Published by :
https://www.ijert.org/
An International Peer-Reviewed Journal

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 04 , April - 2026

Time Based Cryptography Key Validity System

Fabin Jim Cherian Department of Computer Science and Engineering(Cyber Security)
Vimal Jyothi Engineering College
Chemperi, Kannur

Reem Sana
Department of Computer Science and Engineering(Cyber Security)
Vimal Jyothi Engineering College
Chemperi, Kannur

Rizana Ali TP
Department of Computer Science and Engineering(Cyber Security)
Vimal Jyothi Engineering College
Chemperi, Kannur

Safwana Musthafa
Department of Computer Science and Engineering(Cyber Security) Vimal Jyothi Engineering College Chemperi, Kannur

Mr.Arun Pushpan
Assistant Professor
Department of Computer Science
Vimal Jyothi Engineering College
Chemperi, Kannur

***Abstract*—Abstract The Time Based Cryptography Key Validity System is designed to enhance secure communication by combining cryptographic encryption with multi-layer authentication mechanisms. In this system, the sender encrypts a message using AES-256 with GCM mode and generates a unique access key. The system securely sends this access key to the receiver's email as a One-Time Password (OTP), ensuring that only the intended recipient can access it. The sender also defines security parameters such as the allowed network, valid time window, and maximum number of decryption attempts.The receiver must provide the correct OTP along with the access key and satisfy all security conditions to decrypt the message successfully. If any condition fails, such as incorrect OTP, unauthorized network access, or expired time, the system blocks the request. All decryption attempts are recorded in a blockchain-based dashboard, which maintains a tamper-resistant log of activities including receiver details, network used, attempt time, and status. This system improves data security by integrating encryption, time-based access control, OTP verification, and blockchain logging, making it suitable for secure and controlled data sharing applications.**

***Index Terms*—Operating System Security, Behavioral Analysis, Zero-Day Defense, Local AI, Privacy-Preserving Computing, Malware Detection, Proactive Defense**

I. INTRODUCTION

The rapid expansion of digital communication networks has made secure data transmission a critical requirement in modern computing environments. Sensitive information, ranging from personal credentials to confidential organizational data, is routinely exchanged across networks, exposing it to interception, unauthorized access, and misuse. While cryptographic techniques have long served as the foundation of data security, traditional encryption systems predominantly rely on static decryption keys. Once such a key is compromised, the encrypted data becomes fully accessible without any additional barrier to entry. Significant research has explored methods to strengthen access control beyond static key management. Cai and Feng [1] proposed a time-bound access control scheme using Ciphertext-Policy Attribute-Based Encryption (CP-ABE), enabling data access only when both user attributes and time constraints are satisfied. Though effective, the scheme introduces considerable computational overhead due to bilinear pairing operations. Shivaramakrishna and Nagaratna [2] advanced this concept by presenting a hybrid cryptographic framework that combines AES-OTP and RSA encryption with time-limited access control for cloud storage, demonstrating that layered encryption improves confidentiality but increases implementation complexity. Addressing trust in distributed environments, Nie et al. [3] introduced a zero-trust access control mechanism leveraging blockchain and inner-product encryption for IoT systems in 6G networks. Their work establishes that blockchain-based logging ensures tamper-proof transparency, though it introduces storage and computational overhead. Similarly, Xu et al. [4] proposed a post-quantum searchable encryption scheme supporting time-controlled user authorization for outsourced cloud data, highlighting the growing importance of future-proof cryptographic designs. The foundational concept of time-controlled decryption itself traces back to the work of Rivest, Shamir, and Wagner [5], whose timed-release encryption using computational puzzles demonstrated that enforcing temporal access restrictions without a trusted third party is theoretically achievable, albeit computationally expensive. The Gap: While these works individually address aspects of time-based control, multi-factor authentication, or tamper-proof logging, no unified system combines all of these mechanisms into a practical, lightweight framework suitable for controlled digital communication. Most existing systems either lack OTP-based identity verification, do not enforce network-level access restrictions, or provide no transparent audit trail of access attempts. To address these limitations, this work proposes a Time Based Cryptography Key Validity System that integrates AES-256 encryption with GCM mode, email-delivered One-Time Password authentication, time-window enforcement, IP-based network verification, attempt limitation controls, and blockchain-based forensic

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 04 , April - 2026

logging into a single cohesive framework. By ensuring that decryption is granted only when all conditions are simultaneously satisfied, the system significantly reduces the risk of unauthorized access even in scenarios where the access key has been exposed.

II. Overview

The rapid growth of digital communication has made securing sensitive data a critical necessity in modern computing environments. Sensitive information such as personal credentials, financial details, and confidential messages are frequently transmitted across networks, making them vulnerable to interception and unauthorized access. Traditional encryption systems rely primarily on a single static decryption key, which once compromised, grants unrestricted access to encrypted data with no additional safeguard. Furthermore, existing systems lack advanced controls such as time-based validity, network verification, and attempt limitations, leaving significant security gaps that malicious actors can exploit.

To address these critical issues, this work proposes a Time Based Cryptography Key Validity System, a secure communication framework that combines AES-256 encryption with GCM mode, multi-layer authentication, and controlled access mechanisms. The system generates a unique access key for each message and delivers a One-Time Password to the receiver's email, ensuring only the intended recipient can initiate decryption. The sender defines binding security parameters including a valid time window, an authorized network address, and a maximum decryption attempt limit, all of which must be simultaneously satisfied before access is granted. By embedding a blockchain-based forensic dashboard that maintains a tamper-resistant log of all access activities, the system restores transparency and accountability to digital communication.

A. *KEY FEATURES*

1) **AES-256 Encryption Module (Core Security Module):**
   - Encrypts messages using AES-256 with GCM mode, ensuring confidentiality and data integrity during transmission.
   - Guarantees that encrypted data remains unreadable without satisfying all predefined access conditions, moving beyond reliance on a single static decryption key.
2) **Time-Based Access Control:**
   - Enforces decryption only within a sender-defined valid time window, automatically blocking access before the start time or after the expiry time.
   - Ensures that even if an access key is intercepted or leaked, it cannot be used beyond the defined validity period.
3) **OTP-Based Email Authentication:**
   - Generates a One-Time Password and delivers it securely to the receiver's registered email address, adding an additional layer of identity verification.
   - Ensures that unauthorized users cannot complete decryption even if the access key is known, by requiring correct OTP entry before access is granted.
4) **Network and IP Verification Module:**
   - Validates the receiver's IP address against the sender-defined authorized network before permitting any decryption attempt.
   - IAutomatically blocks access requests originating from unauthorized networks or locations, preventing misuse from unknown environments.
5) **Attempt Limitation System:**
   - Restricts the number of decryption attempts to a sender-defined maximum, preventing brute-force attacks and repeated unauthorized access.
   - Automatically triggers OTP verification when the maximum attempt limit is reached, adding a dynamic security response to suspicious activity.
6) **Blockchain-Based Forensic Logging:**
   - Records all access attempts, both successful and failed, in a tamper-resistant blockchain ledger that cannot be altered or deleted.
   - Maintains a detailed forensic log including receiver identity, network details, OTP verification status, timestamps, and access outcome, enabling full traceability and accountability.

The Time Based Cryptography Key Validity System incorporates several distinct modules to ensure robust data security and controlled access efficiency.

III. PROPOSED SYSTEM AND DESIGN

The proposed system, Time Based Cryptography Key Validity System, re-engineers the traditional approach to secure communication by integrating multiple layers of access control directly into a robust validation framework. Its core innovation, the Time Based Key Validity mechanism, enforces strict temporal boundaries on decryption access, ensuring that even a compromised key cannot be exploited beyond its defined validity window. Unlike conventional systems that depend solely on a static decryption key, this system demands the simultaneous satisfaction of multiple security conditions before granting access to encrypted data.

The system is composed of three core components:

- **AES-256 Encryption with GCM Mode:** Located at the heart of the system, this module serves as the primary security mechanism by encrypting messages with AES-256 in GCM mode, guaranteeing both confidentiality and data integrity. A unique access key is generated for each message, ensuring that no two encryption sessions share the same credentials, thereby eliminating the risk of key reuse attacks.
- **Multi-Layer Access Control Engine:** The system enforces a strict set of sender-defined security parameters including time window validation, IP-based network verification, and attempt limitation controls. Access is granted

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 04 , April - 2026

only when all conditions are simultaneously satisfied. If any single condition fails, whether an expired time window, an unauthorized network, or an exceeded attempt limit, the request is immediately denied and logged.

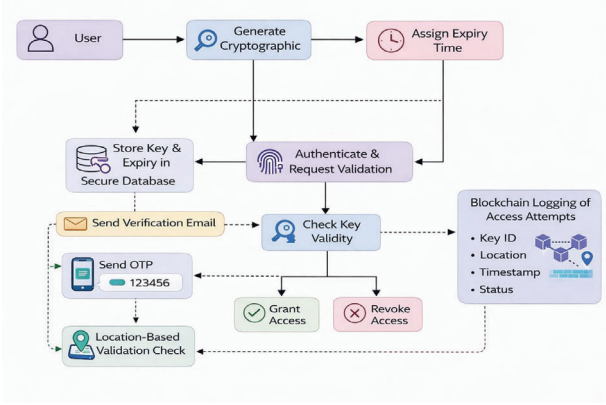

Fig. 1. Private Hybrid AI Assistant

- **Blockchain-Based Forensic Dashboard:** To ensure complete transparency and accountability, all access attempts are recorded in a tamper-resistant blockchain ledger. The dashboard maintains a detailed forensic log of every interaction including receiver identity, email address, allowed IP, access IP, OTP verification status, number of attempts, and final access outcome, enabling full traceability and auditability of system activity.

Overall, the Time Based Cryptography Key Validity System stands as a robust and efficient solution for secure digital communication, strengthening data protection while maintaining a transparent and accountable access environment. By shifting security from static key dependence to dynamic multi-condition validation, it establishes a privacy-centric and highly controlled framework that effectively counters unauthorized access and data breaches.

A. *SYSTEM ARCHITECTURE*

The system architecture of the Time Based Cryptography Key Validity System demonstrates how the framework ensures continuous protection through a structured validation pipeline that enforces security conditions before any decryption is permitted. The process is centered on the Access Control Engine, which acts as the foundational decision layer. When a receiver initiates a decryption request, the system intercepts it and passes it through a sequential verification chain before execution. The request is first validated against the sender-defined time window, confirming that the current timestamp falls within the allowed start and expiry times. Simultaneously, the system verifies the receiver's network by comparing the access IP address against the authorized network defined by the sender. If these conditions are satisfied, the OTP module is triggered, generating a One-Time Password and delivering it to the receiver's registered email address. The receiver must submit the correct OTP to proceed. Throughout this process, the attempt counter tracks the number of requests and enforces the maximum attempt limit. Every access event, regardless of its outcome, is recorded in the blockchain-based forensic dashboard, ensuring a tamper-resistant and fully traceable audit trail.

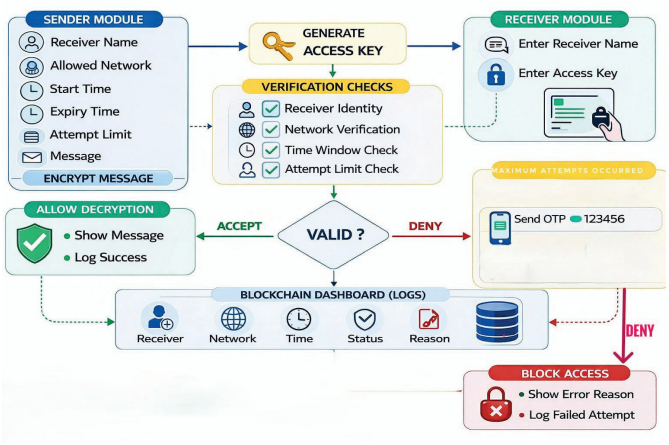

Fig. 2. Architecture Diagram

B. *SYSTEM DESIGN*

The system design is further detailed through Use Case and Data Flow Diagrams. The Use Case Diagram illustrates the interactions between the Sender and the Receiver through the system. The Sender initiates the process by encrypting a message, defining security parameters such as time validity, allowed network, and attempt limits, and generating a unique access key. The Receiver submits a decryption request by providing the access key and satisfying all validation conditions including OTP verification and network authorization.

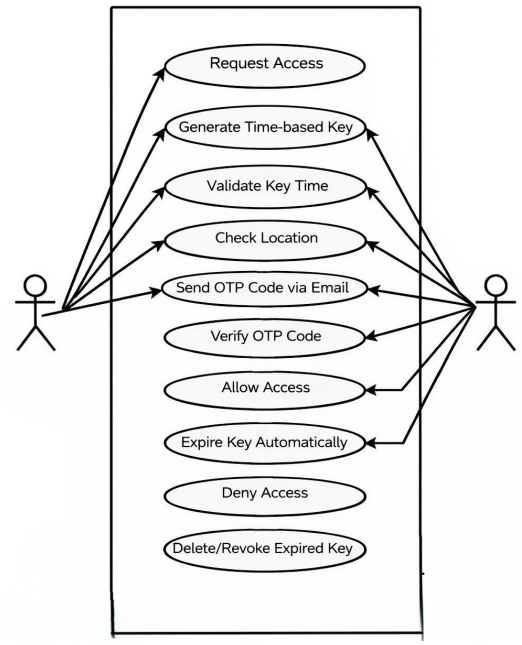

Fig. 3. Use Case Diagram

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 04 , April - 2026

The Data Flow Diagrams illustrate the movement of data through the system. The Level 0 DFD presents the high-level boundary of the system, depicting the Time Based Cryptographic Key Validity Process as the central entity mediating communication between the Sender and the Receiver, with the Key Database managing the storage and retrieval of valid and expired keys.

The Level 1 DFD expands this view to detail the interaction between specific subsystems including the Key Generation Module, Decision Module, OTP Verification Module, IP Location Check, Decryption Module, Access Counter, and the Blockchain Ledger, illustrating how data flows through each validation stage before access is either granted or denied.

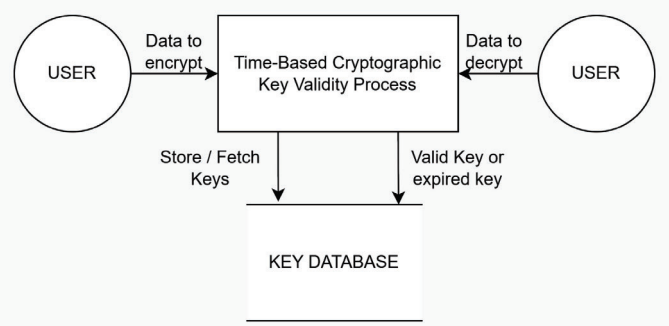

Fig. 4. Data Flow Diagram (Level 0)

The Level 1 Data Flow Diagram expands the central process to detail the interaction between specific subsystems and data repositories.

- Access Control and Validation: The Decision Module is shown as a composite module containing ”Time Window Check,” ”Access Key Validation,” ”Network Verification,” and ”Attempt Limitation Control,” ensuring rigorous vetting of every decryption request before access is considered.
- OTP Authentication: The OTP Module illustrates a secure authentication loop. When the maximum attempt limit is reached or additional verification is required, an OTP is generated and delivered to the receiver’s registered email, ensuring that only the intended user gains access.
- Decryption and Access: The Decryption Module handles the final stage of the workflow. Upon successful validation of all conditions, it decrypts the message using AES-256 with GCM mode and delivers the output to the receiver.
- Blockchain Logging: The diagram shows the Blockchain Ledger receiving activity records from all modules. Every access attempt, whether successful or failed, is logged with details including receiver identity, network, OTP status, timestamp, and access outcome, enabling full traceability and accountability.

IV. IMPLEMENTATION

The implementation of the Time-Based Cryptography Key Validity Control Service is carried out in a structured and

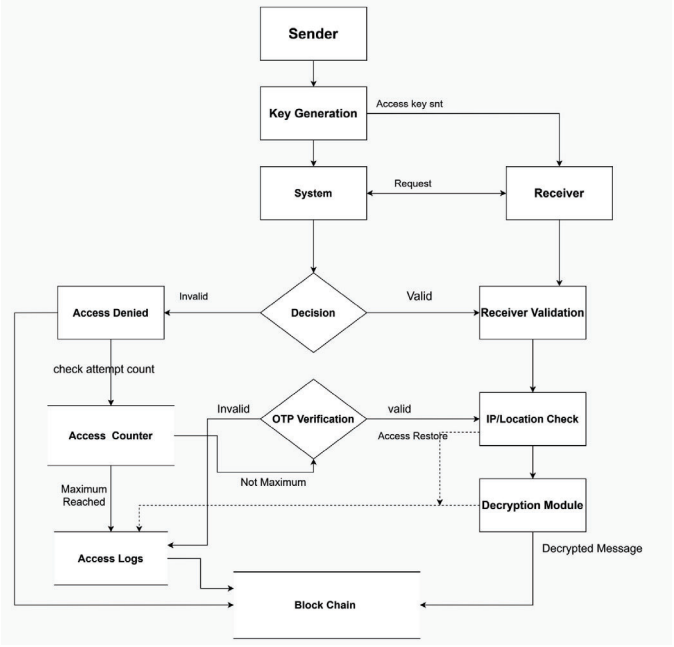

Fig. 5. .Data Flow Diagram (Level 1)

modular manner. The system first generates a secure cryptographic key and assigns a specific time validity to it. The data is then encrypted using the generated key. During decryption, the system checks the current time against the key’s validity period. If the key is valid, access is granted; otherwise, the request is denied. The system ensures that expired keys cannot be reused, thereby improving security and preventing unauthorized access.

A. *MODULES*

Phase 1: System Design and Architecture: In this phase, the overall structure of the Time-Based Cryptography Key Validity Control Service is designed. The system follows a modular architecture that separates key generation, encryption, validation, and access control. A service-oriented approach is adopted so that multiple applications can use this system for secure key management. The design focuses on integrating time-based validation with cryptographic operations.

Phase 2: Key Generation and Encryption Module This phase involves generating secure cryptographic keys using AES-based techniques. Each key is uniquely created for a user or a file and is associated with a predefined time validity. The encryption module uses these keys to convert plaintext data into ciphertext, ensuring confidentiality. The keys are securely stored and linked with metadata such as creation time and expiry time.

Phase 3: Time Validation and Access Control In this phase, the system checks whether the key is valid before allowing decryption. During every access request, the current system time is compared with the key’s validity period. If the time condition is satisfied, access is granted; otherwise, the request

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 04 , April - 2026

is rejected. This ensures that even valid users cannot access data outside the allowed time window.

Phase 4: Key Expiry and Regeneration This phase handles automatic key expiration. Once the defined time period is over, the key becomes invalid and cannot be used again. If the user requires access after expiry, a new key must be generated through the system. This prevents repeated misuse of old keys and ensures controlled access.

Phase 5: Service Integration and User Interaction In the final phase, the system is provided as a security service that can be integrated with applications such as cloud storage, file sharing systems, and secure communication platforms. A simple interface is designed for users to request keys, encrypt data, and perform decryption based on time validation.

B. TOOLS AND TECHNIQUES

The development of the Time-Based Cryptography Key Validity Control Service uses a combination of cryptographic methods and software tools to ensure secure and efficient operation.

- *Programming Languages*: The system is implemented using languages such as Python for backend logic and SQL for database management. Python is chosen because of its simplicity and availability of cryptographic libraries.
- *Cryptographic Techniquess*: The system uses AES (Advanced Encryption Standard), particularly AES-256, for secure encryption and decryption. AES provides strong confidentiality and is widely used in modern security systems. Time-based validation is added as an additional security layer.
- *Database and Storage*: A database such as MySQL is used to store:
  - User details
  - Cryptographic keys
  - Key validity time
  - Access logs

  This ensures proper tracking and management of keys.
- *System Components*: The service consists of multiple components:
  - Key Generation Module
  - Encryption/Decryption Module
  - Time Validation Module
  - Access Control System

  Each component works together to provide secure and controlled data access.
- *Development Tools*: Development is carried out using tools such as:
  - Visual Studio Code (IDE)
  - Python libraries for cryptography
  - Database management systems

  These tools help in efficient coding, testing, and debugging.

V. RESULTS AND DISCUSSION

The proposed Time-Based Cryptography Key Validity Control Service was implemented and evaluated to analyze its effectiveness in enhancing data security through time-restricted access. The system integrates cryptographic key management with temporal validation, ensuring that keys remain usable only within a predefined time interval.

- ***Functional Evaluation***:
  The system was tested for key generation, encryption, decryption, and time-based validation. Each cryptographic key was successfully generated with associated metadata, including creation time and expiry time. During experimentation, the following observations were made:
  - Valid keys allowed successful decryption within the defined time window.
  - Expired keys were automatically rejected by the system
  - Reuse of expired keys was not permitted

  These results confirm that the time validation mechanism operates correctly and enforces strict access control.
- ***Security Analysis***:
  The introduction of time-based constraints significantly reduces the risk associated with long-term key exposure. In traditional systems, compromised keys can be reused multiple times; however, in the proposed service
  - Key usability is limited to a specific duration
  - Unauthorized access attempts after expiry are effectively blocked
  - The impact of key leakage is minimized

  Thus, the system enhances security by incorporating temporal restrictions as an additional protection layer.
- ***Encryption Performance***:
  The system utilizes AES-based encryption to ensure confidentiality of data. Experimental evaluation indicates that:
  - Data is securely encrypted before storage or transmission
  - Decryption is possible only with valid keys within the permitted time
  - Invalid or expired keys result in unsuccessful decryption attempts

  This demonstrates that the system maintains both data confidentiality and controlled accessibility.
- ***Discussion***:
  - The experimental results demonstrate that integrating time-based validity into cryptographic key management provides a robust solution for controlling data access. By restricting the usability of keys to a defined time frame, the system addresses major limitations of conventional cryptographic approaches, particularly the risks associated with prolonged key validity.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 04 , April - 2026

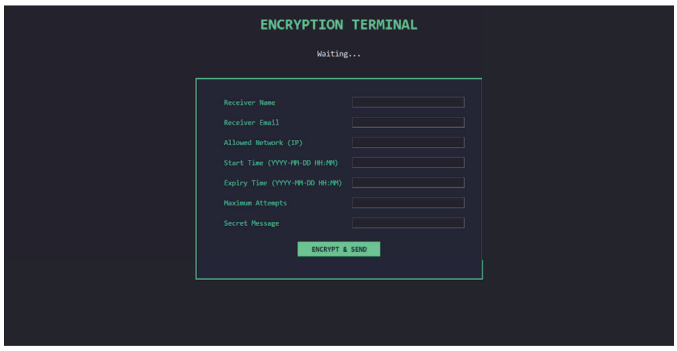

Fig. 6. Senders Screen)

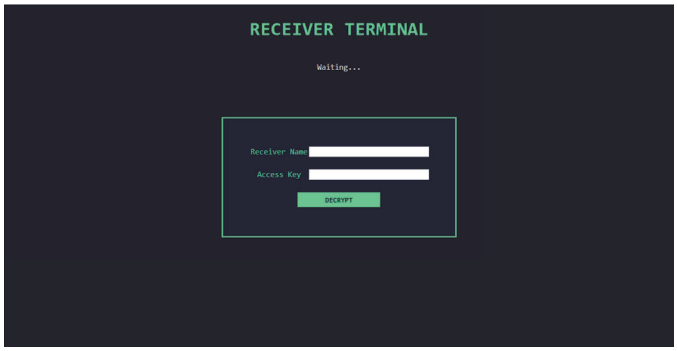

Fig. 7. Receivers Screen)

Fig. 8. BlockChain Interface

VI. CONCLUSION AND FUTURE WORK

A. Conclusion

This project presents a Time-Based Cryptography Key Validity System that provides secure and controlled access to encrypted data by allowing the sender to define parameters such as receiver identity, IP address, time limits, and maximum attempts. The system verifies these conditions on the receiver side before allowing decryption and denies access if any condition fails while tracking attempts to prevent misuse. When the maximum attempt limit is reached, an OTP (One-Time Password) is generated to verify the legitimate user. In addition, a blockchain-based logging system records all activities like successful access, failed attempts, and OTP requests in a secure and tamper-resistant manner, ensuring reliable and traceable data access.

B. Future Work

Future work for this project can include adding biometric authentication such as fingerprint or face recognition to enhance security, and implementing multi-factor authentication by combining OTP, password, and biometrics. The system can be improved using AI-based threat detection to identify suspicious activities and prevent attacks. Dynamic key generation can be introduced to change encryption keys based on time or user behavior. Further enhancements include developing a mobile application for better accessibility, using GPS-based geo-location tracking instead of only IP address, and integrating cloud storage for scalability. Advanced blockchain features like smart contracts can be added for automated control, along with real-time alerts for suspicious access and improvements in the user interface for better usability.

REFERENCES

[1] Y. Cai and M. Feng, “A time-bound data access control scheme based on attribute-based encryption,” pp. 1–5, 2023.
[2] D. Shivaramakrishna and M. Nagaratna, “A novel hybrid cryptographic framework for secure data storage in cloud computing: Integrating aes-otp and rsa with adaptive key management and time-limited access control,” *Alexandria Engineering Journal*, vol. 84, pp. 275–284, 2023.
[3] P. T. Tran-Truong *et al.*, “Time-based access control and key delegation for secure systems,” *Sensors*, vol. 25, no. 550, 2025.
[4] S. Xu, Y. Cao, X. Chen, Y. Guo, Y. Yang, F. Guo, and S.-M. Yiu, “Post-quantum searchable encryption supporting user-authorization for outsourced data management,” 2024.
[5] R. L. Rivest, A. Shamir, and D. Wagner, “Timed-release encryption,” *MIT Computer Science and Artificial Intelligence Laboratory*, 1996.
[6] A. Alabdulatif, “Blockchain-based privacy-preserving authentication and access control model for e-health users,” *Information*, vol. 16, no. 219, 2025.
[7] M. B. Hinojosa-Cabello, R. Aldeco-Perez, M. Morales-Sandoval, and J. J. Garcia-Hernandez, “Blockchain-based decentralization approach for ciphertext-policy attribute-based encryption schemes,” *Frontiers in Blockchain*, vol. 8, p. 1622270, 2025.
[8] S. Wang, N. Luo, B. Xing, Z. Sun, H. Zhang, and C. Sun, “Blockchain-based proxy re-encryption access control method for biological risk privacy protection of agricultural products,” *Scientific Reports*, vol. 14, p. 20048, 2024.
[9] M. A. Lail, M. Moncivais, R. Benton, and A. J. Perez, “Cloud-based access control including time and location,” *Electronics*, vol. 13, no. 14, p. 2812, 2024.
[10] I. M. Opakunle, M. O. Motunrayo, O. A. Shekinah, O. A. Olusola, and O. J. Adegboyega, “Semantic time-based access control: A model for patients’ data security in a cloud environment,” *International Journal of Scientific Engineering and Science*, vol. 7, no. 1, pp. 24–33, 2023.