International Journal on Science and Technology (IJSAT)
E-ISSN: 2229-7677 ● Website: www.ijsat.org ● Email: editor@ijsat.org

High Security Vault for Financial and Legal Documents using AES-GCM Encryption and Custom Multi-factor Authentication

Andrew Rabin D[1], S Annie Angeline Preethi[2]

[1]U.G Student, Department of Electronics and Communication, Sathyabama Institute of Science and Technology, Chennai
[2]Professor, School of Electrical and Electronics, Sathyabama Institute of Science and Technology, Chennai.

Abstract
The **High-Security Vault** is a sophisticated system designed to securely store and manage sensitive documents using advanced encryption, continuous monitoring, and a robust authentication framework. Utilizing AES-GCM encryption, it ensures data confidentiality and integrity, safeguarding against unauthorized access and tampering. Real-time monitoring actively observes stored data, instantly detecting and reporting unauthorized changes to maintain reliability. The authentication process combines two-factor methods, including password-based and one-time verification, with personalized, time-sensitive questions for added security. Its core innovation lies in behavioral biometrics, analyzing user interaction patterns such as typing speed, keypress dynamics, timing patterns, mouse movement linearity, and user-specific input preferences like capitalization and form submission. By integrating encryption, monitoring, and behavioral authentication, the High-Security Vault delivers a secure, adaptable system that effectively protects sensitive information and ensures data integrity.

I. INTRODUCTION

In today's digital landscape, protecting sensitive information has become a paramount concern as cyber threats grow in frequency and sophistication. Financial and legal documents, which often contain critical and confidential information, are especially vulnerable to breaches, tampering, and unauthorized access. These challenges demand advanced security solutions that not only ensure safe data storage but also actively monitor and control access. Traditional security measures, though partially effective, often fall short against the complexity of modern threats, necessitating innovative approaches that prioritize data integrity, confidentiality, and proactive defense.

This paper introduces the High-Security Vault, a sophisticated system designed to redefine secure document storage. At its core, the vault employs AES-GCM (Advanced Encryption Standard in Galois/Counter Mode), a cryptographic standard known for robust encryption and data authenticity. This encryption safeguards stored documents against unauthorized access and malicious modifications, forming a strong foundation for digital security. Complementing this is a real-time monitoring mechanism that actively tracks changes to stored data, flagging unauthorized activities and enabling swift responses to potential threats.

The High-Security Vault goes beyond conventional security methods by integrating a multi-layered authentication framework. This includes two-factor authentication (2FA) with password verification and one-time codes, along with personalized, time-sensitive questions. Its true innovation lies in its behavioral biometrics module, which leverages user-specific interaction patterns for advanced authentication. This module evaluates typing speed, keypress dynamics, mouse movements, and input preferences, creating a unique behavioral profile for each user to ensure access is granted only to legitimate individuals, significantly reducing impersonation risks.

This paper explores the architecture, design, and functionality of the High-Security Vault, highlighting how its integration of cutting-edge encryption, proactive monitoring, and innovative behavioral authentication provides a comprehensive solution to modern data security challenges. By addressing vulnerabilities in existing systems and offering adaptive defenses, the vault sets a new benchmark for securing sensitive information in an increasingly interconnected world

II. LITERATURE REVIEW

The protection of sensitive data is a pivotal challenge in cybersecurity, necessitating systems that combine advanced encryption, continuous monitoring, and robust authentication mechanisms. Recent advancements in these domains have inspired innovative solutions for securing critical financial and legal documents.

Zhao and Wang [1] emphasized the role of behavioral analysis in cybersecurity, particularly in detecting anomalous user activities to prevent unauthorized access. Their findings underline the necessity of continuous behavioral monitoring as a core component of modern security systems, adaptable to evolving threat landscapes. Similarly, Chen and Liu [2] explored multi-layer security strategies for legal document protection, advocating for the integration of encryption and comprehensive authentication protocols. They highlighted AES-GCM encryption as an ideal choice for safeguarding data due to its dual functionality of ensuring confidentiality and integrity.

Kim and Park [3] focused on time-sensitive security mechanisms in financial systems, demonstrating the efficacy of temporal constraints in mitigating risks. Their work emphasized real-time monitoring and immediate anomaly detection, crucial for safeguarding sensitive data during storage and access. Complementing these insights, Chen and Zhao [4] presented an in-depth review of behavioral biometrics techniques, such as keystroke dynamics and mouse movement analysis, showcasing their potential to create unique user profiles for continuous authentication. The study highlighted the scalability and effectiveness of behavioral biometrics in preventing unauthorized access.

Kumar and Gupta [5] investigated advancements in encryption techniques for secure digital storage, emphasizing the necessity of efficient, high-performance cryptographic methods like AES-GCM for securing large datasets. Additionally, Patel and Soni [6] explored the role of behavioral biometrics in continuous authentication systems, providing evidence of their adaptability and effectiveness in detecting unauthorized activities in real-time. Finally, Bhattacharya and Ray [10] demonstrated the critical role of AES-GCM encryption in ensuring document integrity and secure storage, reinforcing its utility in high-security systems.

The High-Security Vault synthesizes these foundational studies to provide a comprehensive solution for securing sensitive documents. It incorporates AES-GCM encryption for robust protection and data integrity, as highlighted by Chen and Liu [2] and Kumar and Gupta [5]. Inspired by Zhao and Wang [1] and Patel and Soni [6], the vault integrates behavioral biometrics to enhance authentication, leveraging

user interaction patterns for advanced security. Building on Kim and Park's [3] work, real-time monitoring and anomaly detection systems ensure timely responses to potential breaches, while insights from Chen and Zhao [4] enable the development of a scalable and adaptable authentication framework.

By drawing on these contributions, the High-Security Vault addresses critical vulnerabilities in data security, offering an innovative and adaptive solution for protecting financial and legal documents in an increasingly complex cybersecurity landscape.

III. WORKING OF VAULT

The High-Security Vault is a highly secure system designed to store, monitor, and protect sensitive financial and legal documents from unauthorized access, data tampering, and cyber threats. It employs advanced encryption, robust multi-factor authentication, and behavioral biometrics to establish a comprehensive security framework. Operating on the principle of layered security, the vault ensures that even if one layer is breached, subsequent layers provide strong defenses. Real-time file integrity monitoring and a failsafe mechanism safeguard data by creating secure backups and formatting compromised vaults.

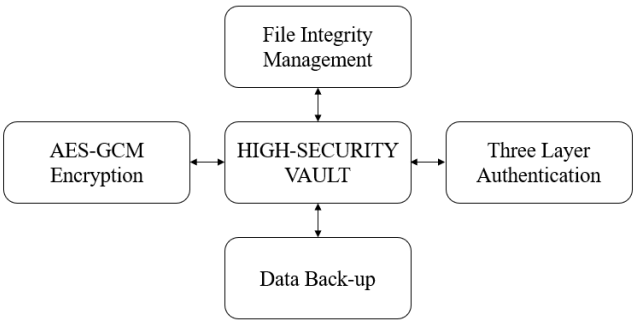

Fig. 1 Integral Components of the High Security Vault

The vault comprises four key components: AES-GCM Encryption, Three-Layer Authentication, File Integrity Management, and Data Backup. AES-GCM Encryption ensures data confidentiality and integrity during storage and transmission. Three-Layer Authentication enhances access security by combining multiple verification methods, reducing the risk of unauthorized access. File Integrity Management continuously monitors and detects unauthorized data modifications, while the Data Backup feature ensures critical data recovery in case of breaches or failures. Together, these components provide a secure, resilient, and efficient solution for protecting sensitive information.

A. FILE INTEGRITY MONITORING

File integrity monitoring is a vital feature of the High-Security Vault, designed to detect and report any unauthorized changes to stored data. Each file is hashed using a secure cryptographic algorithm, creating unique digital fingerprints. These hashes allow the system to detect even the slightest alterations.

At regular intervals or during access attempts, the system recalculates file hashes and compares them to the original values. Any mismatch indicates tampering, prompting instant alerts to notify users and provide details about the potential threat.

The vault includes a failsafe mechanism for critical breaches. If tampering or unauthorized access poses a significant risk, the system automatically formats the vault. Before doing so, it creates an encrypted backup in an isolated location, ensuring users can recover their data securely. This combination of monitoring, al-

erting, and failsafe mechanisms ensures data integrity and robust security.

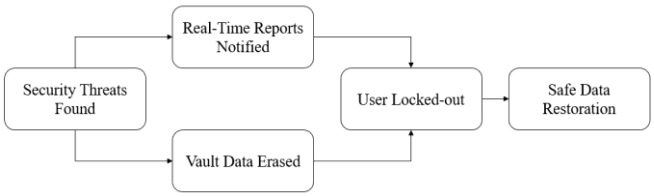

Fig. 2 Threat Response of File Integrity Monitoring

Upon detecting a breach, the File Integrity Management system takes immediate action. It generates real-time alerts to notify users and administrators, activates a user lockout to prevent further unauthorized access, and enforces data erasure to eliminate risks. Once the threat is resolved, the system restores data securely from encrypted backups, ensuring sensitive information is protected without compromise. This proactive strategy enhances resilience and operational reliability.

B. AES-GCM ENCRYPTION

AES-GCM (Advanced Encryption Standard with Galois/Counter Mode) is a widely recognized encryption technique that combines AES's robust security with GCM's ability to ensure both confidentiality and integrity. This dual functionality not only encrypts data but also detects unauthorized modifications, making it essential for safeguarding sensitive information. Its high performance enables efficient encryption even for large datasets, making it suitable for real-time applications. In the High-Security Vault, AES-GCM ensures the secure storage and transmission of financial and legal documents, providing resilience against modern cryptographic attacks and guaranteeing data integrity.

AES-GCM encrypts data in 128-bit blocks using a symmetric key, meaning the same key is used for encryption and decryption. Its key advantage lies in authenticated encryption, where data confidentiality is coupled with integrity verification. This is achieved through an authentication tag—a cryptographic hash generated during encryption—that ensures data remains unaltered during storage or transmission.

The counter-based mechanism in AES-GCM enables parallel processing, making it highly efficient for encrypting large data volumes, such as those in cloud storage or secure management systems like the High-Security Vault. When data is accessed, the authentication tag is verified. Any mismatch indicates tampering, ensuring only authentic documents are accessible, which is critical for protecting sensitive financial and legal records.

AES-GCM is designed for high efficiency, minimizing performance overhead while maintaining robust security. This ensures fast encryption and decryption, balancing user experience and data protection. Its adaptability to real-time systems makes it an ideal choice for securing the High-Security Vault, where speed and reliability are crucial.

In summary, AES-GCM encryption is integral to the High-Security Vault's ability to protect sensitive data. By ensuring confidentiality, integrity, and performance, it fortifies the system against unauthorized access, tampering, and corruption, delivering trust and reliability to users.

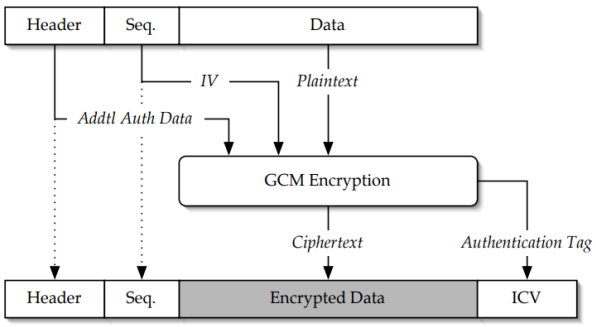

Fig. 3 AES-GCM Encryption

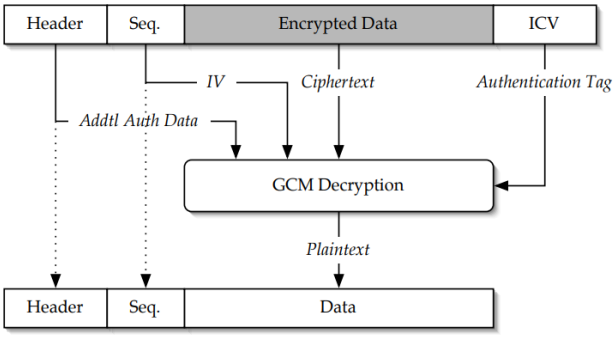

Fig. 4 AES-GCM Decryption

C. TWO-FACTOR AUTHENTCATION

Two-factor authentication (2FA) is a critical security feature in the High-Security Vault that adds an extra layer of protection for sensitive financial and legal documents. It combines two factors: something the user knows (a password) and something the user has (an app-based authenticator, like Google Authenticator). This dual-layer mechanism significantly reduces the risk of unauthorized access, even if one factor is compromised.

The 2FA process begins with the user entering their username and password, which serves as the first authentication layer. Once the password is verified, the system requires a one-time passcode (OTP) generated by the user's authentication app. This OTP is time-sensitive and must be entered within a brief window, ensuring that even if an attacker obtains the code, it quickly becomes invalid.

App-based 2FA enhances security and convenience, as users typically carry their smartphones and can access the authenticator app easily. Unlike email-based 2FA, app-based authentication avoids potential delays or vulnerabilities associated with email systems while providing an equally secure second factor.

In addition to strengthening access control, app-based 2FA supports monitoring and detecting suspicious login attempts, such as repeated failures or logins from unusual locations. Administrators can use this data to identify potential threats and bolster the system's defenses.

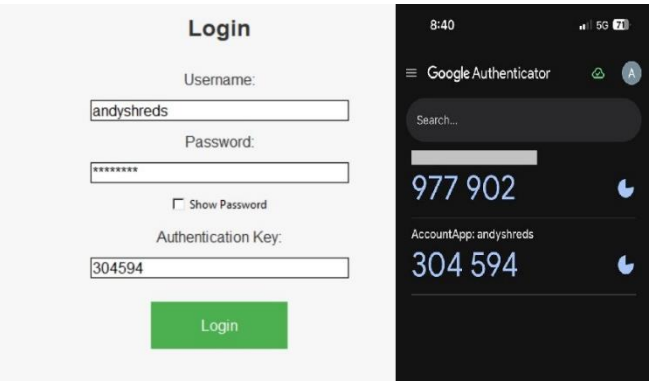

Fig. 5 Two Factor Authentication

In summary, app-based two-factor authentication significantly enhances the security of the High-Security Vault. By combining password protection with a time-sensitive OTP generated on the user's device, the system ensures robust protection of sensitive documents without compromising user convenience..

D. TIME-SENSITIVE AUTHORIZATION

The authentication process advances once the user successfully completes password verification and two-factor authentication (2FA) via email. Following these initial layers, the system transitions to the time-sensitive personalized questions stage, where the user is presented with pre-configured questions tailored to their unique personal information. These questions span diverse topics, from professional details to personal experiences, ensuring they are specific to the user and challenging for unauthorized individuals to predict or discover.

A defining feature of this stage is the strict time limit for answering these questions. Users must respond correctly within the allotted time frame, ensuring active engagement and preventing attackers from delaying responses or attempting to manipulate the system. Failure to answer correctly or within the time limit results in access denial, adding another layer of protection against unauthorized attempts.

This time-sensitive approach offers a significant advantage over static security questions, which can often be guessed or researched. By enforcing a short response window, the system ensures users rely on quick recall, making it nearly impossible for an attacker to look up answers. The carefully designed questions are meaningful and easy for the legitimate user to remember but difficult for others to deduce, enhancing security.

Beyond its security benefits, this method provides a user-friendly experience by leveraging the user's existing knowledge rather than requiring complex passwords or advanced biometrics. Moreover, the answers are securely stored and never transmitted during login attempts, safeguarding them from interception or theft.

Time-sensitive personalized questions not only bolster security but also enhance the user experience, ensuring that only the rightful user, with prior knowledge of these questions, can access sensitive documents. This innovative mechanism plays a critical role in reinforcing the overall protection of financial and legal documents within the High-Security Vault.

E. BEHAVIORAL BIOMETRIC ANALYSIS

Behavioral biometric analysis is a key innovation in the High-Security Vault's authentication system, leveraging users' unique interaction patterns with keyboards and mice to provide a dynamic and adaptive security layer. Unlike static methods like passwords or OTPs, this approach continuously analyzes natural behaviors, making it highly resistant to replication and automated attacks.

Keystroke dynamics captures typing characteristics such as timing, rhythm, and keypress durations, while bot-like input verification identifies unnatural patterns like overly linear mouse movements or irregular keystrokes, flagging suspicious activity. Together, these components enhance security by detecting unauthorized or automated access attempts while maintaining a seamless user experience.

KEY-STROKE DYNAMICS refers to the study and analysis of an individual's typing patterns. Every user has a distinctive way of typing, shaped by factors such as muscle memory, typing habits, and cognitive tendencies. By analyzing these patterns, the vault creates a unique biometric profile for each user, which becomes a critical aspect of the authentication process.

The system records and analyzes several parameters to develop a comprehensive keystroke profile:

Typing Speed: The number of characters a user types per minute, which reflects their overall familiarity with typing and their typical pace.

Key Hold Duration: The time a key is pressed before being released, providing insights into the user's typing rhythm.

Inter-Key Latency: The time interval between successive keystrokes, which varies significantly between individuals.

Error Correction Patterns: The user's behavior when correcting mistakes, such as using the backspace key or typing sequences like "Ctrl + Z".

Transition Patterns: Specific patterns during typing, such as the tendency to press the space bar with one thumb or the other.

During the enrollment phase, the system prompts users to complete typing tasks, recording their keystroke data to establish a baseline profile. Each subsequent login attempt involves collecting real-time typing data and comparing it with the stored profile. The comparison employs advanced machine learning algorithms to identify subtle deviations that could indicate unauthorized access attempts.

Non-Intrusive: The analysis runs seamlessly in the background without requiring additional hardware or explicit actions from the user.

Difficult to Forge: Typing patterns are unique and challenging for attackers to mimic, even with prior knowledge of the user's behavior.

Dynamic Adaptation: The system refines its understanding of the user's typing patterns, accommodating natural variations.

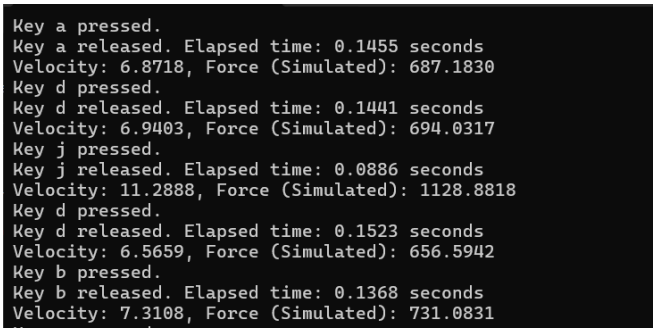

Fig. 6 Analyzing Keystroke Velocity

The keystroke dynamics module is integrated with additional safeguards, such as anomaly detection. If the system detects abnormal behavior—such as unusually fast typing—it flags the activity for further scrutiny, potentially prompting a reauthentication process or notifying the user of suspicious activity.

BOT-LIKE INPUT VERIFICATION mechanism focuses on distinguishing human inputs from automated scripts, which are often used to bypass authentication systems. By analyzing both mouse and keyboard interactions, the system ensures that access attempts originate from genuine users.

***Movement Patterns*:** Human mouse movements are irregular, with varying speeds and directions, unlike the linear and uniform patterns generated by bots.

***Click Timing**:* Human clicks are naturally inconsistent, often influenced by decision-making or reflexes, whereas bots execute clicks with minimal delays.

Navigation Keys: Observes the user's use of keys such as Tab, Enter, or arrow keys during form navigation, ensuring it aligns with natural human behavior. Bots often fail to replicate the erratic yet purposeful switching between keyboard and mouse typical of humans.

```
Mouse moved to (1543, 982)
Mouse moved to (1543, 982)
Mouse moved to (1544, 982)
Mouse moved to (1544, 982)
Mouse moved to (1545, 982)
Mouse moved to (1546, 982)
Mouse moved to (1546, 982)
Mouse moved to (1547, 982)
Mouse moved to (1547, 982)
Mouse moved to (1548, 982)
Mouse moved to (1548, 982)
Mouse clicked at (1548, 982) with Button.left
```

Fig. 7 Capturing Mouse Movements with Inputs

The mouse and keyboard data are cross-referenced with the keystroke dynamics to create a comprehensive behavioral profile. Any anomalies in either input type raise suspicion, prompting additional security measures or outright denial of access.

By combining these components, the behavioral biometric system creates an adaptive and resilient authentication framework. It continuously learns from user interactions, making it increasingly effective at distinguishing legitimate users from impostors. Moreover, this layered approach ensures that even if one factor is compromised, the overall security remains intact.

IV. RESULTS AND DISCUSSION

The High-Security Vault for Financial and Legal Documents demonstrates a comprehensive and innovative approach to safeguarding sensitive data. Integrating features like advanced encryption, multi-layered authentication, and behavioral biometrics, the vault prioritizes not only security but also user convenience. These results are just part of the vault's broader capabilities, which include real-time file integrity monitoring, scalability, and adaptability to diverse use cases, making it a versatile and future-ready solution.

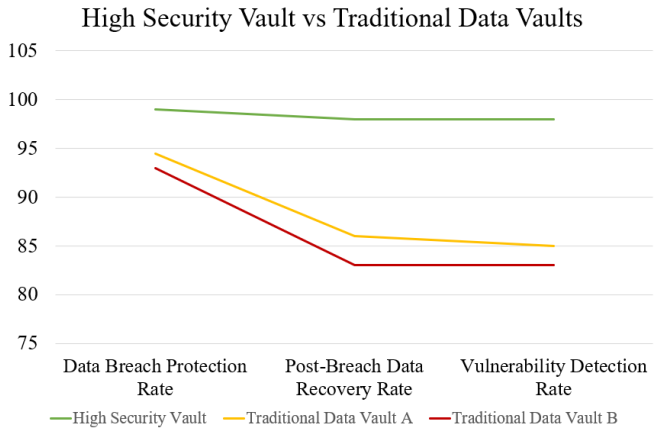

Fig. 8 Efficiency Comparison between the High Security Vault and a Traditional Data Vault

An AI-powered analysis of the comparative performance between the High-Security Vault and traditional vaults (Vault A and Vault B), as illustrated in the graph, highlights the vault's superiority across three critical metrics—Data Breach Protection Rate, Post-Breach Data Recovery Rate, and Vulnerability Detection Rate. The AI evaluated the performance metrics, revealing the vault's near-perfect Data Breach Protection Rate, which underscores its robust encryption and authentication layers, far exceeding the declining performance of the other vaults. Its advanced recovery mechanisms and continuous monitoring ensure rapid post-breach recovery and proactive vulnerability detection, showcasing its resilience and effectiveness in mitigating complex threats.

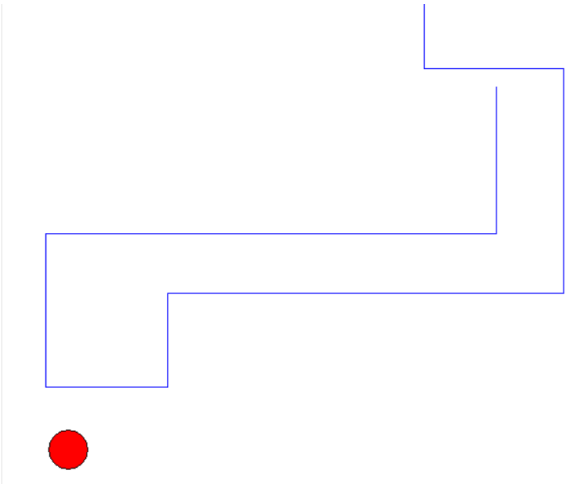

Fig. 9 Artificial bot-like Mouse movements simluated to verify vault's Flagging capabilities

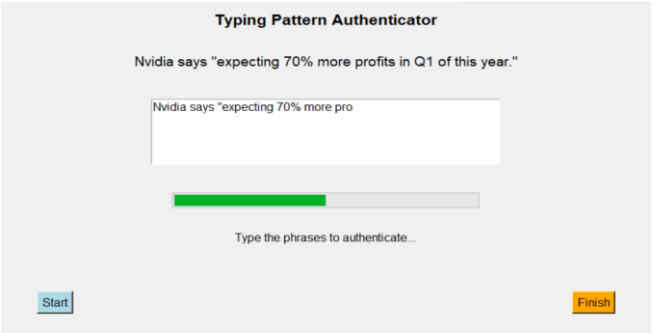

Fig. 10 Verifying the user based on their Typing Behavioral Pattern Analysis

The mouse simulation test further validates the vault's behavioral biometrics, simulating bot-like actions to test its ability to distinguish between human and automated behaviors. The vault successfully flagged these interactions, reinforcing its capability to counter unconventional attack patterns. Similarly, the Typing Pattern Authenticator, another standout feature, analyzes users' typing behavior to enhance authentication security. By monitoring typing speed and rhythm, it creates a unique behavioral profile that's challenging to replicate, providing an added layer of defense while maintaining an intuitive user experience. Combined, these results highlight the vault's exceptional performance while emphasizing its full suite of functionalities.

Real-time file integrity monitoring further strengthens the security of the system by constantly checking for any unauthorized changes to the stored documents. This proactive approach ensures that sensitive documents remain safe and secure, providing users with peace of mind regarding the integrity of their data. The time-sensitive personalized questions offer an intuitive and personalized authentication experience, enhancing both security and user convenience.

In conclusion, the High-Security Vault for Financial and Legal Documents provides a comprehensive, multi-faceted approach to securing sensitive information. The integration of AES-GCM encryption ensures that data is protected with state-of-the-art cryptography, while the multi-layered authentication system, comprising traditional passwords, two-factor authentication, and time-sensitive personalized questions, adds an extra layer of security. Behavioral biometrics plays a pivotal role in ensuring continuous authentication by monitoring user behavior and detecting any anomalies, making it difficult for attackers to bypass the system even after gaining initial access.

V. FUTURE WORK.

The current High-Security Vault provides strong protection for financial and legal documents, but several enhancements can improve its scalability, adaptability, and user experience.

First, optimizing the storage management system will enable the vault to handle larger volumes of data, making it more suitable for businesses managing high volumes of sensitive information. Additionally, refining the behavioral biometrics analysis with machine learning models can improve accuracy by better adapting to evolving user patterns and reducing false negatives.

To strengthen the system's resilience against cybersecurity threats, we plan to implement automated integrity checks and periodic penetration testing. These measures will proactively detect vulnerabilities and ensure system security.

We also aim to introduce dynamic, activity-based time-sensitive questions for user verification, increasing adaptability and security. Furthermore, adding offline access with secure local storage will provide uninterrupted access to critical data during network outages.

Finally, enhancing user experience and administrative controls through detailed analytics and user-friendly dashboards will make the system easier to manage and monitor.

In summary, future work will focus on improving scalability, adaptive biometrics, proactive security checks, dynamic user verification, offline access, and administrative features to ensure the vault remains secure, efficient, and user-friendly.

REFERENCES

1. L. Zhao and Y. Wang, "Behavioral Analysis in Cybersecurity: Current Trends and Future Directions," Journal of Cybersecurity Research, vol. 18, no. 4, pp. 210-227, 2021.

2. Y. Chen and H. Liu, "Multi-Layer Security Approaches in Legal Document Protection," Journal of Legal Studies, vol. 33, no. 2, pp. 110-128, 2021.
3. S. Kim and J. Park, "Time-Sensitive Security Mechanisms in Financial Systems," Journal of Financial Technology, 2023.
4. X. Chen and Y. Zhao, "Behavioral Biometrics in Multi-Factor Authentication Systems," Journal of Cybersecurity Research, vol. 15, no. 1, pp. 45-62, 2023.
5. A. Kumar and R. Gupta, "Advances in Encryption and Security in Digital Storage Systems," Journal of Information Security and Applications, vol. 52, pp. 102487, 2020.
6. S. Patel and A. Soni, "Behavioral Biometrics for Continuous Authentication in Secure Systems," Journal of Information Privacy and Security, vol. 18, no. 3, pp. 218-230, 2022.
7. S. Singh and S. Bansal, "Securing Sensitive Documents in Digital Storage: A Survey on Encryption Techniques," International Journal of Computer Science and Engineering, vol. 9, no. 5, pp. 201-215, 2021.
8. S. Dey and A. Banerjee, "Behavioral Biometrics for Secure Authentication: Challenges and Future Directions," Journal of Cyber Security Technology, vol. 5, no. 1, pp. 22-39, 2021.
9. X. Tang and Y. Zhou, "Enhancing Security and Usability in Financial Systems with Multi-Factor Authentication," Financial Technology Journal, vol. 34, no. 2, pp. 102-119, 2021.
10. S. Bhattacharya and P. Ray, "Leveraging AES-GCM for Secure Document Storage and Integrity Monitoring," Journal of Digital Security, vol. 8, no. 2, pp. 112-124, 2020.
11. Z. Ahmed and H. Malik, "A Review on Multi-Layered Security Approaches for Legal Document Protection," Journal of Law and Technology, vol. 30, no. 2, pp. 145-160, 2022.
12. J. Lee and T. Kim, "Integration of Behavioral Biometrics and Multi-Factor Authentication for Secure Systems," Computers, Security & Privacy, vol. 32, no. 5, pp. 284-295, 2022.
13. P. Yadav and S. Patel, "File Integrity Monitoring in Secure Systems: Techniques and Applications," Journal of Information Security and Cryptography, vol. 10, no. 3, pp. 98-115, 2020.
14. H. Zhang and Q. Liu, "Continuous Authentication Using Behavioral Biometrics for Secure Systems: A Review," Journal of Computer Security, vol. 21, no. 3, pp. 119-133, 2021.
15. S. Hwang and H. Park, "Time-Sensitive Authentication Techniques in Critical Systems," International Journal of Applied Cryptography, vol. 14, no. 4, pp. 32-49, 2021.
16. C. Johnson and S. Reed, "AES-GCM Encryption for Secure Document Storage and Integrity Verification," Journal of Cryptographic Research, vol. 39, no. 3, pp. 147-160, 2020.