© SEP 2026 | IRE Journals | Volume 10 Issue 3 | ISSN: 2456-8880
DOI: https://doi.org/10.64388/IREV10I3-1722956

# Anonymized: Advanced Privacy-Centric Data Security System Using Encryption and Identity Anonymization Methods

B.S. LIYA[1], SWATHI A S[2], SRIGANESHRAJA KANTHASAMY[3], SWEATHAA G[4], GOKULNAATH D[5]

[1,2,3,4,5]*Department of Computer Science and Engineering, Easwari Engineering College, Ramapuram, Chennai, Tamil Nadu, India*

***Abstract-*** ***In modern intelligence environments, secure exchange of sensitive information must address unauthorized disclosure, identity impersonation, insider misuse, data manipulation, and audit-log tampering simultaneously. This paper presents ANONYMIZED, a multi-layer privacy-centric framework integrating ASCON authenticated encryption, RSA-based session-key protection, Face++ biometric verification, data masking, redaction, SHA-256 hashing, and Ethereum smart-contract auditing. Sensitive intelligence files are encrypted with ASCON, while the corresponding symmetric key is protected using RSA. Before classified content is released, the requesting user undergoes role validation and biometric verification. Personally identifiable and operationally sensitive attributes are selectively masked, redacted, or hashed to reduce unnecessary disclosure. Security-relevant events and document hash values are recorded on Ethereum in a controlled Ganache environment to provide traceability and tamper resistance. The architecture is organized around Commander, Intelligence Officer, and Administrative modules and is designed to support confidentiality, integrity, authentication, privacy, non-repudiation, and controlled information exposure. The work provides an integrated defense-in-depth model and a qualitative security evaluation grounded in current privacy-preserving research***

***Index Terms - ASCON, RSA, privacy-preserving communication, data anonymization, biometric authentication, blockchain, Ethereum, SHA-256.***

## I. INTRODUCTION

The rapid digitization of intelligence, defense, governmental, and other security-sensitive environments has increased dependence on interconnected systems for exchanging mission reports, operational instructions, identities, location information, and classified files. Although digital communication improves speed and accessibility, it also creates attack surfaces for unauthorized disclosure, credential theft, identity impersonation, insider misuse, tampering, and manipulation of audit trails.

A major limitation of conventional security designs is that confidentiality, authentication, privacy preservation, and accountability are often treated as independent functions. Encryption can prevent an intercepted document from being read, but it cannot by itself prove that the person requesting the document is the legitimate user. Authentication can verify a user but does not automatically minimize disclosure of personally identifiable or mission-sensitive attributes. Likewise, a centralized log server can provide an audit trail while still remaining vulnerable to privileged alteration or deletion.

Privacy-preserving research increasingly emphasizes the need to balance protection with information utility and operational efficiency. Federated-learning studies demonstrate that retaining raw data locally improves privacy but does not completely prevent leakage from transmitted gradients or parameters [1]. Hybrid anonymization research shows that a single method may produce excessive information loss and that combining techniques can improve the privacy-utility balance [2]. Blockchain offers immutability and decentralized trust, yet its transparency creates a privacy challenge when sensitive data are recorded directly on-chain [3].

High-security communication therefore requires an architecture in which cryptographic protection, user

verification, data minimization, and tamper-resistant accountability operate together. The proposed system, ANONYMIZED, combines ASCON authenticated encryption for protected files, RSA for session-key protection, Face++ biometric verification, masking/redaction/SHA-256 anonymization, and Ethereum smart contracts for security-event logging.

The principal contribution is an integrated defense-indepth workflow rather than a new cryptographic primitive. Each mechanism is assigned a distinct responsibility and is positioned at a defined stage of the access path. The system is organized around Commander, Intelligence Officer, and Administrative modules and is designed for environments where sensitive information must remain confidential while access remains attributable, privacy-aware, and auditable.

## II. LITERATURE REVIEW

The secure exchange of sensitive information is essential in intelligence and defense operations, where unauthorized access, identity impersonation, insider threats, data leakage, and cyberattacks can cause serious consequences. Traditional security systems often rely on individual mechanisms such as encryption, password-based authentication, or centralized storage, which may not provide comprehensive protection against modern security threats..

### A. Lightweight Cryptography

Recent studies on lightweight cryptography have investigated the use of efficient authenticated encryption algorithms for protecting sensitive data in resource-constrained environments. ASCON has gained significant attention because it provides confidentiality and authentication with relatively low computational overhead. However, existing studies primarily focus on the cryptographic performance and security of ASCON rather than integrating it with identity verification, privacy preservation, and decentralized auditing.

### B. Biometric Authentication

Biometric authentication has been widely investigated as an effective mechanism for strengthening user identity verification. Facial recognition-based systems can provide convenient and reliable authentication compared with conventional password-based approaches. However, biometric systems considered independently mainly address identity verification and do not provide comprehensive protection for the sensitive data accessed after authentication.

### C. Privacy-Preserving Data Techniques

Data masking, redaction, and cryptographic hashing are commonly used to minimize exposure of personally identifiable and sensitive information. SHA-256 is particularly useful for integrity verification because modifications to the original data result in a different hash value. Nevertheless, existing privacy-preserving approaches generally focus on protecting individual data fields and do not combine anonymization with strong authentication, encryption, and decentralized auditing.

### D. Blockchain-Based Security

Blockchain technology and smart contracts have been explored for secure access control, immutable logging, and decentralized trust. Ethereum-based smart contracts can maintain tamper-resistant records of access events and verification activities. However, blockchain-based solutions may focus mainly on auditability and access management without integrating lightweight encryption, biometric authentication, and privacy-preserving techniques into a unified security architecture.

### E. Integrated Security Approaches

Recent research increasingly combines multiple security mechanisms to address complex cybersecurity requirements. Such approaches demonstrate that combining cryptography, authentication, privacy protection, and blockchain can provide stronger security than using individual mechanisms independently. However, there remains a gap in developing an integrated framework specifically designed for secure intelligence communication, where confidentiality, identity

verification, privacy, tamper detection, and decentralized auditing are required simultaneously.

F. Secure Intelligence Communication Frameworks

Existing secure communication frameworks for defense and intelligence applications focus on protecting sensitive information through encryption, authentication, and controlled access. These approaches demonstrate the importance of multi-layer security in preventing unauthorized disclosure and cyberattacks. However, many frameworks depend on centralized infrastructure or focus on only selected security mechanisms. Limited integration of lightweight authenticated encryption, biometric verification, privacy-preserving techniques, blockchain auditing, and decentralized storage remains a significant research opportunity.

G. Summary of Literature Review

The reviewed studies demonstrate that cryptography, biometric authentication, privacy-preserving techniques, and blockchain can individually improve data security. However, most existing approaches address these mechanisms separately and have limitations in providing comprehensive protection for intelligence communication. The identified research gap motivates the proposed framework, which integrates ASCON, RSA, Face++ authentication, data anonymization, SHA-256, Ethereum blockchain, and decentralized storage into a unified security architecture. This integration aims to provide stronger confidentiality, integrity, authentication, privacy, auditability, and controlled access for sensitive intelligence information.

## III. RESEARCH GAP

Existing research mainly addresses encryption, biometric authentication, privacy preservation, or blockchain as separate security mechanisms. Limited work integrates these techniques into a single intelligence communication framework. Therefore, this work proposes a unified architecture combining ASCON encryption, RSA-based key protection, Face++ biometric authentication, data anonymization, SHA-256 hashing, Ethereum blockchain, and decentralized storage to provide comprehensive protection for sensitive intelligence information.

© SEP 2026 | IRE Journals | Volume 10 Issue 3 | ISSN: 2456-8880
DOI: https://doi.org/10.64388/IREV10I3-1722956

| Ref. | Study / Approach | Main Technique / Focus | Key Limitations / Research Gap | How Our Work Addresses the Gap |
|---|---|---|---|---|
| A | Lightweight Cryptography [1]–[5] | Use of lightweight authenticated encryption algorithms such as ASCON for confidentiality and authentication. | Focuses mainly on cryptographic performance and security; does not integrate identity verification, privacy preservation, or decentralized auditing. | Integrates ASCON with RSA key protection, biometric authentication, privacy techniques, and blockchain auditing. |
| B | Biometric Authentication [6]–[10] | Facial recognition and biometric systems for user identity verification. | Provides identity verification only; does not ensure end-te-end protection of the sensitive data after authentication. | Combines Face++ biometric authentication with encryption, anonymization, and secure logging. |
| C | Privacy-Preserving Data Techniques [11]–[15] | Data masking, redaction, and cryptographic hashing (e.g., SHA-256) for privacy and integrity protection. | Protects individual data fields; lacks integration with strong authentication, encryption, and decentralized audit mechanisms. | Applies masking, redaction, and SHA-256 hashing along with encryption, biometrics, and blockchain for comprehensive protection. |
| D | Blockchain-Based Security [16]–[20] | Blockchain and smart contracts (primarily Ethereum) for access control, auditability, and immutability. | Focuses mainly on auditability and access management; does not provide complete data protection and privacy preservation. | Uses Ethereum blockchain to store tamper-proof access logs and verification records along with encrypted and anonymized data. |
| E | Integrated Security Approaches [21]–[25] | Combination of multiple security mechanisms to enhance overall system security. | Limited attention to secure intelligence communication; partial integration of security layers. | Proposes a unified framework tailored for intelligence communication that integrates all security layers. |
| F | Secure Communication Systems [26]–[30] | Secure communication frameworks using encryption and access control mechanisms. | Often rely on centralized infrastructure, which introduces single points of failure and scalability issues. | Employs decentralized storage along with encryption and blockchain to eliminate single points of failure and improve availability. |
| G | Overall Gap (Summary) | – | No existing work comprehensively integrates lightweight encryption, biometric authentication, privacy preservation, blockchain auditing, and decentralized storage for secure intelligence communication. | Our proposed system integrates ASCON encryption, RSA key protection, Face++ biometric authentication, data anonymization, SHA-256 hashing, Ethereum blockchain, and decentralized storage into a unified framework. |

TABLE I. RESEARCH GAP MATRIX ANALYSIS

The reviewed studies mainly focus on encryption, biometric authentication, privacy preservation, blockchain, or secure communication individually. However, these approaches have limited integration of multiple security mechanisms for intelligence communication. The proposed system addresses this gap by combining ASCON encryption, RSA key protection, Face++ biometric authentication, data anonymization, SHA-256 hashing, Ethereum blockchain, and decentralized storage into a unified framework. This integration provides comprehensive confidentiality, integrity, authentication, privacy, and auditability.

## IV. COMPARATIVE ANALYSIS OF PRIOR WORK

Table II compares the proposed system with existing approaches based on encryption, biometric authentication, privacy preservation, blockchain, and decentralized storage. Prior works generally focus on one or a few security mechanisms. Lightweight cryptography mainly provides data confidentiality, while biometric approaches focus on identity verification. Privacy-preserving systems protect sensitive information, and blockchain-based approaches mainly provide immutable logging and auditability. However, most existing approaches do

© SEP 2026 | IRE Journals | Volume 10 Issue 3 | ISSN: 2456-8880
DOI: https://doi.org/10.64388/IREV10I3-1722956

not integrate all these mechanisms or continue to depends the on centralized storage.

| Prior Work | Encryption | Biometric Auth. | Privacy / Anonymization | Blockchain | Decentralized Storage | Main Limitation |
|---|---|---|---|---|---|---|
| **Work A – Lightweight Cryptography** | ✓ ASCON | ✗ | ✗ | ✗ | ✗ | Focuses mainly on encryption |
| **Work B – Biometric Security** | Limited | ✓ Facial recognition | ✗ | ✗ | ✗ | Authentication only |
| **Work C – Privacy-Preserving System** | Limited | ✗ | ✓ Masking / Hashing | ✗ | ✗ | Limited access control and auditing |
| **Work D – Blockchain Security** | Limited | ✗ | Limited | ✓ Ethereum / Smart Contract | ✗ | Mainly focuses on logging and auditability |
| **Work E – Integrated Security** | ✓ | ✓ | ✓ | ✓ | ✗ | Partial integration and centralized storage |
| **Work F – Secure Communication** | ✓ | Limited | Limited | Limited | ✗ | Centralized infrastructure |
| **Proposed System** | **✓ ASCON + RSA** | **✓ Face++** | **✓ Masking + Redaction + SHA-256** | **✓ Ethereum** | ✓ | **Integrated multi-layer security** |

TABLE II. COMPARISON OF THE PROPOSED FRAMEWORK AGAINST REPRESENTATIVE PRIOR WORK

The proposed system addresses the identified limitations by integrating multiple complementary security mechanisms into a unified framework. ASCON provides efficient authenticated encryption for sensitive intelligence files and messages, while RSA securely protects the ASCON session keys during transmission. Face++ biometric authentication strengthens access control by verifying the identity of personnel before classified information is accessed. In addition, data masking, redaction, and SHA-256 hashing reduce the exposure of sensitive information and support data integrity and tamper detection. Ethereum blockchain provides immutable access logs and verification records through smart contracts, improving transparency and auditability. Finally, decentralized storage reduces dependence on centralized infrastructure and improves availability and fault tolerance. Overall, the integrated framework provides stronger confidentiality, integrity, authentication, privacy, non-repudiation, auditability, and controlled information access for secure intelligence communication..

## V. PROPOSED METHODOLOGY

The proposed system is organized into five implementation phases, as shown in Fig. 1: (1) user registration and Face++ biometric authentication, (2) ASCON-based data encryption with RSA session-key protection, (3) privacy preservation using data masking, redaction, and SHA-256 hashing, (4) Ethereum blockchain-based access logging and decentralized storage, and (5) secure data retrieval, integrity verification, and end-to-end system evaluation.

© SEP 2026 | IRE Journals | Volume 10 Issue 3 | ISSN: 2456-8880
DOI: https://doi.org/10.64388/IREV10I3-1722956

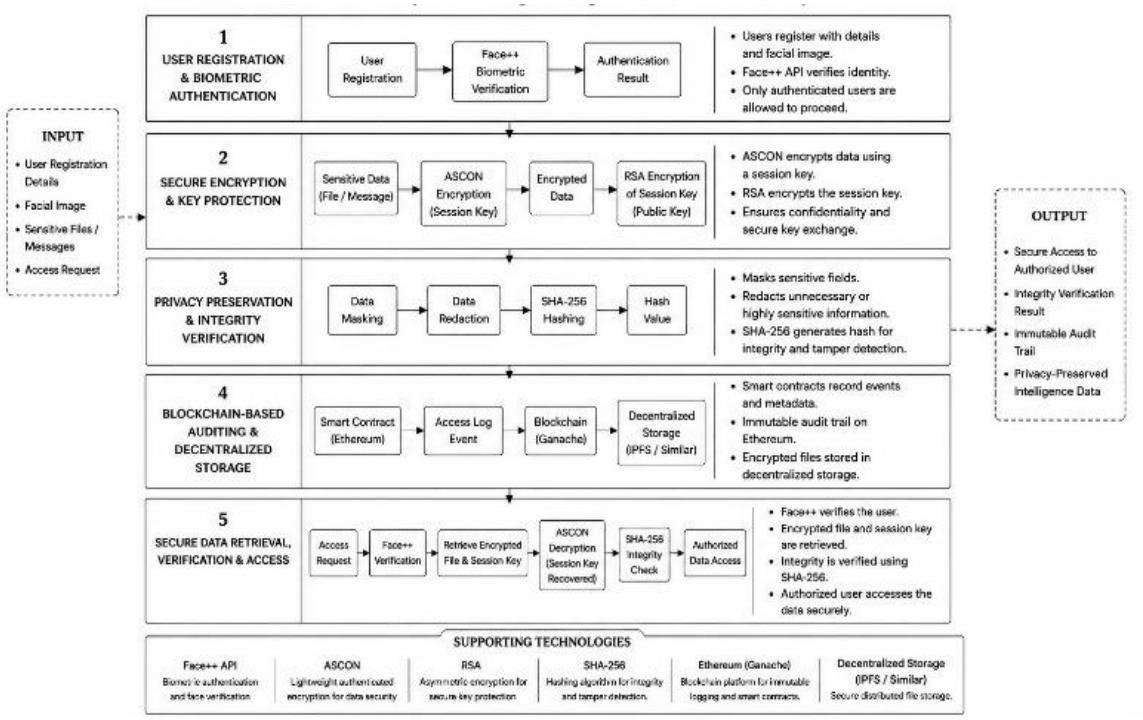


Fig. 1. Proposed Architecture Diagram

A. System Initialization and User Registration

The proposed system starts with the registration of authorized personnel who are permitted to handle classified intelligence information. During registration, the user's identification details and facial image are collected. The facial image is processed through the Face++ API to establish the user's biometric identity. The registered information is associated with the corresponding user account and access privileges. Only registered personnel can initiate the authentication process. This initial stage establishes a trusted identity for subsequent operations and reduces the possibility of unauthorized users entering the system.

B. Biometric-Based Authentication

When a user attempts to access a classified document, the system initiates mandatory facial verification. A new facial image is captured and submitted to the Face++ API, where it is compared with the registered facial information. If the verification is successful, the user is allowed to proceed to the requested resource. If verification fails, access is denied and the authentication event can be recorded for monitoring. Unlike password-only systems, biometric verification provides an additional identity-based security layer and helps mitigate credential sharing and identity impersonation.

C. Secure File and Message Encryption

After authentication, sensitive intelligence files and operational messages are protected using ASCON authenticated encryption. The plaintext information is provided as input to the encryption module along with the generated session key. ASCON produces encrypted ciphertext that cannot be directly interpreted without the appropriate key. Authenticated encryption also enables verification that the protected information has not been improperly modified. This layer is primarily responsible for maintaining the confidentiality and integrity of sensitive operational information.

D. RSA-Based Session-Key Protection

Although ASCON efficiently encrypts the actual data, the session key must also be securely transferred between communicating parties. Therefore, the proposed framework applies RSA asymmetric encryption to protect the ASCON session key. The session key is encrypted using the recipient's RSA public key and can be recovered only

using the corresponding private key. This prevents an attacker monitoring the communication channel from easily obtaining the symmetric encryption key. The combination of ASCON and RSA provides an efficient hybrid cryptographic mechanism.

E. Privacy-Preserving Data Processing

The system introduces a separate privacy layer to control the exposure of sensitive information. Data masking replaces selected confidential values with masked representations, whereas data redaction removes information that should not be disclosed. These techniques can be applied to personnel information, mission identifiers, operational details, and sensitive location attributes. The objective is to ensure that users receive only the information necessary for their authorized operations while minimizing unnecessary exposure of classified data.

F. SHA-256 Integrity Verification

The framework uses SHA-256 to generate a cryptographic hash of relevant files and metadata. The hash value serves as a compact representation of the original information. When the file is subsequently retrieved, its hash can be recalculated and compared with the previously recorded hash. If the values match, the data is considered unchanged; if they differ, the system can identify a potential modification. This mechanism strengthens integrity verification and complements the encryption layer.

G. Blockchain-Based Security Logging

Important system events are recorded using the Ethereum blockchain. The blockchain environment is deployed locally using Ganache, while smart contracts manage the recording of relevant security events. The recorded information may include user authentication status, document identifiers, access timestamps, metadata, hash values, and verification events. Since blockchain transactions provide an append-oriented and tamper-resistant record, the logging mechanism improves transparency and accountability compared with conventional centralized logs.

H. Smart Contract Execution

Smart contracts act as an automated mechanism for recording and validating authorized activities. When an important operation is completed, the corresponding transaction is submitted to the blockchain. The smart contract records the required metadata and verification information without relying entirely on manual intervention. This creates a consistent audit trail for classified-data access. The blockchain therefore serves not as the primary storage location for sensitive files, but as a trusted verification and auditing layer.

I. Decentralized File Storage

The actual intelligence files are maintained separately from blockchain records using a decentralized file-storage mechanism. Before storage, the files are encrypted so that the original sensitive content is not directly exposed. Blockchain stores relevant metadata and hash information rather than the complete classified document. This separation reduces blockchain storage requirements while allowing the integrity and access history of the file to be verified.

J. Secure Data Retrieval

When an authorized user requests a classified file, the system first performs biometric verification. Following successful authentication, the required encrypted file is retrieved from the decentralized storage layer. The corresponding integrity information is obtained and used to verify the retrieved file. If the verification is successful, the system allows controlled access to the information. The access event is subsequently recorded on the blockchain, maintaining a traceable history of the operation.

K. Unauthorized Access Handling

If biometric authentication fails, the system does not release the requested classified information. Similarly, if the integrity verification of a retrieved file fails, the system can prevent the information from being treated as trusted data. These controls provide protection against both unauthorized users and potentially modified files. Access attempts and security-related events can be maintained as part of the audit trail for further investigation.

© SEP 2026 | IRE Journals | Volume 10 Issue 3 | ISSN: 2456-8880
DOI: https://doi.org/10.64388/IREV10I3-1722956

## VI. EVALUATION PLAN AND EXPECTED OUTCOMES

The proposed framework is evaluated based on its security effectiveness, authentication performance, privacy preservation, integrity verification, and system efficiency. The evaluation considers encryption and decryption time, biometric verification accuracy, hash-based tamper detection, blockchain transaction logging, and encrypted file storage and retrieval performance. The system is also tested against unauthorized access attempts and modifications to stored intelligence data.

The expected results indicate that ASCON provides efficient authenticated encryption with reduced processing overhead, while RSA securely protects the session key during communication. Face++ is expected to improve identity verification and prevent unauthorized access to classified resources. Masking and redaction reduce the exposure of sensitive information, whereas SHA-256 enables reliable detection of data modification. Ethereum smart contracts provide immutable and traceable access records, while decentralized storage improves data availability and reduces dependence on centralized infrastructure. Overall, the proposed framework is expected to strengthen confidentiality, integrity, authentication, privacy, auditability, non-repudiation, and controlled access in intelligence communication.

## VII. ADVANTAGES OF THE PROPOSED SYSTEM

The Table III summarizes the major advantages of the proposed privacy-preserving intelligence communication framework. It shows how each security mechanism contributes to the overall protection of sensitive intelligence information.

| Aspect | Advantage | Impact / Benefit |
|---|---|---|
| Data Security | ASCON encryption secures sensitive files and messages with lightweight and authenticated encryption. | Ensures confidentiality and protects data from unauthorized access or leakage. |
| Key Management | RSA protects the ASCON session key during transmission. | Prevents key interception and ensures secure key exchange. |
| User Authentication | Face++ biometric verification allows access only to authorized personnel. | Reduces identity impersonation and prevents unauthorized access. |
| Privacy Preservation | Data masking and redaction hide sensitive information in files and logs. | Minimizes exposure of confidential information. |
| Data Integrity | SHA-256 hashing is used to generate unique hash values of data. | Detects any data modification or tampering effectively. |
| Audit and Accountability | Ethereum smart contracts store access logs and verification events immutably. | Provides a transparent, tamper-proof and traceable audit trail. |
| Storage Reliability | Encrypted files are stored in decentralized storage (e.g., IPFS). | Improves data availability and removes dependence on a single centralized server. |
| Protection Against Insider Threats | Mandatory biometric verification and controlled access reduce internal misuse. | Prevents unauthorized internal access and insider attacks. |
| System Efficiency | Lightweight encryption (ASCON) and optimized processes reduce computational overhead. | Provides faster encryption/decryption and improves overall system performance. |
| Comprehensive Security | Integration of encryption, authentication, privacy, hashing, blockchain, and decentralized storage provides multi-layer protection. | Achieves confidentiality, integrity, authentication, privacy, non-repudiation, auditability, and controlled access. |

TABLE III. ADVANTAGES OF PROPOSED SYSTEM AND ITS IMPACT

The proposed system provides enhanced security for sensitive intelligence files and operational messages through ASCON encryption and RSA-based session-key protection. Face++ biometric authentication ensures that only authorized personnel can access classified information, reducing the risk of identity impersonation and insider threats. Data masking and redaction minimize the exposure of sensitive information, while SHA-256 hashing enables reliable detection of unauthorized data modification. The use of Ethereum blockchain provides an immutable and traceable audit trail for access and verification events.

Decentralized storage improves data availability and reduces dependence on centralized infrastructure. By integrating these mechanisms into a single framework, the system provides comprehensive confidentiality, integrity, authentication, privacy, auditability, non-repudiation, and controlled access.

## VIII. FUTURE SCOPE

The proposed framework can be further enhanced to provide stronger security, scalability, and practical deployment capabilities. Future work can focus on real-time intelligence communication with improved encryption and authentication performance. Advanced AI-based threat detection can be incorporated to identify unusual access patterns and potential insider threats. The biometric layer can be extended to support multi-modal authentication, combining facial recognition with fingerprints, voice, or other authentication factors. Blockchain implementation can be migrated from a local Ganache environment to a scalable permissioned blockchain network for real-world deployment. The decentralized storage layer can also be optimized for faster retrieval and improved fault tolerance. Further research can evaluate the framework using larger datasets, different file sizes, network conditions, encryption latency, storage overhead, and authentication accuracy. These enhancements can help transform the proposed prototype into a scalable solution for real-world defense and intelligence environments.

## IX. CONCLUSION

The proposed Privacy-Preserving Intelligence Communication Framework provides a multi-layered approach for securing sensitive intelligence information against unauthorized access, identity impersonation, data leakage, and tampering. The integration of ASCON encryption and RSA-based key protection ensures secure data and session-key transmission, while Face++ biometric authentication strengthens identity verification. Data masking, redaction, and SHA-256 hashing provide privacy protection and integrity verification. Furthermore, Ethereum blockchain enables immutable access logging and auditability, while decentralized storage improves data availability and resilience. By combining these security mechanisms into a unified framework, the proposed system provides confidentiality, integrity, authentication, privacy, non-repudiation, auditability, and controlled information access, making it a promising approach for secure intelligence communication applications.

## REFERENCES

[1] The Radicati Group Inc. “Cloud Email and Collaboration—Market Quadrant 2019.” [https://www.radicati.com/wp/wp-content/uploads/2019/03/Cloud-Email-and-Collaboration-Market-Quadrant-2019-Brochure.pdf], March 2019, accessed April 8, 2019.

[2] Sadler, T. “The Year of Email Data Breaches.” *Infosecurity Magazine*, [https://www.infosecurity-magazine.com/opinions/2017-email-data-breaches/], January 2018, accessed September 11, 2019.

[3] Wikileaks. “Hillary Clinton Email Archive.” [https://wikileaks.org/clinton-emails/], March 2016, accessed April 8, 2019.

[4] Wikileaks. “The Podesta Emails.” [https://wikileaks.org/podesta-emails/], March 2016, accessed April 8, 2019.

[5] Callas, J., Donnerhacke, L., Finney, H., Shaw, D., and Thayer, R. “OpenPGP Message Format.” [https://tools.ietf.org/html/rfc4880], November 2007, RFC 4880 (Proposed Standard).

[6] Ramsdell, B., and Turner, S. “Secure/Multipurpose Internet Mail Extensions (S/MIME) Version 3.2 Message Specification.” [https://tools.ietf.org/html/rfc5751], January 2010, RFC 5751 (Proposed Standard).

[7] Abu-Salma, R., Sasse, M. A., Bonneau, J., Danilova, A., Naiakshina, A., and Smith, M. “Obstacles to the adoption of secure communication tools.” In *2017 IEEE Symposium on Security and Privacy*. IEEE, 2017, pp. 137–153.

[8] Ruoti, S., Andersen, J., Zappala, D., and Seamons, K. (2015). "Why Johnny Still, Still Can't Encrypt: Evaluating the Usability of a Modern PGP Client." [Online]. Available: [https://arxiv.org/pdf/1510.08555.pdf]

[9] Sheng, S., Broderick, L., Koranda, C. A., and Hyland, J. J. "Why Johnny Still Can't Encrypt: Evaluating the Usability of Email Encryption Software." In *Symposium on Usable Privacy and Security*, 2006, pp. 3–4.

[10] Shamir, A. "Identity-Based Cryptosystems and Signature Schemes." In *Advances in Cryptology—CRYPTO 1984*. Springer, 1984, pp. 47–53.

[11] Proofpoint. "Proofpoint Email Protection." [https://www.proofpoint.com/us/products/email-protection], 2005, accessed April 18, 2019.

[12] DataMotion. "DataMotion SecureMail." [https://www.proofpoint.com/us/products/email-protection], 2013, accessed April 18, 2019.

[13] Unger, N., Dechand, S., Bonneau, J., Fahl, S., Perl, H., Goldberg, I., and Smith, M. "SoK: Secure Messaging." In *2015 IEEE Symposium on Security and Privacy*. IEEE, 2015, pp. 232–249.

[14] Sun, H.-M., Hsieh, B.-T., and Hwang, H.-J. "Secure E-Mail Protocols Providing Perfect Forward Secrecy." *IEEE Communications Letters, 9*(1), 58–60, 2005.

[15] Kwon, J. O., Jeong, I. R., and Lee, D. H. "A Forward-Secure E-Mail Protocol Without Certificated Public Keys." *Information Sciences, 179*(24), 4227–4231, 2009.