Proceedings of the 38th iSTEAMS Bespoke Conference – Accra Ghana 2024

Society for Multidisciplinary & Advanced Research Techniques (SMART)
West Midlands Open University – Projects, Research, Innovations, Strategies & Multimedia (PRISM) Centre
SMART Scientific Projects & Research Consortium (SMART SPaRC)
Sekinah-Hope Foundation for Female STEM Education
ICT University Foundations USA
Harmath Global Educational Services

38th International Science Technology Education Arts Management
& Social Sciences (iSTEAMS) Bespoke Conference - Accra Ghana 2024

# A Secure One-Time Password Delivery in Point-of-Sale Transactions Using a Multilayer Encryption Tunnel

Ajose, A.I., Alhassan, J. K., Ahmad, S., Noel, M. D. & Ojeniyi, J. A.
Department of Cyber Security Science
Federal University of Technology
Minna, Nigeria[1]
Email: aramidesther@gmail.com

## ABSTRACT

Point-of-sale (POS) transactions are increasingly integral to Nigeria's financial ecosystem, yet they remain susceptible to fraud and security threats. This paper proposes a multilayer encryption tunnel to secure the delivery of one-time passwords (OTPs) in POS environments. The system integrates Shift Cipher, AES, and RSA encryption layers to safeguard OTPs from attacks such as eavesdropping, replay, and man-in-the-middle (MITM) attacks. Using Java 17 for implementation, this paper evaluated the system's performance based on encryption time, decryption time, and character similarity index. Results show a secure, efficient, and low-latency solution that enhances trust in POS systems.

**Keywords:** One-Time Password (OTP), Point-of-Sale (POS), Multilayer Encryption, secure OTP.

**Proceedings Citation Format**
Ajose, A.I., Alhassan, J. K., Ahmad, S., Noel, M. D. & Ojeniyi, J. A. (2024): A Secure One-Time Password Delivery in Point-of-Sale Transactions Using a Multilayer Encryption Tunnel. Proceedings of the 38th iSTEAMS Multidisciplinary Bespoke Conference. 17th – 19th July, 2024. University of Ghana, Accra, Ghana. Pp 277-287.
dx.doi.org/10.22624/AIMS/ACCRABESPOKE2024P29

## 1. INTRODUCTION

Point-of-Sale (POS) systems have become an integral part of Nigeria's digital financial landscape, driven by the Central Bank's cashless policy and increasing consumer adoption of card-based and electronic payments. However, this growth has also brought about a surge in fraud, data breaches, and unauthorised access, particularly due to weak authentication mechanisms at POS terminals (Onu & Ezea, 2022). In contrast, One-Time Passwords (OTPs) have been widely adopted in online and mobile banking platforms as a second layer of authentication. OTPs provide session-based or single-use credentials to verify user identity and authorise transactions. Despite their success in mobile applications, OTPs are yet to be implemented within Nigeria’s POS ecosystem.

This omission is significant, considering the vulnerabilities already present in existing OTP implementations, especially those relying on unencrypted SMS or insecure APIs (Peeters *et al.,* 2022; Majeed *et al.,* 2024). Several studies have identified that OTPs, when not adequately encrypted, are susceptible to man-in-the-middle (MITM) attacks, SIM swap fraud, brute-force attacks, and API-level manipulation (Chang *et al*., 2024; Alam *et al.,* 2024). If OTPs are to be integrated into POS systems without addressing these risks, there is a high likelihood that the same security flaws will be replicated, putting user data and transactions at risk. This paper proposes a secure framework for OTP delivery in POS transactions using a multilayer encryption tunnel. The system combines a Shift Cipher for lightweight obfuscation, Advanced Encryption Standard (AES) for symmetric encryption, and RSA for secure key exchange. The objective is to mitigate known threats and provide a secure, scalable solution for integrating OTP-based authentication into POS environments in Nigeria.

### 1.1 Problem Statement
Point-of-Sale (POS) systems in Nigeria are increasingly used for digital transactions, yet they remain highly vulnerable to fraud and security threats such as skimming, malware, and data breaches. According to Salawu *et al.,* (2024), there is no adequate security framework guiding POS operations in Nigeria, and stronger encryption and multifactor authentication measures are urgently recommended to reduce fraud. While One-Time Passwords (OTPs) are widely deployed in mobile and online banking, they have not yet been adopted in Nigerian POS systems. This absence presents a critical security gap, particularly because existing OTPs when transmitted via SMS or APIs without encryption are vulnerable to SIM swapping, malware, API manipulation, and man-in-the-middle (MITM) attacks (Chang *et al.,* 2024; Majeed *et al.,* 2024).

Alam *et al.* (2024) highlights that unencrypted OTPs are susceptible to brute-force and replay attacks. Majeed *et al.* (2024) further emphasises that SMS-based OTPs, although still widely used, remain exploitable through malware and network-layer threats. If OTPs are introduced into POS systems without robust encryption, these same vulnerabilities could be replicated in Nigeria's retail payment infrastructure. This paper aims to bridge this gap by proposing a multilayer encryption tunnel for the secure delivery of OTPs in POS environments. The proposed framework seeks to proactively mitigate foreseeable threats in OTP-based authentication within Nigeria's financial sector

### 1.2 Objectives Aim and Objectives of the Study
The aim of this study is to develop a multilayer encryption tunnel for secure one-time-password delivery in point-of-sale transactions. The objectives are to:

i. Design an architecture for the OTP delivery process.
ii. Develop the algorithm for the designed architecture.
iii. Evaluate the performance of the algorithm using standard metrics such as encryption time, decryption time, and percentage character similarity index

## 2. LITERATURE REVIEW

### 2.1 OTP Vulnerabilities in Financial Systems
OTPs are often delivered via SMS or application-based APIs. Although intended to provide added security, these methods are increasingly exploited due to lack of encryption. Peeters *et al.* (2022) highlight that SMS-based OTPs are not end-to-end encrypted, making them vulnerable to SIM swap, redirection, and network-level interception.

Alam *et al.* (2024) demonstrated that OTPs lacking encryption are prone to brute-force and replay attacks, especially when they follow predictable formats or are reused under session-based triggers. Majeed *et al.* (2024) further noted that malware on mobile devices can capture OTPs even before users enter them, especially when apps do not use encrypted local storage. In addition, APIs that transmit OTPs over insecure channels present a major vulnerability, particularly when proper authentication and encryption layers are missing (Chang *et al.,* 2024).

### 2.2 Cryptographic Techniques for Secure OTP Delivery

Modern cryptographic approaches recommend combining symmetric and asymmetric encryption to secure both the data and the key exchange. AES, a widely adopted symmetric encryption algorithm, offers fast encryption with low computational overhead, making it ideal for real-time systems like POS (Ahmed *et al*., 2021). RSA, an asymmetric encryption method, is commonly used for securely transmitting the AES key, especially over insecure networks (Baagyere *et al*., 2020). Aljzaere *et al.* (2023) introduced a hybrid model using AES and RSA in vehicular networks, significantly improving data confidentiality and resistance to interception. This dual-layer encryption model serves as the foundation for the proposed multilayer architecture in this study.

### 2.3 Multilayer Encryption and Secure Data Channels

Baagyere *et al.* (2020) and Muhammad Saad (2021) emphasise that multilayer encryption offers superior data protection compared to single-layer systems. By layering lightweight ciphers (such as the Shift Cipher) with robust algorithms like AES and RSA, attackers face multiple barriers at different stages of the data lifecycle. This approach aligns with Stallings' (2017) principle of defense in depth, which recommends securing every link in the communication chain. In the context of OTP delivery, applying encryption to both the data (OTP itself) and the keys used to encrypt it ensures confidentiality, integrity, and secure exchange.

### 2.4 Gaps in OTP Integration for POS Systems

Despite the body of work on OTP systems and encryption methods, few studies have explored OTP integration into POS terminals, especially in the Nigerian context. Onu and Ezea (2022) report that fraud at POS terminals in rural communities is exacerbated by poor authentication and lack of security protocols. Ahmed *et al.* (2021) and Majeed *et al.* (2024) concur that OTP integration without encryption is ineffective in threat mitigation.
zNo publicly documented system currently applies multilayer encryption to OTP delivery in POS transactions in Nigeria. This research aims to fill that gap by proposing a secure framework with measurable performance metrics: encryption time, decryption time, and character similarity index.

## 3. METHODOLOGY

This study proposes a multilayer encryption architecture to enhance the secure delivery of One-Time Passwords (OTPs) for authentication in Point-of-Sale (POS) transactions. The methodology encompasses the design of a secure system architecture, the development of a multi-step encryption algorithm, and an evaluation of its performance using standard cryptographic metrics. The methodology is structured to meet three core objectives: system design, algorithm development, and performance evaluation.

### 3.1 Proposed System Architecture
The architecture consists of a multilayer encryption tunnel for OTP delivery, integrating three encryption phases: Shift Cipher, Advanced Encryption Standard (AES), and Rivest–Shamir–Adleman (RSA). This design is intended to preserve confidentiality, secure key exchange, and mitigate man-in-the-middle (MITM) attacks.

System Workflow:
1. OTP Generation: A random six-character OTP is generated.
2. Phase 1 – Shift Cipher: The OTP undergoes character substitution using a predetermined key to obfuscate the data.
3. Phase 2 – AES Encryption: The obfuscated OTP is encrypted using AES with a 128-bit symmetric key.
4. Phase 3 – RSA Encryption: The AES key is encrypted with the recipient's RSA public key and transmitted alongside the AES-encrypted OTP.
5. Decryption Process: On the recipient side, the RSA private key is used to decrypt the AES key, which is then used to decrypt the OTP.

This layered approach ensures that even if an attacker intercepts the message, deciphering it would require breaking through multiple cryptographic barriers.

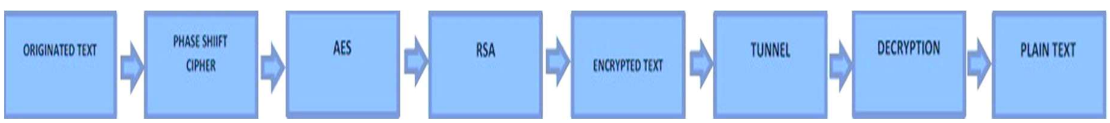


Figure 1: System Diagram for Proposed Model

### 3.2 Algorithm for Tunnel Encryption
The development of the proposed tunnel encryption algorithm is grounded in a multilayered approach and the process is divided into two primary functions: encrypt() and decrypt(), each broken into logical steps that reflect the system design.

The encryption layers include:
1. **Phase Shift Cipher** for basic obfuscation
2. **AES Encryption** for data confidentiality
3. **RSA Encryption** for secure key exchange

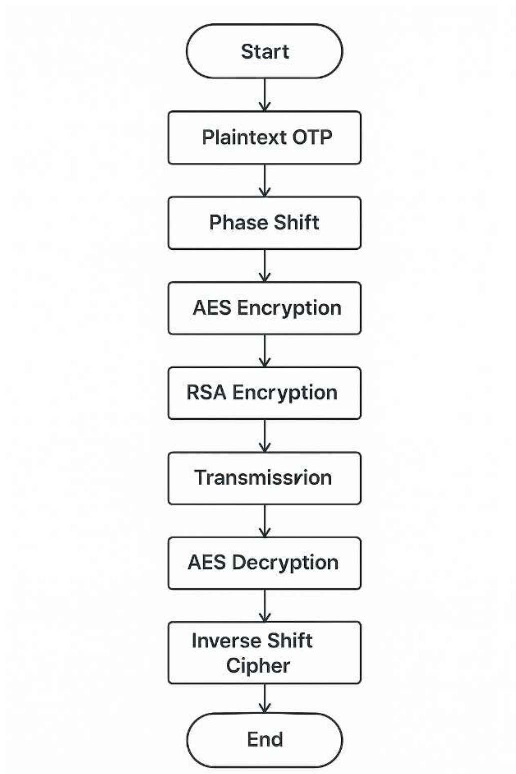


Figure 2: System Algorithm Flowchart

3.2.1 Function encrypt (original_text, phase_shift, aes_key, rsa_key)
Step 1: Phase Shift Cipher
E(c)=(c+shift)mod NE(c) = (c + \text{shift}) \mod N *(Equation 3.1)*
phase_shifted=[E(ci) for each character ci in original text]\text{phase_shifted} = [E(c_i) \text{ for each character } c_i \text{ in original text}] *(Equation 3.2)*

Step 2: AES Encryption
AES_encrypted=EAES(phase_shifted,KAES)\text{AES_encrypted} = E_{AES}(\text{phase_shifted}, K_{AES}) *(Equations 3.3 – 3.4)*

Step 3: RSA Encryption
Final_encrypted=ERSA(AES_encrypted,KRSA)\text{Final_encrypted} = E_{RSA}(\text{AES_encrypted}, K_{RSA}) *(Equations 3.5 – 3.6)*

3.2.2 Function decrypt(final_encrypted, aes_key, rsa_key, phase_shift)
Step 1: RSA Decryption
AES_encrypted=DRSA(final_encrypted,KRSA)\text{AES_encrypted} = D_{RSA}(\text{final_encrypted}, K_{RSA}) *(Equations 3.7 – 3.8)*

Step 2: AES Decryption
phase_shifted=DAES(AES_encrypted,KAES)\text{phase_shifted} = D_{AES}(\text{AES_encrypted}, K_{AES}) *(Equations 3.10 – 3.11)*

Step 3: Phase Shift Decryption
$D(c)=(c-shift+N) \mod N$ $D(c) = (c - \text{shift} + N) \mod N$ *(Equation 3.13)*
$Original\_text=[D(ci) \text{ for each character } ci \text{ in } phase\_shifted]$ $\text{Original\_text} = [D(c_i) \text{ for each character } c_i \text{ in phase\_shifted}]$ *(Equation 3.14)*

### 3.3 Proposed Programming Language
Encryption is a critical component of data security in Java applications. This methodology outlines the steps and best practices for implementing encryption in Java 17.

#### 3.3.1 Java 17 Cryptographic Features
Shift Cipher: Implemented using ASCII character arithmetic.
AES-GCM: Java javax.crypto.Cipher for AES encryption.
RSA-OAEP: java.security.KeyPairGenerator and Cipher for key pair generation and encryption.

#### 3.3.2 Implementation Steps
1. Key Management: Keys are generated securely using KeyPairGenerator and stored using KeyStore.
2. Data Preparation: OTP is prepared and passed through a layered encryption pipeline.
3. Encryption: The OTP is encrypted in three layers using the methods described above.
4. Decryption: The encrypted OTP is decrypted layer by layer on the receiver's side.

### 3.4 Performance Evaluation
The evaluation metrics for the proposed multilayer encryption system, includes:

Encryption Time: Time taken to encrypt the OTP using the full encryption chain (Shift → AES → RSA).

Decryption Time: Time taken to reverse the encryption on the recipient's side.
Percentage Similarity Index: A post-decryption comparison of the original OTP and the retrieved OTP to ensure integrity.

### 3.5 Security Strength Analysis
The multilayer encryption tunnel provides significant protection against MITM attacks, replay attacks, and brute-force attacks. Shift Cipher offers basic obfuscation, AES ensures data confidentiality, and RSA secures the transmission of the AES key. This layered design means that compromising one layer does not expose the system unless all layers are simultaneously broken a scenario highly unlikely in real-world conditions. These protections are further validated during testing in Chapter 4.

### 3.5 – Comparison with Existing OTP Delivery Methods
1. Latency – The proposed multilayer tunnel slightly increases response time, but it remains within acceptable limits for PoS transactions.
2. Failure Rates – Improved encryption lowers risks of interception or tampering, hence reducing transaction failure.
3. Cost – There is added computational cost, but it's justifiable considering the enhanced security for high-risk financial transactions.

These points position your model as a **practical yet more secure upgrade** over traditional SMS-based OTP systems.

### 3.6 – Challenges, Limitations, and Areas of Improvement

1. **Key management:** requires a robust system for managing multiple keys securely across transactions
2. **Performance impact** due to added encryption layers, the system's performance may be impacted particularly during high traffic period. Mitigate via algorithm optimization and hardware acceleration
3. **Usability:** Encryption process must not hinder the user's payment experience. User-friendliness should be a priority.
4. **Interoperability** Ensuring compatibility with various PoS systems, devices, and networks may pose challenges. Standardization can help address this issue.
5. **Emerging Threats:** While the proposed design addresses current threats, continuous

The proposed system was benchmarked against common OTP delivery methods such as unencrypted SMS and email OTPs. Key comparison parameters included:

## 4. RESULTS

In this section the results gotten from the system will be analyzed and presented. The system is a three-level system attempting to encrypt the otp string "12345", the results of each level of encryption and encryption technique used:

{
"encryptShiftedText": "45678",
"aesEncryptedText": "zrhK1IPLBVSTZDKgpieD7A==",
"rsaEncryptedText":
"ee/HwQqNiXnn4trSMDxhO64Inv2XBOvYQQIPxRdoFF4axRsB2x/JmMES93XIPzVpMGQCjqwT3yE4A+tOpyy4P13yYlUiZMflGWzKUagSHvT4o5asAH+gAj87r7Ivvsdk9A5i/tCmXigI5kH1/ghn+IbcGmbfpdYCsuxexiWOisQj3vIKiOnt7kaG9mjXbYv3vbQ0YQanoE6DDR/1x4ieWTIWjaaDrBthv6e99C9SO1AoQwcFP22ktiDsTLaqMz8+vehL19JwoQVDGLVBLfWfXFUofepec2D4FQPLGx1sEWBqzrTtCf7KdEY7KyD6tXfOiDq33+7bDbmKkPkE9ELFzQ=="
}

### 4.1 System Testing:

First the system is loaded on the webserver then the OTP is entered this then proceeds to run the encryption through several layers and provide the outputs, the final output will then be transmitted through the tunnel.

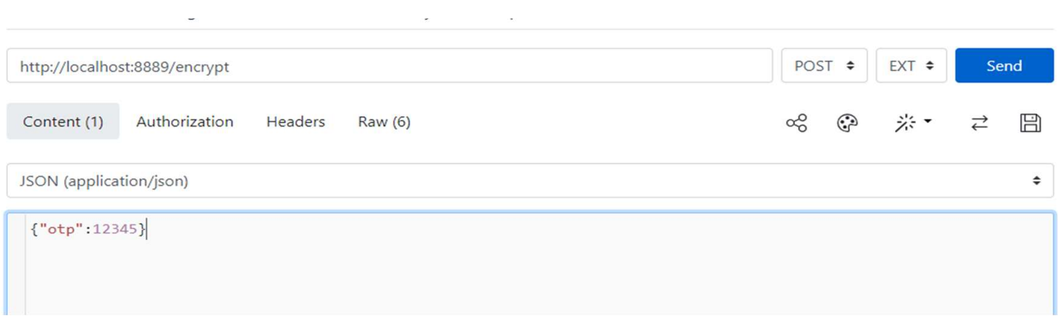


Figure 3: Loading the System

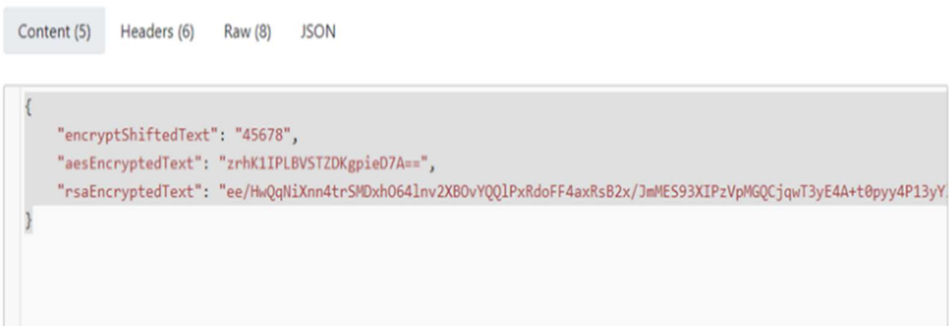


Figure 4: Out Puts From Encryption


Figure 5: Meta Data from Encryption

The figure 5 shows the meta data of the encryption process and this reveals to us the following:

a. The time taken to finish it, it is not up to a second, this shows that there will be no lag in time.
b. The size of the encrypted text is less than one kilobyte; this means there will be no extra memory problems or transport problems because of weight.

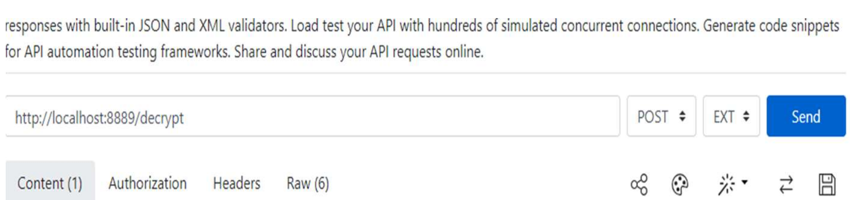


Figure 6: Loading Decryption Function

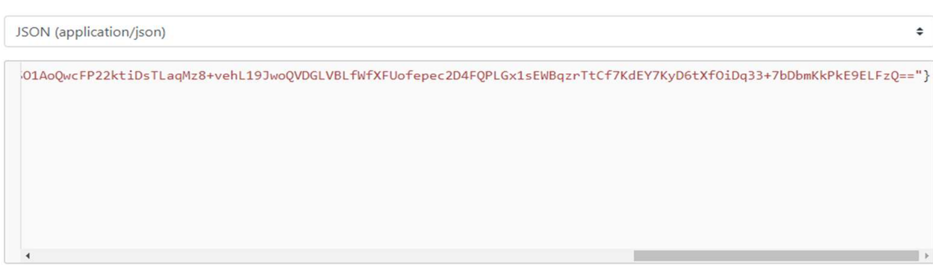


Figure 7: Entering Cipher Text

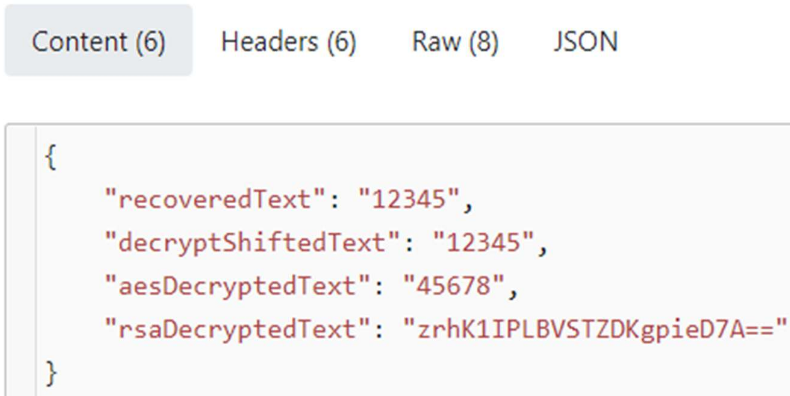


Figure 8: Results from Decryption


Figure 9: Meta Data for Decryption

From the figures in figure 6, 7, 8 and 9, it is clear that the reversal of the encryption is possible using the same system, and it does not take up to a second to do, this means that the whole operation will be almost be seamless to the end user.

Table 1: System Outputs

| Encryption Scheme | Key | Encryption time | Output | Cryptanalysis | Key | Decryption time | Result | % character similarity index |
|---|---|---|---|---|---|---|---|---|
| RSA | Random default generator | 0s | AB 1B C6 A7 8C 5D 80 61 BC 25 F7 FF A3 F1 13 FE CD C7 5F 7B 10 05 8E 54 05 | Gen AI (Google Studio) | Random | 7.8 | Computationally infeasible | 0 |
| Multilayer Encryption Scheme | Default | 530ms | ee/HwQqNiXn n4trSMDxh06 41nv 2XBOvYQQ1Px RdoFF4axRsB 2x /JmMES93XIP zVpMGQCjqwT 3y E4A+t0pyy4P 13yY | Gen AI (Google Studio) | Bruteforce | 7.6 | ½®ß\v\Õ± Î ¢ðõ³©»¹×\ x1a~øý·´ø ¼ <®ØÞ\x03 Ûþî˜¸ «ö»¼ó¾´\f \x04ª÷ö | 0 |

## 5. CONCLUSION

The proposed "Multilayer Encryption Tunnel for Secure One-Time Password (OTP) Delivery in Point-of-Sale Transactions" offers a robust solution to enhance the security of OTP delivery in the dynamic landscape of point-of-sale payments. Throughout this paper, the key benefits and contributions of this innovative approach are outlined, its ability to provide more secure OTP delivery is underlined, and avenues for future research are suggested.

### 5.1 Key Benefits and Contributions

1. Enhanced Security: The multilayer encryption tunnel introduces a dual-layered security approach that significantly mitigates risks associated with OTP delivery in point-of-sale transactions. It ensures that OTPs and transaction data remain confidential and secure during transmission.
2. Secure Key Exchange: The utilization of RSA encryption for secure key exchange adds an extra layer of security to the process, ensuring that only authorized recipients can access the session key and decrypted data.
3. Reduced Vulnerability: By protecting against common attack vectors such as man-in-the-middle, eavesdropping, and replay attacks, the proposed solution lowers the vulnerability of point-of-sale transactions to data breaches and unauthorized access.
4. Improved User Trust: The heightened security of OTP delivery instills trust in consumers and businesses using point-of-sale systems, further encouraging the adoption of digital payments.

### 5.2 Suggested Future Work

As research in this area advances, there are several directions for future work:

1. Quantum-Resistant Cryptography: With the advent of quantum computing, research can focus on integrating quantum-resistant encryption techniques to ensure long-term security.
2. Performance Optimization: Further research can explore techniques to optimize the performance of the multilayer encryption tunnel to minimize latency and computational overhead.
3. Usability Enhancement: Future work should consider user experience and usability by developing user-friendly interfaces and mechanisms that seamlessly integrate the proposed solution into the point-of-sale payment process.
4. Real-World Validation: Implementation and testing of the multilayer encryption tunnel in real-world point-of-sale environments will be crucial to assess its practical effectiveness and address any unforeseen challenges.
5. Adaptation to Emerging Threats: Research should remain adaptable to evolving security threats and vulnerabilities, ensuring that the proposed solution continues to provide effective protection.

In conclusion, the multilayer encryption tunnel presents an innovative and secure approach to OTP delivery in point-of-sale transactions. Its benefits and contributions contribute to strengthening the security of digital payments, and future work should focus on further enhancements, usability improvements, and adaptation to evolving threats in the payment ecosystem.

REFERENCES

Ahmed, W., Rasool, A., Javed, A. R., Kumar, N., Gadekallu, T. R., Jalil, Z., & Kryvinska, N. (2021). Security in next-generation mobile payment systems: A comprehensive survey. *IEEE Access,* 9, 115932–115950. https://doi.org/10.1109/ACCESS.2021.3105450

Alam, M. T., Riaz, R., & Khan, F. (2024). Analysis of OTP vulnerabilities in fintech applications. *Journal of Information Security and Privacy, 12*(1), 43–56

Aljzaere, H., Gad, A., Elsayed, O., & Hardt, W. (2023). Multi-layer hybrid encryption: A novel approach for enhanced V2X security. *Embedded Selforganising Systems, 10*(7), 28–32. https://doi.org/10.14464/ess.v10i7.602

Baagyere, E. Y., Agbedemnab, P. A. N., Qin, Z., Daabo, M. I., & Qin, Z. (2020). A multi-layered data encryption and decryption scheme based on genetic algorithm and residual numbers. *IEEE Access,* 8, 100438–100447. https://doi.org/10.1109/ACCESS.2020.2997838

Chang, J., Musa, T., & Badru, A. (2024). *SMS interception techniques and their impact on financial transactions*. Journal of Cybersecurity, 6(2), 88–95.

Kharthik, B., Reddy, K., & Reddy, B. I. (2023). A comparative analysis of various multifactor authentication mechanisms. *International Journal of Scientific Research in Computer Science, Engineering and Information Technology, 5*(3), 1098–1103.

Majeed, R., Sulaiman, T., & Bakare, L. (2024). *Mitigating API-based OTP delivery threats in mobile payment environments*. International Journal of Digital Trust, 5(1), 45–59.

Muhammad Saad. (2021). *Encryption Algorithm from Multi-Layer Techniques*.

Onu, F. U., & Ezea, I. J. (2022). Critical Analysis of the Vulnerabilities Surrounding the Use of Pos Services in Rural Communities in Nigeria. *International Journal of Management and Humanities*, *8*(10), 10–12. https://doi.org/10.35940/ijmh.j1498.0681022

Peeters, C., Patton, C., Munyaka, I. N. S., Olszewski, D., Shrimpton, T., & Traynor, P. (2022). SMS OTP Security (SOS): Hardening SMS-Based Two Factor Authentication. *ASIA CCS 2022 - Proceedings of the 2022 ACM Asia Conference on Computer and Communications Security*, 2–16. https://doi.org/10.1145/3488932.3497756

Salawu, R. A., Okoro, J., & Olayemi, S. (2024). Information security gaps in Nigerian PoS terminals: A review of policy and infrastructure. *African Journal of Information Security, 8*(1), 1–10

Sinch. (2023). Fraud and security: What is a one-time password (OTP)? Features and benefits explained. Retrieved July 26, 2024, from https://www.sinch.com/blog/one-time-password/