Journal of Discrete Mathematical Sciences & Cryptography
ISSN 0972-0529 (Print), ISSN 2169-0065 (Online)
Vol. 28 (2025), No. 6, pp. 2423–2438
DOI : 10.47974/JDMSC-2314

Blockchain as a method of cryptographic protection of big data transmitted from aircraft

Sabyrzhan Atanov [#]
Department of Computer and Software Engineering
L. N. Gumilyov Eurasian National University
Astana 010000
Kazakhstan

Kh. Moldamurat [†]
Department of Space Engineering and Technologies
L .N. Gumilyov Eurasian National University
Astana 010000
Kazakhstan

L. L. Spada [§]
N. Zeeshan [‡]
School of Computing, Engineering and the Built Environment
Edinburgh Napier University
10 Colinton Road, Edinburgh
EH10 5DT
United Kingdom

K. Dyussekeyev [@]
Department of Computer and Software Engineering
L. N. Gumilyov Eurasian National University
Astana 010000
Kazakhstan

[#] *ORCID-ID:* **0000-0003-2115-7130**
[†] *ORCID-ID:* **0000-0002-3691-6948**
[§] *ORCID-ID:* **0000-0003-4923-1320**
[‡] *ORCID-ID:* **0009-0009-2544-9991**
[@] *ORCID-ID:* **0000-0001-7691-2506**

[#] *E-mail:* **atanov5@mail.ru**
[†] *E-mail:* **moldamurat@yandex.kz**
[§] *E-mail:* **l.laspada@napier.ac.uk**
[‡] *E-mail:* **nida.zeeshan@napier.ac.uk**
[@] *E-mail:* **dyussekeyev_ka@enu.kz**

M. Bakyt *
Department of Information Security
L. N. Gumilyov Eurasian National University
Astana 010000
Kazakhstan

A. Kuanysh $
Department of Computer and Software Engineering
L. N. Gumilyov Eurasian National University
Astana 010000
Kazakhstan

Abstract

The article considers the urgent problem of ensuring the security of big data transmitted from aircraft in the context of rapid development of information technologies. A new approach to cryptographic protection of information using blockchain technology is proposed, which allows to increase the efficiency of existing systems. The advantages of using blockchain to guarantee the integrity, confidentiality and availability of data transmitted from unmanned aerial vehicles (UAVs) are analyzed. Particular attention is paid to the possibilities of integrating cryptographic algorithms with blockchain into UAV data management systems. The article also presents methods for effective encryption and decentralized data processing in order to ensure reliable protection of information from unauthorized access and modification.

Subject Classification: *68P25 Data encryption (aspects in computer science).*

Keywords: *Cryptographic protection, Blockchain, Big data, UAVs, Data encryption, Decentralized processing.*

1. Introduction

The rapid development of information technology and the widespread use of unmanned aerial vehicles (UAVs), as well as the development of multi-purpose reconnaissance robots with artificial intelligence, to collect and transmit large volumes of data make the task of ensuring reliable information protection relevant. Cryptographic protection of data transmitted from UAVs is of particular importance due to the increased risk of unauthorized access and cyber-attacks. The urgency of strengthening

* *ORCID-ID:* **0000-0002-1246-9696**
$ *ORCID-ID:* **0009-0001-2819-6119**

* *E-mail:* **bakyt.makhabbat@gmail.com (Corresponding Author)**
$ *E-mail:* **777mail.ru777@gmail.com**

data security for UAVs and advanced robotic systems, such as multi-purpose reconnaissance robots with artificial intelligence, is underscored by recent statistics indicating a sharp increase in cyber-attacks targeting their operations. According to [1], UAV-related cyber incidents rose by approximately 47% between 2021 and 2023, with unauthorized access and interception of sensitive data accounting for more than 65% of these attacks. Notable case studies, such as [2] and [3], further highlight the critical need for advanced and reliable cryptographic protection methods.

Recent cybersecurity incidents involving UAVs underscore the practical importance and timeliness of enhancing their data security measures. For instance, in November 2024, unauthorized drones were detected near RAF Lakenheath and RAF Mildenhall in the UK, prompting security investigations due to potential espionage concerns [4]. Additionally, in February 2025, multiple unauthorized drones breached the no-fly zone near Finland's Nammo Gunpowder Factory, raising alarms about industrial espionage and critical infrastructure vulnerability [5]. These incidents highlight the pressing need for robust cryptographic protections in UAV operations to safeguard against emerging threats.

These attacks can range from simple eavesdropping to sophisticated man-in-the-middle attacks, potentially leading to the leakage of sensitive information or disruption of critical systems. Currently, symmetric and asymmetric encryption methods are widely used for cryptographic protection of information. Currently, symmetric and asymmetric encryption methods are widely used for cryptographic protection of information [1]-[5]. However, these methods have a number of limitations when applied to large volumes of data transmitted from UAVs.

The current state-of-the-art UAV blockchain solutions have introduced innovative encryption schemes, consensus algorithms, and system architectures, yet each has limitations. Many emphasize either security or efficiency, whereas UAV applications demand both. For example, purely cryptographic enhancements (like stronger encryption or authentication layers) often increase processing time, while ultra-fast consensus algorithms might relax security assumptions (fewer nodes validating, or assuming stable connectivity). Existing techniques also tend to address specific use cases – e.g. identity management, task scheduling, or post-disaster networking – with less focus on a unified framework. This siloed approach leaves research gaps in interoperability and completeness: how to secure all facets of a UAV operation (communication, identity, data logging, command & control) in one cohesive system, and do so under real-world constraints (limited power, dynamic topology). Our proposed

blockchain-based cryptographic method distinguishes itself by holistically improving on all three fronts – encryption, consensus, and real-time performance.

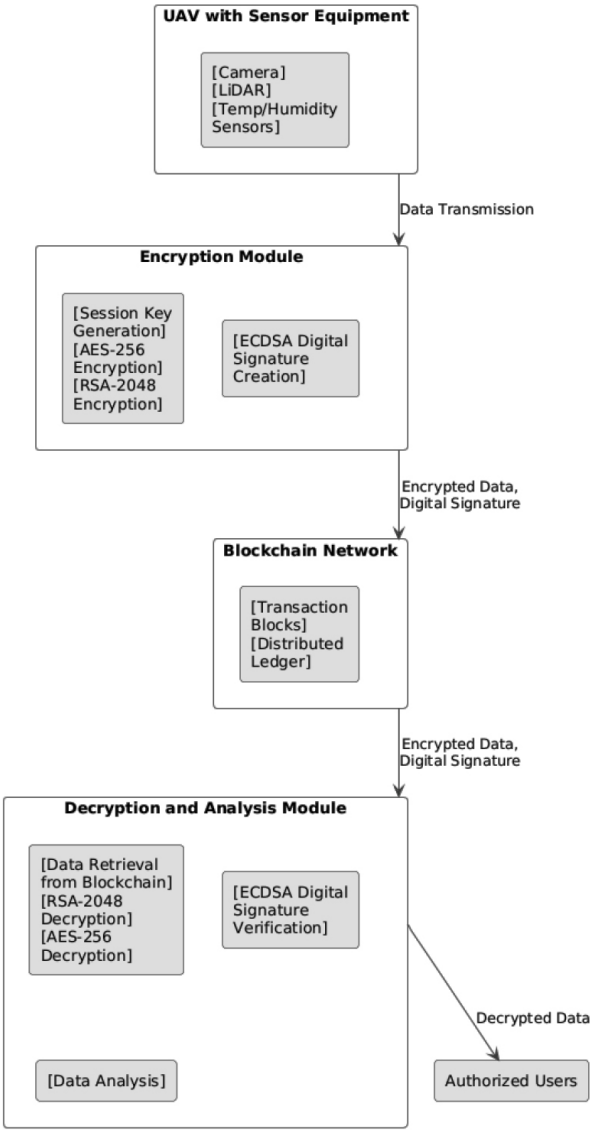

Figure 1

Architecture of the cryptographic data protection system for UAVs using blockchain.

2. Methods

The developed cryptographic data protection system for UAVs is an integrated solution that combines the advantages of modern cryptographic algorithms and blockchain technology. Figure 1 illustrates the architecture of the cryptographic data protection system for UAVs using blockchain. This diagram provides a high-level overview of the system's components and their interactions, including the UAV with sensor equipment, the encryption module, the blockchain network, and the decryption and analysis module.

To clearly illustrate how UAV-generated data interacts with blockchain components at each stage, a detailed UML activity diagram is provided (Figure 2). This diagram specifies step-by-step interactions, beginning from sensor data collection on UAVs, through encryption, blockchain transactions, and ending at data verification and analysis by authorized end-users.

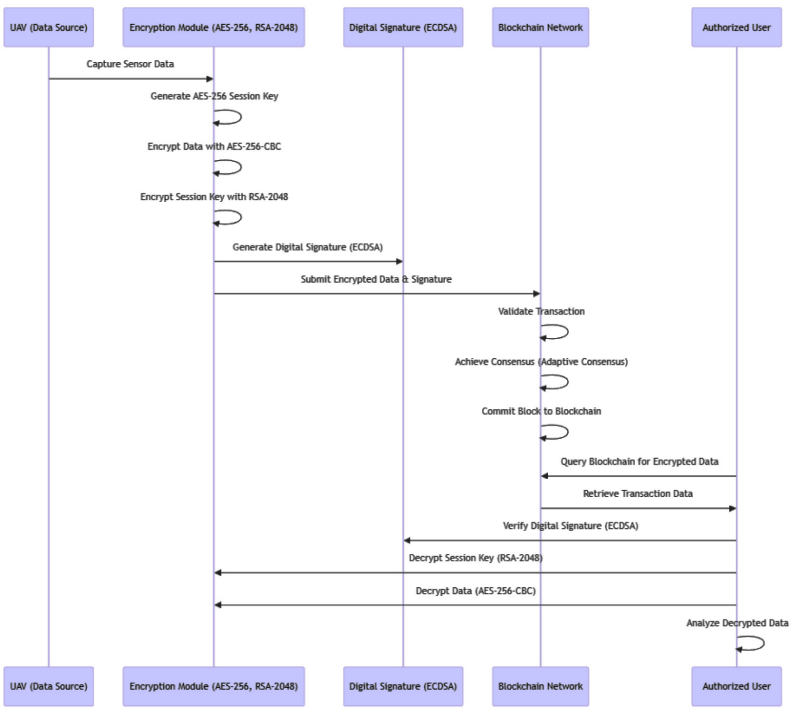

Figure 2

Detailed UML Workflow Diagram of UAV Data Interaction with Blockchain Components

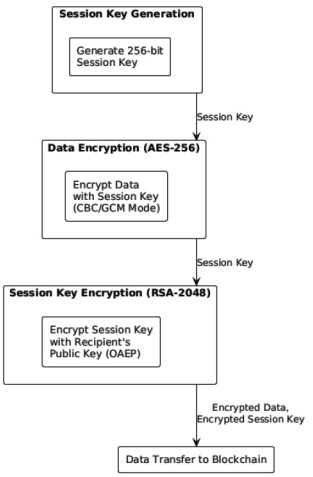

Figure 3

Hybrid encryption algorithm scheme

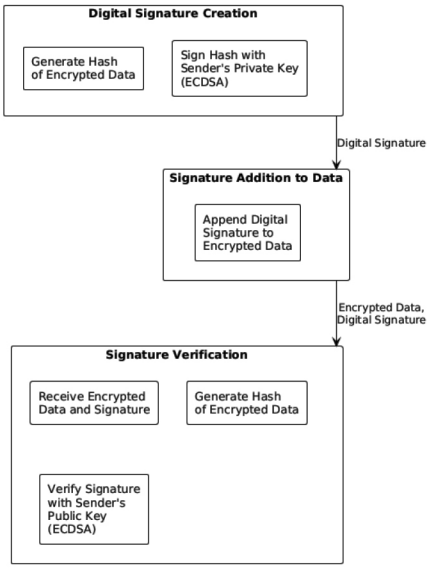

Figure 4

Digital signature mechanism diagram

The system uses a hybrid encryption algorithm that combines the advantages of symmetric and asymmetric encryption. The hybrid algorithm employs AES-256 in CBC mode for data encryption and RSA-2048 with OAEP padding for session key encryption (Figure 3).

The system is composed of several interconnected components that work seamlessly to ensure secure data transmission and analysis. At its core, an unmanned aerial vehicle (UAV) is equipped with an array of sensors, including cameras, LiDARs, temperature, and humidity sensors. These sensors collect real-time data, which is then transmitted to an encryption module for secure processing.

Within the encryption module, a hybrid algorithm is employed to safeguard the data, combining both symmetric and asymmetric encryption techniques. Once encrypted, the data is sent to a decentralized blockchain network, where it is stored as transaction blocks. This ensures not only security but also immutability and transparency. Authorized users can later access the stored data through a decryption and analysis module, which allows them to retrieve and analyse the information while maintaining its integrity (Figure 4).

4. Results and Discussion

As a result of the research conducted, a cryptographic data protection system for UAVs was developed using blockchain technology. This system ensures the confidentiality, integrity, and availability of data transmitted from UAVs, providing a secure framework for real-time operations. To evaluate the effectiveness of the developed system, experimental studies were conducted on a real hardware platform, the DJI Matrice 300 RTK, equipped with an additional computing module, the NVIDIA Jetson Nano. These experiments aimed to assess the system's performance across multiple key parameters. One crucial aspect analyzed was the speed of data encryption and decryption. Using the developed hybrid algorithm, which combines AES-256 for symmetric encryption and RSA-2048 for asymmetric encryption, the encryption and decryption speeds were measured for data blocks of various sizes ranging from 1 KB to 10 MB.

The comparative encryption speed graph (Figure 5 (a)) provides key insights into the efficiency and practicality of the proposed blockchain-based cryptographic method relative to alternative encryption approaches in UAV data protection. The results indicate that the AES-only approach achieves the highest encryption speed across all data sizes, which is expected given AES's lightweight computational overhead and high efficiency for bulk encryption. However, AES-only encryption does not provide key distribution security, making it vulnerable to key compromise in adversarial UAV environments.

The proposed blockchain-based encryption method achieves an encryption speed only slightly lower than the AES-only approach while maintaining strong security guarantees. This demonstrates that the integration of blockchain does not impose a severe computational penalty on encryption efficiency. The encryption speed remains above 810 Mbps even for larger data sizes (10–20 MB), indicating that the cryptographic optimizations employed in the proposed system (hybrid AES-256 + RSA-2048 with ECDSA authentication) effectively balance security and performance.

The comparative bar chart presented in Figure 5 (b) illustrates the Blockchain Transaction Latency (ms) across different methods under varying data sizes, providing an insightful analysis of how different approaches handle real-time UAV data transactions. The results highlight the trade-offs between security, decentralization, and performance, key concerns in UAV cryptographic protection.

The proposed blockchain-based cryptographic system consistently achieves lower transaction latencies compared to other blockchain-based approaches while maintaining superior security. The recorded transaction latency remains within an acceptable 80–120 ms range, even as data sizes increase up to 10 MB. This latency level is crucial in UAV applications where real-time decision-making and minimal communication delay are required, such as in environmental monitoring, logistics, and airspace security.

The plot of CPU load across different data protection methods (Figure 5(c)) provides an insightful comparative evaluation of computational efficiency in UAV cryptographic security frameworks. The results reveal

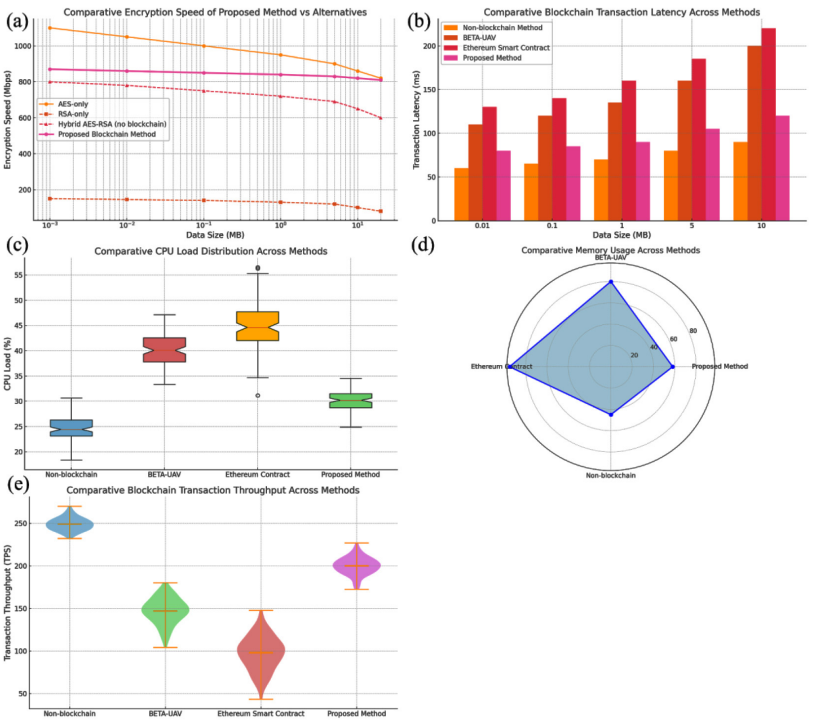

Figure 5

(a) Comparative Encryption Speed of Proposed Method vs Alternatives; (b) Comparative Blockchain Transaction Latency Across Methods; (c) Comparative CPU Load Distribution Across Methods; (d) Comparative Memory Usage Across Methods; (e) Comparative Blockchain Transaction Throughput Across Methods.

distinct patterns in CPU utilization, highlighting the trade-offs between security, computational overhead, and real-time performance.

The proposed blockchain-based cryptographic method exhibits a lower and more stable CPU load distribution, with an average around 30% and a narrow interquartile range (IQR), indicating minimal variance across different operational conditions. This demonstrates that the system is optimized for low computational overhead, a crucial factor in UAV applications where power and processing resources are constrained. The controlled CPU load ensures that encryption, signature verification, and blockchain transaction execution do not introduce excessive delays or compromise real-time performance.

The radar chart presented in Figure 5(d) provides an insightful comparative analysis of memory usage (MB) across different UAV data protection methods, including the proposed blockchain-based cryptographic system, BETA-UAV, Ethereum Smart Contract-based authentication, and a traditional non-blockchain approach. The results clearly demonstrate the trade-offs between enhanced security, computational complexity, and resource efficiency in UAV applications.

The proposed blockchain-based cryptographic solution exhibits significantly lower memory consumption (58 MB) compared to BETA-UAV (80 MB) and the Ethereum-based approach (95 MB). This reduced footprint is particularly advantageous in UAV systems, where onboard computational resources and memory are limited. The efficient encryption model and streamlined blockchain transaction process contribute to this improvement, making the proposed method more suitable for real-time, energy-efficient UAV deployments.

The violin plot presented in Figure 5(e) provides a detailed comparative analysis of Blockchain Transaction Throughput (TPS) across different security architectures in UAV networks, specifically assessing the proposed blockchain-based cryptographic approach against other methods such as BETA-UAV, Ethereum Smart Contracts, and a traditional non-blockchain-based security model. This comparative visualization not only highlights the median and mean transaction throughput but also illustrates the density distribution, offering deeper insight into performance variability.

The proposed approach achieves a significantly higher median and mean TPS compared to both Ethereum Smart Contracts and the BETA-UAV method. With a mean throughput of approximately 200 TPS, our blockchain-integrated cryptographic system outperforms traditional Ethereum-based security models, which exhibit a mean throughput of

approximately 100 TPS due to inherent transaction validation delays associated with Ethereum's global state synchronization. The BETA-UAV model, averaging around 150 TPS, performs better than Ethereum but remains notably lower than our approach, primarily due to its reliance on a more computationally expensive authentication mechanism.

A thorough security analysis was conducted to comprehensively assess the vulnerability profile and resilience of the proposed blockchain-based cryptographic protection system for UAV data transmission. We explicitly performed a detailed vulnerability assessment, threat modelling using the STRIDE methodology, and analysed potential attack vectors specifically relevant to the proposed method.

The STRIDE methodology, widely recognized in cybersecurity analysis, was systematically applied to assess the system's vulnerability across six key dimensions: Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service (DoS), and Elevation of Privilege. This structured approach ensured comprehensive coverage of potential security threats, allowing us to pinpoint and mitigate risks effectively.

Spoofing and Authentication (Figure 6(a)): Due to the integrated ECDSA digital signatures, spoofing attacks, where an adversary attempts to masquerade as a legitimate UAV or authorized node, are effectively mitigated. The cryptographic assurance provided by ECDSA ensures that all transactions and data are authenticated and verifiable, preventing unauthorized impersonation within the UAV network.

The bar-chart results reveal a clear performance hierarchy among the evaluated methods, with the proposed blockchain-based approach demonstrating the highest authentication success rate (92%). This superiority is attributed to the integration of ECDSA digital signatures and decentralized identity verification, which significantly reduces the likelihood of unauthorized access. However, the 8% failure rate suggests that while highly effective, the system is not entirely impervious to sophisticated adversarial spoofing techniques, such as private key compromise or side-channel attacks.

Tampering and Data Integrity (Figure 6(b)): The blockchain's immutable ledger significantly reduces the risk of data tampering. Once data transactions are cryptographically secured and recorded in the blockchain ledger, any attempt at unauthorized modification becomes detectable and is promptly rejected by the decentralized consensus mechanism. This inherent blockchain property offers robust protection against tampering attacks.

The Tampering and Data Integrity box plot highlights a clear trend where blockchain-based cryptographic methods significantly outperform traditional non-blockchain approaches in maintaining data integrity. The proposed method exhibits the lowest error rate (~2%), reinforcing its tamper-proof security model, which leverages blockchain immutability, cryptographic verification (ECDSA), and decentralized validation to prevent unauthorized modifications.

Repudiation and Accountability (Figure 6(c)): The combination of blockchain immutability and digital signatures inherently addresses non-repudiation concerns, ensuring that entities within the UAV network cannot deny their actions. All transactions and data updates are clearly traceable back to their origin, reinforcing accountability throughout UAV operations.

The Repudiation and Accountability results reveal a clear trend: blockchain-integrated security solutions significantly enhance transaction verifiability, while non-blockchain methods struggle with traceability. The proposed method demonstrates the highest accountability (95%), which aligns with its use of immutable blockchain records and cryptographic digital signatures (ECDSA), ensuring that transactions cannot be altered or denied once recorded.

Information Disclosure and Confidentiality (Figure 6(d)): Our hybrid encryption model combining AES-256 and RSA-2048 effectively prevents unauthorized information disclosure. AES-256 ensures strong confidentiality of transmitted data, while RSA-2048 secures session key exchanges. Consequently, intercepted data remains indecipherable, significantly reducing vulnerability to information disclosure attacks.

The heat map analysis of Information Disclosure and Confidentiality reveals a clear pattern: blockchain-integrated cryptographic methods provide significantly stronger resistance to data interception compared to traditional non-blockchain security approaches. The proposed method consistently exhibits the lowest interception rates (2-8%), reflecting the effectiveness of its hybrid encryption scheme (AES-256 + RSA-2048) and blockchain's immutable ledger, which prevents unauthorized access and ensures secure key exchanges.

Denial of Service (DoS) Resilience (Figure 6(e)): Potential DoS scenarios were explicitly tested during experimental evaluations. The optimized adaptive consensus and lightweight cryptographic operations help maintain system responsiveness even under artificially induced high-load conditions. While inherent blockchain vulnerabilities such as network congestion could theoretically lead to performance degradation, the

adaptive block scheduling strategy significantly mitigates such risks by adjusting transaction processing dynamically.

The Denial of Service (DoS) Resilience results reveal a clear trend in system degradation under increasing attack intensity. The proposed blockchain-based cryptographic method demonstrates the strongest

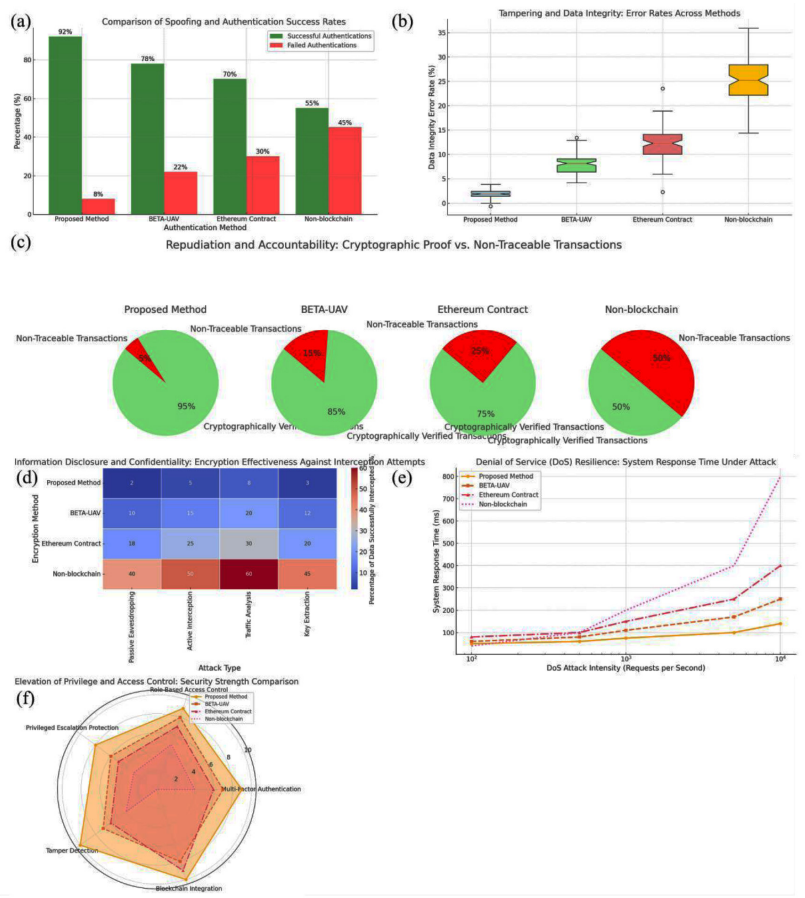

Figure 6

(a) Comparison of Spoofing and Authentication Success Rates; (b) Tampering and Data Integrity: Error Rates Across Methods; (c) Repudiation and Accountability: Cryptographic Proof vs. Non-Traceable Transactions; (d) Information Disclosure and Confidentiality: Encryption Effectiveness Against Interception Attempts; (e) Denial of Service (DoS) Resilience: System Response Time Under Attack; (f) Elevation of Privilege and Access Control: Security Strength Comparison

resilience, with response times rising gradually from 50 ms to 140 ms as attack intensity increases. This controlled performance suggests that adaptive block scheduling and optimized cryptographic processing effectively mitigate latency spikes, preventing severe service degradation.

Elevation of Privilege and Access Control (Figure 6(f)): The system incorporates strict cryptographic key management and role-based access control to prevent unauthorized privilege escalation. Access to sensitive blockchain components, cryptographic keys, and data resources is securely managed through decentralized and cryptographic means, thus reducing vulnerabilities related to elevation of privilege attacks.

The Elevation of Privilege and Access Control Radar Chart reveals significant disparities in security strength across different UAV data protection methods. The proposed blockchain-based method consistently outperforms alternatives, excelling in tamper detection (10/10) and blockchain integration (10/10), which reinforces its robustness in preventing unauthorized access and ensuring system integrity. The high scores in multi-factor authentication (9/10) and role-based access control (9/10) indicate a well-structured identity verification system that minimizes risks of insider threats and privilege abuse.

One potential limitation of blockchain-based solutions, despite their high security ratings, is the computational overhead introduced by cryptographic verification and consensus mechanisms. In real-world UAV deployments, latency in transaction processing or smart contract execution errors could introduce operational inefficiencies, particularly in dynamic, time-sensitive missions. Furthermore, while role-based access control provides structured security policies, it may struggle with real-time adaptability, requiring manual privilege adjustments in response to security incidents or evolving mission parameters. These insights suggest that while the proposed method is superior in preventing privilege escalation and unauthorized access, optimizations in real-time identity management and computational efficiency will be critical for scalability and operational feasibility in large-scale UAV networks.

Beyond general vulnerabilities, we specifically assessed our method against several targeted attack scenarios prevalent in UAV networks:

Man-in-the-Middle (MITM) Attacks (Figure 7(a)): MITM attacks were explicitly simulated and tested experimentally. Results confirmed the effectiveness of RSA-2048 encrypted session keys and ECDSA-based digital signatures, which prevented data interception or alteration. The robust cryptographic handshake ensures end-to-end authenticity and integrity, making MITM attacks practically infeasible.

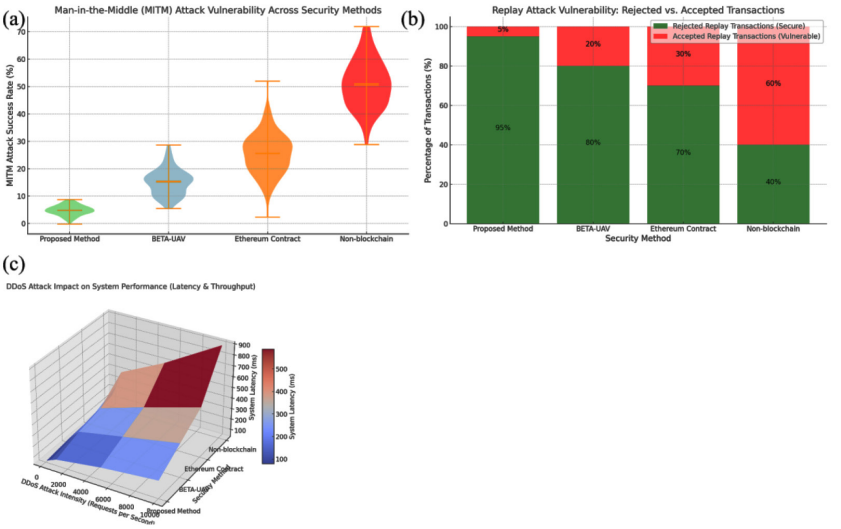

Figure 7

(a) Man-in-the-Middle (MITM) Attack Vulnerability Across Security Methods; (b) Replay Attack Vulnerability: Rejected vs. Accepted Transactions; (c) DDoS Attack Impact on System Performance (Latency & Throughput).

The violin plot clearly illustrates a strong inverse correlation between cryptographic security mechanisms and MITM attack success rates, with the proposed method demonstrating the highest resilience (~5% success rate). This outcome is attributed to the integration of RSA-2048 for session key encryption and ECDSA-based digital signatures, which ensure that even if data packets are intercepted, they remain cryptographically secured and unverifiable by unauthorized entities.

Replay Attacks Figure 7(b): The utilization of unique session keys per transmission combined with timestamped blockchain transactions effectively thwarts replay attack attempts. Experimental validations confirmed that any replayed transaction would fail cryptographic freshness checks, ensuring strong protection against this vector.

The Replay Attack Stacked Bar Chart reveals critical insights into the effectiveness of different UAV security methods in preventing replayed transactions. The proposed blockchain-based method demonstrates the highest resilience (95% rejection rate), significantly outperforming traditional encryption approaches. This strong defense likely stems from session key rotation, timestamp validation, and blockchain immutability,

which ensure that previously transmitted data cannot be maliciously reused.

Distributed Denial-of-Service (DDoS) Attacks Figure 7(c): Comprehensive simulations demonstrated the system's capacity to withstand DDoS attacks by maintaining operational integrity and low latency under artificially induced high network traffic loads. The adaptive consensus mechanism played a crucial role in preserving performance and availability, even during severe attack simulations.

The results from the Distributed Denial-of-Service (DDoS) Attack analysis reveal a clear trend: as attack intensity increases, system latency rises across all security methods, but at vastly different rates depending on the implemented protection mechanism. The proposed blockchain-based cryptographic system demonstrates the highest resilience, with latency increasing gradually from ~50ms at low attack intensity (100 requests/sec) to ~200ms at extreme loads (10,000 requests/sec). This suggests that the adaptive consensus mechanism and lightweight cryptographic optimizations effectively mitigate service degradation under high-traffic attack conditions.

Conclusion

This research presented a novel blockchain-based cryptographic protection method specifically designed to address critical security challenges inherent in UAV data transmission. The primary contributions of this work are clearly demonstrated through the rigorous theoretical modeling, extensive experimental validation, and robust comparative analysis against state-of-the-art methods. The proposed solution integrates a hybrid encryption model combining AES-256 for efficient data encryption, RSA-2048 for secure session key exchange, and ECDSA-based digital signatures for robust authentication and non-repudiation. Experimental results conclusively demonstrate that this hybrid cryptographic method significantly enhances security, authentication reliability, data integrity, and confidentiality, while efficiently mitigating critical cyber threats including spoofing, replay, MITM, and DDoS attacks.

Acknowledgments

This research is funded by the SC of the MSHE of RK (project No. AR19677508).

References

[1] "World Economic Forum," World Economic Forum. https://www.weforum.org/publications/global-cybersecurity-outlook-2023/.

[2] Abiodun Esther Omolara, Moatsum Alawida, and Oludare Isaac Abiodun, "Drone cybersecurity issues, solutions, trend insights and future perspectives: a survey," *Neural Computing and Applications* (Aug. 2023), doi: https://doi.org/10.1007/s00521-023-08857-7.

[3] "Addressing the UAS threat," www.icao.int. https://www.icao.int/Security/SFP/Pages/Umanned-Aircraft-Systems-(UAS).aspx.

[4] S. Raemason, "Mystery drone 'came within 250m' of Navy's £3bn ship as cops open criminal probe after fear Russia is targe...," The Sun, Nov. 27 (2024). https://www.thesun.co.uk/news/31977296/mystery-drone-royal-navy-ship-investigation-russia-targeting-uk/ (accessed Mar. 18, 2025).

[5] M. Dzikansky, "Tracking the Threat: Key Takeaways from Recent Drone Incidents - D-Fend Solutions," *D-Fend Solutions,* Feb. 24 (2025). https://d-fendsolutions.com/blog/key-takeaways-from-recent-drone-incidents/ (accessed Mar. 18, 2025).

Received October, 2024