e-ISSN: 2582-5208
International Research Journal of Modernization in Engineering Technology and Science
(Peer-Reviewed, Open Access, Fully Refereed International Journal)
Volume:06/Issue:05/May-2024 Impact Factor- 7.868 www.irjmets.com

ROBUST DATA ARCHIVING FRAMEWORK FOR DIGITAL FORENSIC READINESS

Mrs. S. Priskilla Manonmani*1, Ms. Supriyaa.G*2

*1Associate Professor, Department Of Information Technology, Meenakshi Sundararajan Engineering College, Chennai, India.

*2Student, Department Of Information Technology, Meenakshi Sundararajan Engineering College, Chennai, India.

DOI : https://www.doi.org/10.56726/IRJMETS55246

ABSTRACT

The proliferation of Cloud storage presents unparalleled scalability but raises concerns regarding data integrity and security. Users relinquishing control over their data upon storage underscores the need for robust security measures. Despite offering utility service for seamless data outsourcing, Cloud computing faces lingering security apprehensions, impeding widespread adoption. Edge storage emerges as an appealing alternative, boasting reduced bandwidth overhead and latency compared to traditional Cloud storage. However, its susceptibility to intentional or accidental disruptions necessitates comprehensive security protocols. To mitigate risks and bolster trust between Cloud clients (CC) and service providers (CSP), security paradigms leveraging third-party auditors (TPA) have emerged. TPAs, tasked with verifying data integrity, face scrutiny due to potential malicious interference. Comprehensive analysis of TPA involvement and privacy-preserving models is crucial to address evolving security threats. Emphasizing dynamic solutions ensures adaptability to changing landscapes, enhancing resilience against emerging vulnerabilities. By enhancing privacy mechanisms and scrutinizing security paradigms, stakeholders can navigate the intricate balance between trust, security, and privacy in Cloud environments. This approach fosters a robust foundation for data integrity and confidentiality, enabling organizations to harness the benefits of Cloud computing while safeguarding sensitive information.

Keywords: Cloud Service Provider (CSP), Third Party Auditor (TPA), Network Management, Cyber-Attacks.

I. INTRODUCTION

Cloud computing represents a paradigm shift in IT infrastructure, offering tailored services accessible without extensive technical expertise. Private clouds cater to a limited user base with highly sensitive data, ensuring stringent security measures. In contrast, public clouds host a diverse range of information, posing risks to data integrity due to the shared environment. Hybrid clouds combine delivery models to balance security and cost-effectiveness, albeit with increased management complexity. Community clouds unite users with shared interests, leveraging a common infrastructure while maintaining data segregation. Despite advancements in security measures, concerns persist, driving cloud service providers to offer increasingly sophisticated solutions. However, lingering ambiguities hinder full adoption, particularly in sectors requiring high levels of trust, such as economics and government. Electronic documents, crucial for global transactions, present security challenges such as cybercrime threats and data loss risks.

Cloud storage addresses these challenges by providing convenient access to data, but regular integrity checks are essential to ensure data reliability. Provable data possession (PDP) protocols enable users to delegate integrity checks to third-party auditors (TPA), ensuring data integrity while minimizing user burden. As data storage demands continue to escalate, traditional storage methods struggle to keep pace, leading to widespread adoption of cloud storage solutions. However, the relinquishment of data control inherent in cloud storage poses inherent risks, necessitating regular integrity verification to maintain trust. TPAs play a critical role in this process, conducting audits to ensure data reliability and integrity. However, challenges such as timeliness and collusion risks must be addressed to maintain the effectiveness of these audits. In summary, cloud computing offers scalable and cost-effective solutions for data storage, but ongoing integrity checks are essential to maintain trust and reliability. TPAs play a vital role in this process, ensuring data integrity in the face of evolving security

e-ISSN: 2582-5208
International Research Journal of Modernization in Engineering Technology and Science
(Peer-Reviewed, Open Access, Fully Refereed International Journal)
Volume:06/Issue:05/May-2024 Impact Factor- 7.868 www.irjmets.com

challenges. Continued research and development efforts are crucial to address these challenges and maintain the integrity of cloud-based data storage solutions.

II. MOTIVATION

Cloud storage is a cornerstone of modern data management, offering scalability, accessibility, and cost-efficiency. However, it also introduces a plethora of security challenges that can compromise the integrity of stored data. Threats such as fire accidents, damage to hard disks, and hacker attacks pose significant risks to data integrity in cloud storage environments. Furthermore, cloud service providers may inadvertently delete data to reduce storage costs or deliberately hide data corruption incidents to maintain their reputation. Ensuring data integrity in the cloud is paramount to maintaining trust and reliability. Regular integrity verification is necessary to detect and mitigate these risks. However, this verification process inevitably increases the computational and communication burden on users, contradicting the original goal of resource-saving on the user side. To address these challenges, third-party auditors (TPAs) have emerged as crucial players in the cloud ecosystem. TPAs are entrusted by users to conduct regular data integrity verifications and provide audit reports to users. These reports serve as a means of transparency and accountability, helping users assess the reliability of their cloud service providers. In the literature, numerous research works have proposed various methods and techniques to enhance data integrity auditing in cloud environments. These include public verification schemes, support for dynamic operations, multiple-replica integrity auditing mechanisms, multi-user settings, and privacy preservation techniques. Each of these approaches aims to improve the effectiveness and efficiency of data integrity audits, ultimately enhancing trust in cloud storage services. However, TPAs are not without their challenges and limitations. While they are generally regarded as semi-trusted parties, there is always a risk that they may fail to meet the requirement of timeliness or even collude with cloud service providers to conceal data loss events. This potential for collusion undermines the integrity of the auditing process and erodes trust in the cloud ecosystem.

It is against this backdrop of challenges and opportunities that our project is motivated. We aim to develop innovative solutions that address the shortcomings of existing data integrity auditing mechanisms and enhance trust and reliability in cloud storage environments. By leveraging advanced technologies such as blockchain and cryptographic techniques, we seek to create a robust and tamper-proof framework for data integrity verification in the cloud. Our project will focus on developing practical tools and methodologies that empower users to verify the integrity of their data in the cloud securely and efficiently. By providing users with greater transparency and control over their data, we aim to instill confidence in cloud storage services and pave the way for wider adoption and acceptance of cloud technologies.

III. LITERATURE SURVEY

In 2022, Singh et al. proposed a Secure Storage Model for Digital Forensic Readiness, aiming to enhance the security of digital evidence storage. The model integrates integrity checks, sandboxing, encryption, two-factor authentication, and random file naming to ensure data integrity and confidentiality. A proof-of-concept tool was developed and tested, demonstrating promising results in security and performance. Overall, the Secure Storage Model offers a cost-effective solution for securely storing digital evidence, contributing to improved forensic practices.

In 2021 Mahrous et al. presented an Enhanced Blockchain-Based IoT Digital Forensics Architecture using Fuzzy Hash. The architecture aims to address security and privacy concerns in IoT systems by integrating blockchain technology with fuzzy hashing for digital evidence processing. By leveraging fuzzy hashing, the architecture enables the identification of potential evidence items that may remain undiscovered using conventional hashing techniques. Simulation results demonstrate the effectiveness of the proposed architecture in enhancing IoT digital forensics.

In 2020 Stoyanova et al conducted a survey on Internet of Things (IoT) Forensics, highlighting challenges, approaches, and open issues in IoT-based investigations. The survey addresses the complexity of IoT data, privacy concerns, and the need for validated tools and techniques to maintain the Chain of Custody. It discusses various theoretical models and frameworks, including privacy-preserving techniques and blockchain-based solutions, to ensure evidence integrity in IoT forensics.

e-ISSN: 2582-5208
International Research Journal of Modernization in Engineering Technology and Science
(Peer-Reviewed, Open Access, Fully Refereed International Journal)
Volume:06/Issue:05/May-2024 Impact Factor- 7.868 www.irjmets.com

In 2021, Al-Dhaqm et al. reviewed digital forensics subdomains and proposed a high-level abstract metamodel to synthesize investigative processes across different domains. The study identifies redundancies and ambiguities in current investigative processes and suggests a unified metamodel to streamline digital forensic investigations across various subdomains

In 2020, Xiao et al. (2019) developed advanced techniques for video-based evidence analysis in digital forensic investigations. Their framework includes video/image enhancement algorithms and deep-learning-based object detection for suspect identification. By enhancing CCTV footage quality and detecting potential evidence items, the framework aids in effective forensic analysis and decision-making.

In 2021 Kumar et al. presented a digital image forensic approach to counter JPEG anti-forensic attacks. Their method, based on second-order statistical analysis using Markov Transition Probability Matrices (MTPMs), effectively detects JPEG compression traces and counters anti-forensic techniques. Experimental results demonstrate the superiority of the proposed approach over existing techniques.

In 2021 Lee and Kim introduced K-FFRaaS, a generic model for Financial Forensic Readiness as a Service in Korea. Based on ISO/IEC 27043:2015, K-FFRaaS facilitates systematic management of financial incident root causes and digital evidence acquisition

IV. EXISTING SYSTEM

Securing digital evidence is pivotal for its admissibility in digital forensic investigations, particularly in upholding the chain of custody. However, existing practices often overlook the security of the environment and access to evidence, leaving them vulnerable to tampering or removal by attackers. Addressing this concern, this paper proposes a comprehensive model for securely storing digital evidence both pre- and post-incident to facilitate reactive forensics. The proposed model integrates several critical components to ensure the integrity and confidentiality of stored evidence. Firstly, integrity checks are employed to verify the soundness of the evidence. Additionally, the environment is sandboxed to prevent unauthorized access, and strong encryption is applied to safeguard sensitive information. Two-factor authentication adds an extra layer of security, while unique random file naming further enhances confidentiality. To validate the efficacy of the proposed model, a proof-of-concept tool was developed and subjected to rigorous testing. Tests evaluated system security, performance, and compliance with requirements. Results demonstrated that securing forensic artifacts can be achieved with minimal effort, offering a cost-effective and reliable solution.

By standardizing evidence storage and implementing high-security standards, the proposed model aims to eliminate the need for creating new systems for the same purpose. Moreover, it facilitates compliance with regulations and privacy policies governing the storage of sensitive data. Additionally, the model enhances the forensic soundness of stored potential digital evidence (PDE), making it admissible in a court of law. The SecureRS model leverages encryption and hashing techniques to align with current security standards, aiding forensic investigations in general. It also includes mechanisms to detect evidence tampering, further ensuring the integrity of stored evidence. This approach not only benefits digital forensic readiness (DFR) but also enhances digital forensics processes overall. Traditionally, the responsibility for ensuring the authenticity and verification of evidence rested solely with forensic investigators. However, with the implementation of the SecureRS model, this burden is alleviated.

Investigators can rely on the platform to securely store evidence, eliminating concerns about its integrity during digital investigations. The SecureRS platform serves as a backup of securely stored evidence, providing additional assurance of its safety. Overall, the proposed model addresses a critical aspect of forensic investigation often overlooked, contributing to the reliability and integrity of digital evidence. With a focus on smaller artifacts for performance evaluation, the SecureRS model offers a comprehensive solution to secure digital evidence and enhance the efficacy of forensic investigations.

V. PROPOSED SYSTEM

Securing digital evidence is pivotal for its admissibility in digital forensic investigations, particularly in upholding the chain of custody. However, existing practices often overlook the security of the environment and access to evidence, leaving them vulnerable to tampering or removal by attackers. Addressing this concern, this paper proposes a comprehensive model for securely storing digital evidence both pre- and post-incident to facilitate

reactive forensics. The proposed model integrates several critical components to ensure the integrity and confidentiality of stored evidence. Firstly, integrity checks are employed to verify the soundness of the evidence. Additionally, the environment is sandboxed to prevent unauthorized access, and strong encryption is applied to safeguard sensitive information. Two-factor authentication adds an extra layer of security, while unique random file naming further enhances confidentiality.

To validate the efficacy of the proposed model, a proof-of-concept tool was developed and subjected to rigorous testing. Tests evaluated system security, performance, and compliance with requirements. Results demonstrated that securing forensic artifacts can be achieved with minimal effort, offering a cost-effective and reliable solution. By standardizing evidence storage and implementing high-security standards, the proposed model aims to eliminate the need for creating new systems for the same purpose. Moreover, it facilitates compliance with regulations and privacy policies governing the storage of sensitive data. Additionally, the model enhances the forensic soundness of stored potential digital evidence (PDE), making it admissible in a court of law.

The SecureRS model leverages encryption and hashing techniques to align with current security standards, aiding forensic investigations in general. It also includes mechanisms to detect evidence tampering, further ensuring the integrity of stored evidence. This approach not only benefits digital forensic readiness (DFR) but also enhances digital forensics processes overall. Traditionally, the responsibility for ensuring the authenticity and verification of evidence rested solely with forensic investigators. However, with the implementation of the SecureRS model, this burden is alleviated. Investigators can rely on the platform to securely store evidence, eliminating concerns about its integrity during digital investigations.

The SecureRS platform serves as a backup of securely stored evidence, providing additional assurance of its safety. Overall, the proposed model addresses a critical aspect of forensic investigation often overlooked, contributing to the reliability and integrity of digital evidence. With a focus on smaller artifacts for performance evaluation, the SecureRS model offers a comprehensive solution to secure digital evidence and enhance the efficacy of forensic investigations.

VI. CONCLUSION

In the information technology field, it is becoming more common to hire third-party auditors to verify if mid-size companies and corporations are adhering to their security frameworks. This same concept has been introduced to cloud computing, in the form of on-the-spot auditing, by implementing the TPA in the solution. Hence, a TPA comes with its issues, mainly trust and an extra cost regarding processing and communication. In order to further secure cloud computing and enhance the trust between its main stakeholders (CSP, CC, and TPA), in this paper, we have proposed a novel protocol: the lightweight accountable privacy-preserving (LAPP) protocol. LAPP aims to provide tools to the CC to audit the auditor. It has been implemented through three algorithms and a mathematical model. In our proposed scheme, no other participating entities including the cloud server or the third party auditor can access the content of the uploaded data, which ensures data integrity and user confidentiality. Moreover, our proposed scheme is more suitable for cloud-assisted applications and outperforms other existing schemes. Testing and evaluation in a simulated environment using Mininet validated the efficacy of our solution, paving the way for optimization and fine-tuning to further enhance performance and resource utilization. Documenting our implementation and findings provides valuable insights for future research and development in the field . In essence, our work contributes to the advancement of Data security by providing a practical and scalable solution to combat lack of integrity in data , safeguarding critical network infrastructure and services.

VII. REFERENCE

[1] Avinash Singh,Richard Adeyemi Ikuesan,Hein Venter Secure Storage Model for Digital Forensic Readiness IEEE Access, 2022

[2] Wael A. Mahrous,Mahmoud Farouk,Saad M. Darwish An Enhanced Blockchain-Based IoT Digital Forensics Architecture Using Fuzzy Hash IEEE Access, 2021

[3] Arafat Al-Dhaqm, Richard Adeyemi Ikuesan, Victor R. Kebande, Shukor Abd Razak, George Grispos, Kim-Kwang Raymond Choo, Bander Ali Saleh Al-Rimy, Abdulrahman A. Alsewari. "Digital Forensics Subdomains: The State of the Art and Future Directions." IEEE Access, 2021.

[4] Jianyu Xiao, Shancang Li, Qingliang Xu. "Video-Based Evidence Analysis and Extraction in Digital Forensic Investigation." IEEE Access, 2019.

[5] Junghoon Oh, Sangjin Lee, Hyunuk Hwang. "Forensic Recovery of File System Metadata for Digital Forensic Investigation." IEEE Access, 2022.

[6] Arafat Al-Dhaqm, Shukor Abd Razak, Siti Hajar Othman, Abdulalem Ali, Fuad A. Ghaleb, Arieff Salleh Rosman, Nurazmallail Marni. "Database Forensic Investigation Process Models: A Review." IEEE Access, 2020.

[7] Amit Kumar, Gurinder Singh, Ankush Kansal, Kulbir Singh. "Digital Image Forensic Approach to Counter the JPEG Anti-Forensic Attacks." IEEE Access, 2020.

[8] Ana Lucila Sandoval Orozco, Carlos Quinto Huamán, Jenny Alexandra Cifuentes Quintero, Luis Javier García Villalba. "Digital Video Source Acquisition Forgery Technique Based on Pattern Sensor Noise Extraction." IEEE Access, 2019.

[9] Sung Jin Lee, Gi Bum Kim. "K-FFRaaS: A Generic Model for Financial Forensic Readiness as a Service in Korea." IEEE Access, 2021.

[10] D. Gonzalez and T. Hayajneh. "Detection and prevention of crypto-ransomware." Proc. IEEE 8th Annu. Ubiquitous Comput. Electron. Mobile Commun. Conf. (UEMCON), pp. 472-478, Oct. 2017.

[11] R. Von Solms and J. Van Niekerk. "From information security to cyber security." Comput. Secur., vol. 38, pp. 97-102, Oct. 2013.