

# ENHANCING BACKUP SECURITY IN THE ERA OF CYBER THREATS

Yazeed Al Moaiad<sup>1</sup>

Faculty of Computer and Information  
Al-Madinah International University  
Kuala Lumpur, Malaysia  
yazeed.alsayed@mediu.edu.my

Abdullatif Abdulsalam<sup>2</sup>

Faculty of Computer & Information Technology  
Al-Madinah International University  
Kuala Lumpur, Malaysia  
BL242@lms.mediu.edu.my

**Abstract**—Ransomware and related intrusions have transformed enterprise backup repositories from passive recovery assets into deliberate attack targets. This paper condenses a thesis-scale systematic literature review of backup security in the 2023–2026 threat landscape. Following a PRISMA-based process, 1,200 records from a broad database and repository search were reduced to 108 included sources. The corpus contains 38 empirical studies (35.2%) and 28 empirically grounded grey-literature sources (25.9%), for a combined evidence base of 66 sources (61.1%). The synthesis identified credential compromise, vulnerability exploitation, and lateral movement as the principal pathways into backup infrastructure. Immutable storage and physical air gaps received the strongest effectiveness ratings, whereas logical air gaps, cloud encryption, and AI/ML detection remained dependent on implementation quality; blockchain verification remained primarily theoretical. Thirty-seven initial codes were consolidated into nine research gaps, led by pre-restoration integrity verification and latent-malware detection. The paper proposes a Five-Layer Backup Resilience Framework—Prevention, Detection, Resilience, Response, and Governance—as a backup-specific operationalization of five NIST CSF 2.0 functions that also aligns with ISO 27001:2022, DORA, NIS2, SAMA, and NCA ECC. The framework is evidence-informed but has not been validated in a production environment; the results therefore support a structured research and implementation agenda rather than measured claims of deployment effectiveness.

**Keywords**— Backup Security; Ransomware; Immutable Storage; Air Gap; Cyber Resilience; Data Integrity; Zero-Trust Architecture; Systematic Literature Review

## I. INTRODUCTION

The ransomware-as-a-service ecosystem has professionalized cybercrime and accelerated the transition from opportunistic encryption to multi-stage recovery denial [1]. Backup systems are therefore no longer only a last line of defense: adversaries increasingly seek backup credentials, management interfaces, catalogues, snapshots, and repositories before encrypting production workloads [2], [3]. The thesis reports that the global median dwell time in investigated incidents reached 14 days in 2025, while ransomware-specific medians remained shorter at 5–9 days [4]. These values describe different incident populations, but both indicate that attackers can have sufficient time to

discover and impair recovery infrastructure before visible disruption.

The practical risk is substantial. The source thesis reports from industry evidence that 94% of ransomware attacks attempt to compromise backups and that 57% of those attempts succeed [2]. A separate cyber-resilience assessment reported that 93% of attacks target backup repositories and that 43% of targeted data is unrecoverable [5], while another survey found that 21% of organizations fail to recover all required data from backup [6]. These values are reported survey findings rather than measurements produced by the present study. Independent empirical work nevertheless supports the strategic importance of recoverability: analysis of 481 police-reported incidents and 237 negotiation transcripts found that fully recoverable backups materially reduced ransom payment behavior [7], and a 450,000-iteration simulation across nine organizational scenarios found that 21% of attacks could disrupt business continuity for at least two weeks [8].

This study addresses three questions: **RQ1**, which cyber threats specifically targeted backup infrastructure during 2023–2026; **RQ2**, which technologies protected backup systems and what documented effectiveness they demonstrated; and **RQ3**, which critical backup-security gaps require further investigation. Its contributions are: (1) a systematic synthesis of 108 academic, governmental, vulnerability, and industry sources; (2) an evidence-based comparison of established and emerging controls; (3) a qualitative ranking of nine research gaps; and (4) a Five-Layer Backup Resilience Framework with an illustrative enterprise implementation mapping. No primary experiment or production deployment was conducted.

## II. RELATED WORK AND SYSTEM CONTEXT

### A. Threat Evolution and Backup Attack Surface

Recent surveys of ransomware research emphasize early detection, behavioral analysis, and attack-chain disruption, but backup-specific detection remains less mature than protection of production endpoints [9], [10]. The thesis bounds the primary threat model to enterprise disk, cloud, and tape backup environments and includes ransomware,

credential compromise, vulnerability exploitation, lateral movement, insider threats, supply-chain compromise, zero-day exploitation, cloud-native attacks, and AI-assisted attacks. DoS/DDoS, man-in-the-middle attacks, physical attacks, fileless attacks, firmware-level attacks, social engineering beyond phishing, non-ransomware exfiltration, and comprehensive APT analysis are treated as adjacent domains rather than evidence for the central framework.

Credential compromise allows an adversary to use legitimate administration paths to alter policies, delete recovery points, or disable immutability. Public disclosures demonstrate that product vulnerabilities can produce the same outcome: CVE-2023-27532 exposed encrypted credentials in Veeam Backup & Replication [11], [12]; CVE-2025-66172 involved improper access logic in Apache CloudStack volume restoration [13]; CVE-2024-48248 was a path-traversal flaw in NAKIVO Backup & Replication [14]; and CVE-2026-22769 affected Dell RecoverPoint for Virtual Machines [15]. The Finland National Cyber Security Centre additionally documented Akira ransomware targeting NAS and tape backup devices [16]. These examples support the thesis's treatment of the backup control plane, identity plane, and storage plane as separate but connected attack surfaces.

### B. Protection Technologies and Their Limits

The 3-2-1 rule improves redundancy through three copies, two media types, and one off-site copy, but it was developed primarily for operational failure and disaster recovery rather than credential-led attacks against connected infrastructure [17], [18]. Immutable storage adds retention-enforced, write-once-read-many behavior and received a high effectiveness rating in the thesis synthesis [19], [20]. Physical air gaps and offline tape received the strongest rating because they remove a continuously reachable control path, although they increase operational complexity and can delay restoration [16], [21], [22]. Logical air gaps offer greater accessibility but remain dependent on identity separation, multi-user authorization, and correct configuration [23].

Cloud encryption protects data confidentiality, but key custody, authorization, and service configuration remain failure points [24]. AI/ML techniques show promising laboratory results: multistage malware detection reported a 96% detection rate with less than 10% performance overhead [25], integrated active protection has been demonstrated in backup workflows [26], and an AI-driven backup-integrity approach reported 98.65% detection accuracy [27]. These are study-specific results, not a pooled performance estimate. The thesis therefore rated AI/ML from low to moderate because the evidence is heterogeneous and adversarial evasion remains a concern. Blockchain-based verification may provide tamper evidence, but the reviewed implementation remained limited by scalability, cost, and a lack of independent validation [28].

## III. METHODOLOGY

### A. Review Design and Selection

A qualitative systematic literature review was conducted under a PRISMA 2020-inspired protocol. Searches covered January 2023 through May 2026. The thesis narrative reports 18 academic databases/registers, while the printed

methodology enumerates 19 named services: ACM Digital Library, arXiv, Google Scholar, MDPI, IEEE Xplore, SpringerLink, ScienceDirect, CORE, DiVA, PQDT Open, ETHOS, CiteSeerX, Semantic Scholar, SSRN, BASE, ScienceOpen, WorldWideScience, OSTI.GOV, and EULC. This internal count discrepancy is retained rather than silently normalized. Search expressions combined terms for backup security, immutable backup, air-gapped storage, ransomware, malware deletion, credential compromise, integrity verification, zero trust, detection, prevention, and recovery.

Eligible sources directly addressed backup-system security, ransomware targeting of backups, or backup-integrity verification and were published in English during the review window. The main exclusions were pre-2023 work, material concerned only with production-system encryption, consumer-only solutions without broader relevance, general cybersecurity without a backup component, and unsupported opinion. Peer-reviewed research was assessed for review status, methodological transparency, recency, and relevance. Grey literature was separately assessed for methodological transparency, recency, direct relevance, and organizational authority, and important commercial claims were triangulated against independent academic, governmental, standards, or vulnerability evidence.

Table 1. Distribution of the 108 included sources

| Source type                       | Count      | Percentage     |
|-----------------------------------|------------|----------------|
| Peer-reviewed journal articles    | 28         | 25.93%         |
| Conference proceedings            | 12         | 11.11%         |
| Doctoral dissertations            | 1          | 0.93%          |
| Master's theses                   | 4          | 3.70%          |
| White papers / technical reports  | 8          | 7.41%          |
| Government / regulatory documents | 10         | 9.26%          |
| Vulnerability databases (CVE/NVD) | 5          | 4.63%          |
| Industry reports / surveys        | 24         | 22.22%         |
| arXiv preprints                   | 6          | 5.56%          |
| Blogs / online articles           | 6          | 5.56%          |
| Book chapters                     | 4          | 3.70%          |
| <b>Total</b>                      | <b>108</b> | <b>100.00%</b> |

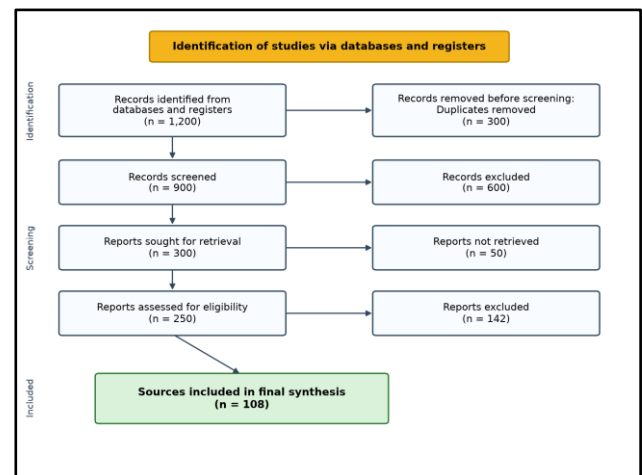


Figure 1. PRISMA-based source-selection flow reconstructed from the thesis.

### B. Data Extraction and Thematic Synthesis

Each included source was coded for bibliographic information, publication year, source type, research focus, key findings, and acknowledged limitations. Open coding produced 37 descriptive codes, including immutable backup, air-gap breach, credential compromise, cloud vulnerability, and AI detection. Axial coding consolidated these into nine categories, and thematic mapping grouped them under the three research questions. The final corpus contained 38 empirical studies (35.2%) based on primary data, controlled experiments, simulations, or case studies, plus 28 empirically grounded grey-literature sources (25.9%) based on incident or survey data. Thus, 66 sources (61.1%) supplied empirical or empirically grounded evidence. This classification describes the thesis corpus; it does not imply uniform design quality or a formal meta-analysis.

## IV. RESULTS

### A. Threats Targeting Backup Infrastructure

The synthesis associated 58 sources with backup-targeting threats. Credential compromise was the most frequently discussed vulnerability (51 sources), followed by misconfiguration (44 sources). Three direct pathways dominated the coded evidence: credential compromise, exploitation of unpatched backup software, and lateral movement from production systems into backup servers. Insider threats, supply-chain compromise, zero days, cloud-native sabotage, and AI-assisted reconnaissance were secondary but recurring categories.

Table 2. Principal backup-targeting threat pathways reported by the thesis

| Threat category            | Specific attack vector                         | Sources mentioning | Thesis example                       |
|----------------------------|------------------------------------------------|--------------------|--------------------------------------|
| Credential compromise      | Phishing, credential dumping, exposed services | 51                 | CVE-2023-27532 [11], [12]            |
| Vulnerability exploitation | Unpatched backup-software flaws                | 44                 | CVE-2025-66172 [13]                  |
| Lateral movement           | Production-to-backup propagation               | 39                 | Akira activity against NAS/tape [16] |

The literature and industry data indicate that recovery denial is an explicit attacker objective rather than a by-product of production encryption [2]–[5]. The thesis also notes that newer ransomware families use intermittent encryption and evasive behavior, complicating entropy- and signature-based detection. Accordingly, repository survivability alone is insufficient if the retained recovery point contains latent malware or if the backup catalogue and identity plane remain writable by compromised administrators.

### B. Effectiveness of Existing Controls

Across the corpus, immutable backup was discussed in 47 sources, air gapping in 39, and AI-based detection in 33. The evidence-based ratings in Table 3 are the thesis's qualitative synthesis, not standardized effect sizes. "High" or "Very High" denotes consistent support across multiple sources with acknowledged limitations; "Moderate" denotes partial or implementation-sensitive effectiveness; and "Low" denotes limited or primarily theoretical validation.

Table 3. Thesis-rated effectiveness of backup-security technologies

| Technology | Rating | Evidence-based interpretation |
|------------|--------|-------------------------------|
|------------|--------|-------------------------------|

| Technology              | Rating                                        | Evidence-based interpretation                                                                                                   |
|-------------------------|-----------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------|
| 3-2-1 rule              | Moderate for failure; Low for targeted attack | Useful redundancy, but connected copies may share credentials or control paths [17], [18].                                      |
| Immutable storage       | High                                          | Strong resistance to alteration during retention; depends on correct locking, identity, and retention configuration [19], [20]. |
| Physical air gap        | Very High                                     | Strong isolation with operational and recovery-time costs [16], [21], [22].                                                     |
| Logical air gap         | Moderate                                      | Useful when control-plane separation and multi-user authorization are correctly enforced [23].                                  |
| Cloud backup encryption | Moderate                                      | Protects confidentiality; key custody and misconfiguration remain material risks [24].                                          |
| AI/ML detection         | Low–Moderate                                  | Promising study-specific detection results, but heterogeneous validation and adversarial evasion [25]–[27].                     |
| Blockchain verification | Low                                           | Mainly theoretical in the reviewed backup context; scalability and independent validation remain limited [28].                  |

The pattern is a security–operability trade-off. Strongly isolated controls reduce attacker reachability but increase media handling, recovery latency, and administrative burden. More accessible controls reduce friction but increase dependence on identity, configuration, and continuous monitoring. No technology in the review addressed every threat and failure mode.

### C. Critical Research Gaps

The 37 open codes were consolidated into nine gaps and ranked qualitatively using three factors: frequency in the reviewed literature, potential impact on organizational resilience, and recurrence across independent academic and industry sources. The ranking is not a mathematical score. Pre-restoration integrity verification and latent-malware detection were critical because both determine whether a retained backup is safe and recoverable at the moment of crisis. Access control ranked next because compromised privilege can undermine otherwise sound storage controls.

Table 4. Research gaps ranked by urgency in the thesis

| Rank | Research gap                               | Sources | Severity    |
|------|--------------------------------------------|---------|-------------|
| 1    | G1—Pre-restoration integrity verification  | 49      | Critical    |
| 2    | G2—Latent-malware detection in backups     | 31      | Critical    |
| 3    | G3—Backup access control / least privilege | 31      | High        |
| 4    | G6—Attack-resilient backup processes       | 22      | High        |
| 5    | G7—Security–operations balance             | 19      | Medium–High |
| 6    | G4—Regulatory compliance                   | 13      | Medium      |
| 7    | G8—Backup software supply-chain security   | 12      | Medium      |
| 8    | G5—Emerging environments (IoT, edge, AI)   | 11      | Medium      |
| 9    | G9—Forensics for backup-targeting attacks  | 4       | Low–Medium  |

Several reviewed systems show progress without closing these gaps. The Remembrall study reported zero false negatives in its evaluated setting [29], while in-operation off-site backup research reported a  $10^{-8}$  false-negative miss-detection rate [30]. Such results remain dependent on each study's architecture and test conditions. The thesis therefore treats them as supporting evidence for attack-resilient process design, not as universal guarantees.

## V. PROPOSED FIVE-LAYER BACKUP RESILIENCE FRAMEWORK

### A. Architecture and Gap Coverage

The proposed framework integrates three established perspectives: the 3-2-1 principle for redundancy, zero-trust controls for identity and access, and defense-in-depth for

overlapping safeguards. It is not presented as a replacement for NIST CSF 2.0 or as a new set of security primitives. Its contribution is to organize known controls around the backup lifecycle and map the nine identified gaps to backup-specific functions.

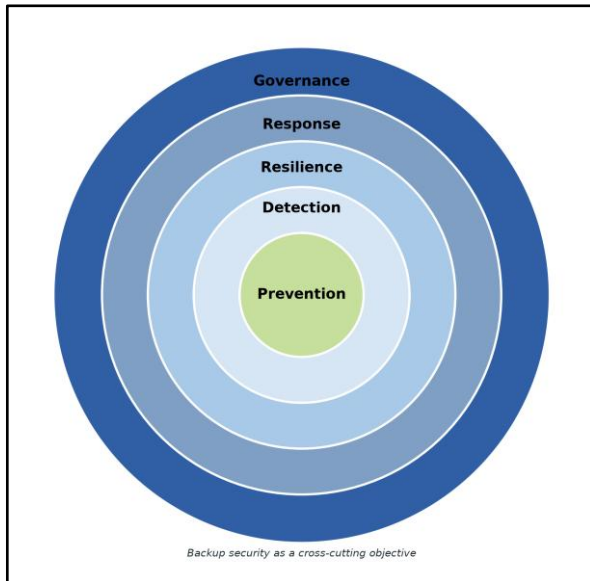


Figure 2. Five-Layer Backup Resilience Framework reconstructed from the thesis.

Table 5. Framework layers, controls, gap coverage, and CSF 2.0 mapping

| Layer      | Backup-specific controls                                       | Gaps addressed     | CSF 2.0 function |
|------------|----------------------------------------------------------------|--------------------|------------------|
| Prevention | Hardening, PAM/MFA, segmentation, backup-CVE patching          | G3, G5, G8         | Protect          |
| Detection  | Integrity checks, anomaly analytics, backup-specific IDS rules | G1, G2, G5, G6     | Detect           |
| Resilience | WORM/immutability, air gaps, geographic distribution           | G5, G7             | Recover          |
| Response   | Malware scanning, clean-room restore, recovery playbooks       | G1, G2, G5, G6, G9 | Respond          |
| Governance | Policy, compliance automation, exercises, metrics              | G3, G4, G5, G8     | Govern           |

The **Prevention** layer reduces initial compromise through hardened backup software, privileged-access management, multi-factor authentication, vulnerability management, and isolation of backup administration. **Detection** applies continuous integrity verification, anomaly analysis of backup operations, and rules for events such as unexpected shadow-copy deletion, catalogue tampering, job failures, or retention changes. **Resilience** preserves recoverable copies through immutable tiers, physical or logical air gaps, and independent geographic copies. **Response** validates and restores data in isolated environments using backup-specific incident playbooks. **Governance** sustains policy, role recertification, recovery exercises, audit evidence, and executive reporting.

The thesis maps these layers respectively to Protect, Detect, Recover, Respond, and Govern in NIST CSF 2.0. CSF 2.0 also contains an Identify function, which the five-layer table does not map to a separate layer; the paper therefore does not claim complete one-to-one coverage of all six CSF functions. The thesis additionally aligns the framework with the backup, integrity, monitoring, continuity, recovery, and governance requirements represented in ISO 27001:2022, the EU Digital Operational

Resilience Act [31], NIS2 guidance [32], the Saudi National Cybersecurity Authority Essential Cybersecurity Controls [33], and the SAMA Cybersecurity Framework [34]. NIST backup and storage guidance provides related operational context [35], [36]. These correspondences are analytical mappings developed in the thesis, not certification claims.

### B. Illustrative Enterprise Implementation

The thesis provides an implementation scenario for a representative hybrid enterprise containing VMware vSphere and Nutanix AHV clusters, Windows and Linux servers, Microsoft SQL Server and Oracle Database, and Veritas NetBackup. In the prevention layer, the mapping calls for a separated backup-management zone, secure baselines, MFA, just-in-time privilege, and prioritized remediation of backup CVEs. Detection sends audit and job telemetry to a SIEM and monitors deletion, policy, size, and retention anomalies. Resilience combines immutable targets, logically isolated repositories, offline tape for critical data, geographic replication, transaction-log protection, and database consistency checks. The main scenario configures WORM retention longer than 14 days; a practice recommendation elsewhere in the thesis gives a 7–14-day minimum derived from the cited 5–9-day ransomware-specific dwell-time range [4]. Longer-dwell operations can exceed either floor.

Response uses predefined recovery order, sandboxed restoration, malware scanning, automated workflows, and explicit RTO/RPO validation. Governance adds periodic access review, compliance evidence, annual architecture review, quarterly disaster-recovery exercises, restore-success reporting, and comparison of measured recovery time with business targets. Automated restore-testing capabilities are available in contemporary platforms [37], but the scenario was not deployed or benchmarked by the thesis. Its “expected benefits” are therefore design expectations rather than measured outcomes.

## VI. DISCUSSION

The central finding is that recoverability depends on coordinated identity, storage, monitoring, restoration, and governance controls. The 3-2-1 rule remains useful for redundancy, but it does not prevent a credentialed adversary from deleting or corrupting several reachable copies. Immutability and physical isolation provide stronger survivability, yet both can be undermined by retention errors, compromised administration, unavailable decryption keys, or untested restoration. Likewise, high detection rates reported in individual AI/ML studies [25]–[27] do not establish general robustness against new ransomware families, adversarial manipulation, or heterogeneous enterprise workloads.

The evidence also reveals a practical imbalance: the strongest controls are often the least convenient, while the most operationally flexible controls depend heavily on correct configuration. The framework therefore places governance around—not after—the technical layers. Recovery exercises, access recertification, key-custody separation, configuration review, and audited evidence are necessary to preserve the value of immutable and isolated copies over time.

### A. Adjacent Threats and Future Research

The primary framework intentionally excludes threat classes that are broader than direct backup compromise. The thesis nevertheless proposes an expanded Eight-Layer research agenda that retains the five core layers and adds **Network Security** for DoS/DDoS and MITM concerns, **Physical and Hardware Security** for theft, sabotage, firmware, and device tampering, and **Human and Behavioral Security** for social engineering beyond phishing. Fileless attacks and comprehensive APT analysis would extend detection and response rather than create separate layers.

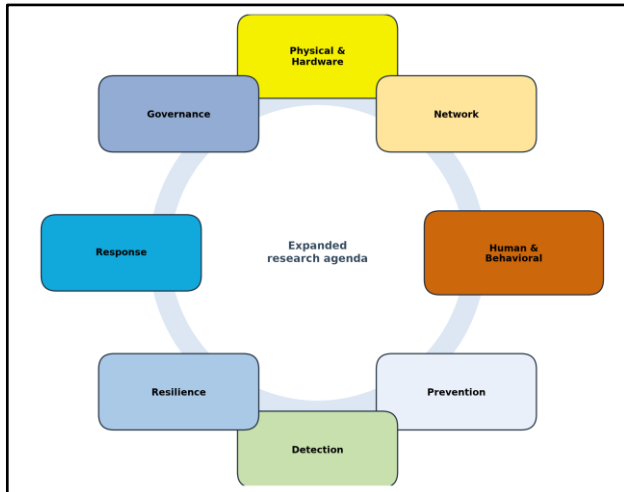


Figure 3. Expanded Eight-Layer Framework proposed as a future research direction.

Priority validation work should include controlled tests on representative backup platforms; ransomware simulations; expert review by backup, security, and disaster-recovery practitioners; pre/post measurement of RTO, RPO, restore success, and integrity-verification outcomes; and longitudinal studies in finance, healthcare, and critical infrastructure. Research is also needed on lightweight pre-restoration verification, latent-malware detection in backup streams, backup-specific zero-trust design, supply-chain assurance, edge/IoT/5G contexts, human factors, and cost-benefit measurement.

### B. Limitations

The paper inherits the thesis's limitations. It is a secondary study based on publicly available English-language material and includes industry reports whose methods and incentives differ from peer-reviewed research. The single-researcher screening and coding process may introduce selection or interpretation bias. Rapidly evolving threats can make findings obsolete, and the enterprise focus limits generalization to consumer systems. Source counts show attention within the corpus, not prevalence in the full literature, and the qualitative effectiveness and urgency ratings are not statistical meta-analytic estimates. Most importantly, neither the Five-Layer Framework nor the enterprise scenario was implemented in a live organization. Claims about effectiveness must remain evidence-informed hypotheses pending controlled and field validation.

## VII. CONCLUSION

This paper synthesized the thesis evidence on backup security during 2023–2026. From 1,200 identified records, 108 sources were included; 66 were empirical or empirically grounded. The synthesis identifies credential compromise, vulnerability exploitation, and lateral movement as the dominant direct pathways into backup infrastructure. Physical air gaps and immutable storage received the strongest qualitative ratings, while AI/ML and blockchain approaches require broader validation. Nine research gaps were identified, with pre-restoration integrity verification and latent-malware detection ranked as the most urgent.

The proposed Five-Layer Backup Resilience Framework organizes prevention, detection, resilience, response, and governance controls around the backup lifecycle and maps them to established cybersecurity and regulatory expectations. It offers a disciplined design and evaluation structure, not proof of operational efficacy. The immediate research priority is to test the framework under repeatable ransomware scenarios and in longitudinal enterprise deployments while measuring recoverability, integrity, operational cost, and governance outcomes.

## VIII. REFERENCES

- [1] S. Razaula, C. Fachkha, C. Markarian, A. Gawanmeh, W. Mansour, B. C. M. Fung, and R. Abbass, "The age of ransomware: A survey on the evolution, taxonomy, and research directions," *IEEE Access*, vol. 11, pp. 40698–40723, 2023, doi: 10.1109/ACCESS.2023.3268535.
- [2] Sophos, "The State of Ransomware 2024," Sophos Whitepaper, Apr. 2024. [Online]. Available: <https://newsletter.radensa.ru/wp-content/uploads/2024/05/sophos-state-of-ransomware-2024-wp.pdf>
- [3] Check Point Software Technologies, "Cyber attack trends report 2025," Check Point Research, 2025. [Online]. Available: <https://engage.checkpoint.com/2025-ai-security-report/>
- [4] Mandiant, "M-Trends 2026: Insights from the frontline," Mandiant/Google Cloud, 2026. [Online]. Available: <https://cloud.google.com/blog/topics/threat-intelligence/m-trends-2026>
- [5] Druva, "Cyber resilience maturity assessment 2025," 2025. [Online]. Available: <https://www.druva.com/why-druva/druva-difference/cyber-resilience-maturity-model/short-assessment>
- [6] Apricorn, "Nearly 20% of US IT security practitioners cite attacks on backups as primary cause of data breach," Apricorn Press, 2025. [Online]. Available: <https://apricorn.com/apricorn-2025-survey-release-3/>
- [7] T. Meurs, A. Cartwright, E. Cartwright, H. Houba, and D. Woods, "The ransomware pricing paradox: An empirical study of the six stages of ransomware negotiations," *Tinbergen Institute Discussion Paper TI 2025-052/VII*, 2025. [Online]. Available: <https://papers.tinbergen.nl/25052.pdf>
- [8] M.-C. Ilau, A. Baldwin, T. Caulfield, and D. Pym, "Modelling and simulating organizational ransomware recovery: Structure, methodology, and decisions," *Journal of Cybersecurity*, 2025, doi: 10.1093/cybsec/tyaf035.
- [9] M. U. Rehman, R. Akbar, M. Omar, and A. R. Gilal, "A systematic literature review of ransomware detection methods and tools for mitigating potential attacks," in *Cybersecurity and Data Protection*. Springer Nature, 2024, pp. 145–178, doi: 10.1007/978-981-99-9589-9\_7.
- [10] L. Albshaier, S. Almarri, and M. M. H. Rahman, "Earlier decision on detection of ransomware identification: A comprehensive systematic literature review," *Information*, vol. 15, no. 8, Art. no. 484, 2024.
- [11] Veeam Software, "KB4424: CVE-2023-27532 vulnerability in Veeam Backup & Replication," 2023. [Online]. Available: <https://www.veeam.com/kb4424>
- [12] Horizon3.ai, "Veeam Backup and Replication CVE-2023-27532 deep dive," 2023. [Online]. Available: <https://www.horizon3.ai/veeam-backup-and-replication-cve-2023-27532-deep-dive/>

- [13] Apache CloudStack, "CVE-2025-66172 security advisory: Improper access logic in volume restoration," Apache Software Foundation, 2026. [Online]. Available: <https://cloudstack.apache.org/>
- [14] NAKIVO, "CVE-2024-48248: Path traversal vulnerability in NAKIVO Backup & Replication," Security Advisory, 2025. [Online]. Available: <https://helpcenter.nakivo.com/Knowledge-Base/Content/Security-Advisory/CVE-2024-48248.htm>
- [15] Dell, "CVE-2026-22769 security advisory: Dell RecoverPoint for Virtual Machines zero-day exploitation," Dell Security, 2026. [Online]. Available: <https://www.dell.com/>
- [16] Finland National Cyber Security Centre, "Akira ransomware warning: Targeting tape and NAS backup devices," NCSC-FI Bulletin 2024-12, 2024. [Online]. Available: <https://www.kyberturvallisuuskeskus.fi/en/news/national-cyber-security-centre-finlands-weekly-review-122024>
- [17] Arcserve, "How to protect against ransomware with a 3-2-1-1 strategy," White Paper, 2024. [Online]. Available: <https://www.arcserve.com/blog/how-protect-against-ransomware-3-2-1-1-strategy>
- [18] Keepit, "3-2-1 backup rule update: Air gap your immutable backups," 2024. [Online]. Available: <https://www.keepit.com/blog/understanding-the-new-backup-rules/>
- [19] A. Anand and V. K. Singh, "Immutable backup architectures as a defensive paradigm against ransomware: Design, evaluation, and performance analysis," Computer Research and Development, vol. 25, no. 12, 2025. [Online]. Available: <https://zenodo.org/records/20478051>
- [20] Object First, "Immutable backups: A comprehensive analysis of their role in cybersecurity, compliance, and data integrity," White Paper, 2025. [Online]. Available: <https://objectfirst.com/>
- [21] TechTarget, "Tape backup and offline storage: Balancing security and operational needs," TechTarget Storage, 2025. [Online]. Available: <https://www.techtarget.com/>
- [22] LTO Consortium, "LTO-10 specification: Multi-layer security support with hardware-based encryption," LTO Technology Provider Group, 2025. [Online]. Available: <https://www.lto.org/>
- [23] Wasabi Technologies, "Logical air gap solution: Multi-user authentication for backup security," 2025. [Online]. Available: <https://wasabi.com/>
- [24] N-able, "Top 9 cloud backup security concerns and fixes," Mar. 7, 2026. [Online]. Available: <https://www.n-able.com/pt-br/blog/cloud-backup-security-concerns>
- [25] P. Novak, V. Oujezsky, P. Kaura, T. Horvath, and M. Holik, "Multistage malware detection method for backup systems," Technologies, vol. 12, no. 2, Art. no. 23, 2024, doi: 10.3390/technologies12020023.
- [26] V. Oujezsky, P. Novak, T. Horvath, M. Holik, and M. Jurcik, "Data backup system with integrated active protection against ransomware," in Proc. 46th Int. Conf. Telecommunications and Signal Processing (TSP), 2023, pp. 1–5, doi: 10.1109/TSP59544.2023.10197687.
- [27] B. Kumar, S. K. Gupta, R. Dwivedi, D. M. Alsekai, D. S. AbdElminaam, and O. Kilickaya, "Artificial intelligence driven approach for securing backup data and enhancing cyber resilience in sustainable smart infrastructure," Scientific Reports, vol. 16, Art. no. 13609, 2026, doi: 10.1038/s41598-026-37802-6.
- [28] S. M. Shakhnazar, "Blockchain based configuration files backup system for enhanced security and integrity," Master's thesis, SDU University, 2025. [Online]. Available: <https://sdu.edu.kz/>
- [29] Y. Hou, L. Guo, C. Zhou, Q. Zhang, W. Liu, C. Sun, and Y. Jiang, "Remembrall: Preventing disruption of system backup against ransomware attacks," Proceedings of the ACM on Software Engineering, vol. 2, ISSTA, Art. no. ISSTA011, 2025, doi: 10.1145/3728880.
- [30] H. Fujinoki, A. A. Towell, and V. A. Thota, "Preventing ransomware damages using in-operation off-site backup to achieve a 10<sup>-8</sup> false-negative miss-detection rate," in Proc. IEEE ICCI, 2025. [Online]. Available: <https://ieeexplore.ieee.org/document/11158394>
- [31] European Union, "Regulation (EU) 2022/2554 on digital operational resilience for the financial sector (DORA)," Official Journal of the European Union, L 333/1, Dec. 2022. [Online]. Available: <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32022R2554>
- [32] IDC, "NIS2 directive compliance requirements: Impact on data protection," International Data Corporation, 2025. [Online]. Available: <https://www.idc.com/>
- [33] Al Moaiad, Y., D., Alkhateeb, M., & Alokla, M. (2024). Enhancing Cybersecurity Practices in Nigerian Government Institutions an Analysis and Framework. J. Electrical Systems, 20(3), 5964-5967.
- [34] Al Moaiad, Y., D., Alkhateeb, M., & Alokla, M. (2024). Deep Analysis of Iris Print and Fingerprint for Detecting Drug Addicts. J. Electrical Systems, 20(3), 5639-5644.
- [35] Al Moaiad, Y., Alobed, M., & Alsakhnini, M. (2024). Python Solutions to Address Natural Language Challenges. International Journal, 10(3), 3594-3603.
- [36] Al Moaiad, Y., Alobed, M., Alsakhnini, M., & Momani, A. M. (2024). Challenges in natural Arabic language processing. Edelweiss Applied Science and Technology, 8(6), 4700-4705.
- [37] Al Moaiad, Y., Alobed, M., Alsakhnini, M., & Momani, A. M. (2024). Challenges in natural Arabic language processing. Edelweiss Applied Science and Technology, 8(6), 4700-4705.