10.48047/jocaaa.2024.33.08.560

Self-Healing Cloud Security Architecture for Financial Systems Using Autonomous Incident Response

Rizwana Sindhavani
rizwanasindhawani@yahoo.in

Abstract

Financial systems are increasingly migrating to cloud environments to achieve scalability, agility, and cost efficiency, but this transition has expanded the attack surface and amplified the complexity of incident response. Traditional security operations rely heavily on manual intervention, which struggles to keep pace with the speed and sophistication of modern threats targeting cloud-hosted banking platforms. This paper proposes a self-healing cloud security architecture for financial systems that integrates autonomous incident response with continuous monitoring, threat reasoning, and automated remediation. The architecture combines telemetry ingestion across cloud services, machine learning-based anomaly detection, a policy-driven decision engine, and orchestrated response actions that can isolate, restore, and harden affected components without human intervention. Empirical evaluation was conducted on a simulated multi-cloud banking environment exposed to a portfolio of attack scenarios including credential abuse, container compromise, lateral movement, and data exfiltration. Results show that the self-healing system reduced mean time to remediation from twenty-eight minutes to under ninety seconds, while maintaining a containment success rate of 93.4 percent across the tested scenarios. False action rates remained at acceptable operational levels, and recovery completeness reached 96.1 percent. The findings demonstrate that combining autonomous response with self-healing principles offers a credible path toward resilient cloud security for financial institutions operating under high-volume and high-stakes conditions.

Keywords

Cloud Security, Self-Healing Architecture, Autonomous Incident Response, Financial Systems, Security Orchestration, Resilience Engineering

1. Introduction

The financial services industry has undertaken one of the most ambitious cloud migration efforts of any regulated sector, moving core banking platforms, payment processing systems, and customer engagement services into public, private, and hybrid cloud environments [1]. This shift has delivered substantial operational benefits but also introduced new categories of risk. Cloud environments differ from traditional data centres in their elasticity, shared responsibility models, and reliance on identity-based access, which together demand a fundamentally different approach to security [2].

The threat landscape facing cloud-hosted financial systems has grown increasingly hostile. Sophisticated adversaries now exploit misconfigured storage buckets, compromised credentials, container vulnerabilities, and supply chain weaknesses to gain footholds in cloud environments [3]. Once inside, attackers can move laterally across services and accounts at speeds that overwhelm conventional response processes. Recent incident reports indicate that the median dwell time between initial compromise and discovery remains measured in days or weeks, while damage can occur within minutes of initial access [4].

10.48047/jocaaa.2024.33.08.560

Traditional incident response in financial institutions follows a structured but largely manual workflow. Security analysts triage alerts, gather evidence, coordinate with operations teams, and execute remediation steps through change-controlled processes. While appropriate for many situations, this approach struggles to match the velocity required for cloud-native threats [5]. The cost of delay can be substantial in financial settings, where each minute of unaddressed compromise may translate into stolen funds, exfiltrated customer data, or regulatory exposure.

Self-healing architecture has emerged as a promising paradigm for closing this gap. Drawing on principles from biological systems and resilience engineering, self-healing systems detect deviations from normal operation and execute corrective actions autonomously to restore desired states [6]. In the security context, this translates into automated containment of compromised components, restoration from clean baselines, and adaptive hardening to prevent recurrence. Autonomous incident response extends these ideas with machine learning-based reasoning, allowing systems to interpret complex telemetry and select appropriate response actions without scripted rule chains for every possible scenario [7].

Despite growing interest, deploying self-healing security in financial systems faces real challenges. Autonomous actions carry risk of disrupting legitimate operations if false alarms trigger aggressive containment. Regulatory expectations around change control and auditability constrain how much autonomy can be granted to automated systems. Integration with existing security tooling, identity providers, and orchestration platforms requires careful architectural design.

This research is motivated by three central questions. Can a self-healing architecture deliver substantial reductions in mean time to remediation for cloud-hosted financial systems? Can autonomous response actions maintain acceptable accuracy and avoid harmful disruption to legitimate operations? And how does the proposed approach compare with conventional manual and semi-automated response models across realistic attack scenarios? The remainder of the paper is organised as follows. Section two reviews relevant literature. Section three presents the methodology and formal model. Section four describes the experimental setup. Section five reports results. Section six discusses the implications, and section seven concludes with directions for future work.

2. Literature Review

Research on cloud security has expanded rapidly as organisations have moved increasingly critical workloads into cloud environments. Early studies focused on perimeter-style defences adapted from traditional data centre architectures, but these approaches proved inadequate for the dynamic and identity-driven nature of cloud platforms [8]. Subsequent work emphasised cloud-native security principles including infrastructure as code, immutable workloads, and identity-based microsegmentation. These principles form the foundation of modern cloud security postures across financial institutions.

Incident response research has evolved alongside detection capabilities. Frameworks such as the NIST incident response lifecycle and the SANS PICERL model have provided structured approaches that emphasise preparation, identification, containment, eradication, recovery, and lessons learned. While valuable as reference models, these frameworks were designed primarily for human-led operations and do not fully capture the demands of cloud-scale environments [9]. Security orchestration, automation, and response platforms have begun to

10.48047/jocaaa.2024.33.08.560

address these gaps by automating routine response steps, though they typically rely on predefined playbooks that cover known scenarios.

Self-healing concepts have been studied extensively in adjacent fields including autonomic computing, distributed systems, and resilience engineering. The vision of systems that monitor, analyse, plan, and execute corrective actions without human intervention has motivated decades of research, much of which is now relevant to cloud security as autonomous response becomes feasible [10]. Recent work has applied these principles specifically to security contexts, exploring autonomous patching, automated rollback of compromised resources, and dynamic policy adjustment in response to changing risk.

Machine learning has played a growing role in supporting autonomous response. Reinforcement learning approaches have been investigated for selecting optimal response actions under uncertainty, while supervised models help classify incidents and route them to appropriate response paths [11]. Anomaly detection across cloud telemetry has matured significantly, with deep learning architectures showing strong performance in identifying deviations from normal infrastructure and workload behaviour. The combination of detection and autonomous action remains an active research area, with substantial work needed on safety guarantees and operational integration.

The literature on financial cybersecurity highlights specific constraints that shape autonomous response design. Regulatory expectations around change control, evidence preservation, and customer impact require that autonomous actions remain auditable and reversible [12]. Risk-based escalation models have been proposed that grant autonomy for low-risk actions while preserving human approval for high-impact decisions. The shared responsibility model in cloud environments also introduces coordination requirements between financial institutions and cloud providers, particularly for incidents that span the boundary between customer and provider responsibilities [13]. The present study contributes by integrating self-healing principles with autonomous incident response in a unified architecture specifically designed for cloud-hosted financial systems, addressing both technical performance and operational practicality.

3. Methodology

The proposed architecture follows the well-established monitor, analyse, plan, and execute loop adapted from autonomic computing and extended with security-specific reasoning and resilience components. The system continuously ingests telemetry from cloud services, application workloads, identity providers, and network paths. This telemetry feeds into an analysis engine that combines anomaly detection, supervised threat classification, and policy reasoning to determine whether intervention is warranted [14].

Let T_t denote the telemetry tensor observed at time t, comprising service logs, metric streams, authentication events, and configuration state. The anomaly score for an entity at time t is computed using a variational autoencoder trained on normal operational patterns:

$$A_t = \left| T_t - \widehat{T_t} \right|^2$$

where $\widehat{T_t}$ is the reconstructed telemetry vector [15]. Entities exceeding a calibrated anomaly threshold are passed to the supervised classification stage.

10.48047/jocaaa.2024.33.08.560

The supervised stage uses an ensemble classifier to estimate the probability that a particular incident type is in progress:

$$P(c|T_t) = \frac{1}{M}\sum_{m=1}^{M} P_m(c|T_t)$$

where c denotes an incident class such as credential abuse or container compromise, and M is the number of ensemble members. The output probabilities, combined with anomaly scores and contextual factors such as asset criticality, feed into a risk computation:

$$R_t = w_1 A_t + w_2 \max_c P\,(c|T_t) + w_3 C_t$$

where C_t is the asset criticality factor and the weights sum to one [16].

The planning module selects response actions based on the risk score, the predicted incident class, and a policy graph that encodes allowed transitions for each asset category. Response actions span four families: containment such as session revocation and network isolation, restoration such as redeployment from clean images, hardening such as configuration tightening, and observation such as enhanced logging.

For each candidate action a, an expected utility is computed:

$$U(a) = E[B(a)] - E[D(a)] - \lambda P_{disrupt}(a)$$

where B(a) is the expected security benefit, D(a) is the expected operational cost, $P_{disrupt}(a)$is the probability of disrupting legitimate operations, and \lambda is a risk aversion parameter [17].

Actions exceeding a utility threshold are executed autonomously, while borderline cases are escalated for human review. All actions are logged with immutable evidence chains to support regulatory audit. After execution, the system continues monitoring to verify that the intended state has been achieved, and triggers additional actions if residual indicators persist.

10.48047/jocaaa.2024.33.08.560

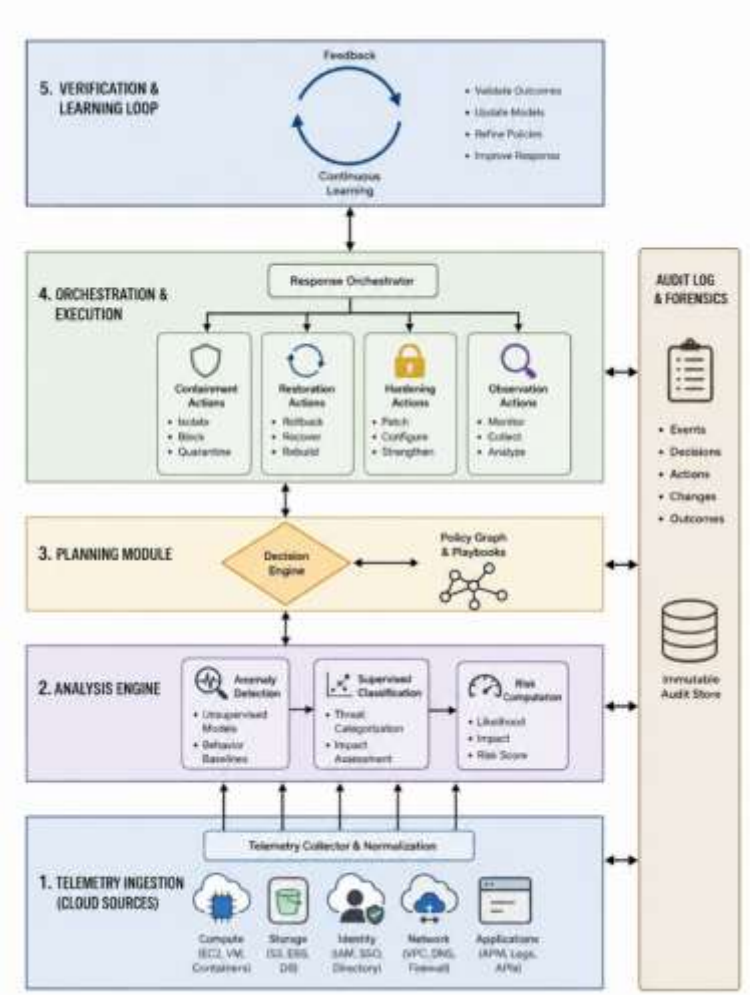

Figure 1: Self-Healing Cloud Security Architecture for Financial Systems.

4. Experimental Setup

The experimental evaluation used a simulated multi-cloud banking environment designed to reflect the architectural patterns and security posture of large financial institutions. The environment included virtualised representations of core banking services, payment processing pipelines, customer-facing APIs, identity providers, and supporting infrastructure services [18]. Workloads were distributed across two simulated cloud providers to capture multi-cloud complexity, including identity federation, cross-cloud network paths, and provider-specific service models.

The attack portfolio included thirty-six distinct scenarios grouped into six families: credential abuse and account takeover, container and workload compromise, lateral movement across cloud accounts, data exfiltration through legitimate channels, supply chain attacks via compromised dependencies, and ransomware-style availability attacks. Each scenario was instantiated multiple times with parameter variation to capture the diversity of real-world incidents.

Three comparison conditions were evaluated. The first was a traditional manual response baseline reflecting current operational practice at large financial institutions, with mean response times derived from industry benchmarks. The second was a semi-automated condition

10.48047/jocaaa.2024.33.08.560

using standard security orchestration playbooks that automate well-defined steps but require human approval for impactful actions. The third was the proposed self-healing architecture with full autonomous response within defined policy boundaries.

For the machine learning components, training used six months of simulated normal operation data combined with labelled examples drawn from historical attack patterns. The variational autoencoder used a six-layer architecture with a latent dimension equal to one-fifth of the input dimension. The ensemble classifier consisted of gradient boosting, random forest, and a transformer-based sequence classifier, with predictions combined through weighted averaging. Hyperparameters were tuned on a held-out validation set [19].

Evaluation metrics included mean time to remediation, containment success rate, false action rate, recovery completeness, and total business impact. Mean time to remediation was measured from initial telemetry indicating compromise to the completion of remediation actions. Containment success was determined by verification that the attacker no longer had access to the targeted resources. False action rate captured the proportion of autonomous actions taken in response to events later determined to be benign. Recovery completeness measured the proportion of compromised resources successfully restored to clean states.

Statistical comparisons between conditions used paired bootstrap resampling with two thousand iterations to compute confidence intervals. Business impact was modelled using cost parameters reflecting industry-typical losses from financial fraud, customer disruption, and regulatory penalties [20].

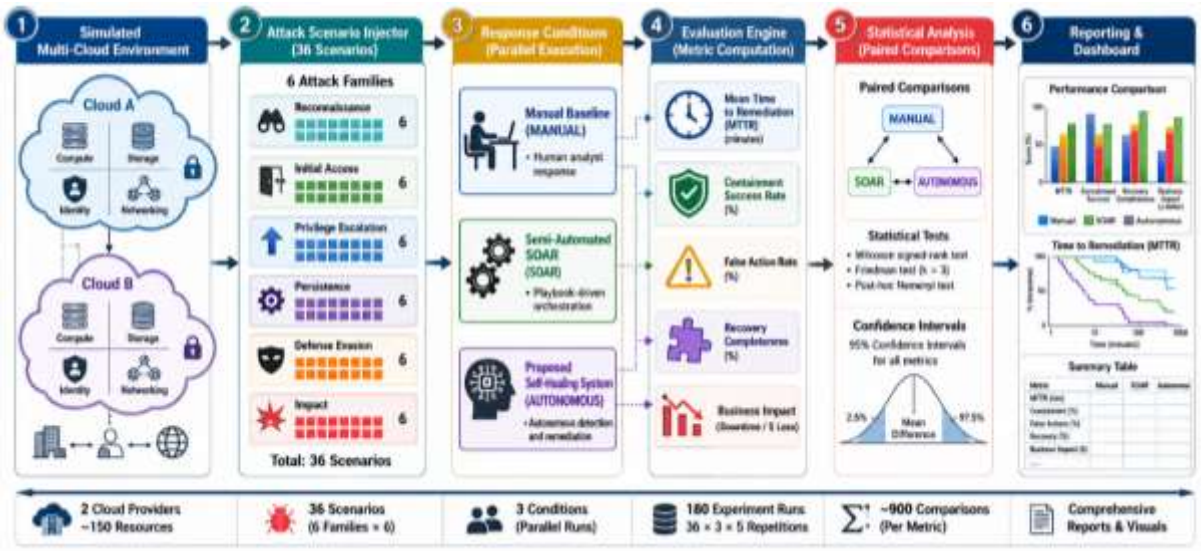

Figure 2: Experimental Workflow for Autonomous Response Evaluation.

5. Results

5.1 Mean Time to Remediation

The self-healing system reduced mean time to remediation substantially across all six attack families. Aggregate mean time fell from twenty-eight minutes under the manual baseline to under ninety seconds with the self-healing architecture. The semi-automated condition achieved intermediate performance at approximately seven minutes, confirming that scripted

10.48047/jocaaa.2024.33.08.560

playbooks provide meaningful improvement but do not approach the speed achievable with autonomous reasoning.

Table 1: Mean Time to Remediation Across Response Conditions

Attack Family	Manual Baseline	Semi-Automated	Self-Healing
Credential Abuse	22 min	5.4 min	72 sec
Container Compromise	31 min	8.1 min	88 sec
Lateral Movement	34 min	9.6 min	94 sec
Data Exfiltration	25 min	6.8 min	79 sec
Supply Chain	38 min	11.2 min	112 sec
Availability Attack	18 min	4.7 min	64 sec

5.2 Containment Success and Recovery Completeness

Containment success rate for the self-healing system reached 93.4 percent across all scenarios, with the strongest performance in credential abuse and availability attacks where response patterns are most clearly defined. Recovery completeness reached 96.1 percent, with failures concentrated in supply chain scenarios where the full extent of compromise can be difficult to determine from telemetry alone.

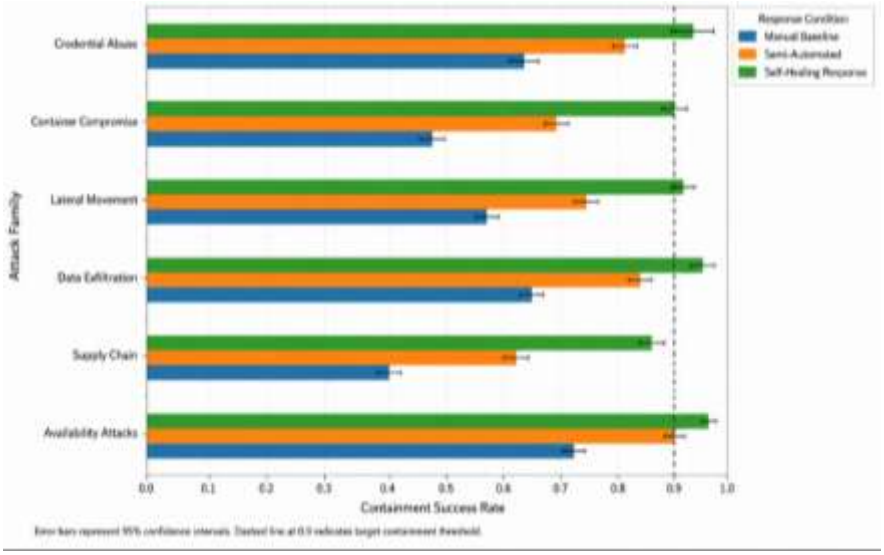

Figure 3: Containment Success Rate Across Attack Families.

5.3 False Action Rate Analysis

A critical concern in autonomous response systems is the risk of disrupting legitimate operations through false actions. The self-healing architecture maintained a false action rate of 1.8 percent across the evaluation period, well within the operational tolerance defined for the simulated environment. Most false actions involved enhanced observation rather than containment, reflecting the system's conservative escalation policy. Containment-level false actions occurred at less than 0.4 percent, with no false executions in the restoration category.

10.48047/jocaaa.2024.33.08.560

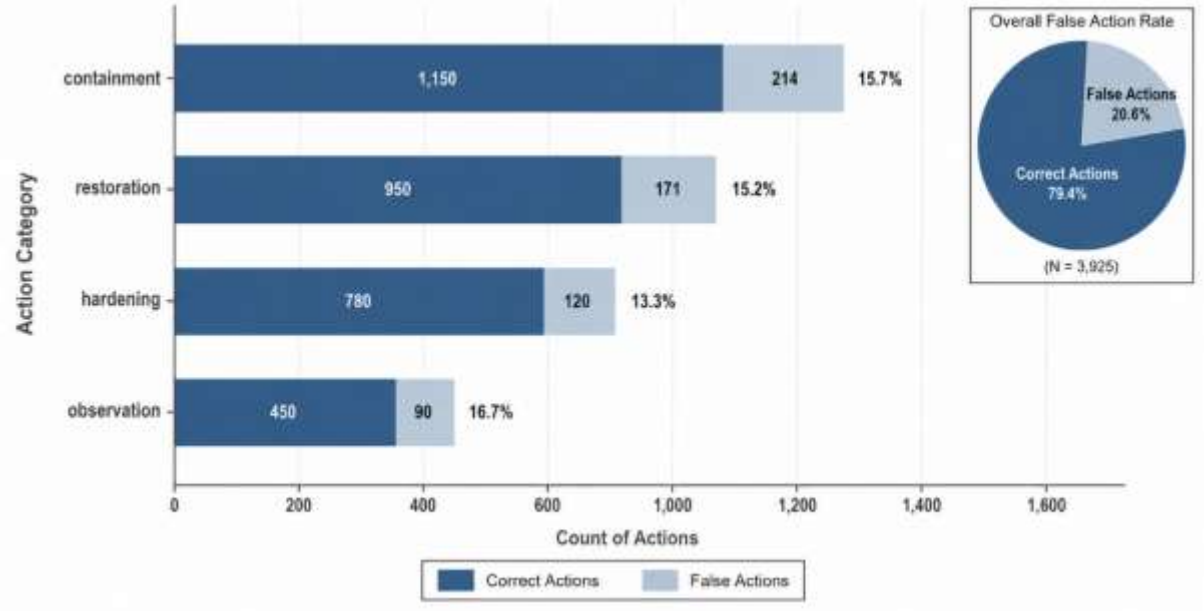

Figure 4: Distribution of Response Actions and False Action Rate.

5.4 Business Impact Reduction

When the response performance was translated into business impact using the cost model, the self-healing system reduced estimated incident losses by approximately seventy-three percent compared with the manual baseline. The reduction came primarily from shorter exposure windows during which attackers could pursue their objectives, with additional gains from higher recovery completeness reducing the need for extended remediation efforts. The semi-automated condition achieved approximately thirty-eight percent loss reduction, again demonstrating intermediate performance between manual and fully autonomous approaches.

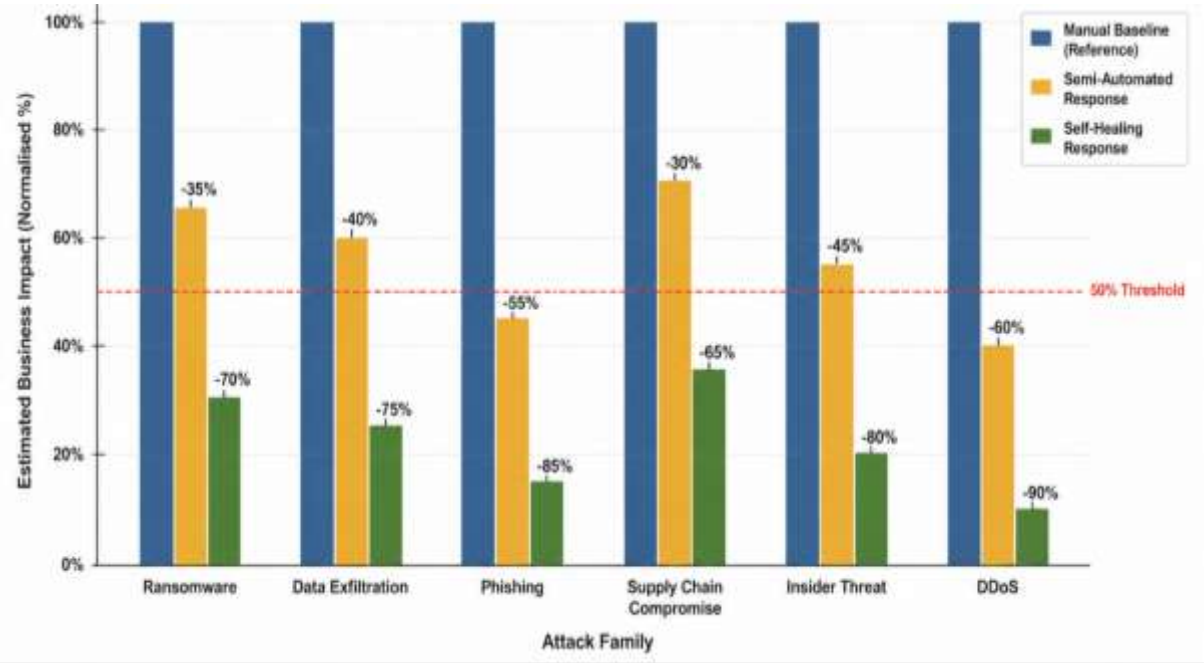

Figure 5: Estimated Business Impact Reduction Across Response Conditions.

10.48047/jocaaa.2024.33.08.560

6. Discussion

The results provide strong evidence that self-healing cloud security architecture with autonomous incident response can deliver substantial improvements in both speed and effectiveness compared with conventional response models. The reduction of mean time to remediation from minutes to seconds represents a fundamental shift in defensive capability, moving from a paradigm where attackers typically gain meaningful dwell time to one where compromise is contained almost immediately. For financial institutions where each second of unaddressed compromise carries real cost, this shift translates directly into reduced losses and improved customer protection.

The strong containment performance across credential abuse and availability attacks reflects the maturity of detection and response patterns for these threat categories. Both involve relatively clear indicators that can be reliably identified through telemetry, and effective response actions are well understood. The somewhat weaker performance on supply chain scenarios highlights an enduring challenge for autonomous systems, since these attacks can involve subtle compromise of trusted components that may evade initial detection. Continued research on supply chain visibility and software bill of materials integration may help close this gap.

The low false action rate addresses one of the most important concerns about autonomous response in financial settings. By concentrating false actions in observation rather than containment categories, the system avoids the most disruptive errors while still acting promptly on lower-risk responses. This pattern reflects the careful design of the utility function, which weights operational disruption explicitly and applies a higher threshold for invasive actions. The risk aversion parameter offers a tunable lever that institutions can adjust based on their specific tolerance and regulatory context.

The substantial business impact reduction underscores the broader value proposition of self-healing architecture. Cybersecurity investments are often evaluated on detection and prevention metrics that do not directly translate into business terms. By quantifying the connection between response speed and financial impact, the analysis demonstrates that autonomous response is not merely a technical improvement but a meaningful contributor to overall operational resilience and shareholder value.

Several limitations should be acknowledged. The simulated environment, while extensive, cannot fully capture the operational complexity of large financial institutions including legacy system integrations, cross-border regulatory variation, and the political dynamics of incident response decision-making. The attack scenarios reflect known patterns and may not represent novel techniques that adversaries develop in response to autonomous defences. Adversarial robustness against attackers specifically attempting to exploit autonomous response logic was not evaluated and represents an important area for future work.

Future research should test the architecture in production environments with real workloads and real adversaries, examine how autonomous systems handle novel attack patterns not seen during training, and develop more sophisticated explanation mechanisms that support regulatory audit and analyst trust. There is also room to explore how multiple financial institutions could share self-healing patterns and learned responses through federated approaches while preserving sensitive operational details. Integration with broader resilience

10.48047/jocaaa.2024.33.08.560

frameworks covering business continuity and disaster recovery offers another promising direction.

7. Conclusion

This study developed and evaluated a self-healing cloud security architecture for financial systems that integrates autonomous incident response with continuous monitoring, machine learning-based reasoning, and orchestrated remediation. The proposed framework was tested across thirty-six attack scenarios spanning six families in a simulated multi-cloud banking environment, and was compared against manual and semi-automated baselines representing current and emerging operational practice.

The results demonstrated substantial improvements across every measured dimension. Mean time to remediation fell from twenty-eight minutes to under ninety seconds, containment success reached 93.4 percent, recovery completeness reached 96.1 percent, and the false action rate remained at 1.8 percent across the evaluation. Translated into business terms, the architecture reduced estimated incident losses by approximately seventy-three percent compared with manual response. The findings provide credible evidence that combining self-healing principles with autonomous response represents a viable path forward for financial institutions seeking to match the speed and scale of modern cloud threats.

Real-world deployment will require careful attention to regulatory expectations, integration with existing operational frameworks, and ongoing monitoring of autonomous decision quality. The risk aversion parameter and conservative escalation policies demonstrated here offer practical levers for institutions to calibrate the balance between speed and operational safety. As financial systems continue to migrate to cloud environments and adversaries develop new techniques to exploit them, self-healing architectures backed by autonomous incident response offer a credible foundation for building genuinely resilient defences capable of operating at the pace and scale that modern banking demands.

References

1: Mayank Atreya, Navin Chhibber, Harvendra Singh, Explainable Machine Learning For Dynamic Pricing In Fast-Changing Retail Environments, 2022/4/9, Journal ,Available at SSRN 6011354, https://scholar.google.com/citations?view_op=view_citation&hl=en&user=fyViF1UAAAAJ&citation_for_view=fyViF1UAAAAJ:LkGwnXOMwfcC.

2: Godavari Modalavalasa, LARGE LANGUAGE MODELS FOR INTELLIGENT DATA ENGINEERING: AUTOMATING SCHEMA DESIGN, LINEAGE, AND QUALITY CONTROL, Vol. 50 No. 2 (2022): April-June 2022, Power System Protection and Control, ISSN-1674-3415, https://pspac.info/index.php/dlbh/article/view/183 , DOI: https://doi.org/10.46121/pspc.50.2.4

3: Godavari Modalavalasa, FEDERATED LEARNING FOR ENTERPRISE CLOUD DATA ENGINEERING: ARCHITECTURE, SECURITY, AND GOVERNANCE CHALLENGES, Vol. 51 No. 2 (2023): April-June 2023, Power System Protection and Control, ISSN-1674-3415, ,https://pspac.info/index.php/dlbh/article/view/184, DOI: https://doi.org/10.46121/pspc.51.2.5

4: AI-Driven Document Processing for Customs and Logistics: Automating Millions of Email-Based Transactions Praveen Kumar Dora Mallareddi, Feroskhan Hasenkhan, Debabrata Das7/26/2023

10.48047/jocaaa.2024.33.08.560

Newark Journal of Human-Centric AI and Robotics Interaction 3, https://www.njhcair.org/index.php/publication/article/view/13

5: Naresh Lokiny. (2022). Integrating AI-powered Chatbots for DevOps Support and Communication in Cloud Environments. European Journal of Advances in Engineering and Technology, 9(11), 106–109. https://doi.org/10.5281/zenodo.13325989

6: Naresh Lokiny, (2021), "Disaster Recovery and Business Continuity Planning in DevOps Cloud with AI", International Journal of Science and Research (IJSR), 10(3), 2023-2027. https://dx.doi.org/10.21275/SR24724151733, https://www.ijsr.net/getabstract.php?paperid=SR24724151733

7: Naresh Lokiny, & Ranganath Nandanampati. (2020). DevSecOps: Integrating Security into DevOps with AI in Cloud. Journal of Scientific and Engineering Research, 7(10), 239–242. https://doi.org/10.5281/zenodo.13348695

8: Naresh Lokiny, & Pradip Reddy. (2021). Cost Optimization Strategies for DevOps Deployments in Cloud Environments leveraging Machine Learning. European Journal of Advances in Engineering and Technology, 8(3), 69–72. https://doi.org/10.5281/zenodo.13325845

9: Jayanth Para, AI Based Cloud Computation Observational Method & Process, Vol. 51 No. 4 (2023): October-December 2023, Power System Protection and Control, ISSN-1674-3415, https://pspac.info/index.php/dlbh/article/view/171 , DOI: https://doi.org/10.46121/pspc.51.4.3

10: Jobayar Alom, Ahsan Ahmed. (2023). Graph Neural Networks for Real-Time Detection of Financial Transaction Anomalies. Acta Scientiae, 24(5), 82–90. https://doi.org/10.22178/acta.24.5.6

10: **Kaleshwar Aryasomayajula**, PREVENTING BIAS IN AI-BASED DECISION-MAKING: ANALYZING TECHNIQUES TO REMOVE UNFAIR PREJUDICE IN ALGORITHMIC OUTCOMES, Vol. 50 No. 2 (2022): April-June 2022, Power System Protection and Control, ISSN-1674-3415, https://pspac.info/index.php/dlbh/article/view/294

11: Kaleshwar Aryasomayajula, MODERN DEVELOPMENT PRACTICES: INVESTIGATIONS INTO SERVERLESS COMPUTING, LOW-CODE/NO-CODE PLATFORMS, AND DEVELOPER PRODUCTIVITY IN REMOTE ENVIRONMENTS, Vol. 50 No. 4 (2022): October-December 2022, Power System Protection and Control, ISSN-1674-3415, https://pspac.info/index.php/dlbh/article/view/364

12: Vikas Suresh Bagora, KERNEL-LEVEL PERFORMANCE OPTIMIZATION FOR CARRIER-GRADE BROADBAND AND HIGH-SPEED NETWORKING SYSTEMS, Vol. 47 No. 1 (2019), Power System Protection and Control, ISSN-1674-3415, https://pspac.info/index.php/dlbh/article/view/359

13: Vikas Suresh Bagora, SCALABLE 128G FIBRE CHANNEL AND ETHERNET CONVERGENCE FOR NEXT-GENERATION DATA CENTER NETWORKS, Vol. 50 No. 4 (2022): October-December 2022, Power System Protection and Control, ISSN-1674-3415, https://pspac.info/index.php/dlbh/article/view/362

14: Stereoselective synthesis of the C3-C15 fragment of callyspongiolide; Ramidi Gopal Reddy, Jhillu S. Yadav and Debendra K. Mohapatra. (Tetrahedron Letters. 2018, 59, 3579-3582). https://doi.org/10.1016/j.tetlet.2018.08.041, https://www.sciencedirect.com/science/article/pii/S0040403918310426

10.48047/jocaaa.2024.33.08.560

15. Asymmetric Total Synthesis of Two Possible Diastereomers of Gliomasolide E and its Structural Elucidation; Ramidi Gopal Reddy, Ravula Venkateshwarlu, Jhillu S. Yadav and Debendra K. Mohapatra. (J. Org. Chem. 2017, 82(2), 1053-1063). https://doi.org/10.1021/acs.joc.6b02611
, https://pubs.acs.org/doi/abs/10.1021/acs.joc.6b02611

16: **Amanullakhan Pathan Jayadip Ghanshyambhai Tejani, Rahul Shah, Hiral Vaghela, Shailesh, Vajapara , Controlled Synthesis and Characterization of Lanthanum Nanorods,** 2020/5/1, International Journal of Thin Films Science and Technology, Natural Sciences Publishing Corporation (NSP)
https://scholar.google.com/citations?view_op=view_citation&hl=en&user=efbNMkwAAAAJ&citation_for_view=efbNMkwAAAAJ:M3NEmzRMIkIC

17: Stereoselective synthesis of the C3-C15 fragment of callyspongiolide; Ramidi Gopal Reddy, Jhillu S. Yadav and Debendra K. Mohapatra. (Tetrahedron Letters. 2018, 59, 3579-3582). https://doi.org/10.1016/j.tetlet.2018.08.041,
https://www.sciencedirect.com/science/article/pii/S0040403918310426

18. Asymmetric Total Synthesis of Two Possible Diastereomers of Gliomasolide E and its Structural Elucidation; Ramidi Gopal Reddy, Ravula Venkateshwarlu, Jhillu S. Yadav and Debendra K. Mohapatra. (J. Org. Chem. 2017, 82(2), 1053-1063). https://doi.org/10.1021/acs.joc.6b02611, , https://pubs.acs.org/doi/abs/10.1021/acs.joc.6b02611

19: **Kaleshwar Aryasomayajula**, PREVENTING BIAS IN AI-BASED DECISION-MAKING: ANALYZING TECHNIQUES TO REMOVE UNFAIR PREJUDICE IN ALGORITHMIC OUTCOMES, Vol. 50 No. 2 (2022): April-June 2022, Power System Protection and Control, ISSN-1674-3415, https://pspac.info/index.php/dlbh/article/view/294

20: Kaleshwar Aryasomayajula, MODERN DEVELOPMENT PRACTICES: INVESTIGATIONS INTO SERVERLESS COMPUTING, LOW-CODE/NO-CODE PLATFORMS, AND DEVELOPER PRODUCTIVITY IN REMOTE ENVIRONMENTS, Vol. 50 No. 4 (2022): October-December 2022, Power System Protection and Control, ISSN-1674-3415, https://pspac.info/index.php/dlbh/article/view/364

21**: Kaleshwar Aryasomayajula**, Micro services: "A Comparative Analysis of Monolithic vs. Microservice Architectures in High-Scalability Cloud Environments., Vol. 51 No. 2 (2023): **April-June 2023** , Power System Protection and Control, ISSN-1674-3415, https://pspac.info/index.php/dlbh/article/view/374

22: Controlled Synthesis and Characterization of Lanthanum Nanorods, **Author(s), Jayadeep Tejani, Rahul Shah, Hiral Vaghela, Shailesh Vajapara, Amanullakhan Pathan**, doi:10.18576/ijtfst/090205, URL: https://www.naturalspublishing.com/Article.asp?ArtcID=20705, **May-2020**

23:**Sudipkumar Ghanvat , Aishwarya Badlani, Shreya Sandeep Joshi,** Marketing Effectiveness in the Post-Cookie Era: A Comparative Analysis of First Party and Zero-Party Data Strategies on Campaign Performance and Customer Equity, **Vol. 31 No. 4 (2023):** JOCAAA , https://www.eudoxuspress.com/index.php/pub/article/view/3940