International Journal of Advanced Research in Engineering Technology & Science
ISSN: 2349-2819
Impact Factor: 7.10
(Peer-Reviewed, Open Access, Fully Refereed International Journal)
Email: editor@ijarets.org Volume-13, Issue-1 January – 2026 www.ijarets.org

Blockchain-Based Approach for Secure Data Backup Against Ransomware Attacks

Kalash Bansal
Student
b.tech computer science

Abstract

In the present digital era, the rapid growth of the Internet and information technology has led to a significant increase in cyberattacks. Ransomware attacks have emerged as one of the most dangerous and rapidly growing threats in the field of cybersecurity. In such attacks, attackers encrypt the critical data of users or organizations and demand a large ransom in exchange for restoring access to the data.

Traditional data backup systems are generally centralized in nature, which makes them more vulnerable to ransomware attacks. If the primary server or backup server is compromised, the entire data may be at risk. This research paper examines a **blockchain-based secure data backup system** as a solution to protect against ransomware attacks.

The characteristics of blockchain technology, such as decentralization, immutability, and transparency, play a crucial role in maintaining data integrity. This study demonstrates that blockchain-based backup systems can provide a more secure and reliable solution compared to traditional backup mechanisms.

Keywords

- **Blockchain** – Secure and distributed data storage technology
- **Cybersecurity** – The field concerned with protecting digital systems
- **Ransomware** – Malware that holds data hostage and demands ransom
- **Data Backup** – Creation of secure copies of data
- **Decentralization** – Lack of dependence on a single central authority
- **Immutability** – Inability to alter stored data

Introduction – Detailed Description

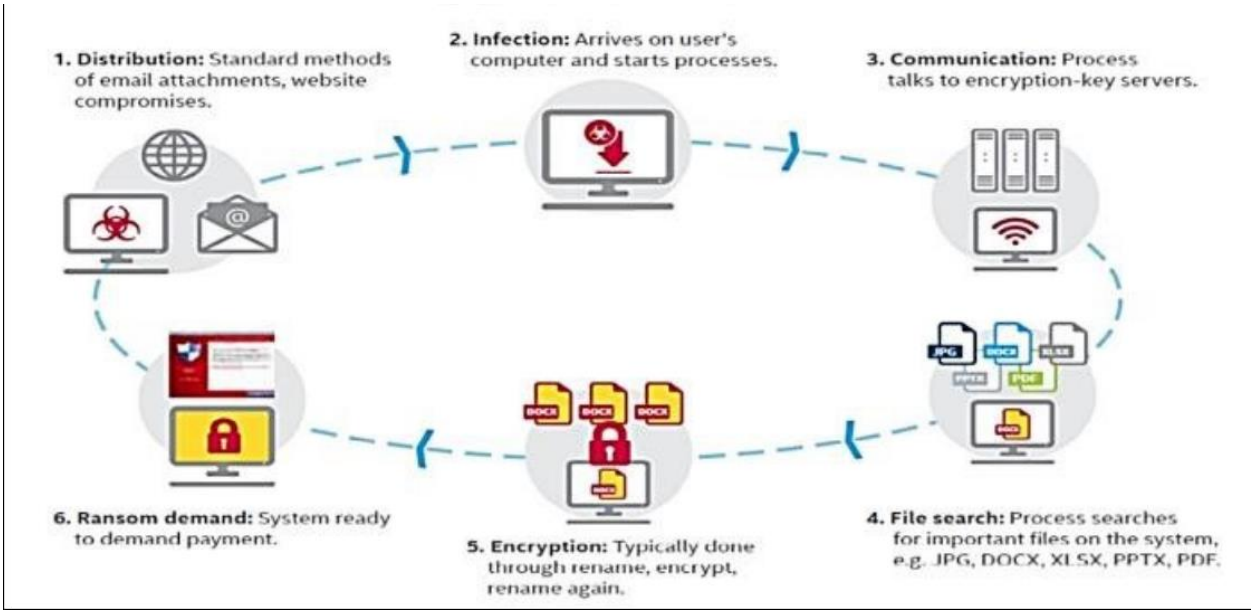
The continuous advancement of information technology has simplified human life; however, it has also resulted in a rapid rise in cybercrimes. Ransomware attacks have become a serious challenge for organizations, educational institutions, hospitals, and government systems.

The primary objective of such attacks is to block users' access to critical data and gain financial benefits. Data backup is considered an effective solution against ransomware attacks, but traditional backup systems, due to their centralized architecture, can themselves become targets of such attacks.

To address this issue, blockchain technology has emerged as an advanced, secure, and reliable alternative that introduces new dimensions to data security.

Overview of Ransomware Attacks

Ransomware is a type of malicious software that infiltrates a system or network and encrypts files and data stored within it. After the attack, the attacker demands ransom from the user or organization to restore access to the encrypted data. Currently, ransomware attacks affect individuals, large enterprises, and government institutions alike, making them a serious concern in cybersecurity.



Loss of Critical Data

During ransomware attacks, essential and sensitive data becomes encrypted, causing users or organizations to lose access to vital information. This not only disrupts daily operations but also hampers decision-making processes. In many cases, permanent data loss may occur, leading to long-term organizational damage.

Disruption of Business Operations

When data becomes temporarily or completely unavailable, daily organizational activities come to a halt. Processes such as production, service delivery, and customer support are adversely affected, resulting in delays and reduced efficiency. This negatively impacts customers, partners, and other stakeholders.

Financial Loss

Ransomware attacks impose heavy financial burdens due to ransom payments, data recovery efforts, system repairs, and security enhancements. Additionally, reputational damage suffered by organizations indirectly amplifies economic losses, which may persist over an extended period.

Violation of Privacy

In ransomware incidents, attackers may steal confidential and personal information and either leak it publicly or misuse it. This reduces user and customer trust in the organization and may also lead to legal and regulatory consequences due to violations of data protection laws.

Introduction to Blockchain Technology

Blockchain is a distributed ledger technology in which data is stored in small blocks. Each block is cryptographically linked to the previous block, making data tampering nearly impossible.

The key characteristics of blockchain technology include decentralization, immutability, transparency, and cryptographic security, which distinguish it from traditional data management systems. Data is distributed across multiple independent nodes rather than being stored on a single central server, eliminating the risk of a single point of failure and ensuring data availability.

Due to the immutable nature of blockchain, once data is recorded, it cannot be altered without the consensus of the network, ensuring data integrity and trustworthiness. Moreover, all transactions are verified collectively by multiple nodes, enhancing transparency and detecting unauthorized or fraudulent activities. Advanced cryptographic encryption and hashing techniques further protect data from unauthorized access, tampering, and cyberattacks.

Blockchain-Based Secure Backup System

In a blockchain-based backup system, data is first encrypted and then stored across a distributed network. This process ensures both data security and availability.

The key advantages of this system include the prevention of unauthorized data modification due to blockchain's immutable structure, protection against data loss even if a single server fails, and the ability to verify and track backup records using time-stamped entries. Additionally, decentralization and encryption make it extremely difficult for ransomware to destroy backup data entirely, enabling secure data recovery.

Role of Blockchain in Protection Against Ransomware

Blockchain-based backup systems provide multi-layered security against ransomware attacks. The data structure is designed to prevent unauthorized modifications, as every record is cryptographically secured and immutable. Data is stored in a distributed manner across multiple nodes, ensuring reliability even if one server fails.

Each backup record is registered with a timestamp, enabling easy verification and tracking. Due to decentralization and advanced encryption mechanisms, ransomware attacks find it extremely difficult to eliminate backup data, ensuring secure and effective data restoration.

Challenges and Limitations

High Storage Cost

Blockchain-based backup systems require substantial storage resources due to data replication across multiple nodes. As a result, storage costs are higher compared to traditional backup systems, posing challenges for small organizations with limited resources.

Scalability Issues

As the volume of data and the number of network participants increase, blockchain performance may degrade. Increased transaction volume can slow network speed and increase latency, creating obstacles for large-scale data backup implementation.

Technical Complexity and Need for Expertise

Designing, implementing, and maintaining blockchain-based backup systems require advanced technical expertise. Components such as smart contracts, cryptography, and network management increase system complexity, while the lack of skilled professionals limits widespread adoption.

High Energy Consumption

Some blockchain networks, particularly those based on Proof of Work consensus mechanisms, consume excessive energy. This increases operational costs and raises environmental concerns, making energy-efficient consensus mechanisms an important research focus.

Conclusion – Detailed Description

This study demonstrates that blockchain-based secure data backup systems offer a robust, reliable, and advanced solution against ransomware attacks. Features such as decentralization and immutability effectively address the limitations of traditional backup systems.

In the future, the development of scalable, energy-efficient, and cost-effective blockchain solutions can play a transformative role in strengthening cybersecurity and protecting critical data from ransomware threats.

References

Alqahtani, A., 2022. *A Survey of Crypto Ransomware Attack Detection Toward Facilitating the Research Community*. *PMC Articles*.

Gómez Hernández, J.A., García Teodoro, P., Magán Carrión, R. and Rodríguez Gómez, R., 2023. *Crypto-Ransomware: A Revision of the State of the Art, Advances and Challenges*. *Electronics*, 12(21), p.4494.

Beaman, C., Barkworth, A., Akande, T.D., Khan, K., 2021. *Ransomware: Recent Advances, Analysis, Challenges and Future Research Directions. Computational Security Review*.

Kritika, E., 2024. *A Comprehensive Literature Review on Ransomware Detection Using Deep Learning*. *Cyber Security and Applications*, Volume 3, 100078.

Yan, P. and Talaei Khoei, T., 2025. *Securing the Internet of Things: A Comprehensive Review of Ransomware Attacks, Detection, Countermeasures, and Future Prospects*. *Fraunhofer Journal*.

Ransomware Detection Methods and Tools Review, 2025. *ResearchGate Publication*.

Clark, B. and Sathik Raja, M., 2025. *Resilience in Backup Systems: Leveraging AI, Blockchain and Encryption to Combat Emerging Cyber Threats*. Unpublished manuscript, ResearchGate.

Yan, P., 2025. *A comprehensive review of ransomware attacks, detection and emerging defense frameworks targeting IoT environments*. Cyber Security and Applications (Elsevier).

Chincholkar, A., Chauhan, A., Gher, Y., Mogarkar, P. and Nirmal, A., 2025. *An Encryption-Based Automated Cloud Backup and Recovery Framework with Ransomware Resistance*. INTERNATIONAL JOURNAL OF ENGINEERING RESEARCH & TECHNOLOGY (IJERT), 14(10), October 2025.

Lee, J., 2025. *Enhancing Data Backup Security with Blockchain and Role-Based Access Control*. International Journal of Multidisciplinary Studies in Management (ICETETI MSM144).

— **Bonus related studies you can cite too:**
Shang, J., Zhang, L. and Zheng, Z., 2025. *From Cyber Threat to Data Shield: Constructing Provably Secure File Erasure with Repurposed Ransomware Cryptography*. arXiv Preprint.

Starchenko, E., et al., 2025. *Decentralized Entropy-Driven Ransomware Detection Using Autonomous Neural Graph Embeddings*. arXiv Preprint.