Geo-Temporal Encrypted File Vault With Secure Access Control And Self-Destruction

Mr.P.Rajapandian[1], Geetha Priya.V[2]
[1] Associate Professor, Department of computer Applications, Sri Manakula Vinayagar Engineering College (Autonomous), Puducherry 605008, India
[2] Post Graduate student, Department of computer Applications, Sri Manakula Vinayagar Engineering College (Autonomous), Puducherry 605008, India

Abstract- *This project titled "Geo-Temporal Encrypted File Vault with Secure Access Control and Self-Destruction", Ensures the increasing demand for highly secure and controlled file transactions, this system introduces an advanced Geo-Temporal Encrypted File Vault, integrating geofencing, time based access control, Elliptic Curve Cryptography (ECC), and automated self- destruction mechanisms. The system ensures that files can only be accessed within a specific geographic location and time window, preventing unauthorized access. The encryption process leverages ECC-based public-key cryptography to ensure lightweight yet robust security. Multi-factor authentication (MFA) using passcodes or OTP verification enhances access control. Upon successful authentication, access details such as geolocation, timestamps, and user credentials are logged and securely sent to the file owner for auditing.*

To maintain data confidentiality and prevent residual exposure, files are automatically deleted after access. This system is ideal for secure document handling in corporate, legal, and classified environments, ensuring zero unauthorized access, strong data encryption, and automatic risk mitigation through self-destruction mechanisms. The development of this project leverages HTML and Bootstrap (CSS) for the front-end, ensuring a visually appealing and responsive design. On the backend, Java and MySQL have been employed to establish a robust foundation for data management and system functionality.

This project titled "Geo-Temporal Encrypted File Vault with Secure Access Control and Self- Destruction", Ensures the increasing demand for highly secure and controlled file transactions, this system introduces an advanced Geo-Temporal Encrypted File Vault, integrating geofencing, time based access control, Elliptic Curve Cryptography (ECC), and automated self- destruction mechanisms. The system ensures that files can only be accessed within a specific geographic location and time window, preventing unauthorized access. The encryption process leverages ECC-based public-key cryptography to ensure lightweight yet robust security.

Multi-factor authentication (MFA) using passcodes or OTP verification enhances access control. Upon successful authentication, access details such as geolocation, timestamps, and user credentials are logged and securely sent to the file owner for auditing. To maintain data confidentiality and prevent residual exposure, files are automatically deleted after access. This system is ideal for secure document handling in corporate, legal, and classified environments, ensuring zero unauthorized access, strong data encryption, and automatic risk mitigation through self-destruction mechanisms. The development of this project leverages HTML and Bootstrap (CSS) for the front-end, ensuring a visually appealing and responsive design. On the backend, Java and MySQL have been employed to establish a robust foundation for data management and system functionality.

The system's architecture emphasizes both security and usability, providing a seamless user experience without compromising on protection. By combining a responsive front-end built with HTML and Bootstrap with a robust Java-MySQL backend, the platform ensures efficient file processing, secure data handling, and real-time user interaction. The audit trail generated during each access attempt not only supports accountability but also enables proactive threat detection and response. This holistic approach makes the solution adaptable for integration into existing enterprise systems, offering a reliable method for organizations to enforce strict data governance policies.

I. INTRODUCTION

In today's digital landscape, the protection of sensitive and confidential data has become a critical concern across industries such as defense, healthcare, legal, and corporate sectors. Traditional encryption methods and access control systems, while effective to some extent, are often insufficient in preventing unauthorized access in scenarios involving physical displacement, delayed access, or insider

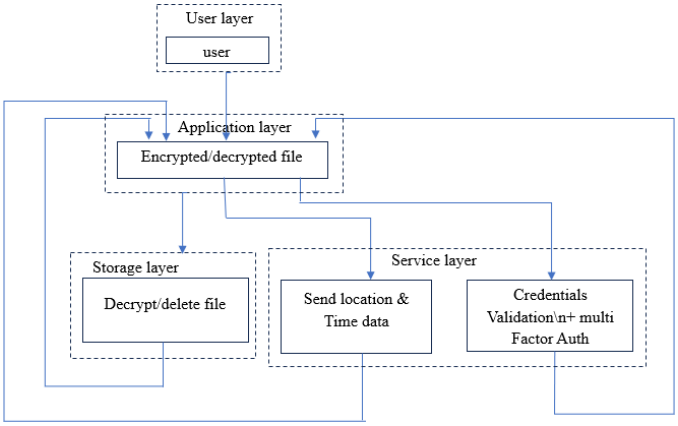
threats. To address these growing challenges, this project introduces an innovative solution: a Geo-Temporal Encrypted File Vault that combines location-based access control, time-bound constraints, advanced cryptography, and self-destruction capabilities.

The system ensures that files are only accessible within a defined geographical location and time window, enforced through device GPS or IP-based geolocation and system time verification. This geo-temporal enforcement prevents unauthorized access outside the permitted region or timeframe, even if credentials are compromised. To secure file contents, the system employs Elliptic Curve Cryptography (ECC) — a lightweight public-key encryption method known for its strong security with shorter key lengths, making it ideal for resource-limited environments.

Security is further strengthened through Multi- Factor Authentication (MFA) mechanisms, including passcodes and one-time passwords (OTP), ensuring that only verified users can initiate access attempts. Once authenticated, each access session is logged with metadata such as timestamp, geolocation, and user ID, which is securely shared with the file owner for audit and traceability. Additionally, a self-destruction mechanism ensures automatic and irreversible deletion of the file after access or upon detection of unauthorized actions, eliminating risks of residual data exposure.

The system is built using HTML and Bootstrap for a responsive and user-friendly front-end interface, while Java and MySQL form the foundation of the back- end logic and database management. By combining modern security protocols with practical access constraints, the proposed vault system represents a comprehensive and proactive approach to secure file sharing and storage in high-risk environments.

In today's digital world, data security has become one of the most important concerns, especially when it comes to storing and sharing confidential files. With the increase in cyber threats, hacking attempts, and unauthorised access, there is a strong need for systems that can provide safe and controlled access to sensitive information. This project, titled "Geo-Temporal Encrypted File Vault with Secure Access Control and Self-Destruction," is designed to solve these problems by using a smart combination of encryption, location and time-based access, and automatic file deletion after access.



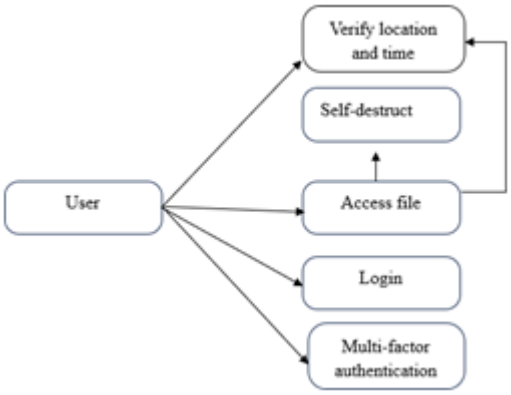
System Architecture

The main idea of this system is to allow users to upload and share files that can be accessed only within a specific geographic area and during a specific time period. The system uses Elliptic Curve Cryptography (ECC) to protect the files, and Multi-Factor Authentication (MFA) to make sure only authorised users get access. Once the file is accessed, it gets automatically deleted to prevent any further use or misuse.

II. PROPOSED SYSTEM

The proposed system introduces a robust and intelligent approach to secure file storage by combining geo-fencing, time-based access, advanced encryption techniques, multi-factor authentication, and a self- destruction mechanism. Unlike traditional file vaults, this system enforces spatial and temporal access constraints, allowing users to define the exact location and time window in which a file can be accessed. This significantly reduces the risk of unauthorized access even in cases where credentials are compromised, as access attempts outside the defined conditions are denied or trigger automatic deletion of the file.

To ensure strong encryption, the system utilizes Elliptic Curve Cryptography (ECC) for public-key encryption. ECC is chosen over conventional algorithms like RSA due to its lightweight computational footprint and enhanced security at lower key sizes, making it ideal for deployment in mobile and cloud-based environments. Each file uploaded to the vault is encrypted using ECC before being stored, and the decryption



Use case diagram

keys are securely managed to ensure that even if storage is breached, the contents remain inaccessible without proper authorization.

For user authentication, the system incorporates Multi-Factor Authentication (MFA), requiring a combination of a password and a dynamically generated One-Time Password (OTP) sent via email or SMS. This prevents unauthorized users from gaining access through password-based attacks alone. Upon successful authentication, the system validates the user's current geolocation (via GPS or IP address) and system time against the predefined access conditions set by the file owner. If the conditions are met, access is granted; otherwise, access is blocked and logged.

To enhance accountability and monitoring, the system logs critical access details such as timestamp, IP address, GPS coordinates, and user identity. These logs are then securely transmitted to the file owner for auditing. This not only helps in tracking legitimate usage but also allows administrators to detect anomalies or unauthorized access attempts in real-time. In case of any suspicious activity, the system is designed to notify the owner immediately and initiate preconfigured defensive actions.

A standout feature of the proposed system is the self-destruction mechanism.

Files are automatically and permanently deleted after a successful access or upon the detection of policy violations, such as multiple failed login attempts or access outside authorized parameters. This eliminates the risk of residual data exposure and ensures that sensitive files are never left vulnerable post-access. This holistic design makes the system highly suitable for secure data handling in industries where confidentiality, accountability, and limited-time access are mission-critical.

FIG 1: Architecture diagram

Fig 1 This layered architecture diagram represents the functional flow of a secure geo-temporal file vault system, structured into four main layers: User Layer, Application Layer, Service Layer, and Storage Layer.

At the top of the architecture, the User Layer comprises the end user who interacts with the system. The user initiates request such as uploading, accessing, or deleting files through the interface provided by the Application Layer. This layer handles the encryption and decryption of files based on access policies and serves as the central control hub for user operations.

The Service Layer plays a crucial role in enforcing access control. It includes two main components: one responsible for Credential Validation and Multi-Factor Authentication (MFA), and another for capturing and sending geolocation and time-based data. These services ensure that file access requests are authenticated and authorized based on the user's identity, location, and time constraints.The Storage Layer contains components that manage the actual file operations, such as decryption and deletion. Files are only decrypted or deleted once proper validation is received from both the Application and Service Layers.

The diagram illustrates the flow of data and control through various layers, starting from user interaction, flowing through authentication and access validation services, and ultimately reaching the secure storage system. This architecture ensures a highly secure, context-aware, and user-validated access control model, emphasizing data confidentiality, integrity, and traceability. The architecture diagram of the Geo- Temporal Encrypted File Vault illustrates the interaction between users, the web interface, backend server, and the database.

III. CONCLUSION AND FUTURE ENHANCEMENT

The Geo-Temporal Encrypted File Vault with Secure Access Control and Self-Destruction provides a comprehensive and intelligent solution to the growing need for secure, context-aware data access. By integrating geofencing and time-based restrictions with strong cryptographic techniques such as Elliptic Curve Cryptography (ECC), the system ensures that sensitive files are accessible only under strictly defined conditions. Multi-factor authentication (MFA) and access logging further strengthen the system by adding layers of user verification and auditability.

The implementation of a self-destruction mechanism sets this system apart from traditional vaults, automatically deleting files after access or upon policy violations to prevent unauthorized use and data leakage. This makes the system ideal for high-security environments where data confidentiality, limited-time availability, and traceability are critical. The combination of a responsive front-end (HTML & Bootstrap) and a robust backend (Java & MySQL) ensures both usability

FIG 2: Use case diagram

Fig 2 The use case diagram in Figure 4.2 illustrates the core interactions between the user and the geo-temporal file vault system. It highlights five primary actions the user can perform: Login, Multi-Factor Authentication, Access File, Verify Location and Time, and Self-Destruct. This diagram effectively represents the functional requirements from the user's perspective, showing what tasks the user is expected to initiate and what validations or responses the system must execute in return.

The first step in the use case flow begins with the Login action. Once the user attempts to access the system, their credentials are validated. Following this, the system enforces Multi-Factor Authentication (MFA) to enhance security. MFA typically involves verifying a secondary factor, such as a One-Time Password (OTP) sent to the user's registered email or mobile number. This step ensures that even if basic login credentials are compromised, unauthorized access can still be prevented.

After successful authentication, users are allowed to initiate the Access File use case. This action involves requesting access to encrypted data stored within the system. Before granting access, the system evaluates several access control policies, including user roles, access time, and location constraints. Only users meeting all required security conditions are permitted to download, view, or decrypt the file. This tightly controlled access ensures that sensitive data remains protected from unauthorized usage.

One of the system’s key innovations is the Verify Location and Time use case. When users request to access a file, the system simultaneously checks their current geolocation and whether the request occurs within the allowed time window. This adds an additional contextual security layer, preventing access outside authorized geographic zones or time frames. It aligns with the platform’s objective to enhance file security using geo-temporal policies.

Another promising enhancement is the use of blockchain technology for immutable logging, ensuring that access logs cannot be altered or deleted, thereby strengthening auditability. Additionally, the system can be expanded to support cloud-based storage with encrypted synchronization across devices, allowing secure access on multiple platforms while maintaining geo-temporal restrictions. Implementing AI-based anomaly detection can also enhance system intelligence by identifying suspicious access patterns in real time.

Lastly, a mobile application version could be developed to enable secure, on-the-go access with GPS integration and push-based MFA.

These enhancements would elevate the system from a secure file vault to a dynamic, scalable, and intelligent data protection platform suitable for evolving cybersecurity demands. The successful implementation of this system demonstrates the effectiveness of combining contextual access control with advanced encryption in modern cybersecurity solutions.

Traditional access control models focus solely on identity verification, whereas this project introduces the critical dimension of where and when data can be accessed. By enforcing geo-temporal policies, the vault system mitigates risks associated with stolen credentials, remote attacks, and insider threats—ensuring that even authorized users cannot access files outside of designated conditions.

Moreover, the system emphasizes user accountability and transparency through real-time access logging and secure notification mechanisms. These features are vital in environments where regulatory compliance, data ownership, and traceability are non- negotiable, such as legal firms, military departments, and healthcare institutions. The inclusion of the self- destruction mechanism further enhances security by ensuring that data does not persist longer than intended, eliminating the threat of residual exposure.

Looking ahead, as data threats continue to evolve, this project serves as a foundation for building more adaptive, intelligent, and policy-driven security solutions. With the growing adoption of edge computing, IoT, and hybrid work environments, there is a strong need for security systems that not only encrypt data but also understand the context in which it is accessed. The Geo- Temporal File Vault paves the way for such systems, and its future iterations can embrace more dynamic controls, AI-based threat prediction, and cross-platform operability to serve both individuals and organizations in an increasingly connected world.

REFERENCES

[1] Yahya, F. – Geofencing for Access Control: Setting Digital Boundaries. Retrieved from https://faisalyahya.com/access-control/geofencing-for-access-control-setting-digital-boundaries/

[2] Hexnode MDM – Geofencing - Location based MDM restriction. Retrieved from https://www.hexnode.com/mobile-device-management/help/geofencing-location-based-mdm-restriction/

[3] Geoplugin – Geofencing Time Clock Explained: Everything You Need To Know. Retrieved from https://www.geoplugin.com/resources/geofencing-time-clock-explained-everything-you-need-to-know/

[4] Amster, H. and Diehl, B. – Against Geofences, Stanford Law Review, 74, 385, 2022.

[5] U.S. Patent No. 12,052,573 B2 – Systems and Methods for Mitigating Fraud Based on Geofencing, 2023. Retrieved from https://patents.google.com/patent/US120525732

[6] Wang, H., et al. – Privacy Preserving Spatio-Temporal Attribute-Based Encryption for Cloud-Based Applications, Cluster Computing, 2024. https://doi.org/10.1007/s10586- 024-04696-w

[7] NIST – Security and Privacy Controls for Information Systems and Organizations (SP 800-53 Rev. 5), National Institute of Standards and Technology, 2020.

[8] Temporal Technologies – Security Model - Temporal Cloud. Retrieved from https://docs.temporal.io/cloud/security

[9] Geambasu, R., et al. – New Directions for Self-Destructing Data Systems, Columbia University, 2011. Retrieved from https://roxanageambasu.github.io/publications/vanish-extensions-techreport11.pdf

[10] Zhang, Y., et al. – Secure File Sharing in Cloud Computing Using Elliptic Curve Cryptography, 2023. ResearchGate.

[11] Kumar, A., et al. – Secure Files Using Secure Hash Algorithm and Elliptical Curve Cryptography, International Journal of Science and Technology, 2025.

[12] Wikipedia – Elliptic-curve cryptography. Retrieved from https://en.wikipedia.org/wiki/Ellipticcurve_cryptography

[13] IJESR – ECC Based File Security in Cloud Applications, 2024. Retrieved from https://www.ijesr.org

[14] Stack Exchange – Can elliptic curve (25519) be used to encrypt file?. Retrieved from https://crypto.stackexchange.com/

[15] HashiCorp – Enable Multi Factor Authentication (MFA) Login | Vault. Retrieved from https://developer.hashicorp.com/vault/

[16] Auto RABIT – Setting Up Multifactor Authentication in Vault. Retrieved from https://knowledgebase.autorabit.com/

[17] OWASP – Multifactor Authentication Cheat Sheet. Retrieved from https://cheatsheetseries.owasp.org/

[18] Super User – Encrypting Files with 2FA. Retrieved from https://superuser.com/

[19] IJEIT – Self Destruction Model for Protecting Data in Cloud Storage, International Journal of Engineering and Innovative Technology, 2016.

[20] David Sklar – Learning PHP, 2nd Edition, O'Reilly Media, 2016.

[21] Alan Forbes – The Joy of PHP: A Beginner's Guide to Programming Interactive Web Applications with PHP and MySQL, 2013.

[22] Paul DuBois – MySQL, 5th Edition, Addison-Wesley, 2013.

[23] Seyed M.M. Tahaghoghi and Hugh Williams – Learning MySQL, O'Reilly Media, 2006.

[24] Jay Greenspan and Brad Bulger – MySQL Weekend Crash Course, Wiley, 2003.

[25] Michael Kofler – The Definitive Guide to MySQL 5, Apress, 2005.

[26] Ben Forta – MySQL Crash Course, Sams Publishing, 2005.

[27] Jacob Lett – Bootstrap 5 Quick Start: Responsive Web Design and Development Basics, Bootstrap Creative, 2021.

[28] Mark Price – Bootstrap 5: Learn the Newest Version of Bootstrap, Independently published, 2021.

[29] David Cochran and Ian Whitley – Foundation Bootstrap, Peachpit Press, 2012.

[30] Syed Fazle Rahman – Responsive Web Design with Bootstrap, Packt Publishing, 2015.

[31] Jake Spurlock – Bootstrap: Responsive Web Development, O'Reilly Media, 2013.

[32] David F. Ferraiolo, D. Richard Kuhn, and Ramaswamy Chandramouli – Role-Based Access Control, Artech House, 2003.

[33] Ravi Sandhu et al. – Role-Based Access Control Models, ACM Computing Surveys, Vol. 35, No. 3, 2003.

[34] Messaoud Benantar – Access Control Systems: Security, Identity Management and Trust Models, Springer, 2006.

[35] Ninghui Li and Ziqing Mao – Administration in Role-Based Access Control, IEEE Computer Security Foundations Workshop, 2007.

[36] Gligor, Virgil D., et al. – On the Formal Definition of Separation-of-Duty Policies and their Composition, IEEE Symposium on Security and Privacy, 1998.

[37] Messaoud Benantar – Access Control Systems: Security, Identity Management and Trust Models, Springer, 2006.

[38] David Ferraiolo and D. Richard Kuhn – A Role-Based Access Control Model, NIST, 1992.
[39] Ravi Sandhu – Engineering Authority and Trust in Cybersecurity, Springer, 2013.
[40] Ronald Leenes, Rosamunde van Brakel, Serge Gutwirth – Digital Privacy: Theory, Technologies, and Practices, Springer, 2008.