CSE

by Cse Cse

Submission date: 01-Feb-2025 04:44AM (UTC-0800)
Submission ID: 2576828313
File name: 0130014734Advanced-Security-In-Digital-Forensic1-journal_1.docx (174.25K)
Word count: 3802
Character count: 24675

Advanced Security In Digital Forensics: Authenticated Storage With Key Based Encryption

1School of Mathematics, Hangzhou Normal University, Hangzhou 311121, China 2Key Laboratory of Cryptography of Zhejiang Province, Hangzhou Normal University, Hangzhou 311121, China 3School of Information Science and Engineering, NingboTech University, Ningbo 315199, China

1School of Mathematics, Hangzhou Normal University, Hangzhou 311121, China 2Key Laboratory of Cryptography of Zhejiang Province, Hangzhou Normal University, Hangzhou 311121, China 3School of Information Science and Engineering, NingboTech University, Ningbo 315199, China

1School of Mathematics, Hangzhou Normal University, Hangzhou 311121, China 2Key Laboratory of Cryptography of Zhejiang Province, Hangzhou Normal University, Hangzhou 311121, China 3School of Information Science and Engineering, NingboTech University, Ningbo 315199, China

1School of Mathematics, Hangzhou Normal University, Hangzhou 311121, China 2Key Laboratory of Cryptography of Zhejiang Province, Hangzhou Normal University, Hangzhou 311121, China 3School of Information Science and Engineering, NingboTech University, Ningbo 315199, China

1School of Mathematics, Hangzhou Normal University, Hangzhou 311121, China 2Key Laboratory of Cryptography of Zhejiang Province, Hangzhou Normal University, Hangzhou 311121, China 3School of Information Science and Engineering, NingboTech University, Ningbo 315199, China

Abstract— **The digital forensics industry requires comprehensive solutions to protect digital evidence faces major challenges. The cloud forensics discipline protects digital evidence through modern techniques that lose credibility when all evidence is stored in one location. This paper presents a novel approach to digital forensic architecture, titled "Advanced Security in Digital Forensics: Authenticated Storage with Key-Based Encryption." Our system brings together SBVM and EEO for security creation while meeting both reliability and strong encryption standards. Our system selects ECC encryption because this technology offers strong security protection. Following encryption the data travels to secure storage spaces on our cloud platform. Our solution delivers higher security outcomes than current practices plus enhances dependability and efficiency for forensic work in cloud settings.**

Keywords- Digital forensics, cloud forensics, secure block verification mechanism, optimal key generation, enhanced equilibrium optimizer, Elliptic Curve Cryptography, data encryption, cloud storage, digital evidence security, forensics architecture, performance metrics.

I. Introduction

Our digital transformation era saw cloud computing become popular because it changed how people and companies handle and access digital data. Cloud adoption now affects digital forensics practices because it creates new problems when protecting digital evidence. In cloud environments, where data is distributed across various locations, frequently updated, and subject to various online threats such as hacking, data tampering, and unauthorized access, the need for robust security and integrity mechanisms has never been more critical. Traditional digital forensic methods, which are typically designed for centralized storage systems, struggle to address these issues in the cloud due to the inherent complexity and dynamic nature of cloud infrastructure. The lack of efficient mechanisms for evidence authentication, secure storage, and reliable retrieval further compounds these challenges.[1]To address these growing concerns, this project presents an innovative forensic architecture called "Advanced Security in Digital Forensics: Authenticated Storage with Key-Based Encryption." This new approach combines the strengths of modern cryptographic and optimization technologies to create a secure and efficient framework for managing digital evidence in cloud environments. One of the key features of the proposed architecture is the Secure Block Verification Mechanism (SBVM), which is designed to authenticate evidence blocks by verifying their integrity and ensuring they have not been tampered with during storage or transfer. SBVM operates by using hash-based methods and digital signatures to ensure the authenticity of each data block, making it resistant to alterations, whether malicious or accidental.[20]

A major challenge in digital forensics is the management of cryptographic keys. For this reason, the architecture

introduces an Enhanced Equilibrium Optimizer (EEO) model for generating secret keys used in encryption processes. The EEO model optimizes the key generation process by considering multiple factors such as security strength, computational efficiency, and resource consumption. This allows for the creation of highly secure yet computationally efficient keys, which are crucial for maintaining the performance of cloud-based systems without sacrificing security[17].

Our proposal uses ECC encryption to strengthen the security of stored data. ECC solves security problems effectively using shorter keys which decreases the hardware resources needed compared to RSA. ECC suits cloud computing because cloud systems typically run on constrained resources with high performance needs. The cloud system safely stores encrypted data so that authorized persons have access to the evidence and unauthorized persons cannot[2].Our design benefits from easy expansion capacity. Our system handles huge digital evidence collections effectively while staying fast. Cloud storage lets the system handle more forensic data while keeping excellent performance which supports today's bigger distributed law enforcement work.

Adding cloud storage helps us easily access evidence correctly while keeping our data safe. Officials can gather and examine digital evidence quickly which makes their work faster and increases digital investigation outcomes. Fast evidence access helps investigators complete their work quickly because time-sensitive cases require fast responses for successful digital forensics[21].

Our project uses modern technology while fixing historic evidence inspection problems to develop a practical secure digital forensics system. The system helps forensic investigators of all backgrounds keep their digital evidence secure while preserving evidence authenticity and simplifying evidence storage or retrieval operations. This advanced architecture responds to cloud challenge growth to offer digital forensics tools that protect evidence quality and make investigators work faster and more effective[15]

A. Objective Of The Study

The objective of this research is to develop an advanced digital forensic architecture, titled "Advanced Security in Digital Forensics: Authenticated Storage with Key-Based Encryption," to address the challenges of securing and preserving digital evidence in cloud environments. This architecture aims to enhance security and reliability by incorporating a Secure Block Verification Mechanism (SBVM) for robust authentication, utilizing an Enhanced Equilibrium Optimizer (EEO) model for efficient key generation, and employing Elliptic Curve Cryptography (ECC) for strong data encryption. By achieving these goals, the proposed model seeks to outperform existing approaches in ensuring the integrity, confidentiality, and accessibility of digital evidence while enhancing the efficiency and reliability of cloud-based forensic investigations[3].

B. Scope Of The Study

This research focuses on developing a secure and efficient digital forensic architecture tailored for cloud environments, addressing challenges in evidence integrity, authentication, and storage. It incorporates a Secure Block Verification Mechanism (SBVM) for authentication, an Enhanced Equilibrium Optimizer (EEO) for key generation, and Elliptic Curve Cryptography (ECC) for encryption. Designed for scalability and adaptability, the architecture aims to support secure and reliable evidence management for forensic investigations, providing improved performance and practical applicability in cloud-based scenarios.

C. Problem statement

[24]The field of digital forensics faces significant challenges in ensuring the security, integrity, and reliability of digital evidence, particularly in cloud environments where centralized evidence collection and storage are vulnerable to online threats and unauthorized access. Existing approaches often lack robust mechanisms for authentication, efficient encryption, and secure key management, leading to compromised evidence integrity and reliability [4]. This highlights the need for a novel forensic architecture that can effectively address these limitations by providing enhanced security, reliable authentication, and efficient data management to safeguard digital evidence in cloud-based forensic investigations.

II. Related Work

[3] Biedermann, A., & Taroni, F. (2018) The role of forensic science in the criminal justice system: A reflection on the concept of evidence and the challenges of advancing towards new paradigms.This study emphasizes the transformative role of forensic science in strengthening the criminal justice system. By examining the evolving nature of forensic evidence, the research underscores the limitations of traditional paradigms in addressing the complexity of modern evidence interpretation. The study advocates for the integration of forensic methods with broader scientific principles to improve evidence credibility and reliability. It also highlights the need for interdisciplinary collaboration and the adoption of innovative technologies to overcome challenges in forensic analysis, interpretation, and presentation in courtrooms[16].

[2] Dykstra, J., & Sherman, A. T. (2013) Design and implementation of FROST: Digital forensic tools for the OpenStack cloud computing platform. This research introduces FROST, a specialized suite of digital forensic tools developed for the OpenStack cloud platform, addressing challenges unique to virtualized infrastructures. The study demonstrates how FROST facilitates secure, scalable, and efficient forensic investigations within cloud environments. Key contributions include methods for the collection, preservation, and analysis of data in a virtualized setting while maintaining chain-of-custody integrity. The implementation of FROST showcases its

utility in reducing complexities associated with data volatility, multi-tenancy, and remote storage, ultimately setting a benchmark for future forensic tools in cloud ecosystems.

[22]Stallings, W. (2016) Cryptography and network security: Principles and practice. This comprehensive text serves as a cornerstone for understanding cryptographic methods and network security principles. It provides an in-depth exploration of encryption techniques, authentication protocols, and secure communication mechanisms. These principles are crucial for implementing robust digital forensic processes and protecting sensitive data. The book also delves into key management strategies, digital signatures, and public key infrastructures, offering practical insights for securing forensic evidence, ensuring data integrity, and safeguarding systems from cyber threats.

[23]Wang, L., Zhang, Z., & Hung, P. C. K. (2012) Cloud computing security: Fundamentals, mechanisms, and applications. This research outlines the foundational principles and security mechanisms necessary for safeguarding cloud computing environments. It offers a detailed analysis of the unique challenges posed by cloud ecosystems, including data breaches, unauthorized access, and regulatory compliance. The study provides actionable solutions for secure application development in the cloud, such as encryption, access control, and intrusion detection systems. These mechanisms play a vital role in forensic investigations within cloud environments by ensuring secure data acquisition, storage, and analysis while maintaining evidence integrity.

[18] Wang, C., Wang, Q., Ren, K., Cao, N., & Lou, W. (2010) Toward secure and dependable storage services in cloud computing. This study proposes a robust framework for enhancing the security and dependability of cloud storage services. By focusing on key aspects like data integrity, confidentiality, and availability, the research addresses critical challenges faced by cloud storage systems. The proposed mechanisms, including dynamic data auditing and distributed storage verification, mitigate risks related to data tampering and loss. These advancements are instrumental for forensic investigations, ensuring that stored evidence remains trustworthy, tamper-proof, and readily accessible during legal proceedings[13].

III. Proposed Cloud-Based Secure Fingerprint Authentication and File Management System

The proposed system enhances cloud forensics by incorporating authenticated storage and key-based encryption. It uses a secure block verification mechanism (SBVM) to ensure evidence integrity, while secret keys are generated using an Enhanced Equilibrium Optimizer (EEO) model. Data is encrypted with Elliptic Curve Cryptography (ECC) and securely stored on the cloud, ensuring both security and privacy. Simulation results show that this approach outperforms existing methods in terms of security, reliability, and efficiency[19].

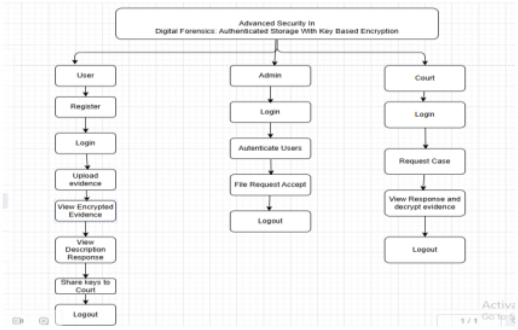

Fig 1 : *Flow chart of Advanced Security In Digital Forensics: Authenticated Storage With Key Based Encryption*

A. Methods

ECC technology develops safe encryption styles through elliptic curves that need less computing power. The ECC system protects data at strength levels similar to RSA but needs only compact encryption keys. Due to their short keys ECC offers faster processing on small devices in both mobile and Internet of Things functions[5]. Thanks to ECDLP and elliptic curve algebra your data stays protected within the Elliptic Curve Cryptography system platform. Organizations use ECC security tools because these tools shield internet services from data theft using SSL/TLS certificates and digital signing methods[14].

B. ECC shows top-level scalability while maintaining excellent system speed. To achieve an equivalent level of protection ECC uses a 256-bit key which requires far less processing and usage space than RSA's 3072-bit key. ECC offers this high efficiency that makes it ideal for Bitcoin use because the network depends on ECC for protecting digital transactions and user signatures. ECC helps build many cryptographic tools by letting users use it for public-key encryption digital signatures and key exchange both in symmetric and asymmetric systems. ECC stays important for secure communication as people need better protection without higher processing costs[6].

C. Advantages

The following are the advantages of our Cloud-Based Secure Fingerprint Authentication and File Management System:

Elliptic Curve Cryptography (ECC) provides several advantages compared to traditional encryption algorithms like RSA. One of its main benefits is that it offers the same level of security as RSA but with significantly smaller key sizes. This results in faster encryption and decryption processes, leading to lower computational demands. As a consequence, ECC is highly efficient, making it ideal for use in devices with limited resources, such as mobile phones, embedded systems, and IoT devices.

In addition to its speed, ECC is known for its low resource consumption. It consumes less memory,

bandwidth, and power, which makes it a great option for environments where resources are constrained. This aspect is particularly valuable in today's technology landscape, where optimizing performance is critical[26].

ECC also stands out for its strong security, which is based on the complexity of the elliptic curve discrete logarithm problem (ECDLP). The difficulty of solving this problem ensures that ECC provides robust protection against various types of attacks. Moreover, ECC is flexible in terms of scalability, allowing the adjustment of security levels by using smaller key sizes without compromising its effectiveness[7].

The combination of these features makes ECC an ideal solution for securing communications and sensitive data, particularly in applications where efficiency, security, and adaptability are crucial.

IV. Modules and its Implementation

User:

1. Login: Investigators log into the system using their credentials.
2. Register: Users can register with providing the required information.
3. Request to admin for share data: The case user should be take a permission from the admin to share the evidence information to the court.
4. View Decryption key response from admin: The admin should be share the decryption key's to the user for decrypt the data
5. Upload Evidence Data: The case user can able to share the evidence information with the encryption format with the decryption key to the requested court.
6. Share to court: Now The user can share the evidence information to the court.
7. Logout: The user should be logout.

Admin Modules:

1. Login: Admins log into the system using their credentials.
2. View Users: Admins view details of all registered users.
3. Manage Evidence: Admins oversee the evidence data collection, and storages of that digital evidence.
4. Monitor Encryption and Key Generation: Admins supervise encryption and key generation processes to the users.
5. Logout: Admin can Logout.

Court Module:

1. Login: Court can login using default credentials.
2. View the case numbers: the court can view the case numbers and can request for file access from evidences.
3. View response: The court can view the evidence response for decryption key from the case users.
4. Logout: the court can logout successfully.

Feature	**Multi homomorphic Encryption (MHE)**	**Elliptic Curve Cryptography (ECC)**
Cryptographic Model	Based on homomorphic encryption, allows computations on encrypted data.	Based on elliptic curves and the difficult elliptic curve discrete logarithm problem (ECDLP).
Security Level	Provides high security for data while enabling computations, but can be slower.	Provides high security with smaller key sizes, ensuring faster computations and reduced overhead.
Efficiency	Can be computationally expensive, particularly for large datasets and complex operations.	ECC is highly efficient, providing robust security with smaller key sizes, making it faster for encryption and decryption.
Key Size	Larger key sizes required for high security levels, leading to increased storage and computational burden.	ECC achieves comparable security with much smaller key sizes, significantly reducing resource requirements.
Scalability	Not as scalable as ECC, with performance degradation for large-scale applications.	ECC is highly scalable, offering adjustable security levels with smaller keys, making it ideal for resource-constrained devices.
Computational Overhead	High computational overhead, especially when handling large volumes of encrypted data.	ECC has lower computational overhead compared to other cryptographic methods like RSA, making it suitable for

		mobile and IoT devices.
Resource Consumption	Requires significant resources, including memory and bandwidth.	ECC consumes less memory, bandwidth, and power, making it ideal for low-resource environments.
Use Cases	Mainly used in applications that require secure computations on encrypted data, such as privacy-preserving computations.	ECC is widely used for secure communications, digital signatures, and key exchange protocols, particularly in mobile networks and IoT devices.
Security Foundation	Built on the hardness of mathematical problems in homomorphic encryption.	ECC's security is based on the elliptic curve discrete logarithm problem (ECDLP), which is difficult to solve.
Implementation Complexity	More complex to implement due to the need for specialized algorithms and larger key management.	ECC is relatively easier to implement compared to multi homomorphic encryption, with widespread support in cryptographic libraries.

V. RESULTS

The admin is responsible for managing user access by reviewing and either authenticating or rejecting users based on set criteria[27]. This ensures that only verified users are allowed to interact with the platform. Once authenticated, users can access uploaded data, though it remains encrypted to maintain confidentiality. This encryption ensures that sensitive information is protected from unauthorized access. Additionally, the admin has the authority to approve or deny access to uploaded files, notifying users when they are granted permission to view the data.[12]

When users request access to files, the admin reviews and responds to these requests, ensuring that file access is granted or denied according to the platform's access control policies. After the admin approves a file request, users receive an email notification informing them when the data is ready for decryption. To access the decrypted data, users must enter a decryption key, which guarantees that only authorized individuals are able to view the sensitive content. This secure process ensures that both data privacy and user access are carefully managed [8].

VI. CONCLUSION

In conclusion, the proposed "Advanced Security in Digital Forensics: Authenticated Storage with Key-Based Encryption" architecture provides a robust solution to the challenges of securing digital evidence in cloud environments. By integrating secure block verification, key-based encryption using an Enhanced Equilibrium Optimizer model for key generation, and Elliptic Curve Cryptography[9] for data encryption, this approach ensures both the integrity and confidentiality of digital evidence. The simulation results validate its superior performance, demonstrating improved security, reliability, and efficiency compared to existing methods, making it a promising advancement for digital forensics in cloud-based settings[25].

VII. FUTURE ENHANCEMENT

Future enhancements to the proposed architecture could involve incorporating advanced machine learning techniques for real-time threat detection and dynamic adaptation to evolving cyberattacks, further improving the system's security. Additionally, integrating decentralized storage solutions, such as blockchain, could[10] enhance evidence integrity and transparency by providing an immutable ledger of data access and modifications. Exploring lightweight cryptographic algorithms optimized for cloud environments could also improve performance without compromising security. Furthermore, the system could be extended to support multi-cloud environments, ensuring scalability and broader applicability across diverse forensic scenarios, thereby strengthening the resilience of digital forensics in complex cloud ecosystems[11].

VIII. REFERENCES

[1]. Abaido, G. M. (2020). Cyberbullying on social media platforms among university students in the United Arab Emirates. *International Journal of Adolescence and Youth*, *25*(1), 407–420. https://doi.org/10.1080/02673843.2019.1669059

[2]. Aboujaoude, E., Savage, M. W., Starcevic, V., & Salame, W. O. (2015). Cyberbullying: Review of an old problem gone viral. *Journal of Adolescent Health*, *57*(1), 10–18. https://doi.org/10.1016/J.JADOHEALTH.2015.04.011

[3]. Adinolf, S., & Türkay, S. (2018). Toxic behaviors in eSports games: Player perceptions and coping strategies. *CHI PLAY 2018 - Proceedings of the 2018 Annual Symposium on Computer-Human Interaction in Play Companion Extended Abstracts*, 365–372. https://doi.org/10.1145/3270316.3271545

[4]. Alenezi, A., Atlam, H. F., & Wills, G. B. (2019a). Experts reviews of a cloud forensic readiness framework for organizations. *Journal of Cloud Computing*, *8*(1), 1–14. https://doi.org/10.1186/S13677-019-0133-Z/FIGURES/3

[5]. Alenezi, A., Atlam, H. F., & Wills, G. B. (2019b). Experts reviews of a cloud forensic readiness framework for organizations. *Journal of Cloud Computing*, *8*(1), 1–14. https://doi.org/10.1186/S13677-019-0133-Z/FIGURES/3

[6]. Alouffi, B., Hasnain, M., Alharbi, A., Alosaimi, W., Alyami, H., & Ayaz, M. (2021). A Systematic Literature Review on Cloud Computing Security: Threats and Mitigation Strategies. *IEEE Access*, *9*, 57792–57807. https://doi.org/10.1109/ACCESS.2021.3073203

[7]. Alshabibi, M. M., Bu dookhi, A. K., & Hafizur Rahman, M. M. (2024). Forensic Investigation, Challenges, and Issues of Cloud Data: A Systematic Literature Review. *Computers 2024, Vol. 13, Page 213*, *13*(8), 213. https://doi.org/10.3390/COMPUTERS13080213

[8]. Bharadiya, J. (2023). Machine Learning in Cybersecurity: Techniques and Challenges. *European Journal of Technology*, *7*(2), 1–14. https://doi.org/10.47672/EJT.1486

[9]. Chen, J. G. (2018). Electrochemical CO2 Reduction via Low-Valent Nickel Single-Atom Catalyst. *Joule*, *2*(4), 587–589. https://doi.org/10.1016/J.JOULE.2018.03.018

[10]. Infante, L., Hallman, R. A., Hays, J., Cronnon, E., & Stav, U. (2024). Recovery CAT: A Digital Forensics Tool for Cryptocurrency Investigations. *12th International Symposium on Digital Forensics and Security, ISDFS 2024*. https://doi.org/10.1109/ISDFS60797.2024.10527279

[11]. Khalaf, R. S., & Varol, A. (2019). Digital forensics: Focusing on image forensics. *7th International Symposium on Digital Forensics and Security, ISDFS 2019*. https://doi.org/10.1109/ISDFS.2019.8757557

[12]. Khalil, I. M., Khreishah, A., & Azeem, M. (2014). Cloud computing security: A survey. *Computers*, *3*(1). https://doi.org/10.3390/COMPUTERS3010001

[13]. Majed, H., Noura, H. N., & Chehab, A. (2020). Overview of Digital Forensics and Anti-Forensics Techniques. *8th International Symposium on Digital Forensics and Security, ISDFS 2020*. https://doi.org/10.1109/ISDFS49300.2020.9116399

[14]. Malik, A. W., Bhatti, D. S., Park, T. J., Ishtiaq, H. U., Ryou, J. C., & Kim, K. Il. (2024). Cloud Digital Forensics: Beyond Tools, Techniques, and Challenges. *Sensors (Basel, Switzerland)*, *24*(2), 433. https://doi.org/10.3390/S24020433

[15]. Mieremet, A., Alberink, I., Hoogeboom, B., & Vrijdag, D. (2018). Probability intervals of speed estimations from video images: The Markov Chain Monte Carlo approach. *Forensic Science International*, *288*, 29–35. https://doi.org/10.1016/J.FORSCIINT.2018.04.003

[16]. Paruchuri, S., Perry-Smith, J. E., Chattopadhyay, P., & Shaw, J. D. (2018). New Ways of Seeing: Pitfalls and Opportunities in Multilevel Research. *Academy of Management Journal*, *61*(3), 797–801. https://doi.org/10.5465/AMJ.2018.4003

[17]. Patel, S. H., Morreale, S. J., Panagopoulou, A., Bailey, H., Robinson, N. J., Paladino, F. V., Margaritoulis, D., & Spotila, J. R. (2015). Changepoint analysis: A new approach for revealing animal movements and behaviors from satellite telemetry data. *Ecosphere*, *6*(12). https://doi.org/10.1890/ES15-00358.1

[18]. Ratmele, A. (2018). Wormhole Detection and Removal Algorithm in Mobile Ad-hoc Networks using Enhanced Cluster based Technique. *International Journal of Computer Applications*, *179*(30), 975–8887.

[19]. Rivest, R. L., Shamir, A., & Adleman, L. (1978). A method for obtaining digital signatures and public-key cryptosystems. *Communications of the ACM*, *21*(2), 120–126. https://doi.org/10.1145/359340.359342

[20]. Roussev, V., & Quates, C. (2013). File fragment encoding classification—An empirical approach. *Digital Investigation*, *10*, S69–S77. https://doi.org/10.1016/J.DIIN.2013.06.008

[21]. Silvarajoo, V. R., Yun Lim, S., & Daud, P. (2021). Digital Evidence Case Management Tool for Collaborative Digital Forensics Investigation. *2021 3rd International Cyber Resilience Conference, CRC 2021*. https://doi.org/10.1109/CRC50527.2021.9392497

[22]. Suvarna, D., Km, M., Gupta, M., Gabburi, S., Honnavalli, P., & Vm, S. (2024). The Development of a Digital Forensic Framework for Ease of Forensic Analysis. *12th International Symposium on Digital Forensics and Security, ISDFS 2024*. https://doi.org/10.1109/ISDFS60797.2024.10527263

[23]. *Vol. 8 No. 5 (2017): May-June 2017 | International Journal of Advanced Research in Computer Science*. (n.d.). Retrieved February 1, 2025, from https://ijarcs.info/index.php/Ijarcs/issue/view/64

[24]. Warbhe, A. D., Dharaskar, R. V., & Thakare, V. M. (2016). Digital image forensics: An affine transform robust copy-paste tampering detection. *Proceedings of the 10th International Conference on Intelligent Systems and Control, ISCO 2016*. https://doi.org/10.1109/ISCO.2016.7727045

[25]. Xu, R., Baracaldo, N., & Joshi, J. (2021). *Privacy-Preserving Machine Learning: Methods, Challenges and Directions*. https://arxiv.org/abs/2108.04417v2

CSE

ORIGINALITY REPORT

10%	7%	8%	2%
SIMILARITY INDEX	INTERNET SOURCES	PUBLICATIONS	STUDENT PAPERS

PRIMARY SOURCES

1	www.aimspress.com Internet Source	3%
2	ijcem.in Internet Source	1%
3	www.scipublications.com Internet Source	1%
4	Submitted to The Moraitis School Student Paper	<1%
5	Submitted to Vientiane International School Student Paper	<1%
6	"Crime Scene Management within Forensic Science", Springer Science and Business Media LLC, 2022 Publication	<1%
7	Arukala, Himateja. "Factorization in Cybersecurity: A Dual Role of Defense and Vulnerability in the Age of Quantum Computing", Illinois State University, 2024 Publication	<1%

8	Munirah Maher Alshabibi, Alanood Khaled Bu dookhi, M. M. Hafizur Rahman. "Forensic Investigation, Challenges, and Issues of Cloud Data: A Systematic Literature Review", Computers, 2024 Publication	<1 %
9	www.switchtraining.eu Internet Source	<1 %
10	Siraj Uddin Qureshi, Jingsha He, Saima Tunio, Nafei Zhu, Ahsan Nazir, Ahsan Wajahat, Faheem Ullah, Abdul Wadud. "Systematic review of deep learning solutions for malware detection and forensic analysis in IoT", Journal of King Saud University - Computer and Information Sciences, 2024 Publication	<1 %
11	crypto.stanford.edu Internet Source	<1 %
12	dfrws.org Internet Source	<1 %
13	Abdullah Mujawib Alashjaee, Fahad Alqahtani. "Improving Digital Forensic Security: A Secure Storage Model with Authentication and Optimal Key Generation based Encryption", IEEE Access, 2024 Publication	<1 %

14	H S Madhusudhan, Punit Gupta, Pradeep Singh Rawat. "Advanced Computing Techniques for Optimization in Cloud", CRC Press, 2024 Publication	<1 %
15	eitca.org Internet Source	<1 %
16	eprints.utm.my Internet Source	<1 %
17	Chang, Chin-Chen, Chin-Yu Sun, and Ting-Fang Cheng. "A dependable storage service system in cloud environment : A dependable storage service system in cloud environment", Security and Communication Networks, 2014. Publication	<1 %
18	Anuj Kumar Singh, Sachin Kumar. "Security, Privacy, and Trust in WBANs and E-Healthcare", CRC Press, 2024 Publication	<1 %
19	Chun-Ting Huang, Lei Huang, Zhongyuan Qin, Hang Yuan, Lan Zhou, Vijay Varadharajan, C.-C. Jay Kuo. "Survey on securing data storage in the cloud", APSIPA Transactions on Signal and Information Processing, 2014 Publication	<1 %
	mdsoar.org	

20	Internet Source	<1%
21	link.springer.com Internet Source	<1%

Exclude quotes	Off	Exclude matches	Off
Exclude bibliography	On		

CSE

GRADEMARK REPORT

FINAL GRADE

/0

GENERAL COMMENTS

PAGE 1

PAGE 2

PAGE 3

PAGE 4

PAGE 5

PAGE 6

PAGE 7