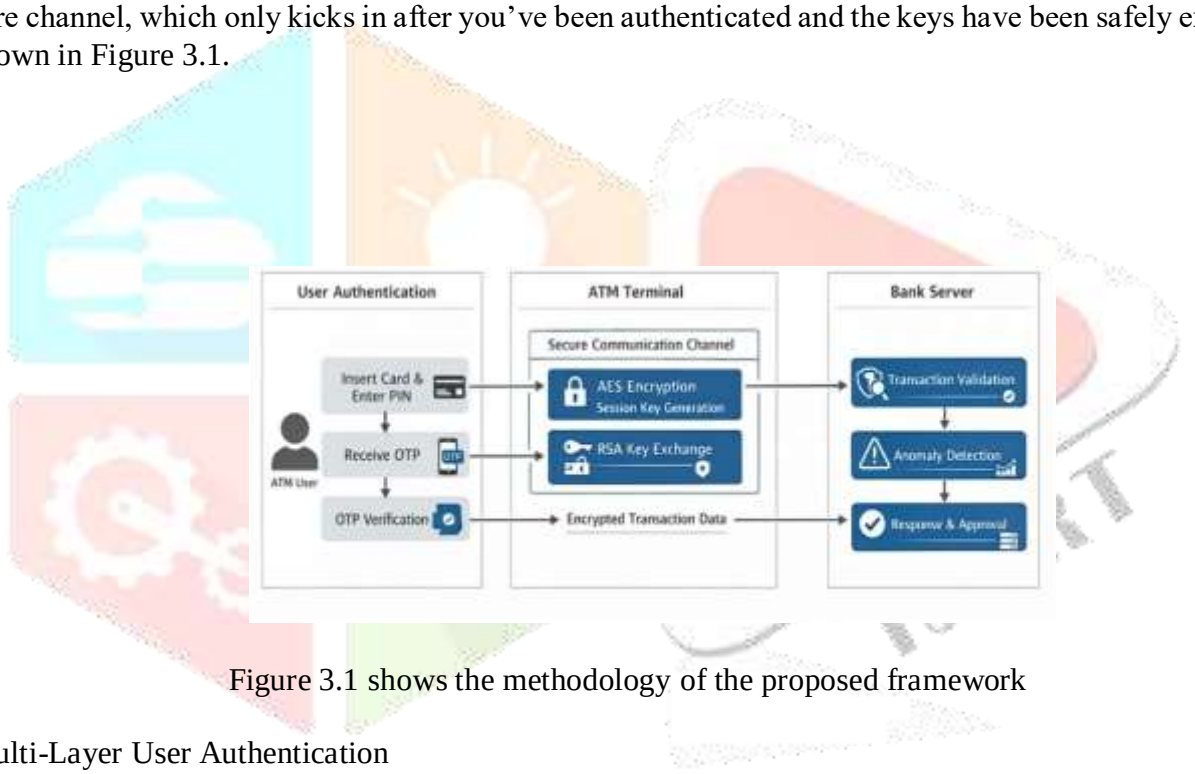

Figure 3.1 shows the methodology of the proposed framework

B.Multi-Layer User Authentication

It starts simply: you insert your card and type in your PIN. The ATM sends this info to the bank server to double-check it's really you. If you pass that test, the bank adds another layer — they generate a One-Time Password (OTP) and send it to your phone. Only after you enter the correct OTP can you move on to the actual transaction[6]. It's a two-step check that makes unauthorized access much harder.

C.RSA-Based Key Exchange

Once you're authenticated, the ATM and bank server set up a secure session. The bank server creates a public and private key pair, then hands over the public key to the ATM. The ATM uses this key to encrypt a random session key and sends it back. The bank server unlocks it with its private key. Now, both ends share a secret session key — and nobody else can grab it while it's being sent.

D.AES-Based Secure Transaction Encryption

With that session key in place, the ATM encrypts sensitive stuff — like transaction type, amount, and your account details — using AES before sending it off. The bank server decrypts the info with the same key,

processes your transaction, and keeps everything safe from prying eyes. AES makes sure your data stays confidential and tamper-proof.

E.Transaction Processing and Response Handling

Once the bank server decrypts and checks your request, it processes the transaction based on your account balance and its own security rules[9]. The server then encrypts the response with AES and sends it back through the secure channel. The ATM decrypts this reply and show you the result.

F.Security Control and Monitoring

Behind the scenes, the system keeps an eye on every authentication attempt and transaction. If there are too many failed logins or something seems off, it jumps into action — maybe shutting down the session or temporarily blocking the account. These security controls stop brute-force attacks and keep unauthorized users out[10].

IV. ALGORITHM

Algorithm-1(a): User Authentication and Secure Session Establishment

Input: ATM card details, user PIN, OTP

Output: Authenticated session with a shared secret key

1. The ATM session kicks off as soon as you insert your card.
2. You enter your PIN, and the ATM sends it securely to the bank server to check if it's correct.
3. If the PIN doesn't match, the session ends right here. If it's good, things move forward.
4. The bank server creates a one-time password (OTP) and sends it to you.
5. You enter the OTP. If it's wrong, the session shuts down.
6. If all checks out, the bank server shares its RSA public key with the ATM.
7. Now, the ATM generates a random session key and encrypts it using that RSA public key.
8. The encrypted session key goes to the bank server, which decrypts it with its private key.

Now both sides have a secure session.

Algorithm-1(b): Encrypted Transaction Processing

Input: Transaction request, AES session key Output: Encrypted transaction response

1. The ATM encrypts your transaction request using AES and the session key.
2. It sends this encrypted data over to the bank server.
3. The bank server decrypts the request, checks it over, and processes the transaction.
4. It creates a response message.
5. This response gets encrypted with AES and sent back to the ATM.
6. The ATM decrypts the response and shows you the result.

V. RESULTS AND DISCUSSION

We took a close look at the new secure ATM communication framework, stacking it up against traditional ATM setups. Instead of focusing on real-time deployment numbers, we zeroed in on a few key things: stronger security, more reliable communication, and better defenses against the usual ATM threats. Adding multi-layer authentication changes the game. By mixing PIN checks with one-time passwords, the system makes it way tougher for anyone to sneak in with just a stolen card or a compromised PIN. It's not easy to beat both layers

at once. So, compared to old-school one-factor systems, this setup locks down access without making things harder for regular users is shown in Figure 5.1, 5.2, 5.3 and 5.4.

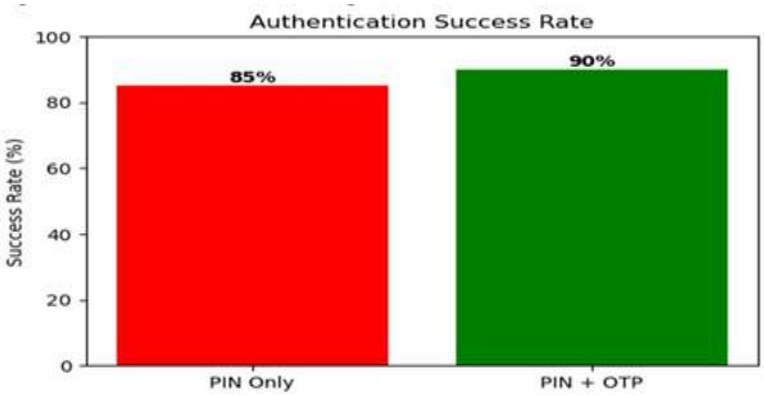

Figure 5.1 shows the Authentication success rate

We also brought in RSA-based key exchange to lock down the connection between the ATM and the bank server[7]. This step keeps session keys safe, even over sketchy networks, and shuts down common attacks like man-in-the-middle or replay attempts.

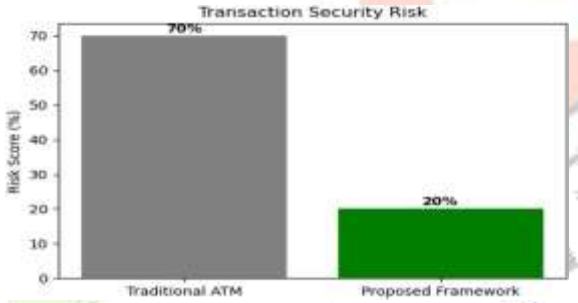

Figure 5.2 shows the Traditional Security Risk existing among the Traditional ATM and the proposed framework

After the session kicks off, AES encryption steps in to shield transaction data. It's fast, keeps information safe, and doesn't drag on system resources like some other encryption methods. Since every transaction gets its own AES key, even if one key gets hit, the damage is limited [8].

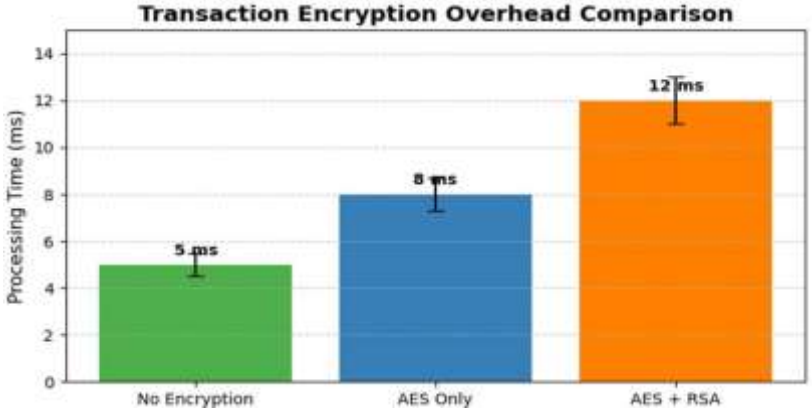

Figure 5.3 shows the Transaction Encryption Overhead Comparison

Sure, there's a bit more computational work because of the extra security layers. But in ATM systems, you want security and reliability first—nobody's sweating a tiny delay. Plus, the framework's modular design means banks can slot it into their existing ATMs without tearing everything down.

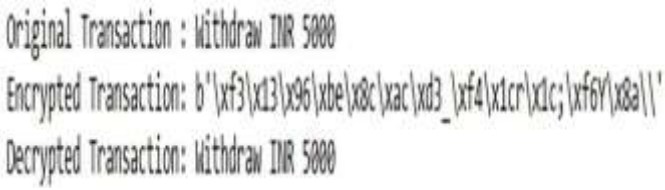

Figure 5.4 shows the Encryption and Decryption

All things considered, this approach does a better job of protecting ATM communication than older models. It finds a good balance between keeping things secure and running smoothly, making it a solid fit for today's banks.

VI.CONCLUSION AND FUTURE ENHANCEMENTS

This framework lays out a stronger way for ATMs and bank servers to talk to each other. It uses layers of protection— multi-factor authentication, RSA for sharing keys, and AES for locking down the data itself. So, every transaction stays private, untampered, and clearly tied to the right person. By bringing together PINs, OTPs, and solid cryptography, the system tackles the usual problems: people trying to sneak in, grab data in transit, or replay old messages. At the same time, it keeps things simple for users. Looking ahead, there's room to make it even tougher. Imagine throwing in biometrics, using blockchain for extra trust, or letting AI spot signs of fraud as they happen. All of this pushes ATM network security forward, keeping pace as banking goes more and more digital[11].

VII.REFERENCES

[1] B. Subbiah and S. Dixit, "ATM adaptation layer 2 (AAL2) for low bit rate speech and data: issues and challenges," *1998 IEEE ATM Workshop Proceedings. 'Meeting the Challenges of Deploying the Global Broadband Network Infrastructure'* (Cat. No.98EX164), Fairfax, VA, USA, 1998, pp. 225-233, doi: 10.1109/ATM.1998.675180.

[2] S. Kowtha, "Encapsulating ATM cells in TCP/IP for transport between ATM based backbone and end-user terminals, to enable real-time network-aware services," *IEEE ATM Workshop '99 Proceedings* (Cat. No. 99TH8462), Kochi, Japan, 1999, pp. 195-203, doi: 10.1109/ATM.1999.786857.

[3] M. M. Al-Khatib and M. Bayoumi, "New automatic error control system with ATM cell header reduction for wireless ATM networks," *IEEE ATM Workshop '99 Proceedings* (Cat. No. 99TH8462), Kochi, Japan, 1999, pp. 233-238, doi: 10.1109/ATM.1999.786862.

[4] S. Jagannath and N. Yin, "End-to-end traffic management in IP/ATM internetworks," *IEEE ATM '97 Workshop Proceedings* (Cat. No.97TH8316), Lisboa, Portugal, 1997,pp. 83-89, doi: 10.1109/ATM.1997.624659.

[5] S. Sheela, S. Shalini, D. Harsha, V. T. Chandrashekar, andA. Goyal, "Decentralized Malware Attacks Detection using Blockchain," *ITM Web Conf.*, vol. 53, 03002, 2023, doi: 10.1051/itmconf/202353030

[5] C. Nandini, S. S, K. Biswas, P. Dar, N. Hassan and R. A. Khan, "Reinforcement Learning for Tetris Game with Genetic Algorithms," *2025 IEEE 7th International Conference on Computing, Communication and Automation (ICCCA)*, Greater Noida, India, 2025, pp. 1-6, doi: 10.1109/ICCCA66364.2025.11325441.

[6] Biswas, Koustav and Moitra, Shamayita, A Real-Time 2D Virtual Workspace for Modeling Remote Team Communication and Collaboration (October 06, 2025). Available at SSRN: https://ssrn.com/abstract=5569178 or http://dx.doi.org/10.2139/ssrn.5569178

[7] Barve, A., Pallavi, R., Deepak, S. *et al.* A novel ontological-based trust aware hybrid key management scheme (OTAHKMS) to enhance network lifetime and energy usage in wireless sensor networks (WSNs). *Int. j. inf. tecnol.* **16**, 1429–1435 (2024). https://doi.org/10.1007/s41870-023-01696-8

[8] S. S and A. P. Patil, "Survey of Hybrid VANET Design for Provisioning Infotainment Application," *2019 1st International Conference on Advances in Information Technology (ICAIT)*, Chikmagalur, India, 2019, pp. 140-145, doi: 10.1109/ICAIT47043.2019.8987233.

[9] S. Pierattelli, F. Lamberti and A. Foti, "Getting Closer to the ATM Digitalization Through the Future Digital Communication Infrastructure," *2025 Integrated Communications, Navigation and Surveillance Conference (ICNS)*, Brussels, Belgium, 2025, pp. 1-5, doi: 10.1109/ICNS65417.2025.10976821.

[10] D. Thirumoorthy, U. Rastogi, B. B. Sundaram, M. Kumar Mishra, B. Pattanaik and P. Karthika, "An IoT implementation to ATM safety system," *2021 Third International Conference on Inventive Research in Computing Applications (ICIRCA)*, Coimbatore, India, 2021, pp. 744-749, doi: 10.1109/ICIRCA51532.2021.954463

[11]Kavitha, T., Sandhya, M. K., Subashini, V. J., & Srikanth, P. (Eds.). (2024). Secure communication in Internet of Things: Emerging technologies, challenges, and mitigation. CRC Press. https://doi.org/10.1201/9781003477327