International Research Journal of Innovations in Engineering and Technology (IRJIET)

ISSN (online): 2581-3048
Volume 10, Issue 1, pp 190-197, January-2026
https://doi.org/10.47001/IRJIET/2026.101024

Towards Enhancing Privacy Preservation in Cloud Based Applications: A Hybrid Approach using Bloom Filters and Blockchain PKI for Secure Multi Party Collaboration

[1]Ami Choksi, [2]Dr. Ravi Gulati

[1]PhD Scholar, Veer Narmad South Gujarat University, Surat, India
[2]Professor, Veer Narmad South Gujarat University, Surat, India

Abstract - **Preserving privacy in cloud-based apps is a significant issue, especially in multi-party collaborations, where data security, authentication, and effective administration are essential. This study presents a hybrid paradigm that integrates Bloom Filters with Blockchain Public Key Infrastructure to improve data privacy and security. Bloom Filters facilitate effective data validation with little processing resources, whilst Blockchain PKI guarantees decentralized and tamper-resistant authentication. This method resolves current deficiencies in scalability, computing efficiency, and robustness, presenting prospective applications in sectors such as education, healthcare, and IoT. The advantages, obstacles, and constraints are examined to offer a conceptual comprehension of the suggested method.**

Keywords: Privacy Preservation, Cloud-Based Applications, Bloom Filters, Blockchain PKI, Decentralized Authentication.

I. INTRODUCTION

In the age of swift digital transformation, cloud-based applications are essential for facilitating collaboration and data sharing across various sectors. Nonetheless, these developments present considerable hurdles, especially in safeguarding data privacy and maintaining secure connections. Privacy-preserving technologies have arisen as essential solutions for mitigating the dangers linked to data breaches, unlawful access, and trust challenges in collaborative settings.

Contextual Relevance to the Indian Education System

The implementation of cloud technology in India has revolutionized the education sector by enhancing operational efficiency and expanding resource accessibility. Cloud solutions enable centralized administration of student records, real-time collaboration among educators, and integration of e-learning resources. Notwithstanding these advantages, apprehensions regarding the confidentiality and integrity of sensitive data have emerged. Occurrences of data breaches and illegal access highlight the necessity for strong privacy-preserving methods (Tran et al., 2021; Feng et al., 2024) [2], [3].

Introduction to Proposed Technologies

Two technologies, Bloom Filters and Blockchain PKI, are notable for their capacity to tackle the issues of data privacy and safe collaboration:

1. **Bloom Filters:** These are efficient data structures engineered for rapid verification of data existence without retaining the actual data. Hash functions are employed to succinctly represent datasets, facilitating rapid lookup times while minimizing memory consumption. Nonetheless, their probabilistic characteristics present a minor risk of false positives, which can be alleviated with supplementary verification measures (Khan *et al.*, 2023) [7].
2. **Blockchain PKI:** Public Key Infrastructure (PKI) executed on a Blockchain removes dependence on centralized authorities, guaranteeing decentralized authentication and immutable certificate administration. This method is especially beneficial in collaborative settings where several parties must build confidence (Nakamoto, 2008) [11].

Research Purpose

This study presents a hybrid solution that blends the distinct advantages of Bloom Filters and Blockchain PKI. The suggested resolution seeks to:

- Augment privacy protection with streamlined data validation.
- Guarantee safe, tamper-resistant authentication and transaction documentation.
- Rectify current deficiencies in scalability and computational efficiency.

Objectives

The subsequent objectives have been delineated to direct the research and guarantee practical significance:

ISSN (online): 2581-3048
Volume 10, Issue 1, pp 190-197, January-2026
https://doi.org/10.47001/IRJIET/2026.101024

1. **Construct a Hybrid Model:** Formulate an extensive framework that integrates Bloom Filters for data validation with Blockchain Public Key Infrastructure for authentication and transaction oversight. This connection utilizes the efficiency of Bloom Filters and the strong security of Blockchain. (Hameed *et al.*, 2022) [6].
2. **Examine the Constraints of Existing Methodologies**: Examine and address the limitations of current privacy-preserving solutions, including elevated computational expenses in Blockchain-based Public Key Infrastructure and scalability challenges in conventional systems. The hybrid methodology seeks to reconcile efficiency with security. Honar Pajooh *et al.*, 2021 [8].
3. **Investigate Possible Applications:** Examine the relevance of the hybrid model in sectors such as education, healthcare, and IoT, emphasizing practical applications. For example:
    - **Education:** Ensured protection and dissemination of student information and academic transcripts.
    - **Healthcare:** Confidential communication of sensitive patient data.
    - **Internet of Things:** Optimized access regulation and secure device interaction. (Tran *et al.*, 2021; Feng *et al.*, 2024) [2], [3].

II. LITERATURE REVIEW

The literature study offers a comprehensive examination of cutting-edge strategies for privacy protection in secure multi-party cooperation, emphasizing contemporary techniques, their applications, and their limits. This section emphasizes three principal study domains: privacy preservation in multi-party collaboration, blockchain technology, and Bloom filters.

2.1 Privacy Preservation in Multi-Party Collaboration

Multi-party collaboration frequently necessitates secure methods for disseminating sensitive information across several parties. Current privacy-preserving techniques mostly depend on encryption protocols, access control mechanisms, and Public Key Infrastructure (PKI). These techniques guarantee anonymity and regulated access, yet have fundamental challenges:

1. **Encryption and Access Control:** These techniques safeguard data by permitting access just to authorized individuals. Managing encryption keys for numerous participants is computationally demanding, particularly in cloud-based systems that handle extensive datasets (Feng *et al.*, 2024; Khedr, 2020). [3], [10].
2. **Certificate Revocation in PKI:** Although PKI is a prevalent authentication mechanism, it frequently encounters inefficiencies with certificate management, especially in situations necessitating frequent revocations or updates. Traditional PKI is inadequate for dynamic and large-scale collaborative contexts (Khan *et al.*, 2023). [7].
3. **Challenges of Scalability:** The computational burden of these technologies restricts their scalability, especially for applications necessitating real-time processing and high throughput.

These problems underscore the necessity for creative solutions that reconcile privacy preservation with computational efficiency.

2.2 Blockchain for Privacy Preservation

Blockchain technology has attracted significant attention for its capacity to ensure privacy protection due to its decentralized and immutable properties. Unlike traditional centralized systems, Blockchain offers all users access to a secure and immutable record, making it appropriate for collaborative applications.

1. Key Features:

- **Immutability:** Blockchain guarantees that once data is recorded, it remains unalterable, thereby ensuring data integrity.
- **Decentralization:** Removes the necessity for a central authority, diminishing vulnerabilities and fostering confidence among untrusted entities (Zhang & Datta, 2023; Yuan & Wang, 2016) [4], [16].

2. Applications:

- **Healthcare:** Blockchain has been utilized to safeguard sensitive patient information, assuring responsibility and thwarting illegal access.
- **The Internet of Things (IoT)** enables safe data transmission between interconnected devices, hence improving trust and interoperability.

3. Limitations:

- **Scalability:** The decentralized structure of Blockchain results in diminished transaction speeds as participant numbers rise.
- **Computational Expenses:** Mining and consensus mechanisms, such as Proof of Work (PoW), necessitate substantial computational resources, rendering them impractical for lightweight applications.

These constraints underscore the necessity of amalgamating Blockchain with alternative technologies to augment its scalability and efficiency.

ISSN (online): 2581-3048
Volume 10, Issue 1, pp 190-197, January-2026
https://doi.org/10.47001/IRJIET/2026.101024

2.3 Bloom Filters for Efficient Data Handling

Bloom Filters are probabilistic data structures intended for swift and efficient data validation. They are especially beneficial in situations necessitating frequent queries or verifications, as they reduce memory consumption while ensuring rapid lookup speeds.

1. Mechanism:

- Bloom Filters function by hashing an input item with several hash functions and activating the appropriate bits in a bit array. To confirm the existence of an object, identical hash functions are utilized, and the relevant bits are examined.
- This technique is efficient and does not necessitate the storage of actual data, rendering Bloom Filters suitable for resource-constrained applications (Khan *et al.*, 2021; Khedr, 2020) [9], [10].

2. Applications:

- **Text Ownership Protection:** Bloom Filters confirm text ownership while safeguarding sensitive content.
- **Video File Retrieval:** They improve the efficiency of video file retrieval in secure systems by rapidly validating file information.

3. Limitations:

- **False Positives:** The probabilistic characteristics of Bloom Filters may occasionally lead to false positives, wherein an item is erroneously recognized as present.
- **Supplementary Verification:** To mitigate false positives, additional levels of verification are frequently necessary, potentially augmenting overall system complexity.

Notwithstanding these constraints, Bloom Filters continue to be an effective instrument for streamlined and efficient data management, especially when integrated with auxiliary technologies.

III. OVERVIEW OF THE PROPOSED HYBRID APPROACH

The suggested hybrid methodology integrates the efficacy of Bloom Filters with the strong security of Blockchain PKI, tackling significant limits in scalability, computing efficiency, and centralized vulnerabilities seen in current privacy-preserving approaches. The hybrid model utilizes the complimentary qualities of these technologies to offer a scalable and secure solution for multi-party collaboration in cloud-based applications.

3.1 Bloom Filters in the Hybrid Model

Bloom Filters are a lightweight, probabilistic data structure intended to compactly describe datasets and rapidly validate data existence. Their capacity to swiftly ascertain the presence of a certain piece inside a dataset without necessitating physical storage renders them an essential feature in privacy-preserving frameworks.

Key Features of Bloom Filters:

1. **Efficiency:** Bloom Filters facilitate rapid lookup operations, markedly diminishing computing overhead relative to conventional database queries.
2. **Privacy Preservation:** By refraining from retaining actual data, Bloom Filters reduce exposure risks, hence safeguarding sensitive information.
3. **Economical Storage:** They utilize a constant memory allocation regardless of the dataset's magnitude, rendering them suitable for extensive applications (Khan *et al.*, 2021; Khedr, 2020) [9], [10].

Application Example: In a secure file retrieval system, Bloom Filters can ascertain the presence of file metadata. Upon a user's request for a file, the system verifies the file's existence using the Bloom Filter, circumventing the need to access the entire dataset. This method safeguards the foundational data while delivering swift query replies.

3.2 Blockchain PKI for Secure Collaboration

Blockchain PKI combines Blockchain's decentralized framework with PKI's authentication features to create a safe and tamper-resistant environment for multi-party collaboration.

Key Advantages of Blockchain PKI:

1. **Decentralized Authentication:** Blockchain PKI obviates the necessity for centralized authorities, hence mitigating risks linked to single points of failure.
2. **Tamper-Proof Certificates:** The immutable ledger of blockchain guarantees the security of all certificates and authentication documents, preventing any retroactive alterations.
3. **Transparency and Accountability:** All transactions and certifications are documented on a distributed ledger, ensuring total transparency in multi-party cooperation (Hameed *et al.*, 2022; Shafagh *et al.*, 2017) [6], [18].

In contrast to traditional PKI, which depends on central authorities for the issue and revocation of certificates, Blockchain PKI decentralizes these functions throughout the network, hence enhancing resilience against tampering and unauthorized revocations.

ISSN (online): 2581-3048
Volume 10, Issue 1, pp 190-197, January-2026
https://doi.org/10.47001/IRJIET/2026.101024

Application Example: In collaborative research, participants may verify their identities with Blockchain Public Key Infrastructure (PKI). The public key and certificate of each participant are recorded on the Blockchain, facilitating secure and authenticated communication independent of a central certifying body.

3.3 Hybrid Model Architecture

The suggested hybrid architecture amalgamates Bloom Filters and Blockchain PKI into a unified framework, utilizing their distinct advantages to develop an efficient, safe, and scalable solution for privacy-preserving cooperation.

Key Components of the Hybrid Architecture:

1. **Data Preprocessing:** Bloom Filters preprocess data by mapping elements into a concise bit array through the utilization of hash functions. This step guarantees that only authenticated participants and data requests advance to the subsequent stage, thereby considerably diminishing the computational burden on Blockchain operations.
2. **Authentication:** Blockchain PKI facilitates authentication by securely preserving participant keys and certificates on an unalterable ledger. Transactions are validated by Blockchain's decentralized consensus method, guaranteeing secure authentication.
3. The hybrid architecture enables safe multi-party communication using hash-based verification. Bloom Filters efficiently authenticate participants, whereas Blockchain records and safeguards all interactions, fostering a cohesive and reliable collaborative environment (Feng *et al.*, 2024; Zhang *et al.*, 2023) [3], [4].

Process Workflow of the Hybrid Model:

- Step 1: Participants and their public keys are incorporated into the Bloom Filter and Blockchain.
- Step 2: Data requests and transactions undergo verification through the Bloom Filter for expedited validation.
- Step 3: Valid transactions are recorded and safeguarded via Blockchain Public Key Infrastructure (PKI).
- Step 4: Blocks are mined to incorporate validated transactions into the Blockchain, so maintaining integrity and accountability.

Benefits of the Architecture:

- **Scalability:** The effective management of extensive datasets with Bloom Filters alleviates the burden on Blockchain operations.
- **Augmented Security:** Blockchain PKI guarantees immutable authentication and transparency.
- **Effective Collaboration:** Streamlined validation and secure logging render the hybrid architecture appropriate for real-time multi-party engagements in sectors such as education, healthcare, and IoT.

Figure 1 illustrates the vertical workflow of the proposed hybrid model architecture. The procedure commences with data entry at the Bloom Filter Module, where participants are authenticated via efficient hash-based verifications. Validated participants are subsequently authenticated and recorded in the Blockchain PKI Module, guaranteeing tamper-proof transaction management and secure storage on an immutable ledger. Ultimately, at the Collaboration Layer, verified and authenticated participants partake in secure multi-party interactions, utilizing the system's privacy-preserving features. A feedback loop from the Immutable Ledger to the collaboration layer guarantees continuous trust and iterative data utilization. This diagram elucidates the integration and workflow of the hybrid paradigm, showcasing its scalability and security for cloud-based applications.

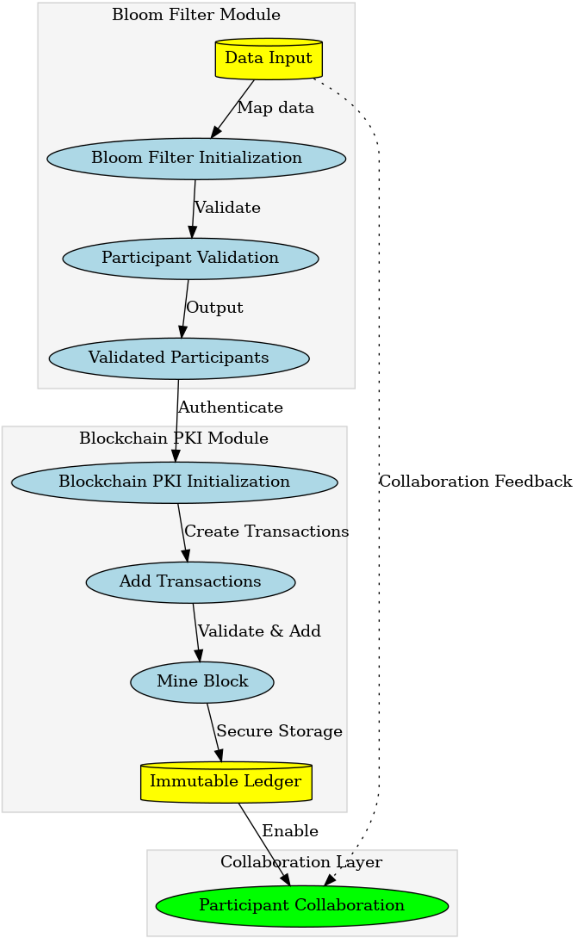

Figure 1: Proposed Hybrid Model Architecture

ISSN (online): 2581-3048
Volume 10, Issue 1, pp 190-197, January-2026
https://doi.org/10.47001/IRJIET/2026.101024

IV. DISCUSSIONS

This study proposes a hybrid strategy that utilizes the advantages of Bloom Filters and Blockchain PKI to develop an efficient and safe paradigm for privacy-preserving cloud applications. This section rigorously assesses the advantages and obstacles of the model and examines its prospective applicability across several fields.

4.1 Benefits

The suggested hybrid model presents multiple benefits that mitigate significant shortcomings of conventional privacy-preserving methods:

- **Scalability:** Bloom Filters are intrinsically lightweight and memory-efficient, rendering them optimal for managing extensive datasets. The paradigm facilitates swift data verification without retaining actual data, hence minimizing computational overhead, especially in settings that necessitate frequent queries. This scalability guarantees the model's appropriateness for cloud-based applications involving large datasets, such as those in education and healthcare systems (Khan *et al.,* 2021; Khedr, 2020). [9], [10].
- **Augmented Security:** Blockchain PKI offers decentralized authentication and immutable data storage. The decentralized architecture of Blockchain guarantees the absence of a singular point of failure, rendering the system exceptionally robust against attacks. The immutable nature of Blockchain guarantees that transaction records and certificates are secure and unchangeable, hence enhancing confidence among participants (Zheng *et al.*, 2017). [12].
- **Interoperability:** The hybrid model's architecture facilitates easy integration across various cloud-based apps. The concept integrates the efficient validation of Bloom Filters with the safe transaction recording of Blockchain, hence promoting interoperability in sectors such as education, healthcare, and IoT, where secure multi-party collaboration is essential (Hameed *et al.,* 2022). [6].

4.2 Bottlenecks

Notwithstanding its myriad advantages, the hybrid approach possesses inherent limits. The subsequent issues must be resolved to guarantee its extensive applicability:

- The probabilistic characteristics of Bloom Filters result in false positives, when a non-existent element is erroneously recognized as present. This issue is acceptable in situations where approximate results suffice; but, important applications may necessitate further verification layers, thereby increasing system complexity (Khan *et al.*, 2021). [9].
- **Computational Expenses in Blockchain Public Key Infrastructure:** Although Blockchain provides substantial security, the processing resources necessary for mining and consensus processes can be considerable. In smaller-scale applications or resource-constrained situations, these expenses may surpass the advantages, prompting the investigation of more efficient Blockchain processes or refined consensus procedures (Yuan & Wang, 2016). [16].

4.3 Application Areas

The hybrid model's adaptability renders it suitable for diverse fields, especially those necessitating safe and scalable multi-party collaboration.

- Cloud technology in education frequently manage sensitive information, including student records, examination results, and collaborative research initiatives. The hybrid paradigm can facilitate secure data sharing while preserving privacy. Student records can be authenticated via Bloom Filters, whilst Blockchain PKI guarantees safe and immutable authentication among collaborators (Tran *et al.,* 2021; Khan *et al.,* 2021). [2], [9].
- In healthcare, the privacy and security of sensitive patient data are of utmost importance, as this information is often exchanged across providers, insurers, and researchers. The hybrid paradigm facilitates privacy-preserving patient data sharing and secure identification, assuring adherence to regulatory standards such as HIPAA. The immutability of blockchain ensures the integrity of patient records, whilst Bloom Filters improve query efficiency (Esposito *et al.*, 2018). [26].
- The Internet of Things (IoT) encompasses a multitude of interconnected gadgets that transmit data instantaneously. Ensuring secure and efficient access control in this fluid environment is arduous. The hybrid solution utilizes Bloom Filters for efficient device validation and Blockchain PKI for safe connection and data sharing. This amalgamation augments confidence and interoperability among IoT devices (Shafagh *et al.*, 2017; Viriyasitavat *et al.*, 2019). [18], [13].

4.4 Hybrid Implementation: Pseudo Code Overview

The following pseudo code demonstrates the integration of Bloom Filters with Blockchain PKI to conceptualize the proposed hybrid approach. This hybrid system integrates effective participant validation with secure transaction management, guaranteeing privacy and scalability in cloud-based applications.

ISSN (online): 2581-3048
Volume 10, Issue 1, pp 190-197, January-2026
https://doi.org/10.47001/IRJIET/2026.101024

Integrated Hybrid Model Pseudo Code

The integrated concept establishes a Bloom Filter for participant authentication and a Blockchain instance for safe transaction documentation. Participants undergo validation through the Bloom Filter prior to the inclusion of their transactions in the Blockchain, thereby assuring computational efficiency and the preservation of privacy.

```
Begin
  Initialize Bloom Filter and Blockchain Instances
  Add Initial Participants to Bloom Filter
  Process Transactions:
    - Validate Participants via Bloom Filter
    - Log Transactions in Blockchain
  Mine New Block
  Display Blockchain State
End
```

Explanation:

1. **Initialization:** The Bloom Filter is configured with specified settings (size and hash functions) to effectively store participants. A Blockchain instance is established with Public Key Infrastructure for safe communication.
2. **Validation and Logging:** Transactions are executed solely if participants are present in the Bloom Filter, hence minimizing superfluous Blockchain processes.
3. **Mining and Display:** A fresh block is generated for authenticated transactions, guaranteeing immutability and integrity.

This comprehensive method improves scalability and security by utilizing the efficient validation of Bloom Filters and the strong authentication provided by Blockchain PKI. It establishes a robust basis for subsequent deployment and experimentation.

V. CONCLUSION AND FUTURE WORK

The suggested hybrid solution proficiently integrates Bloom Filters with Blockchain PKI to tackle privacy preservation issues in cloud-based applications. It improves scalability, efficiency, and security, providing a comprehensive solution for secure multi-party collaboration. Utilizing the lightweight characteristics of Bloom Filters and the decentralized authentication provided by Blockchain, the concept addresses issues related to computational inefficiencies and centralized vulnerabilities.

Prospective Endeavours: Future research should prioritize minimizing the false-positive rate of Bloom Filters and creating lightweight Blockchain consensus mechanisms to enhance energy efficiency. Furthermore, practical testing and incorporation of new technologies such as quantum cryptography or federated learning might enhance the model's relevance and robustness across several fields.

REFERENCES

[1] Keshk, M., Turnbull, B., Sitnikova, E., Vatsalan, D., & Moustafa, N. (2021). Privacy-preserving schemes for safeguarding heterogeneous data sources in cyber-physical systems. *IEEE Access*, 9, 55077-55097.

[2] Tran, Q. N., Turnbull, B. P., Wu, H. T., De Silva, A. J. S., Kormusheva, K., & Hu, J. (2021). A survey on privacy-preserving blockchain systems (PPBS) and a novel PPBS-based framework for smart agriculture. *IEEE Open Journal of the Computer Society*, 2, 72-84.

[3] Feng, X., Cui, K., Wang, L., Liu, Z., & Ma, J. (2024). PBAG: A Privacy-Preserving Blockchain-Based Authentication Protocol With Global-Updated Commitment in IoVs. *IEEE Transactions on Intelligent Transportation Systems*.

[4] Zhang, J., & Datta, A. (2023). Blockchain-enabled Data Governance for Privacy-Preserved Sharing of Confidential Data. *arXiv preprint arXiv*:2309.04125.

[5] IZADEEN, G. Y., ABDULLAH, N. A. M., RASHID, Z. N., JGHEF, Y. S., SAMI, T. M. G., & ABDULNABI, N. L. PRIVACY PRESERVATION IN: INFORMATION, WEB TECHNOLOGY, SEMANTIC WEB, PARALLEL AND CLOUD COMPUTING.

[6] Hameed, K., Barika, M., Garg, S., Amin, M. B., & Kang, B. (2022). A taxonomy study on securing Blockchain-based Industrial applications: An overview, application perspectives, requirements, attacks, countermeasures, and open issues. *Journal of Industrial Information Integration*, 26, 100312.

[7] Khan, S., Luo, F., Zhang, Z., Ullah, F., Amin, F., Qadri, S. F., ... & Wu, K. (2023). A survey on X. 509 public-key infrastructure, certificate revocation, and their modern implementation on blockchain and ledger technologies. *IEEE Communications Surveys & Tutorials*.

[8] Honar Pajooh, H., Rashid, M., Alam, F., & Demidenko, S. (2021). Multi-layer blockchain-based security architecture for internet of things. *Sensors*, 21(3), 772.

[9] Khan, K., Nisha, S. S., & Sathik, M. M. (2021). Secure and efficient retrieval of video file using bloom filter and hybrid encryption algorithms. *J. Math. Comput. Sci.*, 11(5), 5525-5535.

[10] Khedr, W. I. (2020). A novel Bloom-filter-based scheme for secure text ownership protection. *Wireless Networks*, 26, 3831-3845.

ISSN (online): 2581-3048

Volume 10, Issue 1, pp 190-197, January-2026

https://doi.org/10.47001/IRJIET/2026.101024

[11] Nakamoto, S., & Bitcoin, A. (2008). A peer-to-peer electronic cash system. *Bitcoin.–URL*: https://bitcoin. org/bitcoin. pdf, 4(2), 15.

[12] Zheng, Z., Xie, S., Dai, H., Chen, X., & Wang, H. (2017, June). An overview of blockchain technology: Architecture, consensus, and future trends. *In 2017 IEEE international congress on big data (BigData congress)* (pp. 557-564). Ieee.

[13] Viriyasitavat, W., Da Xu, L., Bi, Z., & Hoonsopon, D. (2019). Blockchain technology for applications in internet of things—mapping from system design perspective. *IEEE Internet of Things Journal*, 6(5), 8155-8168.

[14] Guo, Y., Zhang, C., Wang, C., & Jia, X. (2022). Towards public verifiable and forward-privacy encrypted search by using blockchain. *IEEE Transactions on Dependable and Secure Computing*, 20(3), 2111-2126.

[15] Liang, X., Zhao, J., Shetty, S., & Li, D. (2017, October). Towards data assurance and resilience in IoT using blockchain. *In MILCOM 2017-2017 IEEE Military Communications Conference (MILCOM)* (pp. 261-266). IEEE.

[16] Yuan, Y., & Wang, F. Y. (2016). Blockchain: the state of the art and future trends. *Acta automatica sinica*, 42(4), 481-494.

[17] Christidis, K., & Devetsikiotis, M. (2016). Blockchains and smart contracts for the internet of things. *IEEE access*, 4, 2292-2303.

[18] Shafagh, H., Hithnawi, A., Burkhalter, L., Fischli, P., & Duquennoy, S. (2017, November). Secure sharing of partially homomorphic encrypted IoT data. *In Proceedings of the 15th ACM Conference on Embedded Network Sensor Systems* (pp. 1-14).

[19] Conti, M., Kumar, E. S., Lal, C., & Ruj, S. (2018). A survey on security and privacy issues of bitcoin. *IEEE communications surveys & tutorials*, 20(4), 3416-3452.

[20] Di Luzio, A., Mei, A., & Stefa, J. (2017, June). Consensus robustness and transaction de-anonymization in the ripple currency exchange system. *In 2017 IEEE 37th International Conference on Distributed Computing Systems (ICDCS)* (pp. 140-150). IEEE.

[21] Benet, J. (2014). Ipfs-content addressed, versioned, p2p file system. *arXiv preprint arXiv*:1407.3561.

[22] Shamir, A. (1985). Identity-based cryptosystems and signature schemes. In Advances in Cryptology: Proceedings of CRYPTO 84 4 (pp. 47-53). *Springer Berlin Heidelberg*.

[23] Merkle, R. C. (2019). Protocols for public key cryptosystems. In Secure communications and asymmetric cryptosystems (pp. 73-104). *Routledge*.

[24] Fan, K., Ren, Y., Wang, Y., Li, H., & Yang, Y. (2018). Blockchain-based efficient privacy preserving and data sharing scheme of content-centric network in 5G. *IET communications*, 12(5), 527-532.

[25] Zyskind, G., & Nathan, O. (2015, May). Decentralizing privacy: Using blockchain to protect personal data. *In 2015 IEEE security and privacy workshops* (pp. 180-184). *IEEE*.

[26] Esposito, C., De Santis, A., Tortora, G., Chang, H., & Choo, K. K. R. (2018). Blockchain: A panacea for healthcare cloud-based data security and privacy?. *IEEE cloud computing*, 5(1), 31-37.

[27] Nakamoto, S. (2008). Bitcoin P2P e-cash paper. The Cryptography Mailing List. *Nakamoto Institute*.

[28] Buterin, V. (2014). A next-generation smart contract and decentralized application platform. *White paper*, 3(37), 2-1.

[29] Mettler, M. (2016, September). Blockchain technology in healthcare: The revolution starts here. *In 2016 IEEE 18th international conference on e-health networking, applications and services (Healthcom)* (pp. 1-3). *IEEE*.

[30] Li, X., Jiang, P., Chen, T., Luo, X., & Wen, Q. (2020). A survey on the security of blockchain systems. *Future generation computer systems*, 107, 841-853.

[31] Kim, H. M., & Laskowski, M. (2018). Toward an ontology-driven blockchain design for supply-chain provenance. Intelligent Systems in Accounting, *Finance and Management*, 25(1), 18-27.

[32] Sun, S., Du, R., Chen, S., & Li, W. (2021). Blockchain-based IoT access control system: towards security, lightweight, and cross-domain. *IEEE Access*, 9, 36868-36878.

[33] Chen, L., Lee, W. K., Chang, C. C., Choo, K. K. R., & Zhang, N. (2019). Blockchain based searchable encryption for electronic health record sharing. *Future generation computer systems*, 95, 420-429.

[34] Yue, D., Li, R., Zhang, Y., Tian, W., & Peng, C. (2018, December). Blockchain based data integrity verification in P2P cloud storage. *In 2018 IEEE 24th international conference on parallel and distributed systems (ICPADS)* (pp. 561-568). IEEE.

Citation of this Article:

Ami Choksi, & Dr. Ravi Gulati. (2026). Towards Enhancing Privacy Preservation in Cloud Based Applications: A Hybrid Approach using Bloom Filters and Blockchain PKI for Secure Multi Party Collaboration. *International Research Journal of Innovations in Engineering and Technology - IRJIET*, 10(1), 190-197. Article DOI https://doi.org/10.47001/IRJIET/2026.101024

****