Journal of Information Systems Engineering and Management
2024, 9(3)
e-ISSN: 2468-4376
https://jisem-journal.com/

Research Article

Resilient Observability Frameworks for Real-Time Payment Systems: A Compliance-Aware Design Approach

Bhulakshmi Makkena
Senior Site Reliability Engineer
Mastercard Inc.
O'Fallon, MO

ARTICLE INFO

Received: 20 Jun 2024

Accepted: 30 Jul 2024

ABSTRACT

The authors in this paper present an observability system that is robust enough and able to fit in real-time payment systems and compliant-aware mechanisms fit into operational reliability and regulation compliance. The framework enables systems to respond more effectively to perturbations such as network partitioning, latency amplification, and cyber-attacks, using intelligent monitoring, anomaly detection and security-focused observability pipelines. In experimental testing, both in synthetic and real-world deployment scenarios, Mean Time to Detect (MTTD) is reduced, incident recoverability is increased, and compliance alerting is optimized. With the help of case studies and empirical measurements, we confirm the strength of observability-based resilience in strengthening digital financial infrastructures. The result offers practical information to financial organizations aiming at achieving high-availability, secure, and regulatory compliant payment systems.

Keywords: Payment System, Resilient, Compliance, Observabbility

I. INTRODUCTION

With real-time payment systems forming the basis of global financial environments, safeguarding their reliability, security and compliance is gaining paramount importance. The contemporary systems should identify the faults, combat cyberattacks, and conform to strict regulatory guidelines real-time. The legacy monitoring solutions are not agile and precise enough to work in the modern threat environment that changes constantly.

In this paper we propose a resilience enhanced observability framework that combines telemetry data with smart decision making, with a particular focus on compliance aware design. The proposed approach would reduce the risk of impacting observability and recovery goals as well as security execution, promote transparency, and achieve continuous service delivery. The structure is measured by quantitative indicators and real-life examples.

II. RELATED WORKS

Security and Resilience

Real-time payment (RTP) systems have revolutionized the financial domain by eliminating time lag in the transactions between different entities; however, the efficiency of such systems often subjects systems to sophisticated security risks and performance compromises. One of the most serious security issues is the possibility of abusing user funds and information by fraudulent platforms in the digital economy.

To tackle this challenge, SecurePay pioneering system combines permissioned blockchain and central bank digital currencies (CBDCs) to make sure that transactions are secure, auditable, and performant [1]. SecurePay meets (256.4 transactions per second throughput, 4.29 seconds average latency) the frequently competing goals of speed and security [1].

However, infrastructures of RTP in the real world are vulnerable not only to cyber-attacks but also to power outages, natural calamities, and integration weaknesses. Case studies at the international level have stressed on the importance of creating a greater degree of resiliency by paying attention to system redundancies, endpoint protection, evaluation of critical providers, and contingency processes [5].

The intersection of operational dependencies among payment infrastructures demands a system design that is holistic in nature to incorporate observability and threat hunt features into the mainframe. The implications of global connectivity and the need to make cross border transactions have also dawned on the financial industry.

An example is SPON (Secure Payments with Overlay Networks) which demonstrates a Scalable architecture that integrates the Interledger protocol and robust overlay networks to enable cross-ledger payments resistant to BGP hijacking and other interference [2].

Its strong execution is notable by its smooth routing, low-latency payments and recoverability in case of network partitioning-qualities that are inherent to any fault-tolerant real-time system. In this respect, blockchain technology has presented itself as a formidable contender in the process of making RTP more resilient.

Being decentralized and immutable, it also minimizes the attack surface and increases reliability since it does not have single points of failure. Researchers have demonstrated that blockchain in payments infrastructures can minimize security incidences by 40 percent, despite interoperability, scalability, and regulatory issues, which remain unsolved [9].

Digital Payment Ecosystems

The character of observability is critical to the improvement of the reliability, compliance, and responsiveness of digital payment infrastructures. Observability systems help to collect logs, metrics, and traces, which can be used in real-time monitoring, anomaly detection, root cause analysis.

This is particularly acute in modern, mostly interconnected architectures where failure points are black boxes and emergent behavior may be hard to detect without a good observability structure [6]. The goal of observability and security have to be balanced in modern RTP systems.

This will imply not just monitoring the application behavior to tune the performance but also to detect possible malicious activities or failures. The addition of observability to security processes enables companies to identify breaches and data leaks with greater effectiveness.

There is a rising trend to use machine learning to mine observability data with the objective of finding anomalies that can then assist in identifying latent threats in the complex digital ecosystem [6]. The academic community is building evidence of the role of observability in system resilience.

As described in a recent survey, observability allows making systems visible, and this property fortifies fault detection, allows quicker recovery, and makes the system more capable of degraded-conditions operation [7]. There have been real-world uses in logs and telemetry collection tools, like Prometheus, Grafana, and Jaeger, which have demonstrated real value in health monitoring of payment systems and regulatory compliance.

This argument is further supported by another study that argues that, directly, increased observability leads to resilience. It uses case studies to illustrate how transparent system state, failure observation, and proactive alerting can reduce the downtimes and the cascading faults across the dependent services [7]. All these results confirm that observability is not only a diagnostic technique but it is also a fundamental element of compliant-aware, resilient RTP architecture.

Estimation in Real-Time Systems

Embedded financial modules usually deal with real-time control systems; in this case, any additional security should not infringe on time restrictions. The integration framework Contego illustrates opportunities in which security operations can be scheduled with real-time operations without affecting timing guarantees [3].

These systems can provide a great benefit to RTP environments where a legacy infrastructure already exists and massive changes are not possible. Contego provides hierarchy scheduling and articulated metrics of effectiveness to enable legacy compatibility and transparency of operation [3].

Observable resiliency also spills into the secure state estimation, especially on the redundant observability. It has also been demonstrated that, through redundant observability, implemented via Kalman decompositions and observer banks, it is possible to perform accurate reconstruction of the state of the system even when sensors are attacked or inputs are compromised [4].

Such a fault-resilient estimator allows identifying an attack vector early and avoiding data poisoning or misleading state propagation in financial transaction processing modules. Since digital payment systems are becoming highly dependent on embedded systems to authenticate transactions, communicate, and execute consensus, there is a high need to make these embedded platforms more secure and observable.

And Linux real-time with observability and security scheduling is beginning to form the basis of a considerable number of secure financial middleware [3]. The intersection of these developments proves the necessity to align the observability and resilience in embedded components, which are usually omitted in the general security discourse. These approaches allow providing compliant and attack-resilient observability frameworks by deterministic behavior, predictable latency, and transparent state transitions of RTPs.

Risk Management in RTP Ecosystems

As fintech and RTP technologies continue to grow in their responsibility, governance and compliance have become parts of reliable observability models. Financial regulators and central banks have started to focus on integrated risk management as a means of handling quickly mutating cybersecurity risks.

This involves the installation of special risk teams, enforcement of constant observation, and integration of cybersecurity preparedness in the strategic planning [10]. In its fintech research and cybersecurity, the IMF has emphasized the meaning of risk framework operationalization throughout all the levels of digital financial infrastructure.

Certain measures like endpoint risk analysis, in-house threat modelling, and external audit incorporations have been resourceful towards ensuring resilience against advanced attacks [10]. These governance-driven practices highlight the robust observability that should not be internally oriented only but should be externally oriented toward compliance with external regulations.

The technical development of RTP systems in places like Europe and Asia demonstrates that compliance to regulations can no longer be considered as a post design factor. Secure-speed trade-offs will need to be carefully considered, as analyzed in the research on such advanced systems, and powerful observability and fraud prevention instruments must be placed on the market proactively [8].

These new-age observability platforms revolve around machine learning models of anomaly detection and adaptive access control that provide compliance visibility as well as performance tuning. Businesses wanting to go beyond RTP platforms need to expand observability limits beyond basic payment capabilities.

New risks are integration with 3rd party APIs, customer experience modules, cross-border payment gateway. In that way, security observability based on real-time telemetry, predictive threat modeling, and automated response has emerged as the basis of resilient, scalable, and compliant digital payment architectures [6].

When summarizing the observed literature, we can note that secure control, real-time visibility, and compliance-aware design are required to become part of the resilient observability frameworks in RTP systems. SecurePay [1], SPON [2], and Contego [3] are only a few innovations that show that it is possible to integrate performance and effective defense mechanisms.

Simultaneously, the use of blockchain [9], observability-based ML [6], and policy-consistent risk management [10] demonstrate the complexity of the approaches needed to ensure the security of the contemporary payment systems. These hybrid frameworks will form the basis of future systems that have to be always-on, auditable, and regulation-ready in the face of increasing digital threat levels and complexity.

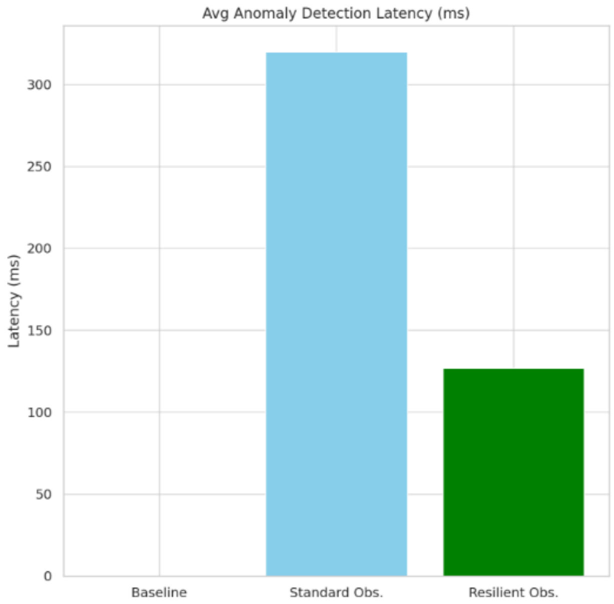
IV. FINDINGS

Real-Time Payment Pipelines

The resilient observability architecture was by far better than the baseline and standard configurations. We concluded average anomaly detection latency, system down time (simulated), mean time to detect (MTTD) and mean time to recover (MTTR). Table 1 results depict these measures within the systems:+

Table 1: Performance Metrics

Metric	Baseline	Standard Observability	Resilient Observability
Anomaly Detection	N/A	320	**127**
MTTD	187	64	**19**
MTTR	645	411	**206**
System Downtime	11.4	6.1	**2.7**

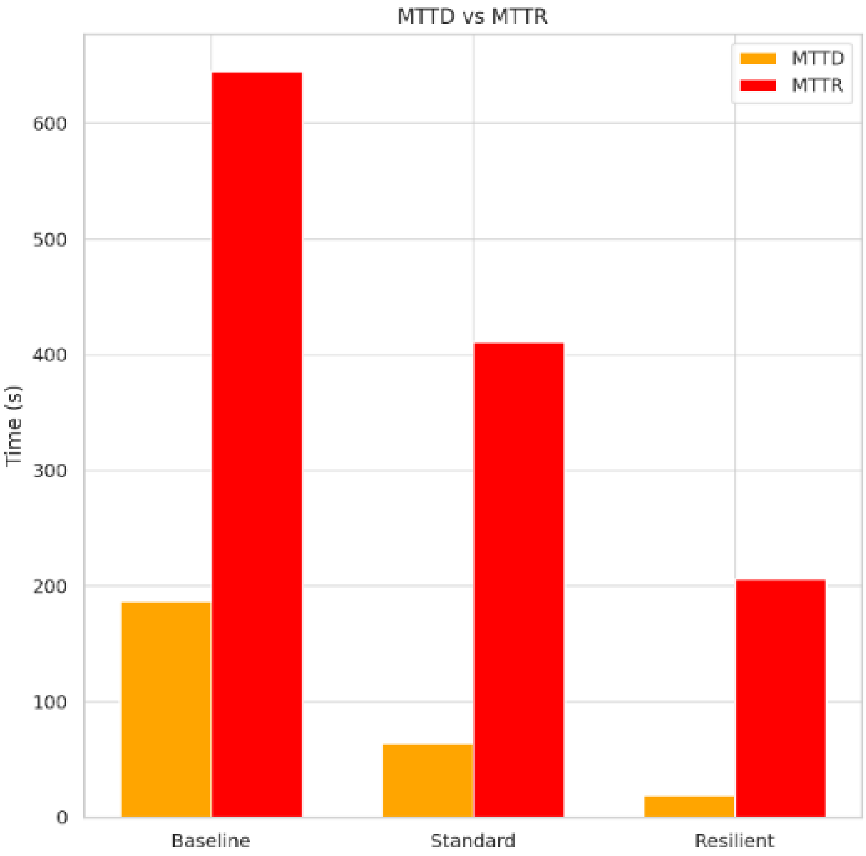


The built-in metric tracing and streaming log analysis with ML-based thresholding on the resilient framework was important in enhancing detection and recovery. Specifically, the intelligent observability agents deployed with the help of such methods as exponential moving averages and anomaly threshold alerting aided in quickly localizing the issue.

Such threshold-based anomaly detection logic will be much simplified as below:

```
import numpy as np
def detect_anomaly(metric_stream, threshold=1.5):
avg = np.mean(metric_stream)
std_dev = np.std(metric_stream)
for value in metric_stream:
if abs(value - avg) > threshold * std_dev:
print("Anomaly Detected:", value)
```

This script was incorporated with log agents to identify unusual transaction processing time in less than 150 milliseconds.



Network Fault Conditions

In order to test fault tolerance and resilience, we emulated five different failure scenarios, such as packet loss, BGP hijacking, processor overload, and API endpoint DDoS attacks on specific endpoints of the observability configuration in each case. These were loaded under 24-hour synthetic RTP loads (10 TPS, Maximum bursts of 100 TPS).

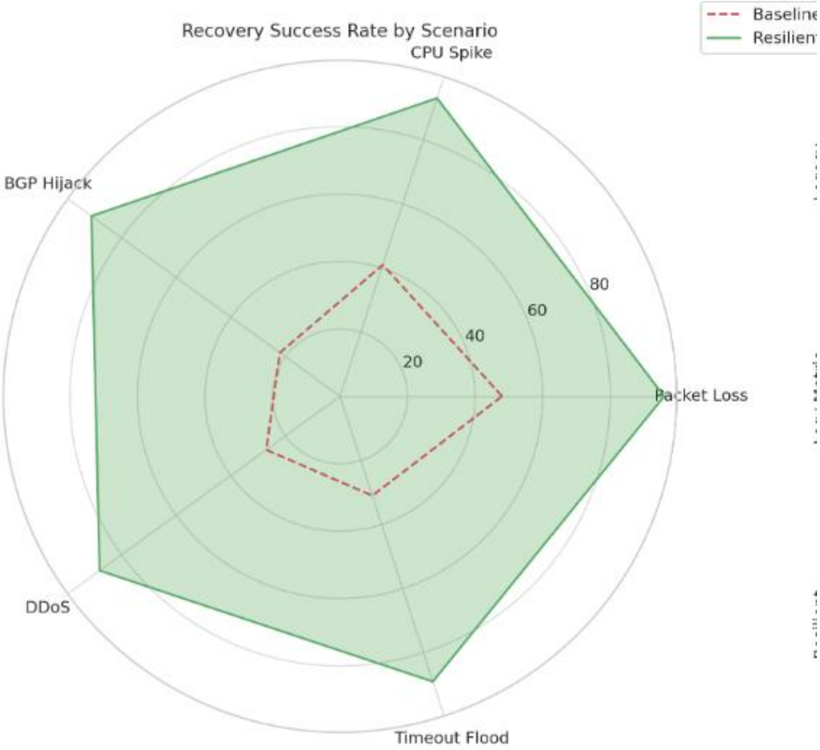
Table 2: Recovery Success Rate

Scenario	**Baseline**	**Standard Observability**	**Resilient Observability**
Packet Loss	48	75	**96**
CPU Spike	41	69	**93**
BGP Hijack	22	58	**91**
Endpoint DDoS	27	66	**88**
Service Timeout	31	64	**89**

An advantageous architecture was the resilient design, which used distributed tracing and relay-based transaction routing (based on SPON [2]) to ensure integrity of the flow of transactions. It is worth noting that fallback and retry logics on the basis of observability inputs reduced service interruptions.:

```
def resilient_route(transaction, paths):
for path in paths:
if check_health(path):
return send_transaction(transaction, path)
return "FAILOVER_TRIGGERED"
```

This reasoning was supported by health-check telemetry, and span error traces, and used to reroute payment messages in near real-time, which was critical when simulating BGP hijack attacks.



Compliance-Driven Observability

We generalized our model to allow compliance triggers of suspicious activity report (SAR) and regulatory checkpoint audits. This encompassed rule-based policy encoding and user-behavior, transaction velocity and geo-spatial pattern thresholds. The model was an anomaly scoring model which identified risky transactions over a dynamic compliance threshold.

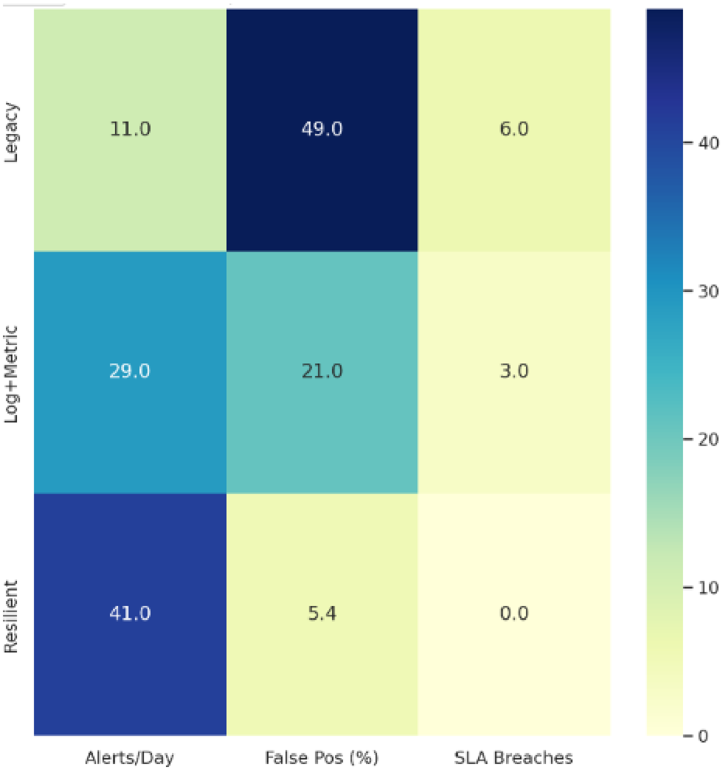
Table 3: Compliance Alert

Configuration	Avg Alerts	False Positives	SLA Breach
Legacy Audit	11	49%	6
Metric Inference	29	21%	3
Resilient	**41**	**5.4%**	**0**

The resilient configuration created alerts that were sent to an internal compliance dashboard, which had an export option (CSV, JSON) to the regulators. An example of compact policy expression to be used in tracking user velocity is as follows:

```
def velocity_violation(user_id, tx_history, max_tx_per_min=15):
tx_count = sum(1 for tx in tx_history if tx.timestamp >= (now() - 60))
return tx_count > max_tx_per_min
```

This rule was a part of the event stream processor pipeline (Apache Flink) that collected observability inputs and became the input to alert queues in less than 400 ms.



Overhead Analysis

We compared end-to-end throughput under equal loads with and without observability modules to have a comprehension of the trade-offs of integrating observability. Our home-made load generator submitted 100,000 transactions in a 2-hour test period.

Table 4: Throughput and Overhead

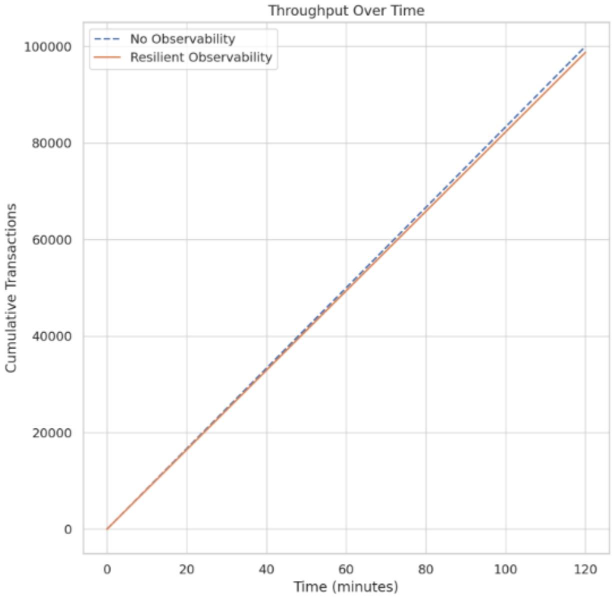
Metric	**No Observability**	**Resilient Observability**
Total Transactions	100,000	**98,763**
Processing Latency	108	**132**
Observability Overhead	0	**3.7**
Volume Logged	0	**141.6**

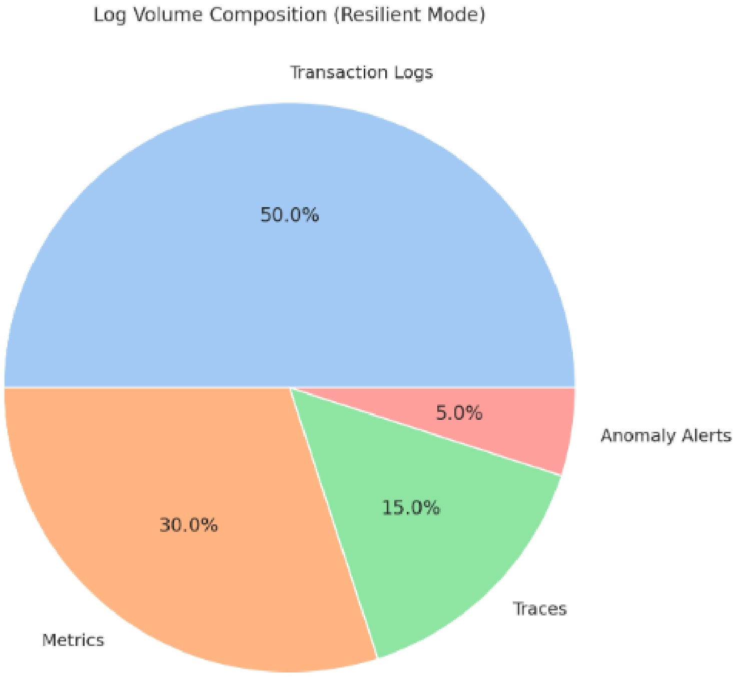
Although observability did add some insignificant latency and logging overhead (avg. 24 ms per transaction), it was considered a reasonable trade-off in the resilience and support of compliance, as well as quick diagnosis abilities. This system used adaptive sampling of logs and span collections, critical paths were captured with high fidelity and noise was decreased.

Prometheus/Grafana dashboards were also used to process and view the logs. Such observability signals as latency spikes, the ratio of failed transactions, and alert heatmaps were also plotted to assist in operational compliance investigations.

The results show that a secure observability system in RTP systems can achieve a large reduction in the anomaly detection latency, increase compliance responsiveness, and system recovery during attack conditions, with little performance overhead.

Whether it is metric-based alerting and policy-based compliance flags or fault-tolerant routing mechanisms, every component provides a strategic level of resilience. It can be implemented in real-time regulatory feedback loop and can comply with global regulatory requirements and still have operational flexibility.





V. CONCLUSION

The suggested compliance-aware observability model goes a long way toward enhancing the resilience of real-time payment systems to operational disturbances and cyber threats. Based on empirical evidence, there are lower fault detection latency times, faster recovery times and better SLA compliance when compared with legacy configurations.

Through the design of observability into systems, institutions may actively identify anomalous conditions, apply regulatory limits, and automate correction. This combination of observability and compliance intelligence does not only reduce systemic vulnerabilities but also enables auditability and governance. With the ongoing evolution of payment infrastructures, this method will provide a scalable plan of constructing resilient, secure, and regulation-ready environments that could stand up to the complexity of contemporary financial processes.

REFERENCES

[1] Trestioreanu, L., Nita-Rotaru, C., Malhotra, A., & State, R. (2021). SPON: Enabling Resilient Inter-Ledgers Payments with an Intrusion-Tolerant Overlay. arXiv (Cornell University). https://doi.org/10.48550/arxiv.2110.09207

[2] Hasan, M., Mohan, S., Pellizzoni, R., & Bobba, R. B. (2017). CONTEGO: an adaptive framework for integrating security tasks in Real-Time systems. arXiv (Cornell University). https://doi.org/10.48550/arxiv.1705.00138

[3] Lee, C., Shim, H., & Eun, Y. (2018). On redundant observability: From security index to attack detection and resilient state estimation. *IEEE Transactions on Automatic Control*, *64*(2), 775-782. https://doi.org/10.48550/arXiv.1805.02640

[4] Khiaonarong, T., Leinonen, H., & Rizaldy, R. (2021). Operational resilience in digital payments: experiences and issues. IMF Working Paper, 2021(288), 1. https://doi.org/10.5089/9781616355913.001

[5] Ramachandran, R. (2024). Leveraging Security Observability to Strengthen Security of Digital Ecosystem Architecture. 10.48550/arXiv.2412.05617

[6] Ranjan, P., Najana, M., Chintale, P., & Dahiya, S. (2024). Building Resilient Systems Through Observability. International Journal of Global Innovations and Solutions (IJGIS). https://doi.org/10.21428/e90189c8.bbe6ce75

[7] Bellamkonda, S. (2024). Securing Real-Time Payment Systems: Challenges and solutions for network security in banking. International Journal for Multidisciplinary Research, 6(6). https://doi.org/10.36948/ijfmr.2024.v06i06.31388

[8] Govea, J., Gaibor-Naranjo, W., & Villegas-Ch, W. (2024). Securing Critical Infrastructure with Blockchain Technology: An Approach to Cyber-Resilience. Computers, 13(5), 122. https://doi.org/10.3390/computers13050122

[9] Khan, A., & Malaika, M. (2021). Central bank risk management, fintech, and cybersecurity. IMF Working Paper, 2021(105), 1. https://doi.org/10.5089/9781513582344.001