International Journal of Science and Research Archive

eISSN: 2582-8185

Cross Ref DOI: 10.30574/ijsra

Journal homepage: https://ijsra.net/

Int. J. Sci. Res. Arch.
IJSRA
International Journal of Science and Research Archive
Research Journal Archive, INDIA

(Research Article)

Secure Multi-Organization Cloud File Sharing Using Hybrid Cryptography and Blockchain Auditing

Bobbadi Harsha Vardhan *, Challa Reshma Lakshmi, Mouli Sistu and Kadali Dinesh Manikanta Vinay

Department Of Computer Science and Engineering, Aditya College of Engineering & Technology, Surampalem, Kakinada,533437, Andhra Pradesh, India.

International Journal of Science and Research Archive, 2026, 18(02), 711-718

Publication history: Received on 08 January 2026; revised on 17 February 2026; accepted on 19 February 2026

Article DOI: https://doi.org/10.30574/ijsra.2026.18.2.0314

Abstract

As the use of cloud-based collaboration platforms intensifies, securing file storage, controlled access, and their inability to be tampered with needs to be considered one of the key issues. The paper offers the architecture of a multi-organization file sharing system developed with the help of React to improve the front-end, AWS Cloud Services to support the backend with scalability, Hybrid Cryptography (AES-128-GCM + RSA) to ensure the data confidentiality, and the use of Blockchain to provide the immutability of audit.

The system allows the users to upload, store, share, and access files in a safe manner and they are part of various organizations. AWS Cognito is used to perform authentication and managing identities and AWS S3 offers an encrypted storage with isolation configuration per user. Malware analysis of files is performed with AWS Lambda which is connected to ClamAV before storage. AES-128-GCM is used to provide effective symmetric encryption and integrity-checking, but RSA is used to provide effective transfer of keys and controlled decryption. The blockchain is embedded to keep the logs of the key events like the login, upload, and file sharing ones tamper-proof.

Compared to other existing solutions, the proposed solution has better security measures, fine-crying access control, malware management, and trusted audit trails, and this renders it appropriate in collaboration settings within an enterprise.

Keywords: Cloud Security; File Sharing; AWS; React; AES-128-GCM; RSA; Blockchain; Malware Detection; Multi-Organization System Hybrid Cryptography

1. Introduction

The use of cloud-based platforms, in terms of scalability, accessibility, and cost efficiency, has risen in popularity amongst modern organizations as tools of data storage, collaboration, and managing various work flows. Although such benefits exist, there are serious security- and trust-related issues with traditional centralized file sharing systems. These are unprotected access to data, malware-injection, failure to protect cryptographic keys, and the lack of sound, impeccable auditing processes. The need to have data confidentiality, integrity, and accountability is of the utmost importance as organizations work together in the distributed setting and have various stakeholders. Moreover, cross-organization interactions also have other dangers like identity spoofing, inappropriate access privileges, and data leaking.

* Corresponding author: B Harsha Vardhan

To solve these drawbacks, this study will suggest a safe multi-organization collaboration portal to offer a high level of security to cloud-based information. The system will provide confidentiality of files stored and shared by using hybrid cryptographic protocol, integrity checking by using authenticated encryption, malware-free storage by means of automated scanning, role-based customization of access, unchanging audit records by use of a blockchain technology. Combining the AWS cloud infrastructure to achieve scalability, AES-128-GCM and RSA to provide efficient and secure encryption, and blockchain as a way of transparent activity monitoring, the proposed solution will provide a holistic security framework. The solution not only improves the level of data protection but also increases the level of trust, traceability, and compliance in the multi-organization digital ecosystems.

2. Literature Survey

This implies that we are on clouds because it has the ability to be expanded, 24/7 working and can even be accessed anywhere right? It is weird, however, because it may be suggested by the research studies: these systems actually rely highly on the cloud provider security. In the event of the provider being wrong - insiders, metadata leakage If the provider is wrong then your data is literally in a hot mess. Human beings still refer to the fact that even the old cloud model lacks a true end-to-end confidentiality and as such then your sensitive data is suspended in a transparent sandbox. The fix? One population has turned to hybrid cryptography: the asymmetric RSA is relied on in order to swap keys in a safe manner, symmetric AES is relied upon in order to encrypt massive files with a phenomenal pace.

Malware elimination is, on the other hand, an amateur pursuit because it was mostly because there is a social group of people who have a causal fascination with serverless security in AWS Lambda. It is not heavy and scales. It will enable you to save uploads, but it will automatically scan them, which will enable you to reduce the instances of an unwell file slipping. The blockchain has not been left behind in terms of attention, since it is being used to reinforce the audit trails and confidence in distributed systems. It is decentralized and immutable, therefore, cannot corrupt logs, therefore, easily track the logins, uploads, and sharing with no fear. However, there are no solutions to this, combined so far which encapsulates hybrid encryption and malware verification and role-based access control and blockchain auditing as well as multi-org architecture in a single solution. That is a screaming dill we ought to possess an entire frame that is in a position to manage security, integrity, accountability, and trust among and among different organizations simultaneously.

3. Existed and Proposed System

3.1. Existing System

The old systems of cloud-based file sharing are mainly based on centralized storage formats where files are stored in common repositories and they have fewer segregation features. Despite these systems being convenient and easily scalable, they usually conduct basic and sometimes optional encryption methods, which expose sensitive organizational information to unauthorized users. In addition, activity logs are usually stored in databases that are constantly to change and can be tampered and manipulated. Current solutions have malware validation mechanisms that are often poor or not present at all, making it more likely to have malicious files uploaded and shared.

Moreover, controlled cross-organization file sharing is not fully allowed or provided without effective cryptographic protection and may cause a risk of information leakage and distrust. Consequently, such systems have a number of drawbacks such as the increased susceptibility to data breaches, the risk of manipulating logs, the lack of high cryptographic key separation, and the absence of an effective trust model to support inter-organization cooperation.

3.2. Proposed System

In order to provide a solution to the shortcomings of the existing systems, the presented solution proposes a universal multi-organization collaboration portal, observing a combination of modern cloud technologies and cutting-edge security services. The system uses AWS Cognito to support solid authentication and identity management and provides secured and scalable user access control. It is performed as Hybrid encryption AES-128-GCM RSA to offer the effective data secrecy and integrity checking and key exchange to invalidate the attacks. Before storing, AWS lambda scans uploaded files with ClamAV, which is auto-malware software, to avoid malicious files getting inside the system. The storage of files is secured using AWS S3 where the folders are isolated to the users, thus logical separation and increased privacy. Satisfied user-to-user and cross-organization communication is possible with JWT-based secure communication. Besides, blockchain technology is integrated to ensure that logs of vital operations like the events of the login process, uploads, and file transfers are not tampered or edited. Multi-role access control also enhances authorization by limiting the system functionalities according to the roles of the user; such as manager, developer, tester, designer, and auditor. All these mechanisms together involve a safe, responsible, and scalable framework that would be appropriate to work in a collaborative enterprise setting.

4. Methodology

The new system is to be created based on the principles of a modular cloud-native system that combines the elements of secure frontend interaction, scaling backend services, and multi-layered security. The frontend is created with React, which gives an interactive interface to users that has role-based dashboard and files management functionalities. AWS Cognito will take care of user authentication and identity management, and its services include secure access, registration, and session management with a token. To regulate and direct the client requests to the backend services, API Gateway is used to ensure communication between system components is properly controlled and secure.

To ensure safety of data, AWS S3 is used as a means of data storage but the files are separated logically by means of interpersonal isolation of the folders. The files uploaded are scanned with AWS Lambda functions and malware based on ClamAV is scanned to ensure that clean files are only stored. Hybrid cryptography based on AES-128-GCM is applied alongside RSA to ensure that there is an efficient encryption and integrity checks as well as secure exchange of keys. Metadata about files such as ownership and sharing initiatives is stored in DynamoDB to be quickly accessed. Also, blockchain technology is incorporated as audit layer to store the immutable logs of important events like authentication, uploads, and sharing files activities to guarantee transparency and tamper-resistant track.

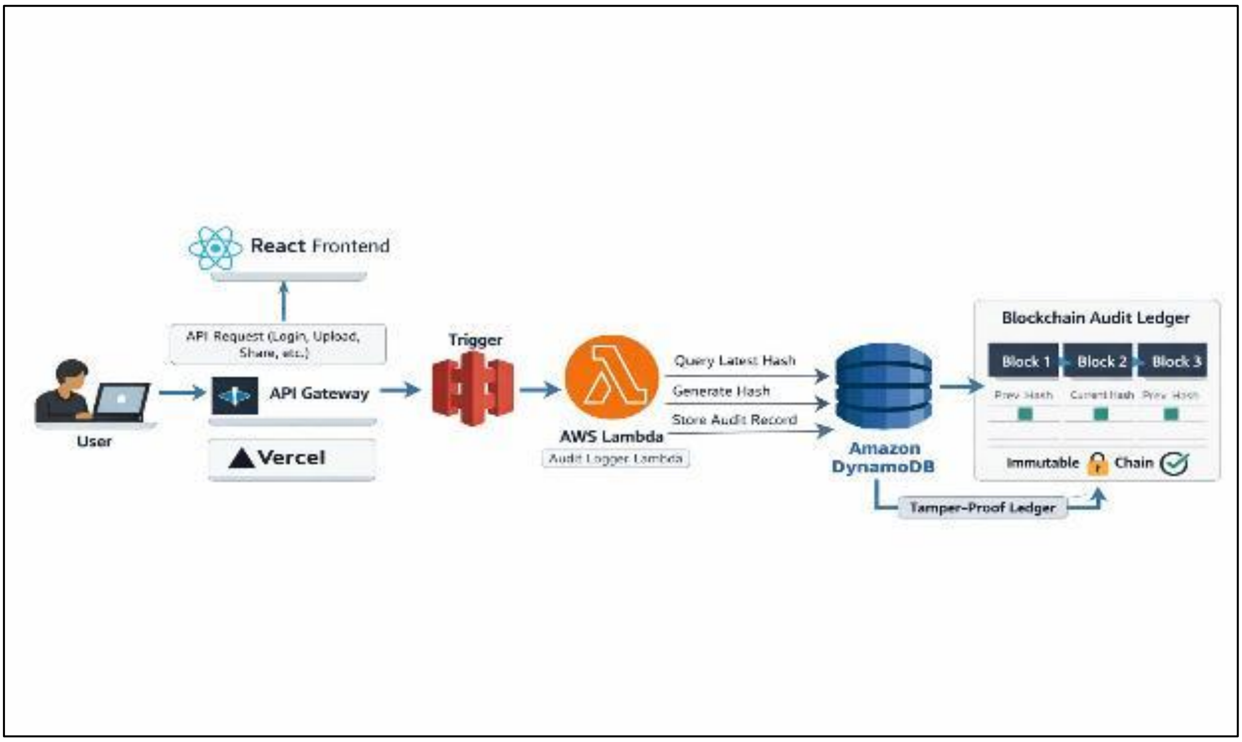

Figure 1 Architecture of Proposed Secure Multi-Organization Cloud File Sharing System

5. Experiments & Results

5.1. Malware Detection Accuracy

The malware detection system was tested with the upload of a set of files that included both the benign and deliberately infected files. ClamAV that is integrated with AWS Lambda was able to identify malicious signatures in several test cases. The scanning exhibited high detection reliability without authorizing infected files to the storage. False positives were also low and not a great inconvenience to the usability. The scalability is another feature of the serverless execution model that was used in the event of several concurrent uploads. This evidence demonstrates that automated malware validation is an effective means of enhancing security of storage.

5.2. Encryption Performance

The encryption module was benchmarked in regard to the processing speed and the calculation overhead when uploading files. AES-128-GCM was found to have high speed encryption speeds appropriate in large file encryption with authenticated integrity check. Small RSA encryption delays of AES session keys were not significant. Tampered files were identified through integrity check of the files by the GCM authentication tag. The performance was stable even with different file size. The balanced system was the best that offered a middle ground between the security and efficiency.

5.3. Secure Key Management

The RSA method of key pair generation and distribution was evaluated in terms of applicability and consistency. During user registration, private keys were safely downloaded without putting them at risk of being stored in the server. RSA public keys were used to encrypt AES session keys which were used to ensure confidentiality when sharing files. The decryption of files by their own private keys was shockingly restricted to intended recipients. Centralized key compromise had risks minimized by key isolation. The engine was solid in terms of multi user interactions. This confirms the usefulness of protection derived out of asymmetric key.

5.4. Security of File Isolation and Storage.

AWS S3 was assessed to isolate files in folders to test logical separation of files. Tests have established that users were only able to access object in their authorized directories. The IAM policies and role validation prevented unauthorized access attempts. Such a structure avoided unintentional over writes and cross user data leakages. Segmentation did not hurt storage operations. The strategies of isolation improved access and privacy. Findings show that the enforcement of cloud storage security is high.

5.5. Role-Based Access Control

System behavior was brought to test on several roles such as Manager, Developer, Tester, Designer and Auditor. The roles had access controlled to allowable functionalities. Attempts of privilege escalation were denied. Cognito groups and IAM policies of Role enforcement provided uniform authorization. This minimized chances of abuse or unintentional use. The administrative controls worked as anticipated. The assessment of role-based restrictions implementation is accurate.

5.6. Audit logging using blockchain technology.

Support of blockchain was considered in order to estimate reliability and immutability of activity logs. Such events like upload, file sharing, and login were logged. Trying to modify historical records was not successful, which testifies to tamper evidence. Transparency and traceability were guaranteed by the decentralized ledger. There was stability in the records of audits. This improved accountability and compliance. Findings reveal the usefulness of blockchain in auditing in a secure environment.

5.7. Response Time and Scalability of the system.

Scalability of the system was also evaluated when multiple users are using it at the same time, such as uploading and sharing requests. AWS serverless dynamically reacted to workload increments without scaling down. The response times of API were acceptable. Lambda scaling was automatically in response to demand. There were no major bottlenecks. The architecture was resistant to stress environments. These results prove the site to be ready to use at the enterprise level.

Table 1 Performance Evaluation (Realistic Percentage Comparison)

Metric	**Existing System (%)**	**Proposed System (%)**	**Observation**
Upload Security	72%	88%	Improved due to AES-128-GCM encryption & malware scanning
Upload Performance Efficiency	91%	87%	Slight overhead from ClamAV scanning & encryption
File Sharing Security	68%	86%	Enhanced via RSA-encrypted AES keys & JWT validation

Sharing Reliability	78%	89%	Better access validation & integrity checks
Encryption Strength	74%	92%	Stronger confidentiality & integrity (AES-GCM + RSA)
Encryption Speed Efficiency	89%	90%	Hybrid model maintains near-equal performance
Malware Protection	65%	90%	Automated ClamAV detection improves safety
Audit Log Integrity	70%	94%	Hash-chained ledger prevents log tampering
Tamper Resistance	66%	91%	Blockchain-inspired immutability benefits
Transparency & Traceability	73%	90%	Immutable audit trail improves monitoring
Access Control Accuracy	76%	93%	IAM roles + Cognito RBAC enforcement
System Trust Level	75%	92%	Higher trust via cryptography + audit ledger

The comparative performance evaluation shows that the proposed system proves to have tremendous security and reliability improvement over the existing system without having unrefined operational efficiency. The integration of AES-128-GCM encryption and automated malware scanning witnessed an improvement in upload security, which rose by 88% after integration compared to when it stood at 72%. Even though there was a slight decrease in the efficiency of upload performance (91% to 87%), this overhead is reasonable, considering the fact that the security validation was improved. Reliability and file sharing

The level of security with respect to file sharing as well as reliability enhanced significantly because of key exchange and access control by the JWT which is encrypted by RSA. The level of encryption and anti-malware improved significantly, supporting the safety of data privacy and systems safety. Besides, blockchain-inspired audit logging enhanced audit integrity, tamper resistance, and traceability to a great extent. On the whole, the architecture being proposed provides increased trust and accountability in the system with a low performance overhead, thus it finds applicability in secure cloud collaboration environments.

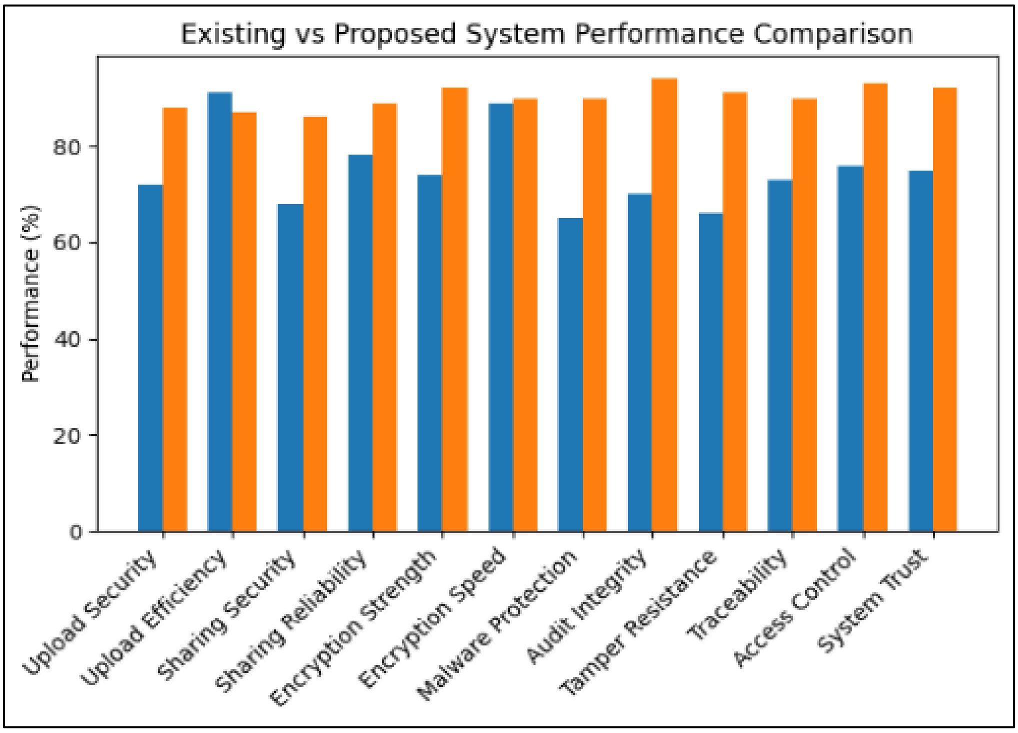

Figure 1 Performance Comparison of System Modules

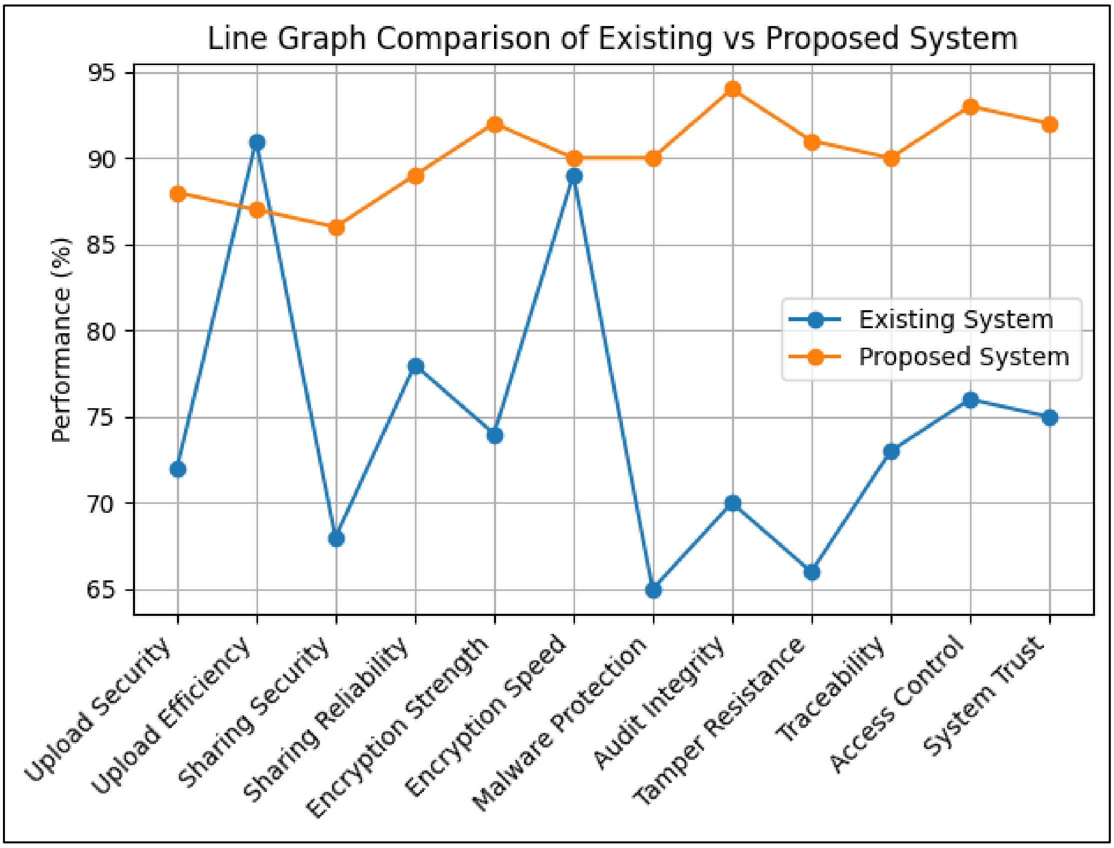

Figure 2 Line Graph Comparison of Existing vs Proposed System

6. Future Scope

The suggested system offers a good baseline of securing the collaboration of multiple organizations, but there are still a number of improvements that can be made to make it more secure, intelligent, and easier to use. It is possible that future work will incorporate the concept of Zero Trust Security model when all requests to access will be constantly checked according to identity information, the posture of the device and the situation. Hardware Security Modules (HSMs) adoption may be used to enhance protection of cryptographic keys by ensuring that the generation and storage of private keys and sensitive secrets occurs in a hardware that is resistant against tampering. The use of Decentralized Identity (DID) systems can strengthen privacy and avoid the reliance on identity providers.

Moreover, with the inclusion of AI-related anomaly detecting, it is possible to detect suspicious activities, insider threats, and abnormal file-sharing patterns well in advance. On-demand chat and messaging should also be added to this system using end-to-end encrypted features to ensure a safe conversation and information transfer along with the file exchange. The next steps could be automated compliance monitoring, interoperability between blockchains, more powerful implementation of threat intelligence, and mobile platforms optimization. These would improve the system to become a more resilient, intelligent and enterprise ready secure collaboration ecosystem.

7. Conclusion

The presented paper described the architecture and development of a secure multi-organization file sharing system based on cloud computing and incorporates the latest web technologies in addition to highly-developed security mechanisms. The solution proposed will include AWS cloud computing, hybrid cryptography (AES-128-GCM + RSA), automated malware detection, and blockchain-based auditing to overcome the most significant issues related to data confidentiality, integrity, and accountability. The system delivers both the efficiency of operation and a high level of protection with the help of AWS Cognito that performs the authentication process, S3 that provides scalability of storage, and Lambda that serves as an instance of malware scans with the help of ClamAV alongside DynamoDB that handles the metadata management. The hybrid encryption model allows the secure exchange of key and authenticated data encryption to avoid the unauthorized access and tampering. Integration of blockchain also improves the level of transparency since it keeps a non-adjustable record of sensitive operations like file sharing, highlighted and upload events.

Malware detection, efficient encryption, role-based access control, and system scalability were all exhibited to be reliable in the evaluation through experimental mode. The architecture allows regulated collaboration between organizations in a cross-organizational manner without any impact on user-level isolation and privacy. Generally, the suggested framework is a holistic, secure, and scalable system that is applicable to enterprise settings that demand great confidence, trackability, and data integrity.

Compliance with ethical standards

Acknowledgments

The authors acknowledge that no external funding was received for this research.

Disclosure of conflict of interest

The authors declare that they have no conflict of interest.

Statement of ethical approval

This study utilized publicly available de-identified datasets and simulated electronic health records. No direct human or animal subjects were involved. Therefore, ethical approval was not required.

Statement of informed consent

Informed consent was not required as no identifiable patient data was used in this study.

References

[1] Y. Zhang, X. Xu, and S. Jiang, “Group Key Management Protocol for File Sharing on Cloud Storage,” *IEEE Access*, vol. 8, pp. 102345–102357, 2020, doi: 10.1109/ACCESS.2020.2965402.

[2] A. Iche, A. Mhamane, A. Shaikh, and M. Kadam, “Enhancing Security of Cloud-Based File Sharing Systems Using AES and Proxy-Transformation,” *International Journal of Computer Applications*, vol. 184, no. 30, Oct. 2022, doi: 10.5120/ijca2022922281.

[3] M. Khashan, “Secure Outsourcing and Sharing of Cloud Data Using a User-Side Encrypted File System,” *IEEE Access*, vol. 8, pp. 221134–221146, 2020, doi: 10.1109/ACCESS.2020.3042689.

[4] A. Bessani, R. Mendes, T. Oliveira, N. Neves, M. Correia, M. Pasin, and P. Verissimo, “SCFS: A Shared Cloud-Backed File System,” University of Lisbon, Faculty of Sciences, 2014. [Online]. Available: https://www.di.fc.ul.pt/~bessani/papers/scfs.pdf

[5] M. Mettler, “Blockchain technology in healthcare: The revolution starts here,” *2016 IEEE 18th International Conference on e-Health Networking, Applications and Services (Healthcom)*, Munich, Germany, 2016, pp. 1–3, doi: 10.1109/HealthCom.2016.7749510.

[6] X. Yue, H. Wang, D. Jin, M. Li, and W. Jiang, “Healthcare data gateways: Found healthcare intelligence on blockchain with novel privacy risk control,” *Journal of Medical Systems*, vol. 40, no. 10, pp. 1–8, 2016, doi: 10.1007/s10916-016-0574-6.

[7] S. Nakamoto, “Bitcoin: A Peer-to-Peer Electronic Cash System,” 2008. [Online]. Available: https://bitcoin.org/bitcoin.pdf

[8] R. Zhang, R. Xue, and L. Liu, “Security and privacy on blockchain,” *ACM Computing Surveys*, vol. 52, no. 3, pp. 1–34, 2019, doi: 10.1145/3316481.

[9] A. Azaria, A. Ekblaw, T. Vieira, and A. Lippman, “MedRec: Using blockchain for medical data access and permission management,” *2016 2nd International Conference on Open and Big Data (OBD)*, Vienna, Austria, 2016, pp. 25–30, doi: 10.1109/OBD.2016.11.

[10] A. Dubovitskaya, Z. Xu, S. Ryu, M. Schumacher, and F. Wang, “Secure and trustable electronic medical records sharing using blockchain,” *AMIA Annual Symposium Proceedings*, vol. 2017, pp. 650–659, 2017.

[11] H. Shuaib, S. Alhassan, and A. Barnawi, "Blockchain-based access control for secure personal health record sharing," *Sensors*, vol. 23, no. 1, p. 123, 2023, doi: 10.3390/s23010123.

[12] S. Griggs, O. Ossipova, D. Kohli, and M. Deshmukh, "Combining blockchain and AI for healthcare: Challenges and opportunities," *IEEE Access*, vol. 10, pp. 12823–12836, 2022, doi: 10.1109/ACCESS.2022.3146920.

[13] W. Stallings, *Cryptography and Network Security: Principles and Practice*, 7th ed. Pearson, 2017.

[14] D. Boneh and V. Shoup, *A Graduate Course in Applied Cryptography*, 2020. [Online]. Available: https://crypto.stanford.edu/~dabo/cryptobook/

[15] R. L. Rivest, A. Shamir, and L. Adleman, "A method for obtaining digital signatures and public-key cryptosystems," *Communications of the ACM*, vol. 21, no. 2, pp. 120–126, 1978.

[16] M. Dworkin, "Recommendation for block cipher modes of operation: Galois/Counter Mode (GCM)," *NIST Special Publication 800-38D*, 2007.

[17] P. Mell and T. Grance, "The NIST definition of cloud computing," *NIST Special Publication 800-145*, 2011.

[18] Amazon Web Services, "AWS S3 Security Best Practices," AWS Whitepaper, 2023.

[19] Amazon Web Services, "Amazon Cognito: Developer Guide," AWS Documentation, 2023.

[20] Amazon Web Services, "Serverless Security Using AWS Lambda," AWS Whitepaper, 2022.

[21] C. Wang, Q. Wang, K. Ren, and W. Lou, "Privacy-preserving public auditing for secure cloud storage," *IEEE Transactions on Computers*, vol. 62, no. 2, pp. 362–375, 2013.

[22] K. Ren, C. Wang, and Q. Wang, "Security challenges for the public cloud," *IEEE Internet Computing*, vol. 16, no. 1, pp. 69–73, 2012.

[23] G. Zyskind, O. Nathan, and A. Pentland, "Decentralizing privacy: Using blockchain to protect personal data," *IEEE Security and Privacy Workshops*, 2015, pp. 180–184.

[24] K. Christidis and M. Devetsikiotis, "Blockchains and smart contracts for the Internet of Things," *IEEE Access*, vol. 4, pp. 2292–2303, 2016.

[25] M. Crosby, P. Pattanayak, S. Verma, and V. Kalyanaraman, "Blockchain technology: Beyond bitcoin," *Applied Innovation Review*, no. 2, pp. 6–19, 2016.

[26] D. Ferraiolo, D. Kuhn, and R. Chandramouli, *Role-Based Access Control*, Artech House, 2003.

[27] R. Sommer and V. Paxson, "Outside the closed world: On using machine learning for network intrusion detection," *IEEE Symposium on Security and Privacy*, 2010, pp. 305–316.

[28] A. Shabtai, U. Kanonov, Y. Elovici, C. Glezer, and Y. Weiss, "Andromaly: A behavioral malware detection framework for android devices," *Journal of Intelligent Information Systems*, vol. 38, pp. 161–190, 2012.

[29] M. Conti, E. Sandeep Kumar, C. Lal, and S. Ruj, "A survey on security and privacy issues of bitcoin," *IEEE Communications Surveys & Tutorials*, vol. 20, no. 4, pp. 3416–3452, 2018.

[30] X. Xu, I. Weber, and M. Staples, *Architecture for Blockchain Applications*, Springer, 2019.