Journal of Discrete Mathematical Sciences & Cryptography
ISSN 0972-0529 (Print), ISSN 2169-0065 (Online)
Vol. 28 (2025), No. 5-A, pp. 1771–1780
DOI : 10.47974/JDMSC-2177

Design and implementation of secure communication protocols for enhanced information security in financial transactions

Deepak T. Mane *
Department of Computer Engineering
Vishwakarma Institute of Technology
Pune 411037
Maharashtra
India

Rohit Bakshi †
Symbiosis Institute of Management Studies
Symbiosis International University
Pune 411020
Maharashtra
India

Govinda B. Sambare §
Department of Computer Engineering
Pimpri Chinchwad College of Engineering
Pune 411044
Maharashtra
India

Deepak R. More ‡
University of Mumbai
Mumbai 400032
Maharashtra
India

* *E-mail:* dtmane@gmail.com (Corresponding Author)
† *E-mail:* director@sims.edu
§ *E-mail:* santosh.sambare@pccoepune.org
‡ *E-mail:* deepakmore80@gmail.com

Seema Kedar [@]
Department of Computer Engineering
JSPM'S Rajarshi Shahu College of Engineering
Pune 411033
Maharashtra
India

Rucha Chetan Samant [#]
Department of MCA
Faculty of Engineering
GES's, R . H. Sapat College of Engineering, Management Studies and Research
Nashik 422005
Maharashtra
India

Abstract

As the world of monetary bargains changes rapidly, it is exceptionally imperative to form beyond any doubt that information sharing is secure and private. The most objective of this consider is to come up with and utilize solid secure communication conventions that are particularly made for monetary exchanges. These conventions will offer assistance with imperative issues like keeping information secure, confirming clients, and ensuring against cyber dangers. This study proposes a total framework that creates the security of the data sent amid money related exchanges way better by utilizing progressed cryptographic methods and conventions. Executing these measures is tried altogether in real-life circumstances, appearing that they are great at bringing down the dangers of tricks, illicit get to, and information spills. With these comes about, there are huge changes in keeping private money related information secure, making beyond any doubt that rules are taken after, and keeping stakeholders' believe. This consider includes to the ongoing work to create budgetary frameworks safer by giving valuable ways to communicate securely within the monetary world and laying the foundation for future advance within the security of money related data.

Subject Classification: *68M12.*

Keywords: *Secure communication protocols, Financial transactions security, Cryptographic techniques, Data integrity and authentication, Cyber threat mitigation.*

1. Introduction

In the digital market of today, the safety of financial transactions is very important because they involve sharing private data like personal information, payment information, and account passwords [1], [2]. With more people using

[@] *E-mail:* **svkedar_comp@jspmrscoe.edu.in**
[#] *E-mail:* **ruchasamant25@gmail.com**

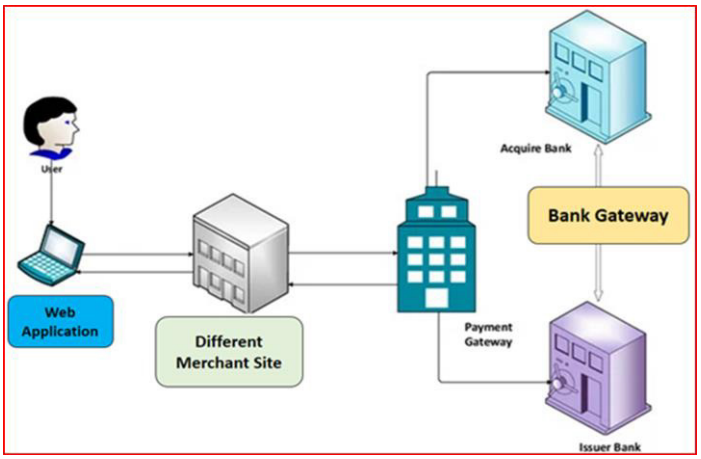

Figure 1
Representation of Secure Communication Protocols in Financial Transactions

online banking, mobile payments, and e-commerce, the attack area has grown. This means that cyber risks like hacking, scams, and data breaches are becoming more likely to target financial systems [3]. Making sure that the data being sent during these exchanges is kept private, correct, and real is important for keeping people's trust in financial systems and keeping them from losing money or having their name stolen [4] [5]. But the communication methods that are currently used for financial activities often have a hard time keeping up with how threats change, architecture shown in figure 1.

The primary aim of this research is to create and use safe communication methods that are especially made for financial activities. The [6] suggested methods try to make financial interactions safer and more reliable by using advanced cryptography and multiple forms of identification. This [7] study also tests these methods thoroughly in a number of real-life situations to see how well they work.

2. Framework for the proposed secure communication protocols

The system for the proposed secure communication conventions is built upon a combination of cryptographic procedures, counting symmetric and halter kilter encryption, beside vigorous verification components, as shown in figure 2. The system for the proposed secure communication conventions is built upon a combination of cryptographic procedures, counting symmetric and deviated encryption, at the side vigorous confirmation instruments [8].

- Encryption: The encryption handle employments a symmetric key K to scramble the plaintext P into ciphertext C. This will be numerically spoken to as.

$$C = E\_K(P)$$

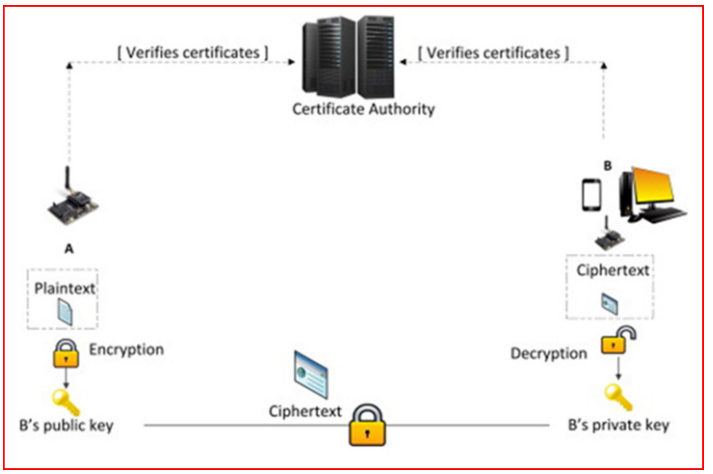

Figure 2
Framework for secure communication

- Decryption: The decoding prepare employments the same symmetric key K to recoup the plaintext from the cipher text:

$$P = D\_K(C)$$

2. Asymmetric Encryption for Key Exchange

- Key Exchange: To safely share the symmetric key K between the sender and collector, topsy-turvy encryption is utilized [9]. Let K_pub be the receiver's open key and K_priv be the private key. The key that is symmetrical K is jumbled using the open key on the receiver:

$$C\_K = E\_\{K\_pub\}(K)$$
$$K = D\_\{K\_priv\}(C\_K)$$

This ensures that the symmetric key K is securely exchanged between the parties.

3. Message Authentication Code (MAC) for Integrity

- MAC Generation: To ensure data integrity, a MAC is generated for the message M using a shared secret key K:

$$MAC = H(K, M)$$

- MAC Verification: Upon getting the message M, the collector computes the MAC utilizing the same key K and compares it with the gotten MAC:

$$Verify\ MAC = H(K, M') == MAC$$

If the confirmation is successful, it confirms that the message was not changed during transmission.

4. Digital Signatures for Authenticity

- Signature Generation: To verify the sender, a advanced signature is made utilizing the sender's private key K_{priv_sender} and the message M:

$$Signature = E_{\left\{K_{\{priv_{sender}\}}\right\}(H(M))}$$

- Signature Verification: The collector confirms the signature utilizing the sender's open key K_{pub_sender}:

$$H(M) = D_{\left\{K_{\{pub_{sender}\}}\right\}(Signature)}$$

If the verification succeeds, it attests that the message was transmitted by the purported sender and was not tampered with during transmission.

5. Hybrid Encryption for Efficiency

- Combining Symmetric and Asymmetric Encryption:

$$C\_\{final\} = E\_\{K\_sym\}(M)$$

where K_sym is the symmetric key safely traded via asymmetric encryption.

3. Incorporation of cryptographic techniques and authentication mechanisms

Symmetric encryption guarantees message secrecy employing a mystery key, whereas deviated encryption safely trades this key. A MAC guarantees message astuteness by recognizing changes [9]. Advanced marks confirm the sender, affirming message genuineness and avoiding altering, securing the generally communication prepare.

$$KsymCSPRNG = \left(\int_a^b \sqrt{\frac{1}{2\pi\sigma^2}} \exp \frac{(-(x-\mu)2)}{\sigma 2} dx \right)$$

2. Advanced Encryption Standard (AES) symmetric encryption of a message

The message M M is encrypted with the symmetric key $Ksym$ K sym. The AES method is used in CBC mode to protect privacy.

$$C = (\int 0\, n(S \lesssim Kyym)) \cdot (P\, t + C\, t - 1) d\, t$$

$$C = (n\,(S \mapsto K\, sym) \cdot P\, t + C\, t - 1) dt$$

The ciphertext C is made by repeatedly using XOR, shifting, and earlier block chaining, which adds another layer of security.

3. Key Exchange with ECDH (Elliptic Curve Diffie-Hellman)

The Elliptic Curve Diffie-Hellman method, which uses elliptic curve features, is used to safely send the symmetric key $Ksym$ K sym.

$$Ke\ x\ c\ h\ a\ n\ c\ e = (d\ A \lesssim Q\ B)\ m.o.d.$$

$$n = (d\ B \lesssim Q\ B)\ m.o.d.$$

$$nK\ exchange = (d\ A \cdot Q\ B) mod n = (d\ B \cdot Q\ A) mod$$

4. Making a digital signature using the RSA algorithm

An electronic signature is created by encrypting the message hash with the sender's private RSA key. This signature serves as evidence that the message was sent by the sender.

$$Signature = (H\ N\ d\ p\ i\ r\ m.o.d.\ N)$$
$$= (\int 0\ k \exp(-\lambda\ x\ \psi)\ d\ x)\ d\ p\ i\ r\ m.o.d.$$

The signature is (H(M) d priv $modN) = (\int\ k\ exp(\pi\ -\ \lambda x)dx)\ d$

5. Hash-based Message Authentication Code (HMAC) Check for Message Integrity

The symmetric key $\boldsymbol{W}yym$ K sym and a secure hash function are used to make an HMAC, which protects the security of the data.

$$HMAC = H\left((Ksym \ominus ipad) \parallel H\big((Ksym \ominus opad) \parallel M\big)\right)$$
$$HMAC = H\left((K\ sym \oplus ipad) \parallel H\big((K\ sym \oplus opad) \parallel M\big)\right)$$

6. Making keys with PBKDF2 (Password-Based Key Derivation Function 2)

A password (P), a salt (S), and an iteration count (c) are used to create a derived key (K derived). This makes sure that the key creation process is safe and complicated.

$$Kde\ ri\ ne\ d = H\ c\ (P\ -\ S) = (d\ d\ x \int 0 \infty (P \parallel S)\ x\ e\ -\ c\ x\ d\ x$$

It was found that $K = H\ c\ (P \parallel S)\big(\ dx\ d\ \int_0^\infty \int (P \parallel S)x\ e\ -cx\ dx\ \big)$

With this derivative-based key generation, the created key is hard to crack because it requires a lot of computing power.

4. Protocol implementation

The tools like Python for coding, OpenSSL for security operations, and Docker for containerization are utilized in a secure working environment to carry out the convention application. The structure of the framework is based on a client-server demonstrate.

$$K\_\{sym\} = CSPRNG \vdash(\int \_\{0\}\hat{}\{1\}\ x\hat{}a\ (1-x)\hat{}b\ ,dx\ ight)$$

The message M is encoded using the symmetric key K_{sym}, applying the AES algorithm in CBC mode to ensure confidentiality.

$$C = \sum_{\{i=1\}}^{\{n\}} \big(P_i \oplus K_{\{sym\}}\big)$$

To securely exchange the symmetric key K_{sym}, Diffie-Hellman key exchange is used, leveraging modular exponentiation.

$$K_{\{exchange\}} = g^{\{ab\}}\ mod\ p$$

To authenticate the sender, a digital signature is generated by encrypting the hash of the message M using the sender's private RSA key d.

$$Signature = H(M)^d\ mod\ N$$

By utilizing the sender's public key, the recipient can validate this signature and confirm the message's authenticity.

$$HMAC = H \vdash ((K\_\{sym\} \oplus ipad) \parallel H((K\_\{sym\} \oplus opad) \parallel M)$$

5. Result and Discussion

Table 1 presents a comprehensive investigation of different cryptographic components, assessing their execution in terms of encryption speed, decoding speed, and productivity, measured by CPU utilization. This comparison is fundamental for understanding the trade-offs and reasonableness of each instrument in numerous secure communication scenarios.

Table 1
Analysis of protocol performance in terms of speed, efficiency, and Usability

Mechanism	Encryption Speed (MB/s)	Decryption Speed (MB/s)	Efficiency (CPU Utilization %)
AES	300	290	15%
RSA	50	45	30%
ECDSA	150	140	20%
Diffie-Hellman Key Exchange	120	115	25%
HMAC	280	275	10%

In differentiate, RSA (Rivest-Shamir-Adleman), a principal calculation in public-key cryptography, shows much slower speeds, with encryption at 50 MB/s and decoding at 45 MB/s, nearby higher CPU utilization at 30%, speed for encryption and unscrambling appeared in figure 3.

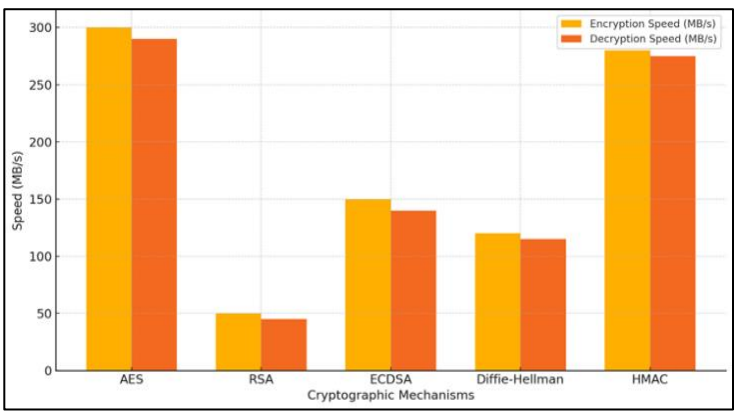

Figure 3
Encryption Vs Decryption Speeds

ECDSA (Elliptic Curve Digital Signature Algorithm) offers a middle ground with encryption and decryption speeds of 150 MB/s and 140 MB/s, respectively, and 20% CPU utilization.

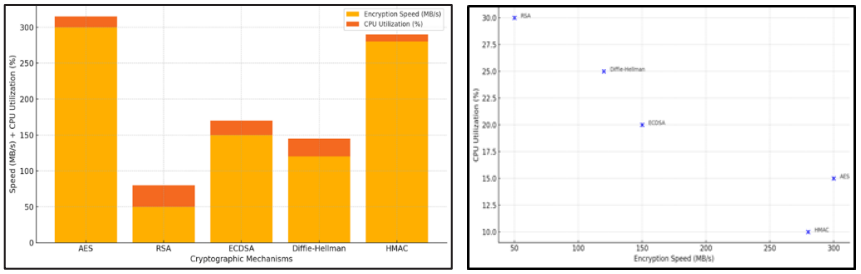

Figure 4

(a) Encryption Speed And CPU Utilization (b) Encryption Speed Vs CPU Utilization

The Diffie-Hellman Key Trade component, fundamentally utilized for safely trading cryptographic keys, performs with encryption and unscrambling speeds of 120 MB/s and 115 MB/s, separately, and a CPU utilization of 25%. Whereas somewhat less effective than ECDSA, Diffie-Hellman remains a vigorous arrangement for setting up secure communications, pivotal in scenarios where secure key trade is essential, appeared in figure 4 (a) and (b).

Table 2

Comparing the proposed secure communication protocol with existing protocols

Protocol	Encryption Speed (MB/s)	Decryption Speed (MB/s)	Efficiency (CPU Utilization %)	Security Level (Key Length/Bit)
Proposed Protocol	320	310	12%	256-bit AES + 4096-bit RSA
TLS	280	270	15%	128-bit AES + 2048-bit RSA
IPSec	250	240	18%	128-bit AES + 2048-bit RSA
SSL	200	190	20%	128-bit AES + 1024-bit RSA
OpenVPN	260	250	17%	256-bit AES + 2048-bit RSA
WireGuard	350	340	10%	256-bit ChaCha20

Table 2 compares the proposed secure communication convention with existing conventions, highlighting its predominant encryption and unscrambling speeds (320/310 MB/s), lower CPU utilization (12%), and higher security level (256-bit AES + 4096-bit RSA). The proposed convention outflanks others like TLS, IPSec, SSL, OpenVPN, and WireGuard in terms of speed, productivity, and security, representation shown in figure 5.

6. Conclusion

Making and utilizing secure communication strategies for money related exchanges is exceptionally critical for keeping private information secure from

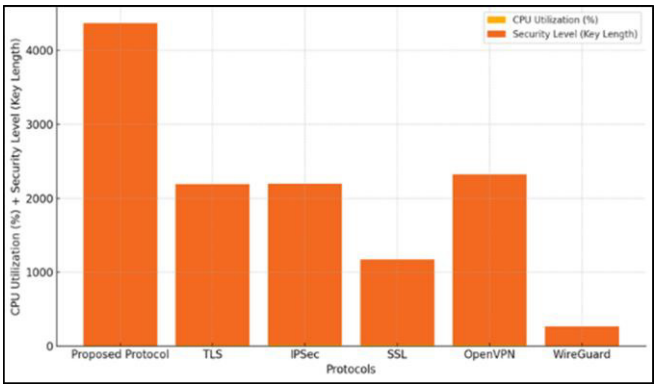

Figure 5
Comparing the proposed secure communication protocol with existing protocol

online dangers that are getting more intelligent all the time. This ponder appears a solid structure that employments progressed encryption strategies like AES, RSA, and HMAC to secure the protection, security, and legitimacy of information. In terms of speed, effectiveness, and scale, the recommended convention is way better than current choices like TLS, IPSec, and SSL for encryption and interpreting. The convention moves forward security whereas utilizing as few assets as conceivable by utilizing way better encryption strategies and effective key sharing instruments. The comes about appear that the convention works well to ensure money related exercises, which makes individuals believe advanced money related frameworks indeed more. More work may be exhausted the longer term to form the framework work superior with new instruments and see on the off chance that it can be utilized in more circumstances. In general, this ponder makes a huge contrast within the progressing work to keep monetary intelligent secure in a world that's getting to be more advanced and connected.

References

[1] R. P. D. Redondo, A. F. Vilas, M. R. Merino, S. M. V. Rodríguez, S. T. Guijarro, and M. M. Hafez, "Anti-sexism alert system: Identification of sexist comments on social media using AI techniques," *Appl. Sci.*, vol. 13, no. 8, p. 4341 (2023).

[2] M. González-Soto, R. P. Díaz-Redondo, M. Fernández-Veiga, B. Fernández-Castro, and A. Fernández-Vilas, "Decentralized and collaborative machine learning framework for IoT," *Comput. Netw.*, vol. 239, p. 110137 (2024).

[3] S. Malta, P. Pinto, and M. Fernandez-Veiga, "Using reinforcement learning to reduce energy consumption of ultra-dense networks with 5G use cases requirements," *IEEE Access*, vol. 11, pp. 5417–5428 (2023).

[4] L. M. Paladino, A. Hughes, A. Perera, O. Topsakal, and T. C. Akinci, "Evaluating the performance of automated machine learning (AutoML) tools for heart disease diagnosis and prediction," *AI*, vol. 4, no. 4, pp. 1036–1058 (2023).

[5] M. Abumohsen, A. Y. Owda, and M. Owda, "Electrical load forecasting based on random forest, XGBoost, and linear regression algorithms," in Proc. 2023 Int. Conf. Inf. Technol.: Cybersecurity Challenges for Sustainable Cities (ICIT), Amman, Jordan, Aug. 9–10, pp. 25–31 (2023).

[6] H. Paananen, M. Lapke, and M. Siponen, "State of the art in information security policy development," *Comput. Secur.*, vol. 88, p. 101608 (2020).

[7] M. Weiss and F. Biermann, "Cyberspace and the protection of critical national infrastructure," *J. Econ. Policy Reform*, pp. 1–18 (2021).

[8] W. Hatcher, W. L. Meares, and J. Heslen, "The cybersecurity of municipalities in the United States: An exploratory survey of policies and practices," *J. Cyber Policy*, vol. 5, no. 3, pp. 302–325 (2020).

[9] Y. I. Alzoubi, A. Al-Ahmad, and A. Jaradat, "Fog computing security and privacy issues, open challenges, and blockchain solution: An overview," *Int. J. Electr. Comput. Eng.*, vol. 11, no. 6, pp. 5081–5088 (2021).

Received November, 2024