International Journal of Advance Scientific Research
(ISSN – 2750-1396)
VOLUME 06 ISSUE 05 Pages: 31-35
OCLC – 1368736135

Journal Website: http://sciencebring.com/index.php/ijasr

Research Article

A Hybrid Cryptography-Based Secure Data Exchange Algorithm for Blockchain-Enabled IoT Systems

Submission Date: March 26, 2026, **Accepted Date:** April 22, 2026,
Published Date: May 11, 2026
Crossref doi: https://doi.org/10.37547/ijasr-06-05-04

Seidullayev M.K.
Tashkent University of Information Technologies named after Muhammad al-Khwarizmi, Uzbekistan

Abstract

The rapid development of Internet of Things (IoT) technologies has significantly increased the demand for secure and efficient communication mechanisms. However, traditional security approaches are often unsuitable for IoT environments due to limited computational resources and vulnerability to various cyberattacks. This paper proposes a secure data exchange algorithm based on blockchain technology and hybrid cryptography. The proposed method integrates an enhanced elliptic curve-based digital signature algorithm (EECHERI) with symmetric encryption (AES-192) to ensure authentication, confidentiality, and integrity. A cluster-based architecture is adopted to improve scalability and efficiency, while a dynamic session key generation mechanism enhances security. The communication protocol is designed in seven sequential steps, ensuring secure device-to-device interaction. The proposed approach provides strong resistance against spoofing, replay, and unauthorized access attacks while maintaining low computational overhead, making it suitable for real-world IoT applications.

Keywords

Network security, Intrusion Detection Systems (IDS), anomaly detection, signature-based analysis, artificial intelligence, network monitoring, XDR.

International Journal of Advance Scientific Research
(ISSN – 2750-1396)
VOLUME 06 ISSUE 05 Pages: 31-35
OCLC – 1368736135

ISSN-2750-1396

INTRODUCTION

The Internet of Things (IoT) has emerged as a transformative technology, enabling seamless communication between devices across various domains such as healthcare, smart cities, and industrial automation. Despite its advantages, IoT systems face significant security challenges due to their distributed nature and resource constraints.

One of the most critical aspects of IoT security is ensuring secure data exchange between devices. Traditional cryptographic approaches, while effective in conventional systems, are often too resource-intensive for IoT devices. Moreover, identity-based authentication alone is insufficient, as it can be compromised through spoofing or replay attacks.

Blockchain technology has recently been introduced as a promising solution due to its decentralized and tamper-resistant properties. However, blockchain alone does not fully address communication security between devices. Therefore, a hybrid approach that combines blockchain with efficient cryptographic techniques is required.

This paper proposes a secure data exchange algorithm that integrates:

- Elliptic Curve Cryptography (ECC) for authentication,
- AES-based symmetric encryption for efficient communication,
- Blockchain for secure and immutable record-keeping.

2. Background and Related Concepts

2.1 Elliptic Curve-Based Digital Signature (EECHERI)

The proposed system utilizes an enhanced elliptic curve-based digital signature algorithm (EECHERI), which is derived from the traditional Digital Signature Algorithm (DSA). EECHERI is specifically designed for environments with limited computational resources, such as IoT networks.

In this approach, when a device M_isends a message to another device M_j, it first signs the message using its private key. The receiver verifies the signature using the sender's public key. This process ensures:

- Authentication of the sender,
- Integrity of the transmitted data.

The use of elliptic curve cryptography provides high security with smaller key sizes, making it suitable for IoT applications.

2.2 AES-Based Symmetric Encryption

To ensure data confidentiality, the system employs the Advanced Encryption Standard (AES). AES is a widely used symmetric encryption algorithm that supports key sizes of 128, 192, and 256 bits.

In this work, AES-192 is selected due to its balance between security and computational efficiency. Communication between cluster members is encrypted using this algorithm, ensuring that data remains protected from external threats.

2.3 Hybrid Cryptographic Model

International Journal of Advance Scientific Research
(ISSN – 2750-1396)
VOLUME 06 ISSUE 05 Pages: 31-35
OCLC – 1368736135

The proposed system adopts a hybrid cryptographic approach, combining:

- Asymmetric cryptography (EECHERI) for authentication and key exchange,
- Symmetric cryptography (AES) for data encryption.

This combination leverages the strengths of both methods, providing strong security while maintaining efficiency.

3. Proposed Secure Data Exchange Algorithm

The proposed communication protocol consists of seven steps that ensure secure interaction between IoT devices within a cluster-based architecture.

Step 1: Request Generation

A device M_i initiates communication by sending a request:

$$Req[M_i \parallel T_i]$$

to device M_j, where T_i is the timestamp.

Step 2: Request Validation

Device M_j verifies the timestamp:

$$\Delta T_1 \geq T_i^* - T_i$$

If valid, the request is forwarded to the cluster head in encrypted form:

$$Req[E(TB_{pub}(M_i \parallel M_j \parallel T_i \parallel T_j))]$$

Step 3: Authentication and Key Generation

The cluster head:

- Verifies both devices,
- Generates a one-time session key S_k,
- Sends encrypted responses to both devices.

Step 4: Session Key Retrieval

Device M_i decrypts the response and extracts:

$$S_k = A \oplus M_i$$

The session key is stored for further communication.

Step 5: Communication Confirmation

Device M_j sends:

$$Res[T_i \parallel T_j]$$

confirming readiness.

Step 6: Secure Message Transmission

Device M_i encrypts and sends:

$$E(S_k(\text{Message}_1))$$

Step 7: Response Communication

Device M_j decrypts, processes, and responds:

$$E(S_k(\text{Message}_2))$$

This establishes secure bidirectional communication.

4. One-Time Secret Key Generation

A dynamic key generation algorithm is used to enhance security.

Algorithm 3:

- Generate random numbers Q_n and R_n,
- If both are prime:

$$N = (Q_n - 1)(R_n - 1)$$

Compute:

$$E = randomNumber \bmod 1000$$

Generate:

$$S_k = N^E$$

This ensures that each session uses a unique key.

5. Security Analysis

The proposed method provides protection against:

- **Replay attacks** → prevented by timestamps,
- **Spoofing attacks** → mitigated by digital signatures,
- **Unauthorized access** → controlled by cluster head verification,

International Journal of Advance Scientific Research
(ISSN – 2750-1396)
VOLUME 06 ISSUE 05 Pages: 31-35
OCLC – 1368736135

ISSN-2750-1396

- **Data tampering** → prevented using encryption and blockchain.

The integration of hybrid cryptography and blockchain significantly enhances overall system security.

Conclusion

This paper presented a hybrid cryptography-based secure data exchange algorithm for blockchain-enabled IoT systems. By combining EECHERI, AES-192, and dynamic key generation, the proposed method achieves a high level of security while maintaining efficiency.

The structured communication protocol ensures reliable device interaction, while blockchain provides a secure and immutable record of transactions. The proposed approach is suitable for real-world IoT applications and can be extended further in future research.

References

1. Whitfield Diffie and Martin Hellman, "New Directions in Cryptography," IEEE Transactions on Information Theory, vol. 22, no. 6, pp. 644–654, 1976.
2. Victor S. Miller, "Use of Elliptic Curves in Cryptography," Advances in Cryptology (CRYPTO'85), Springer, 1986.
3. Neal Koblitz, "Elliptic Curve Cryptosystems," Mathematics of Computation, vol. 48, no. 177, pp. 203–209, 1987.
4. NIST, "Digital Signature Standard (DSS)," FIPS PUB 186-4, 2013.
5. NIST, "Advanced Encryption Standard (AES)," FIPS PUB 197, 2001.
6. Satoshi Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System," 2008.
7. Vitalik Buterin, "A Next-Generation Smart Contract and Decentralized Application Platform," 2014.
8. Dorri, A., Kanhere, S. S., and Jurdak, R., "Blockchain in Internet of Things: Challenges and Solutions," IEEE Communications Surveys & Tutorials, vol. 19, no. 3, pp. 200–234, 2017.
9. Christidis, K., and Devetsikiotis, M., "Blockchains and Smart Contracts for the Internet of Things," IEEE Access, vol. 4, pp. 2292–2303, 2016.
10. Alaba, F. A., Othman, M., Hashem, I. A. T., and Alotaibi, F., "Internet of Things Security: A Survey," Journal of Network and Computer Applications, vol. 88, pp. 10–28, 2017.
11. Hankerson, D., Vanstone, S., and Menezes, A., Guide to Elliptic Curve Cryptography, Springer, 2004.
12. Dobraunig, C., Eichlseder, M., and Mendel, F., "Ascon v1.2: Lightweight Authenticated Encryption," 2016.
13. Singh, S., Sharma, P. K., Moon, S. Y., and Park, J. H., "Advanced Lightweight Encryption Techniques for IoT," Future Generation Computer Systems, vol. 49, pp. 1–14, 2019.
14. Zhang, Y., Kasahara, S., Shen, Y., Jiang, X., and Wan, J., "Smart Contract-Based Access Control for IoT," IEEE Internet of Things Journal, vol. 6, no. 2, pp. 1594–1605, 2019.
15. Xu, X., Weber, I., and Staples, M., Architecture for Blockchain Applications, Springer, 2019.
16. Roman, R., Zhou, J., and Lopez, J., "On the Features and Challenges of Security in IoT," Computer Networks, vol. 57, no. 10, pp. 2266–2279, 2013.
17. Sicari, S., Rizzardi, A., Grieco, L. A., and Coen-Porisini, A., "Security, Privacy and Trust in IoT," Computer Networks, vol. 76, pp. 146–164, 2015.

International Journal of Advance Scientific Research
(ISSN – 2750-1396)
VOLUME 06 ISSUE 05 Pages: 31-35
OCLC – 1368736135

18. Biryukov, A., Dinu, D., and Khovratovich, D., "Argon2: The Memory-Hard Function for Password Hashing," 2016.
19. Internet of Things xavfsizligi va blokcheyn integratsiyasi bo'yicha zamonaviy ilmiy sharhlar, Springer, 2025.
20. Blockchain Technology asosida IoT tizimlarida xavfsiz ma'lumot almashish usullari bo'yicha tadqiqotlar, IEEE, 2024.