International Journal of Computing Sciences Research (ISSN print: 2546-0552; ISSN online: 2546-115X)
Vol. 7, pp. 2348-2357
doi: 10.25147/ijcsr.2017.001.1.164
https://stepacademic.net

Concept Paper

File Integrity Verifier Using Digital Signature Algorithm and SHA-256 with Memory-Mapping Technique

Joy C. Bañas
School of Graduate Studies, AMA Computer University, Philippines
jcbanas@amaes.edu.ph
(corresponding author)

Jonilo C. Mababa
College of Computer Studies, Angeles University Foundation, Philippines
mababa.jonilo@auf.edu.ph

Date received: July 2, 2023
Date received in revised form: July 28, 2023; July 31, 2023
Date accepted: August 1, 2023

Recommended citation:

Bañas, J. C. & Mababa, J. C. (2023). File integrity verifier using a digital signature algorithm and SHA-256 with memory-mapping technique. *International Journal of Computing Sciences Research*, *7*, 2348-2357. https://doi.org/10.25147/ijcsr.2017.001.1.164

Abstract

Purpose – The study aims to develop a specialized File Integrity Verifier system tailored for educational sectors, with a primary focus on the Philippine Society of Information Technology Educators-Central Luzon (PSITE-CL). The system will employ various advanced methods, including the Digital Signature Algorithm (DSA), Secure Hash Algorithm 256-bit (SHA-256), Memory-Mapping technique, Laravel PHP framework, and Argon2 hashing algorithm, to ensure the utmost security and effective digital file management. The ultimate goal is to guarantee accuracy and efficiency in handling confidential and critical data within these organizations.

Method – This study will employ a combination of Descriptive and Research and Development (R&D) methods. By integrating descriptive research and R&D, the study will gain comprehensive insights into the current systems, technologies, and user behaviors, leading to the development of innovative solutions.

Conclusion - The implementation of a file integrity verifier system offers numerous benefits, including enhanced data security, accuracy, and efficiency. By adopting this system, educational sectors can ensure the authenticity and integrity of digital documents, prevent non-repudiation of uploaded files, streamline workflows, reduce cyber-attack risks, and

maintain the credibility of academic records. Furthermore, the technologies and methods that will be used in this system can overcome the limitations of traditional hash function-based approaches, addressing issues related to time consumption, resource utilization, and vulnerability to attacks.

Recommendation - This study strongly recommends the adoption of the proposed system in educational sectors, with a specific focus on the PSITE-CL. Implementing this technology will significantly enhance data security measures, ensure compliance with privacy regulations, and mitigate the risks associated with unauthorized modifications to digital records.

Practical Implication - The File Integrity Verifier system holds the potential to benefit not only educational sectors, and students but also regulatory bodies, future researchers, and developers.

Keywords – file integrity verifier, digital signature algorithm, SHA-256, memory-mapping technique, PSITE-CL

INTRODUCTION

In the present time, digital technologies have resulted in a significant increase in the volume of data and records stored in digital formats within educational institutions and academic organizations. Among these digital repositories, institutional databases hold valuable and confidential information, including academic credentials, member records, and seminar certificates. The shift towards digital records represents a substantial advancement in process efficiency, making it easier for academic organizations to manage and access pertinent data. However, this transition has also introduced new challenges concerning data security and integrity. The confidential nature of the stored data necessitates stringent measures to safeguard against unauthorized access, tampering, or modification of these documents. Any such unauthorized activities can lead to severe repercussions for both the academic organization and the integrity of the members' records.

One of the primary obstacles encountered by the majority of educational institutions and academic organizations is ensuring the integrity of their members' data. The process of file integrity verification is essential as it guarantees that files and documents have not been tampered with or altered since their initial creation. This aspect is particularly crucial in academic organizations and institutions, where the accuracy and integrity of all records hold immense importance. Unauthorized modifications to data can result in severe consequences, including loss of trust, legal liabilities, and damage to reputation. Furthermore, in the digital era, the traditional method of file integrity verification involves using hash functions to generate checksums for files. While this approach is effective, it has drawbacks such as being time-consuming due to the need to

process each file's data and resource-intensive, especially for large files, as it requires significant CPU and memory resources. Moreover, it is susceptible to attacks that can modify both the file and its corresponding checksum, making it less secure.

The primary goal of the proposed study is to develop a File Integrity Verifier that will significantly enhance the accuracy, efficiency, integrity, and security of file verification processes within academic organizations and educational institutions. This system will incorporate the use of the Digital Signature Algorithm, SHA-256, and Memory-Mapping technique, implemented through the Laravel PHP framework and Argon2 hashing algorithm. Given that file integrity systems are not widely adopted in academic settings, this innovation holds great potential and promises to deliver swift, secure, and well-organized data management processes.

LITERATURE REVIEW

Numerous academic studies have delved into different approaches aimed at enhancing privacy, security, and integrity in document authentication and certificate management systems. For instance, Wellem et al. (2022) propose an academic document authentication system that employs QR codes containing digital signatures generated using the Elliptic Curve Digital Signature Algorithm (ECDSA). Addressing challenges faced by traditional student certificate management systems, Dewangan et al. (2023) propose a solution that combines blockchain and the InterPlanetary File System (IPFS). Their decentralized system ensures transparency, security, and authenticity of certificates while preserving privacy by storing sensitive data off-chain. Saepulrohman et al. (2021) offer an overview of the Digital Signature Algorithm (DSA) and its application in ensuring data integrity and security in electronic systems. They discuss the need for digital signatures, their properties, and how DSA effectively prevents common attacks. Focusing on cryptographic techniques for data integrity and security, Nazal et al. (2019) highlight the use of Keccak as a hash function and DSA for data authenticity and sender verification. Li et al. (2019) present a blockchain-based system employing permissioned blockchain and smart contracts for security and efficiency. They evaluate the system's performance and security, demonstrating its advantages over traditional database systems.

Bacusmo et al. (2022) and conducted a comparative study of five hash functions—Message-Digest Algorithm 5 (MD5), Secure Hash Algorithm 1 (SHA-1), Secure Hash Algorithm 224 (SHA-224), Secure Hash Algorithm 256-bit (SHA-256), and Secure Hash Algorithm 384 (SHA-384)—in conjunction with digital signatures to verify file integrity. Their evaluation indicates that SHA-256 and SHA-384 are efficient options for this purpose. These studies collectively provide valuable insights into the use of digital signatures, blockchain, cryptographic techniques, and hash functions to ensure data integrity, security, and privacy in academic document authentication, certificate management, and file integrity verification systems. For instance, Paderanga et al. (2021) propose a File Integrity Verification method utilizing a digital signature with SHA-256 as the checksum generator, demonstrating improved verification time and security compared to alternative methods.

Bascon et al. (2020) evaluated different versions of the Secure Hash Algorithm (SHA) for File Integrity Verification with digital signatures, concluding that SHA-256 offers the best overall performance. Rosales (2020) compares three digital signature algorithms—Rivest-Shamir-Adleman (RSA), Digital Signature Algorithm (DSA), and Elliptic Curve Digital Signature Algorithm (ECDSA)—for File Integrity Verification, highlighting their high-level security, with RSA and DSA being more efficient than ECDSA. Additionally, Gacutan et al. (2019) presented a technique for File Integrity Verification and digital signatures using SHA-256 in cloud computing, demonstrating faster verification time and enhanced security compared to other methods.

Rachmawanto et al. (2022) introduced a novel approach to digital certificate authentication, enhancing secure internet communication through the utilization of Triple DES cryptography, hash functions, and the DSA algorithm. Kammoun et al. (2022) explore the use of digital signatures to ensure data integrity in IoT environments and propose employing the DSA and SHA-256 algorithms for authentication. In the realm of secure document storage and File Integrity Verification, Prathibha et al. (2021) leverage blockchain technology to guarantee authenticity via unique document fingerprints and smart contracts. Sharif et al. (2021) presented a solution for the secure verification of inclusive PDF files using RSA digital signatures and the SHA-3 hash function. Regarding educational institutions, Aliyu et al. (2019) propose an enhanced digital signature algorithm to authenticate student transcripts, incorporating hash functions, asymmetric encryption, and digital signatures. Local studies in the Philippines highlight the potential of blockchain technology in securing student records and improving transparency and efficiency.

Garcia et al. (2021) emphasized the use of blockchain technology in Philippine Higher Education Institutions to address challenges in student records management. Deeb et al. (2020) utilize memory mapping and SHA-256 for securing electronic student records stored in a blockchain, ensuring tamper-proof and transparent data. Casia et al. (2020) develop an Electronic Credentials Verification system using blockchain and smart contracts to combat fraudulent credentials in the Philippines. Lepiten (2019) proposes a unified student record system in the Philippines, leveraging blockchain technology to address inconsistencies across institutions.

After synthesizing the reviewed literature and studies, a clear emphasis emerges on the crucial aspects of data security, integrity, and transparency across various domains. The use of cryptographic techniques and digital signatures plays a prominent role in ensuring secure and efficient file integrity verification and management. These studies provide a robust foundation of knowledge and insights, underscoring the importance and potential impact of the proposed research on the file integrity verifier.

PROPOSED METHODOLOGY

The researcher will employ a combination of Descriptive Research and Research and Development (R&D) methods for this study. Descriptive research involves gathering

survey-based data to accurately describe the subject under investigation and identify patterns and trends (McCombes, 2023). On the other hand, R&D methods, including literature review, experimental research, and innovation, will be used to advance knowledge, enhance efficiency, and optimize algorithms (CFI, 2023). By integrating both descriptive research and R&D, the study will obtain a comprehensive understanding of current systems, technologies, and user behaviors, leading to valuable insights, innovative solutions, and the development of novel approaches to tackle real-world challenges associated with the proposed system (Ortiz, 2007).

To ensure the reliability of the file integrity verifier system, it is vital to test and evaluate its software quality characteristics based on ISO/IEC 25010:2011, an international standard that provides guidelines for assessing the quality of software products. The proposed study aims to examine various aspects, including functionality, reliability, usability, performance, security, and maintainability. Each characteristic will be further assessed based on specific sub-characteristics to gauge the overall software quality of the system. To conduct this evaluation, a survey questionnaire based on ISO/IEC 25010:2011 will be distributed to a target population. This evaluation process aims to assess the overall effectiveness of the system by analyzing relevant criteria and metrics.

System Development

The proposed study aims to develop a file integrity verifier that leverages multiple techniques to create an accurate, efficient, and secure system for verifying uploaded files in academic organizations, educational institutions, and related fields.

The system will use the Digital Signature Algorithm (DSA) to generate public and private keys based on public-key cryptography. These keys will be hashed using SHA-256 to achieve multiple-factor authentication and ensure the authenticity, integrity, and non-repudiation of each uploaded file. SHA-256 will further hash the related keys created by the Digital Signature, and the resulting hash value will be encrypted using Argon2id for enhanced security.

To optimize performance and reduce overhead, the system will implement a memory-mapping technique, enabling direct file access from memory through a virtual memory area associated with each file. MySQL Database Management System (DBMS) will store user data, file metadata, and audit trail information.

The user interface (UI) will be developed using the Laravel PHP framework, allowing users to select the file they want to verify and initiate the verification process. The user interface will be designed using Bootstrap5 Framework, Native Java Script (Native JS), and Cascading Style Sheets (CSS) within the Laravel Framework, enabling user interaction with the process.

For secure accessibility over the internet, the system will be deployed on Amazon Web Services (AWS). AWS cloud provides scalability, reliability, and cost-effectiveness.

In summary, the proposed study will introduce a file integrity verifier system that incorporates multiple-factor authentication and document fingerprinting. It will utilize the Digital Signature Algorithm (DSA) and SHA-256 hashing to generate unique hash values for each file, creating digital signatures that act as fingerprints. The system will consist of two components: File Upload, where unique IDs and keys will be created, encrypted files will be stored in the database, and Verification, where files will be compared against stored signatures using OpenSSL. The system will enhance security by employing an encryption technique like Argon2id to protect hash values from unauthorized modifications. To improve efficiency, a memory-mapping technique will allow direct file access from memory, enhancing data processing speed and overall performance.

CONCLUSIONS AND FUTURE RESEARCH

In the modern digital era, the adoption of a file integrity verifier system that utilizes various methods is of paramount importance, particularly as academic records increasingly transition to digital formats. This system plays a critical role in mitigating the risks associated with unauthorized alterations to digital records, safeguarding the credibility of academic records, and ensuring adherence to privacy regulations. Despite potential challenges in implementing the system, such as resource utilization and user adoption, the potential benefits far outweigh these obstacles. The study aims to underscore the significance of digital security and data integrity in academic organizations and educational institutions. By implementing a file integrity verifier system, these institutions can fortify their data security measures, streamline workflows, and reduce the susceptibility to cyber-attacks. The findings of this study enrich the existing understanding of file integrity verification and provide valuable insights for future research in this domain.

The multiple-factor authentication provided by the Digital Signature Algorithm and SHA-256 ensures that each uploaded file possesses a unique identifier and digital signature, making it difficult for unauthorized individuals to tamper with or alter the file without detection. The use of encryption techniques, particularly Argon2id, adds another layer of security by encrypting the generated hash value, significantly impeding attackers from manipulating the file and its corresponding integrity verification. Furthermore, the implementation of the Memory-Mapping technique significantly improves the efficiency and performance of the file integrity verification process. By allowing direct file access from memory, the system reduces processing time, resource utilization, and overhead, resulting in faster and more streamlined file verification procedures. This efficiency is particularly crucial for academic organizations and educational institutions managing large volumes of digital files and records. Overall, the proposed file integrity verifier system offers a secure, efficient, and reliable solution for managing and verifying the integrity of digital documents, ensuring the accuracy and trustworthiness of academic records.

However, there are several areas for future research and improvement. Firstly, the proposed system could be further evaluated and optimized in terms of intensive performance. Another area for future research is the real-world implementation and

evaluation of the proposed system in academic organizations and educational institutions. Conducting pilot studies and gathering user feedback can provide valuable insights into the system's usability, effectiveness, and areas for improvement. Additionally, assessing the system's compliance with relevant privacy regulations and standards is essential. Lastly, exploring the potential integration of machine learning and artificial intelligence techniques for anomaly detection and fraud prevention could be beneficial. Such techniques can help identify suspicious patterns or activities that may indicate unauthorized modifications or tampering with files. Integrating such capabilities into the File Integrity Verifier system can enhance its security and detection capabilities.

In conclusion, the proposed File Integrity Verifier system offers a robust solution for ensuring data security and integrity in academic organizations and educational institutions. Future research can focus on optimizing the system's performance, exploring blockchain integration, evaluating its implementation in real-world settings, and incorporating advanced techniques for anomaly detection and fraud prevention. By addressing these areas, the proposed system can further enhance data protection, streamline workflows, and contribute to the overall improvement of academic records management.

PRACTICAL IMPLICATIONS

The proposed file integrity verifier system bears significant importance for academic organizations, educational institutions, and their members. By employing multiple-factor authentication and encryption techniques, the system can enhance data security, ensuring the authenticity and integrity of digital files. It also enables the institutions to meet compliance requirements, streamlines workflows by simplifying file verification processes, and guarantees the reliability of academic records for accreditation and verification purposes. Additionally, the system can serve as a means of fraud prevention by promptly detecting any tampering or unauthorized modifications to files. The findings of the proposed study hold value as a reference for future research and development in the field, opening possibilities for further advancements in file management systems. Overall, the implementation of a file integrity verifier system will bolster data management processes and fortify the integrity of digital files in academic settings.

DECLARATIONS

Conflict of Interest

I affirm that there are no conflicts of interest that could potentially influence the outcomes and objectives of file integrity verification in academic organizations and educational institutions. I have no financial or personal relationships with any individuals, organizations, or entities that might compromise the impartiality of the research.

Informed Consent

Consent will be obtained from all participants involved in the study. It is crucial to ensure that they are fully informed about the purpose, procedures, potential risks, and benefits of their involvement. They will be provided with a clear explanation of their rights and their voluntary nature. Confidentiality and anonymity will be maintained throughout the study, and consent forms will be obtained before their participation.

Ethics Approval

I recognize the significance of ethical research practices and commit to conducting the study with utmost integrity, adhering to all relevant guidelines and regulations. I take complete responsibility for the precision and authenticity of the information presented in this proposal.

ACKNOWLEDGMENT

We would like to extend our heartfelt appreciation to the individuals and organizations who have played a significant role in supporting us throughout the development of this concept paper.

First and foremost, we express our sincere gratitude to our research advisor, Dr. Jenny Lyn V. Abamo, for her invaluable guidance, expertise, and unwavering support throughout the conceptualization of this paper.

We also wish to acknowledge the valuable contributions of the members of our research team: Engr. Delaney Ofrecio, Prof. Gerard Nathaniel Ngo, Prof. Karren De Lara and Ms. Ai Lopez. Their active participation in brainstorming sessions, discussions, and critical reviews has significantly shaped the ideas presented in this concept paper.

Furthermore, we are grateful to PSITE-CL and AMA Education System for providing us with the necessary resources and facilities to conduct our research. Their support has been indispensable in gathering relevant information and data to inform the development of our concept.

Finally, we want to express our deep appreciation to our beloved Nanay Ligaya, siblings Jhoan and John Paul, Mama Dolly, and my life partner Ley. Their unwavering support, patience, and understanding throughout this research endeavor have been a constant source of motivation, propelling us to strive for academic excellence.

References

Aliyu, G. N., & Adesina, A. O. (2019). An Enhanced Digital Signature Algorithm for Student Transcript Authentication. In *2019 International Conference on Computer Science and Information Technology (CSIT)* (pp. 20-25).

Arreza, M. Q., & Jover, J. M. (2020). The Security of Academic Records through Blockchain Technology. In *2020 15th International Conference on Humanoid, Nanotechnology, Information Technology, Communication and Control, Environment, and Management (HNICEM)* (pp. 81-85).

Bacusmo, J. T., & Paderanga, F. L. (2022). A Comparative Analysis of Hash Functions in File Integrity Checker with Digital Signature. In *2022 IEEE 14th International Conference on Humanoid, Nanotechnology, Information Technology, Communication and Control, Environment, and Management (HNICEM)* (pp. 1-6).

Bascon, J. B., Paderanga, F. L., & Bacusmo, J. T. (2020). A Comparative Study of File Integrity Checkers using SHA-1, SHA-256, and SHA-512 with Digital Signature. In *2020 IEEE 10th International Conference on Humanoid, Nanotechnology, Information Technology, Communication and Control, Environment, and Management (HNICEM)* (pp. 1-6).

Casia, A. C., Alampay, J. M., Dulay, N. R., & Ong, E. J. (2020). A Blockchain-Based Electronic Credentials Verification System for the Philippines: Design, Implementation, and Evaluation. In *8th International Conference on Information Technology and Multimedia (ICIMU 2020)* (pp. 8-12).

CFI Team. (2023). *Research and Development (R&D)*. Retrieved from https://corporatefinanceinstitute.com/resources/accounting/research-and-development-rd.

Deeb A., & Ayad, M. (2020). Securing Electronic Student Records using Blockchain Technology. In *2020 IEEE 4th International Conference on Computational Systems and Information Technology for Sustainable Solutions (CSITSS)* (pp. 17-24).

Dewangan, N. K., Chandrakar, P., Kumari, S., & Rodrigues, J. J. (2023). Enhanced privacy-preserving in student certificate management in blockchain and interplanetary file systems. Multimedia Tools and Applications, 82(8), 12595-12614.

Gacutan, R. J. P., Sarmiento, R. F., & Tuazon, R. B. (2019). Digital Signature Verification and File Integrity Check using SHA-256 in Cloud Computing. In *2019 IEEE 11th International Conference on Humanoid, Nanotechnology, Information Technology, Communication and Control, Environment, and Management (HNICEM)* (pp. 1-6).

Garcia, A. A., & Bautista, R. R. (2021). Enhancing Security of Student Records Using Blockchain Technology in Philippine Higher Education Institutions. In *2021 International Journal of Advanced Research in Computer Science and Software Engineering* (pp. 12-20).

Kammoun, N., Douss, A. B. C., Abassi, R., & Guemara, S. (2022). Ensuring Data Integrity Using Digital Signature in an IoT Environment. In 2022 *International Conference on Advanced Information Networking and Applications*. Advanced Information Networking and Applications (pp. 482–491).

Lepiten, M. C., Clamor, A. E., Beley, J. V., & Bucu, J. E. (2019). Development of a Unified Student Record System Using Blockchain Technology in the Philippines. In *2019 4th International Conference on Computer Science and Technologies in Education* (pp. 1-8).

Li, L., Xu, K., Zhao, J., Chen, X., & Liao, X. (2019). A Blockchain-Based Student Academic Record Management System. *In 2019 International Journal of Grid and Distributed Computing*, 12(4), 45-54.

McCombes, S. (2023). *Descriptive Research | Definition, Types, Methods & Examples.* Retrieved from https://www.scribbr.com/methodology/descriptive-research.

Nazal, M. A., Pulungan, R., & Riasetiawan, M. (2019). Data integrity and security using keccak and digital signature algorithm (DSA). In *2019 Indonesian Journal of Computing and Cybernetics Systems (IJCCS)*, 13(3), 273-282.

Ortiz, D., & Greene, J. (2007). Research design: qualitative, quantitative, and mixed methods approaches. *Qualitative Research Journal*, 6(2), 205-208.

Paderanga, F. L., & Bacusmo, J. T. (2021). Hash-based File Integrity Checker with Digital Signature for Security Enhancement. In *3rd International Conference on Industrial Applications of Computing* (pp. 1-6). ACM.

Prathibha, S., Sona, T. R., & Priya, K. (2021). Secured Storage and Verification of Documents Using Blockchain Technology. *Transforming Cybersecurity Solutions using Blockchain* (pp. 71-90).

Rachmawanto, E. H., Handoko, L. B., Umam, C., Jatmoko, C., & Ali, R. R. (2022, September). Triple DES Cryptography Based on Hash Function and DSA for Digital Certificate Authentication. In *2022 International Seminar on Application for Technology of Information and Communication (iSemantic)* (pp. 71-76). IEEE.

Rosales, J. V. (2020). A Comparative Study of Digital Signatures in File Integrity Verification. In *2020 7th International Conference on Control, Decision and Information Technologies (CoDIT)* (pp. 56-61).

Saepulrohman, A., & Ismangil, A. (2021). Data integrity and security of digital signatures on electronic systems using the digital signature algorithm (DSA). *International Journal of Electronics and Communications System (IJECS)*, 1(1), 11-15.

Sharif, A., Ginting, D. S. B., & Dias, A. D. (2021). Securing the Integrity of PDF Files using RSA Digital Signature and SHA-3 Hash Function. *In 2021 International Conference on Data Science, Artificial Intelligence, and Business Analytics (DATABIA)* (pp. 4-11).

Wellem, T., Nataliani, Y., & Iriani, A. (2022). Academic Document Authentication using Elliptic Curve Digital Signature Algorithm and QR Code. In *International Journal on Informatics and Visualization*, 6(3), 667-675.

Author's Biography

Joy Camagon Bañas is a Master of Science in Computer Science candidate specializing in Computer Science Theory at the School of Graduate Studies, AMA Computer University. She holds a Bachelor of Science degree in Computer Science (2009) from Pamantasan ng Lungsod ng Muntinlupa, Philippines. Her research involves various algorithm integration and implementation for file efficiency, integrity, and security. She currently works as a Senior IT Supervisor in the Information Technology Department of AMA Education System, Philippines. She has distinguished experience in Academic Information Systems, with an emphasis on overall AIS analysis and functional components.

Dr. Jonilo Caro Mababa is a distinguished academic and a beacon of knowledge in the field of Information Technology. He is a graduate Doctor of Information Technology and currently taking up his Doctor of Philosophy in Education. He is currently the Program Chair of the Information Technology Department at Angeles University Foundation and Director of Eruma Education.