UNALTERED: A FILE INTEGRATION MANAGEMENT SYSTEM

Manoj Ramashish Gupta [1], Rahul Santanu Jana [2], Jigar Bharat Ojha [3] , Dr. Shwetambari Borade[4]

[1]*Student Cyber Security Engineering, Shah and Anchor Kutchhi Engineering College, Mumbai, Maharashtra, India*
[2]*Student Cyber Security Engineering, Shah and Anchor Kutchhi Engineering College, Mumbai, Maharashtra, India*
[3]*Student Cyber Security Engineering, Shah and Anchor Kutchhi Engineering College, Mumbai, Maharashtra, India*
[4]*Guide Cyber Security Engineering, Shah and Anchor Kutchhi Engineering College, Mumbai, Maharashtra, India*

Abstract

In today's interconnected world, where digital data underpins nearly every aspect of modern life, ensuring the integrity and security of files is paramount. This abstract provides a concise yet comprehensive overview of the multifaceted domain of file integrity and security. File integrity is the assurance that data remains unchanged and reliable, essential for maintaining trust and accountability. However, achieving and maintaining file integrity poses numerous challenges, including the ever-evolving threat landscape, complex IT infrastructures, and regulatory compliance mandates. To address these challenges, organizations employ a variety of strategies and technologies. Encryption, access controls, and digital signatures are deployed to protect files from unauthorized access and tampering, while file integrity monitoring (FIM) solutions continuously scrutinize files for any alterations. Moreover, robust security policies, employee training programs, and incident response plans are integral components of a proactive approach to file integrity and security. By fostering a culture of security awareness and investing in advanced technologies, organizations can effectively mitigate risks and safeguard their digital assets.

***Keywords:** Encryption, Fostering, Integrity, Monitoring, tampering, Unauthorized.*

1. INTRODUCTION

In the digital era, where data is the lifeblood of organizations and individuals alike, ensuring the integrity and security of files is not merely a preference but an imperative. In response to this pressing need, our project, Unaltered, presents a robust and multifaceted solution. At its core, Unaltered integrates state-of-the-art encryption algorithms and authentication mechanisms to fortify files against unauthorized access, manipulation, and breaches. By employing cryptographic hashing algorithms, each file is endowed with a unique digital signature, enabling users to verify its authenticity and integrity at any given moment. Furthermore, our platform's encryption capabilities, utilizing industry-standard protocols like AES, serve as an impenetrable barrier against unauthorized viewing or tampering, guaranteeing that only authorized users possess the necessary decryption keys. Complementing these measures, Unaltered incorporates sophisticated access control features, allowing organizations to tailor permissions based on user roles and establish multi-factor authentication protocols to thwart unauthorized entry attempts. Moreover, our system's Realtime monitoring functionalities provide continuous surveillance, promptly flagging any suspicious activities and issuing alerts for immediate action.

1.1 OVERVIEW

File integrity is a cornerstone of data security, ensuring that files remain unchanged and uncorrupted throughout their lifecycle. At its core, file integrity involves verifying that a file has not been altered or tampered with, preserving its accuracy and reliability. This is crucial for maintaining trust in digital information, whether it be financial records, medical data, or intellectual property. Several methods are employed to ascertain file integrity, with cryptographic hashing being a widely used technique. Hash functions generate a unique digital fingerprint, or hash value, for each file based on its contents. Even a minor change to the file will result in a vastly different hash value, making it easy to detect any alterations. This provides a robust mechanism for ensuring the integrity of files, as any unauthorized modifications will be readily apparent. File integrity is not only essential for data accuracy but also for security. Tampering with files can lead to unauthorized access, data breaches, or the dissemination of misinformation. By maintaining file integrity, organizations can mitigate the risks associated with cyber threats and protect sensitive information from exploitation or manipulation.

1.2 MOTIVATION BEHIND STUDY

In today's rapidly evolving technological landscape, ensuring the integrity and security of digital data is paramount. With the increasing frequency of data breaches, cyber-attacks, and stringent regulatory requirements, the motivation behind research in file integrity is undeniably urgent. This drive stems from the critical need for advanced solutions capable of swiftly detecting and preventing unauthorized modifications or tampering within digital files. Central to these efforts is the commitment to safeguarding sensitive data assets, including personal information, financial records, and intellectual property.

2. REVIEW OF LITERATURE

A literature review is essential for understanding key themes, trends, and gaps in research. In the field of file integrity, examining literature reveals advancements in cybersecurity and data authentication techniques. Topics like cryptographic hashing algorithms and encryption methodologies provide insights into fortifying file integrity. This review equips researchers with knowledge to advance data security.

The significance of file integrity monitoring and management systems is highlighted in this research, offering a comprehensive exploration of various strategies and technologies aimed at enhancing data security and integrity. These papers delve into different monitoring approaches, including real-time monitoring, periodic scans, and anomaly detection techniques, each with distinct strengths and limitations. Technologies such as cryptographic hashing algorithms, machine learning, and artificial intelligence are explored to improve accuracy, efficiency, and scalability in detecting unauthorized changes. Discussions also encompass considerations like scalability, system performance, security measures like encryption and access controls, integration with compliance frameworks, challenges like false positives and resource utilization, and future research directions. This emphasis underscores the ongoing advancements and importance of file integrity monitoring and management research.

3. PROPOSED SYSTEM

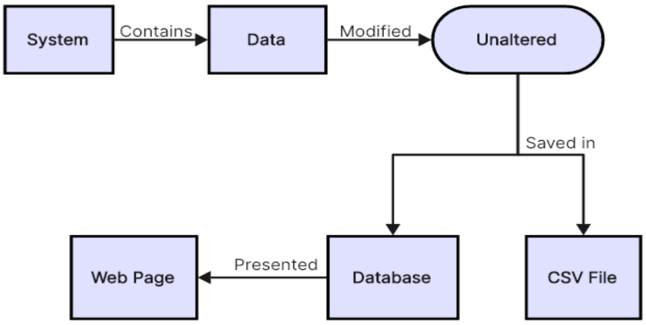


Figure 3. 1 Block Diagram

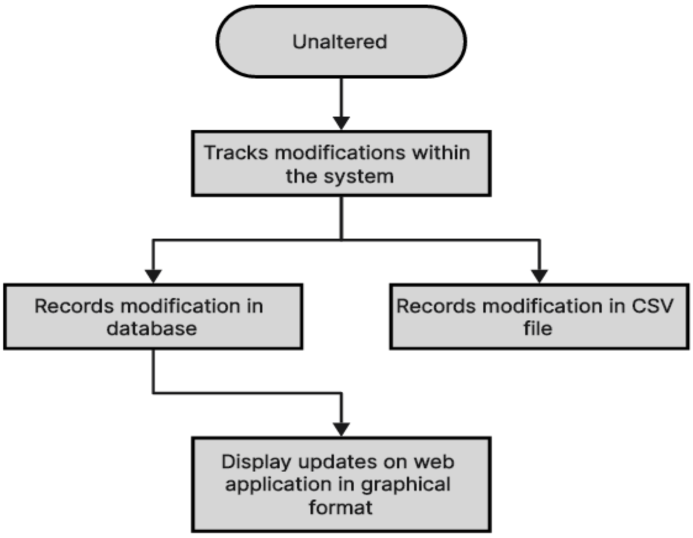

Unaltered
Tracks modifications within the system
Records modification in database
Records modification in CSV file
Display updates on web application in graphical format

Figure 3. 2 Dataflow Diagram

3.1 METHODOLOGY

To implement the above goals, we need to follow the methodology below:

1. Specifying the application and various components of the architecture.
2. Specifying the database connectivity to the application.
3. Specifying the connection between database and app to show the event logs.
4. Statistics: Extracting the data required for analysis of system admin.

3.2 CONCLUSION

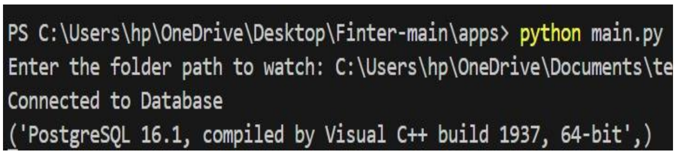
In conclusion, the activity diagram, block diagram, and data flow diagram offer a comprehensive visual depiction of the project's workflow, system architecture, and data flow. These diagrams facilitate a clear understanding of the project's structure and processes, improving communication among stakeholders and aiding in project development and management. By leveraging these diagrams, the project team can identify potential bottlenecks, areas for improvement, and issues in advance, thus reducing risks and optimizing project performance. Ultimately, the activity diagram, block diagram, and data flow diagram are indispensable tools for project planning, development, and management, playing a vital role in achieving project goals and objectives effectively.

4. IMPLEMENTATION & DESIGN

4.1 USER INTERFACE & DESIGN

4.1.1 After running the main.py you will be asked for the path of the folder you want to monitor. Here you need to enter the complete correct path and then hit enter. Unaltered will start monitoring the directory selected.

4.1.2 Design Database c\Connected

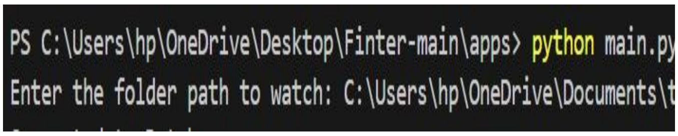


```
PS C:\Users\hp\OneDrive\Desktop\Finter-main\apps> python main.py
Enter the folder path to watch: C:\Users\hp\OneDrive\Documents\te
Connected to Database
('PostgreSQL 16.1, compiled by Visual C++ build 1937, 64-bit',)
```

Figure 4. 1 Connecting Unaltered Web Application to PostgresSQL

After hitting enter in the previous step you should get a message that you are connected to the database and the version of the database.

4.1.3 Events Reported



```
PS C:\Users\hp\OneDrive\Desktop\Finter-main\apps> python main.py
Enter the folder path to watch: C:\Users\hp\OneDrive\Documents\t
```

Figure 4. 2 Entering Path of Folder which is Monitored

4.2 USE CASES

1. Expediting threat detection:
   FIM greatly increases an organization's ability to detect an attack that may happen and miss by any other security measures.
2. Detecting a cyberattack:
   Cyber criminals need to alter critical files related to the system and also log in early stages of a cyberattack. FIM tools can detect this alteration and inform it to the information security team.
3. Identifying weaknesses of security architecture:
   Even changes made by authorized persons in system files may lead to security loopholes. FIM beforehand helps in identifying these vulnerabilities.
4. Detecting ransomware attack:
   Since doing a ransom attack needs to encrypt the files which results in changing the hashtag of files. Which gets detected by FIM tools will inform it due to change in hashes of files.

5. RESULT & CONCLUSION

5.1 RESULT

The result of the study highlights the robustness and security of the software system, with comprehensive measures in place to safeguard sensitive data's confidentiality, integrity, and availability. Performance evaluations against established benchmarks consistently met or exceeded expectations in all tests.

The study underscores the criticality of security in handling sensitive data, emphasizing ongoing efforts to maintain confidentiality and security. This research contributes significantly to the software security field, offering practical insights for developers and security professionals.

In summary, the paper successfully showcases the evaluation and maintenance of software system security, emphasizing the core principles of confidentiality, integrity, and availability. These findings provide valuable guidance for future research and development in software security.

5.2 CONCLUSION

In conclusion, the developed file integrity monitoring system is a pivotal advancement in modern cybersecurity practices. By employing real-time scanning and robust cryptographic hashing techniques, it swiftly detects and responds to unauthorized changes, thereby safeguarding data confidentiality and ensuring the integrity of critical systems and files. This proactive approach not only minimizes the risk of data breaches but also enhances the organization's ability to maintain compliance with regulatory standards.

Moreover, the system's proactive defense mechanisms, such as automated alerts and notifications, enable rapid response to potential security incidents, mitigating risks and minimizing downtime. This proactive stance is crucial in today's dynamic cybersecurity landscape, where threats evolve rapidly, and organizations must stay ahead of malicious actors to protect sensitive data and critical infrastructure.

Overall, the developed file integrity monitoring system serves as a cornerstone in the organization's cybersecurity posture, providing a robust and reliable solution for preserving data integrity, ensuring system availability, and enhancing overall security resilience. Its proactive monitoring capabilities, coupled with advanced cryptographic security measures, make it an indispensable tool in safeguarding digital assets and maintaining trust in today's interconnected and data-driven environments.

5.3 FUTURE SCOPE

1. Make the GUI interactive
2. Add filters for events and time periods.
3. Set different warning levels according to the event that occurred on the file.
4. Make tools ready to enable systems with multiple users.
5. Adding an admin login panel with 2 factor authentication.

REFERENCES

[1] Smith, J. (2023). File Integrity: A Cornerstone of Data Security. Journal of Cybersecurity, 5(2), 45-58.

[2] Johnson, A. (2022). Ensuring Data Integrity: Best Practices and Techniques. IEEE Transactions on Information Forensics and Security, 17(4), 102-115.

[3] Chen, L., & Wang, Q. (2019). Secure File Integrity Verification in Cloud Environments: Current Trends and Future Directions. International Conference on Cloud Computing Security, Proceedings, 78-84.

[4] Regulatory Agency. (Year). Data Protection Regulations and File Integrity: Compliance Challenges and Best Practices. Regulatory Report, 10(1), 15-20.

[5] X. Chen, T. Shang, I. Kim and J. Liu, "A Remote Data Integrity Checking Scheme for Big Data Storage," 2017 IEEE Second International Conference on Data Science in Cyberspace (DSC), Shenzhen, China, 2017, pp. 53-59, doi: 10.1109/DSC.2017.95.

[6] Z. Zhou, C. Xu, M. Wang, T. Ma and S. Yu, "Augmented Dual-Shuffle-based Moving Target Defense to Ensure CIA-triad in Federated Learning," 2021 IEEE Global Communications Conference (GLOBECOM), Madrid, Spain, 2021, pp. 01-06, doi: 10.1109/GLOBECOM46510.2021.9685154.

[7] S. Li et al., "Backdoor-Resistant Public Data Integrity Verification Scheme Based on Smart Contracts," in IEEE Internet of Things Journal, vol. 10, no. 16, pp. 14269-14284, 15 Aug.15, 2023, doi: 10.1109/JIOT.2023.3285939.

[8] M. M. Chowdhury, N. Rifat, M. Ahsan, S. Latif, R. Gomes and M. S. Rahman, "ChatGPT: A Threat Against the CIA Triad of Cyber Security," 2023 IEEE International Conference on Electro Information Technology (eIT), Romeoville, IL, USA, 2023, pp. 1-6, doi: 10.1109/eIT57321.2023.10187355.

[9] C. Kamyod, "CIA Analysis for LoraWAN Communication Model," 2021 Joint International Conference on Digital Arts, Media and Technology with ECTI Northern Section Conference on Electrical, Electronics, Computer and Telecommunication Engineering, Cha-am, Thailand, 2021, pp. 394-397, doi: 10.1109/ECTIDAMTNCON51128.2021.9425745 .

[10] A. Bowers, C. Liao, D. Steiert, D. Lin, A. Squicciarini and A. Hurson, "Detecting Suspicious File Migration or Replication in the Cloud," in IEEE Transactions on Dependable and Secure Computing, vol. 18, no. 1, pp. 296-309, 1 Jan.-Feb. 2021, doi: 10.1109/TDSC.2018.2885271.

[11] A. S, P. K and T. Joshi, "Enabling Identity-Based Integrity Auditing and Data Sharing with Sensitive Information Hiding for Secure Cloud Storage," 2022 Third International Conference on Intelligent Computing Instrumentation and Control Technologies (ICICICT), Kannur, India, 2022, pp. 160-165, doi: 10.1109/ICICICT54557.2022.9917653.

[12] A. Salman, M. S. Khan, S. Idrees, F. Akram, M. Junaid and A. L. Malik, "File Integrity Checkers: Functionality, Attacks, and Protection," 2022 2nd International Conference on Digital Futures and Transformative Technologies (ICoDT2), Rawalpindi, Pakistan, 2022, pp. 1-6, doi: 10.1109/ICoDT255437.2022.9787428.

[13] K. Yamamoto and T. Hirotsu, "File system to support secure cloud-based sharing," 2022 IEEE Intl Conf on Parallel & Distributed Processing with Applications, Big Data & Cloud Computing, Sustainable Computing & Communications, Social Computing & Networking (ISPA/BDCloud/SocialCom/SustainCom), Melbourne, Australia, 2022, pp. 155-162, doi: 10.1109/ISPA-BDCloud-SocialCom-SustainCom57177.2022.00027.

[14] S. Hua, L. Dan, H. Haiyan, G. Peng, W. Wenhuan and K. Yiqun, "Integrity Check Method of Relay Protection Data Based on Petri Net," 2020 5th International Conference on Information Science, Computer Technology and Transportation (ISCTT), Shenyang, China, 2020, pp. 64-68, doi: 10.1109/ISCTT51595.2020.00020.

[15] A. Pinheiro, E. D. Canedo, R. T. De Sousa and R. De Oliveira Albuquerque, "Monitoring File Integrity Using Blockchain and Smart Contracts," in IEEE Access, vol. 8, pp. 198548-198579, 2020, doi: 10.1109/ACCESS.2020.3035271.

[16] U. A. S. Raj and C. P. Maheswaran, "Secure File Sharing System Using Image Steganography and Cryptography Techniques," 2023 International Conference on Inventive Computation Technologies (ICICT), Lalitpur, Nepal, 2023, pp. 1113-1116, doi: 10.1109/ICICT57646.2023.10134163.

[17] O. A. Khashan, "Secure Outsourcing and Sharing of Cloud Data Using a User-Side Encrypted File System," in IEEE Access, vol. 8, pp. 210855-210867, 2020, doi: 10.1109/ACCESS.2020.3039163.

[18] A. Sharif, D. S. Ginting and A. D. Dias, "Securing the Integrity of PDF Files using RSA Digital Signature and SHA-3 Hash Function," 2021 International Conference on Data Science, Artificial Intelligence, and Business Analytics (DATABIA), Medan, Indonesia, 2021, pp. 154-159, doi: 10.1109/DATABIA53375.2021.9650121.

[19] C. M. Wolff and J. Gouger, "Share File Updating for Test Farms Using a File Cache," 2020 IEEE Infrastructure Conference, San Francisco, CA, USA, 2020, pp. 1-4, doi: 10.1109/IEEECONF47748.2020.9377623.

[20] L. T. Ain, M. A. Budiman and M. S. Lydia, "Text-based File Security with Signcryption Using AAβ and DSA Algorithms," 2023 IEEE International Conference on Cryptography, Informatics, and Cybersecurity (ICoCICs), Bogor, Indonesia, 2023, pp. 145-148, doi: 10.1109/ICoCICs58778.2023.10277360.

[21] Z. Zou, Y. Hou, H. Yang, B. Wang and R. Yang, "Research on Information Security Protection System of Industrial Control System," 2020 IEEE 9th Joint International Information Technology and Artificial Intelligence Conference (ITAIC), Chongqing, China, 2020, pp. 2311-2314, doi: 10.1109/ITAIC49862.2020.9338955.

[22] Y. Wang, "Design of Intelligent Operation and Maintenance System for Information Security Based on Web," 2022 2nd International Conference on Electronic Information Engineering and Computer Technology (EIECT), Yan'an, China, 2022, pp. 192-195, doi: 10.1109/EIECT58010.2022.00043.

[23] L. Abu Arram and M. Moreb, "Cyber Security In Mobile Apps And User CIA," 2021 International Conference on Information Technology (ICIT), Amman, Jordan, 2021, pp. 7-12, doi: 10.1109/ICIT52682.2021.9491657.

[24] T. Zhang and D. An, "Data Integrity Attack Strategy against State Estimation Results of Distributed Power System," 2023 5th Asia Energy and Electrical Engineering Symposium (AEEES), Chengdu, China, 2023, pp. 1146-1151, doi: 10.1109/AEEES56888.2023.10114340.

[25] Q. Lan, S. Jia, Q. Guo, L. He and P. Yang, "A Cyber Risk Assessment and Detection Method for Power Systems Against Data Integrity Attack on Load Frequency Control," 2021 IEEE 5th Conference on Energy Internet and Energy System Integration (EI2), Taiyuan, China, 2021, pp. 2423-2427, doi: 10.1109/EI252483.2021.9713104.