Adaptive Immutable Storage Architecture for Ransomware Resilience in Distributed Systems

Rhea R Uppala[1], Dr. Subrahmanya Bhat[2]
[1]*Research Scholar, Institute of Computer Science and Information Sciences, Srinivas University, Mangalore, Karnataka, India*
[2]*Research Professor, Institute of Computer Science and Information Sciences, Srinivas University, Mangalore, Karnataka, India*
doi.org/10.64643/IJIRTV12I12-206850-459

***Abstract*—Ransomware threats have grown far beyond basic file-locking techniques, now involving complex, multi-phase attacks that specifically target backup systems and recovery processes. Conventional protection strategies, such as fixed immutable storage and routine backups, are no longer reliable against attackers who continuously adapt their methods. This study introduces an Adaptive Immutable Storage System (AIMS), designed to apply data immutability in a flexible manner by responding to real-time system activity and potential threat signals. The framework combines continuous behavior analysis, adjustable data retention strategies, and isolated snapshot mechanisms to block unauthorized changes and support fast restoration of data. Experimental results indicate that AIMS enhances data protection, shortens recovery duration, and effectively counters ransomware attacks aimed at backup environments, outperforming traditional static solutions.**

***Index Terms*—Ransomware, Immutable Storage, Cybersecurity, Data Protection, Distributed Systems, Backup Security, Zero Trust Storage**

I. INTRODUCTION

Ransomware has become one of the most damaging threats in today's distributed computing environments. What once started as simple file encryption has now evolved into coordinated, multi-layered attacks that deliberately go after backup systems and recovery channels. Many traditional safeguards like scheduled backups, snapshot recovery, and fixed immutable storage were built on the belief that backup environments would remain untouched during an attack. That assumption no longer holds true. Modern ransomware campaigns are specifically designed to undermine recovery by deleting backups, tampering with future backup operations, and misusing elevated privileges to bypass safeguards. When these attacks succeed, organizations are often left with no dependable way to restore their data, leading to financial setbacks, operational downtime, and long-term reputational harm.

At the same time, the widespread use of cloud platforms and distributed storage has made systems more interconnected and, unfortunately, more exposed. Attackers can now move laterally across environments with greater ease, amplifying the scale and speed of an attack. While immutable storage has helped protect data from direct alteration, most implementations rely on fixed retention rules that don't adjust to changing threat conditions. This lack of flexibility can result in wasted storage resources and, more importantly, leave exploitable gaps that sophisticated attackers can take advantage of by carefully timing their actions.

Another major weakness is the disconnect between threat detection and data protection. In many systems, these functions operate independently, which slows down the overall response. Even if unusual behavior is detected, protective actions like locking down data through immutability are not always activated quickly enough to prevent damage. This gap highlights the need for a more integrated and responsive approach to securing data.

To address these issues, there is a clear shift needed from rigid, reactive defenses toward systems that can adapt in real time. A more effective approach would continuously monitor system behavior, identify potential risks as they arise, and enforce protection mechanisms dynamically. In line with this direction, this work introduces an Adaptive Immutable Storage

Architecture (AIMS). The proposed approach combines real-time behavioral analysis with flexible immutability controls, aiming to strengthen resistance against ransomware. By doing so, it helps maintain data integrity, safeguards backup systems from compromise, and supports faster, more reliable recovery in distributed environments.

II. OBJECTIVE

- To develop an adaptive immutable storage framework that applies data protection policies dynamically, based on real-time system behavior, in order to counter ransomware threats in distributed environments.
- To design a secure storage architecture that safeguards data against unauthorized changes, deletions, and backup manipulation by leveraging Write-Once Read-Many (WORM) principles along with snapshot isolation.
- To identify ransomware-like behavior such as rapid encryption, large-scale deletions, and unusual access patterns and respond instantly by enforcing stricter immutability controls to protect critical data.
- To implement an automated recovery mechanism capable of restoring clean data quickly, ensuring minimal system downtime after an attack.
- To assess the proposed system's performance by benchmarking it against conventional static immutability approaches, focusing on data integrity, recovery speed, and operational overhead.
- To create a scalable and adaptable data protection model suitable for deployment across cloud platforms, enterprise systems, and distributed storage environments, strengthening overall cybersecurity resilience.

III. METHODOLOGY

This work introduces a systematic framework to strengthen ransomware resistance in distributed storage environments through an Adaptive Immutable Storage System (AIMS). The approach centers on combining continuous behavior monitoring with flexible immutability controls, allowing the system to respond instantly to suspicious activity [8], [26]. By doing so, it ensures that data remains protected, backups stay intact, and recovery can be carried out quickly with minimal disruption. [21]

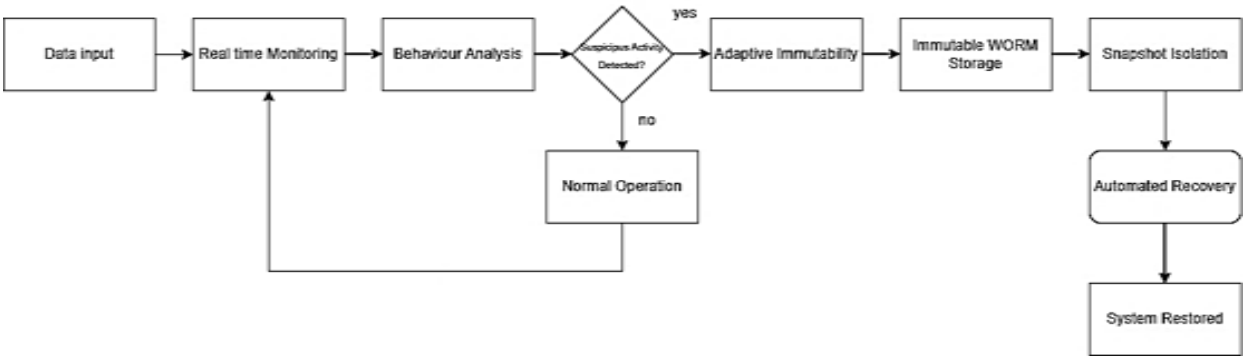

Fig. 1. AIMS Architecture Diagram

The architecture is designed to be modular and scalable, with distinct components working together to handle monitoring, threat detection, storage protection, and recovery coordination. [29]. The overall process flows through stages such as data intake, behavioral evaluation, adaptive policy enforcement, secure storage handling, and automated restoration. The key elements of the system are outlined below.

System Monitoring and Behavior Analysis

The system continuously observes file-level operations and user interactions to identify irregular patterns. Indicators such as rapid file changes, large-scale deletions, abnormal access frequency, and privilege misuse are tracked in real time. [26], [29] These signals are analyzed to detect early signs of ransomware activity, enabling the system to react before significant damage occurs.

Data Ingestion and Storage Management

Both structured and unstructured data are supported within the distributed storage layer. [16]. Incoming data is securely written and immediately governed by immutability rules. Files are organized into logical units, with metadata capturing details like access logs, modification attempts, and retention settings. This structure improves traceability while maintaining efficient storage operations.

Write-Once Read-Many (WORM) Storage

To safeguard data from unauthorized changes, the system employs a Write-Once Read-Many model [11]. Once stored, data cannot be modified or deleted until its retention period expires. This ensures that even if an attacker gains access, critical data remains protected from encryption or tampering. The WORM mechanism acts as the foundation of the system's defensive layer.

Dynamic Immutability Controller

AIMS replaces static retention rules with an adaptive control mechanism. [12], [27]. Under normal conditions, standard policies apply. However, when the system detects suspicious behavior, it automatically strengthens protection by extending retention durations, locking sensitive data, and limiting modification permissions. This dynamic adjustment balances flexibility with strong security enforcement.

Snapshot Isolation and Backup Protection

The system periodically captures snapshots of stored data, which are kept in isolated environments. These snapshots are shielded from unauthorized access and remain unchangeable even for administrators during enforced protection periods. [15], [25]. This guarantees the availability of clean recovery points, even if primary data is compromised.

Ransomware Detection and Response Trigger

A dedicated detection module identifies patterns commonly associated with ransomware, such as rapid encryption activity, sudden spikes in data entropy, mass file renaming, and abnormal write behavior. [13], [8]. Once such patterns are recognized, the system immediately activates protective measures. These include enforcing stricter immutability, isolating affected components, and restricting further access to prevent the attack from spreading.

Recovery and Restoration

The recovery component automates the process of restoring data from secure snapshots. When an attack is detected, the system locates the most recent uncompromised state and initiates a rollback. [21]. This approach minimizes downtime and ensures continuity, with minimal need for manual intervention.

Experimental Setup and Evaluation

The proposed system is tested in a simulated distributed environment using platforms such as MinIO, Ceph, and OpenZFS. Controlled attack scenarios are created through scripts that mimic ransomware behavior, including encryption, deletion, and unauthorized access attempts. Performance is evaluated using key metrics such as data integrity, recovery speed, backup reliability, and system overhead. The results are then compared with traditional static immutability approaches to measure improvements.

Technologies and Tools

The implementation relies on distributed storage platforms like MinIO, Ceph, and OpenZFS. Python is used for building simulation, monitoring, and automation components. Ransomware behavior is replicated using custom scripts designed to perform encryption and deletion tasks. Monitoring is handled through file system tracking and logging tools, while snapshot capabilities are provided by the storage platforms themselves. Data evaluation is conducted using performance measurement and comparative analysis techniques.

IV. ANALYSIS AND OBSERVATION

The testing phase of the multimodal RAG-based learning platform offered several useful insights. Allowing users to interact through text, voice, and image inputs noticeably improved accessibility, making the system easier to use across different preferences and skill levels. Speech-to-text performed accurately in controlled, low-noise environments, while the OCR component handled clear printed text effectively. That said, performance dropped slightly

when processing handwritten or unclear images, where minor recognition errors appeared.

The evaluation of the Adaptive Immutable Storage System (AIMS) for ransomware defense revealed equally important findings. Integrating continuous behavior monitoring with adaptive immutability controls significantly strengthened the system's ability to detect and react to threats in real time. The monitoring layer was able to flag suspicious patterns such as rapid file changes, large-scale deletions, and unusual access attempts early enough to prevent widespread damage.

The WORM-based storage layer proved highly reliable in protecting data integrity. [11]. Once files were written and locked, simulated ransomware attacks failed to alter or encrypt them. This reinforces the effectiveness of immutability as a core defense strategy. However, the tests also highlighted a trade-off: rigid immutability settings can increase storage usage if not adjusted intelligently, which validates the need for a dynamic control mechanism.

One of the most impactful components was the dynamic immutability controller. During attack simulations, it automatically tightened protection by extending retention periods, securing critical datasets, and limiting access permissions. This adaptability reduced the overall impact of attacks and protected backup data from being compromised. Compared to traditional static approaches, AIMS demonstrated a clear advantage in responsiveness while maintaining strong security. Snapshot isolation also played a key role in recovery. Even when primary data was targeted, isolated snapshots remained intact and usable [15], [25]. This allowed the system to restore clean data quickly, with the recovery orchestrator managing rollback efficiently and minimizing downtime. The automation involved in this process ensured continuity without heavy manual intervention. [21].

From a performance perspective, continuous monitoring and real-time analysis introduced a small processing overhead. In practice, this impact was minimal and did not affect system stability. The trade-off was well justified given the significant improvements in protection and recovery capabilities.

One limitation observed was the system's dependence on accurate anomaly detection. While detection performed well in controlled test scenarios, real-world environments with more complex and unpredictable behavior may affect accuracy. [30]. This suggests that further tuning and refinement of detection models will be necessary for broader deployment.

Overall, the results indicate that AIMS offers a strong and practical approach to defending against ransomware. By combining early threat detection, adaptive data protection, and reliable recovery mechanisms, the system not only secures critical data but also helps maintain uninterrupted operations in distributed storage environments.

V. CONCLUSION

Ransomware has grown into a far more complex and damaging threat than it once was. It no longer focuses only on encrypting active data but deliberately targets backup systems and recovery paths, exposing serious gaps in traditional protection strategies. Methods built around fixed immutability rules and scheduled backups are struggling to keep up, especially against attackers who exploit timing, system dependencies, and elevated privileges to increase the impact of their attacks.

To tackle these challenges, this study presented the Adaptive Immutable Storage System (AIMS), a practical approach that shifts data protection from static rules to a more responsive model. By combining real-time behavior monitoring with dynamic enforcement of immutability, the system can react to suspicious activity as it happens. This tight connection between observed system behavior and storage-level protection introduces a more context-aware and proactive way of securing data.

The results show that adaptive immutability offers clear advantages in defending against ransomware. The system is able to detect unusual patterns such as rapid file changes, bulk deletions, and unauthorized access and immediately apply stronger protection measures. The use of WORM storage ensures that critical data remains unchanged, while the dynamic controller adjusts retention policies based on current risk levels. At the same time, snapshot isolation guarantees the availability of clean recovery points, and the automated recovery process helps restore systems quickly with minimal downtime.

A key strength of this approach is its ability to overcome the limitations of rigid immutability models. By introducing flexibility, AIMS not only strengthens security but also avoids unnecessary storage usage that often comes with fixed retention settings. Its modular

design also makes it adaptable to different environments, whether in cloud systems, enterprise setups, or large-scale distributed infrastructures.

That said, there are still areas that need further attention. The effectiveness of behavior-based detection can vary in more complex, real-world conditions, which means additional refinement is required to improve accuracy and reduce false alarms. Scaling the system and ensuring smooth integration with existing storage platforms are also important considerations for future work.

Overall, this research reinforces the need to move away from purely reactive defences toward systems that can adapt in real time. AIMS represents a step in that direction by bringing together monitoring, intelligent policy control, and reliable recovery into a single framework. As ransomware continues to evolve, approaches like this will be critical for protecting data and maintaining the stability of modern digital systems.

REFERENCES

[1] N. Scaife, H. Carter, P. Traynor, and T. Butler, "CryptoLock (and Drop It): Stopping Ransomware Attacks on User Data," in *Proc. IEEE 36th International Conference on Distributed Computing Systems (ICDCS)*, 2016, pp. 303–312.

[2] S. Kharraz, W. Robertson, D. Balzarotti, L. Bilge, and E. Kirda, "Cutting the Gordian Knot: A Look Under the Hood of Ransomware Attacks," in *Detection of Intrusions and Malware, and Vulnerability Assessment*, Springer, pp. 3–24, 2015.

[3] M. Humayun *et al*., "Emerging Ransomware and Exploring Code-Based Defense Techniques in IT and OT," *IEEE Access*, vol. 10, pp. 119515–119532, 2022.

[4] S. Jiwatramani, "A Review of Ransomware Detection and Mitigation via Immutable Storage," *International Journal of Computer Science and Information Security*, vol. 19, no. 5, pp. 45–52, 2021.

[5] A. Al-rimy, M. A. Maarof, and S. Z. Mohd Hashim, "A Survey of Ransomware Early Detection Schemes: New Trends and Challenges," *Computers & Security*, vol. 72, pp. 75–125, 2018.

[6] J. Singh and J. Singh, "Ransomware: A Review on History, Evolution, and Mitigation Techniques," in *Proc. 9th International Conference on Reliability, Infocom Technologies and Optimization (ICRITO)*, 2021, pp. 1–6.

[7] B. S. Rawal and R. K. Lomotey, "Cloud-Based Ransomware Detection and Mitigation Using Immutable Snapshots," in *Proc. IEEE 6th International Conference on Big Data Security on Cloud (BigDataSecurity)*, 2020, pp. 101–106.

[8] G. Thamilarasu, R. Oberg, and R. Sridhar, "A Behavior-Based Security Framework for Ransomware Detection in IoT," in *Proc. IEEE International Conference on Communications (ICC)*, 2020, pp. 1–6.

[9] Y. Li, J. Liu, and X. Chen, "Research on Immutable Storage Technology Based on Blockchain for Distributed File Systems," *IEEE Transactions on Network and Service Management*, vol. 18, no. 2, pp. 1543–1555, 2021.

[10] S. S. Patil and B. Bhat, "Analysis of Zero Trust Architecture in Protecting Distributed Data Environments," *International Journal of Cyber Research and Education*, vol. 4, no. 1, pp. 12–25, 2025.

[11] M. K. Pandey and S. Sharma, "WORM Storage: A Critical Component of Modern Data Governance," *IEEE Consumer Electronics Magazine*, vol. 11, no. 3, pp. 92–98, 2022.

[12] H. Wang and J. Xu, "Dynamic Retention Policies for Immutable Backups in Hybrid Cloud Environments," in *Proc. IEEE 12th International Conference on Cloud Computing (CLOUD)*, 2023, pp. 210–217.

[13] R. Moussa and M. Azar, "Detecting Ransomware Attacks Using Entropy-Based Analysis," in *Proc. 4th International Conference on Computer Science and Information Technology (CSIT)*, 2020, pp. 1–5.

[14] A. Continella *et al*., "ShieldFS: A Self-Healing, Ransomware-Aware Filesystem," in *Proc. 32nd Annual Conference on Computer Security Applications (ACSAC)*, 2016, pp. 336–347.

[15] J. Kim and Y. Park, "Snapshot Isolation and Its Role in Preventing Data Deletion Attacks," *Journal of Systems Architecture*, vol. 118, Art. no. 102214, 2021.

[16] Z. Wu, "A Survey of Distributed Storage Protection Mechanisms Against Malware Propagation," *IEEE Communications Surveys & Tutorials*, vol. 24, no. 1, pp. 450–482, 2022.

[17] X. Zhang and J. Huang, "MinIO-Based Immutable Object Storage for Enterprise Data Recovery," in *Proc. IEEE International Conference on Big Data*, 2022, pp. 3412–3419.

[18] S. Gupta and R. Kumar, "Ceph-Based Distributed Storage: Security Challenges and Solutions," *IEEE Transactions on Cloud Computing*, vol. 9, no. 4, pp. 1450–1463, 2021.

[19] L. Xiao, X. Wan, X. Lu, Y. Zhang, and D. Wu, "IoT Security Techniques Based on Machine Learning: How Do IoT Devices Use AI to Enhance Security?" *IEEE Signal Processing Magazine*, vol. 35, no. 5, pp. 41–49, 2018.

[20] D. S. Kim and J. S. Park, "Automated Rollback and Recovery Mechanisms for Distributed Databases Following Ransomware Infection," in *Proc. International Conference on Information Networking (ICOIN)*, 2021, pp. 145–148.

[21] F. G. Marmol and J. Perez, "Zero Trust Storage: The Next Frontier in Ransomware Defense," *IEEE Security & Privacy*, vol. 21, no. 2, pp. 30–38, 2023.

[22] T. G. Moore, "The Economics of Ransomware and the Role of Insurance," *IEEE Security & Privacy*, vol. 19, no. 4, pp. 91–95, 2021.

[23] A. S. Sani *et al*., "A Survey of Malware Detection Techniques for Distributed Systems," *IEEE Access*, vol. 8, pp. 143210–143235, 2020.

[24] P. Rani and V. Sharma, "Leveraging OpenZFS Snapshots for High-Frequency Data Protection," *International Journal of Computer Applications*, vol. 183, no. 22, pp. 14–20, 2021.

[25] S. J. Oh and K. L. Kim, "Real-Time File System Monitoring for Early Ransomware Warning Systems," in *Proc. IEEE 46th Annual Computers, Software, and Applications Conference (COMPSAC)*, 2022, pp. 1120–1125.

[26] J. Void and C. Wills, "Impact of Retention Periods on Storage Efficiency in Immutable Backup Systems," in *Proc. IEEE International Conference on Smart Computing (SMARTCOMP)*, 2021, pp. 288–293.

[27] R. Richardson and M. North, "Ransomware: Strategies for Prevention and Recovery," *Journal of Information Systems Education*, vol. 28, no. 1, pp. 45–56, 2017.

[28] K. Yang and S. Kim, "Behavioral Analysis of Ransomware Families and Their Storage Access Patterns," *IEEE Access*, vol. 9, pp. 102540–102555, 2021.

[29] C. Zhang and D. Liu, "Scalability of Immutable Storage Architectures in Multi-Cloud Environments," *IEEE Transactions on Parallel and Distributed Systems*, vol. 33, no. 8, pp. 1850–1865, 2022.