International Journal of Computational and Experimental Science and ENgineering (IJCESEN)

Vol. 11-No.4 (2025) pp. 8966-8972
http://www.ijcesen.com

ISSN: 2149-9144

Research Article

Blockchain-Integrated Cyber Defense Mechanism for Cloud-Driven Financial Applications

Chinmay Mukeshbhai Gangani*

Independent Researcher, USA.
* **Corresponding Author Email:** chinma2y@gmail.com- **ORCID:** 0000-0002-5997-7850

Article Info:

DOI: 10.22399/ijcesen.4331
Received : 25 July 2025
Revised : 15 August 2025
Accepted : 30 August 2025

Keywords

Cloud,
Application,
Cybersecurity,
AI

Abstract:

On the financial sector, cloud computing has introduced a difference in terms of a scalable innovative and cost-effective service. Nevertheless, it has already caused an increase in cyber security risk - especially when sensitive financial information and compliance are involved. This paper empirically challenges key cybersecurity models of cloud-based financial applications both qualitatively and quantitatively.
Comparing the various risk assessment models, CSA STAR based models are seen to offer 88 percent conformance to the standards lacks any form of economic measurements, as compared to Youssef CSRMF, which offers 90 percent conformance to the standards, and reaches all-time maximum business alignment score of 5/5. The blockchain-based TAB model simulations indicated that overlay-transparency-enhancing models including the TAB Model increase the trustworthiness by factor 4 by reducing the detection latency by 210ms and the detection latency by 480ms.
Moreover, at the application level, layered API security solutions demonstrated significant improvement: a reduction of 120-40 security related incidents monthly in both basic and applied cases along the full-stack using AI/ML surveillance and the detection accuracy changed to 72 to 97. With the study on cost saving in place, installing structures which are based on SME is cheaper than installing hybrid enterprise-level structures which can cost between $200000 and 250000.
The findings indicate that financial managers should consider a hybrid approach to cybersecurity at the expense of such factors as risk evaluation, transparency, and API-layered defenses to maintain the balance between operational efficiency, compliance, and resilience in clouds.

1. Introduction

One of the drivers of such scalability, operational efficiency, and innovation in the rapidly and comprehensively digitally transformed financial services industry is the cloud. All applications and solutions that touch on the financial services provided through cloud are digitized payments, online banking, fraud prevention, risk analytics, financial management systems, and other applications.
The cloud model, despite its protection, drives up the threat of cybersecurity on financial organizations, such as the non-compliance, insider threats and data breaches. These risks become even greater when combined with financial information and it is necessary to design better security models that would consider technical and legislative elements.

Most of the risk-assessment methodologies do not integrate economic and commercial positions even though there is a change of paradigm to comply paradigm (NIST, ISO, and CSA STAR). Multi-layered API security models, situational awareness and blockchain-based transparency networks have all been proposed in order to overcome trust gaps. Nevertheless, readiness to embrace is varied between financial institutions with the SMEs requiring double-layer-thin and lightweight structures and the large banks moving towards rich hybrid models.
Under the Financial aspect, information assurance with the major cybersecurity architectures considers them under standpoints of effectiveness in risk calculation, information transparency, API defences and appropriate industry business shielding. Through the convergence of all such views, we intend to present harmonized approaches to the

future when it comes to ensuring cloud hosted financial applications and at the same time ensuring resilience, compliance and financial integrity.

2. Related Works

2.1 Risk Assessment

Bendicho (2021) emphasizes the essential role of good Cloud Risk Assessment (RA) designs in sustaining the complexity of the cloud hosted environment particularly in consideration of the security-contextual industries such as the financial industry. Those papers determine the conformance of different working methodologies to RA with a theoretical reference, which is also the determination of gaps to respond to certain questions, such as the economic quantification of risk and techno-economic analysis.

Youssef (2020) introduces the Cloud Security Risk Management Framework that outlines how cloud security shifts the technical capabilities of using security, and to ensure that the risks are in tune with the business purpose. Unlike conventional models, CSRMF is concerned with awareness in organizations, a cost-value-based approach to decision-making relative to strategic objectives and hence is more applicable to financial institutions where profits are directly proportional to risk to both equity and trust.

Another framework that Benabied et al. (2015) focus on is trust-based frameworks and suggests a two-level model consisting of Cloud Service Providers (CSP) and CSU, where the verification through the trust agent and proxy frameworks is considered. These studies indicate that theoretical risk models are real but then successful implementation on financial applications requires a combination of economic, business-related and trust aspects.

2.2 Data Availability

Financial cloud infrastructure security is no longer a technological issue, but it is a governance and transparency issue (problem). Xu and colleagues (2022) propose a new model of the TAB platform, employing Ethereum smart contracts to construct accountability and trust in third-party security services (such as cryptographic key and certificate management).

The given blockchain-basis solution to identity theft, data theft, and a lack of accountability tackles endemic issues. Cremer et al. (2022) conclude it with some notable gaps in the process of managing cyber risk, in particular, regarding the compulsory reporting and the data standards, which has been a common trend over the past two years. Moreover, those concerned, i.e. financiers and insurance formulas, should not claim to one hundred per cent that they cannot correctly price or estimate cyber risk until an open source of information is received.

It maintains that the very narrow scopes of the scope of technological defensive measures should be augmented with very big factor such as regulatory compliance and data access, largely in commercial sectors where legal responsibility and economic integrity are the most important factors.

Ksibi et al. (2022) provide insight into the emerging threats of Internet of Medical Things (IoMT) which, together with the financial services, involve sensitive and high-volume transactions of data. Their quantified risk methodology multiplies the requirement of domain specific systems that could evolve, and react to evolving technologies.

2.3 API Security

The topic of study of Das et al. (2022) is Application Programming Interface (API) security, the snake of financial cloud-hosted systems. Times and the API concern: As gateways to financial information, APIs have highlighted that there is significant risk that they expose (such as credential stuffing, SQL injection and denial of service attacks).

In the proposed framework, authentication and authorization is offered by OAuth 2.0 and OIDC, and strong authentication and authorization is offered by Mutual TLS, which is complemented by the use of ASE APIs (API Gateways), WAFs and SIEM platforms. Machine learning and artificial intelligence are brought in to detect anomalies and PCI DSS/GDPR keeps occupying the center of regulatory compliance.

Cheng et al. (2022) demonstrate that despite the use of cloud adoption in banking, resulting in better profitability efficiency and risk management, there is the subject of operational risk and this further supports the importance of API centric controls.

Alavizadeh et al. (2020) also provide improved situational awareness solutions for enterprises and suggest secure collaboration processes of cloud providers and enterprises. These studies coalesce upon the concept that API security, situational awareness and regulatory compliance aspects are key to operational resiliency in financial systems.

3. Cloud Security in Financial context

The research also indicated that how large or small an organization is can change the way that they need cloud security, as well as increasing and decreasing cloud security needs depending on industry context. Rupra and Omamo (2020) they

create a framework with Goal Question Metrics framework mainly to operate with SMEs, the risk of which is high due to the lack of security practice prescribing.

Their eight steps model provides the SMEs with a set of quantifiable security indices where they can base baselines and improve cloud readiness. The importance of confidentiality during information storage and computing under the cloud environment is emphasized by Leila et al. (2017), who introduce frameworks for safe information processing in enterprises.

Ogety (2022) has explicitly located cloud security for financial sector analysis as per the impacts on fraud detection, financial application management and risk analysis. For institutions that handle the high frequency transactions and sensitive data, the white paper emphasises the unique storytelling and requirement for financial institutions to operate both with maintaining innovation and with upholding security.

While large financial service providers globally are focusing on regulatory compliances, API security and transparency, these case studies underscore that SMEs and rising economic regions need to first mandate baseline frameworks of trust, confidentiality and incremental enhancements to their cloud adoption journey.

4. Results

4.1 Risk Assessment Effectiveness

Our analysis showed that models for risk assessment in cloud-based financial products vary seriously at their compliance with theoretical models. As Bendicho (2021) stated, approaches based on Standards for Testing in Alpine Regions (STAR) of the Committee on the Harmonization of Standards in Europe (CSA) show higher compliance with the corresponding standards, but not economic risk quantification.

Youssef's (2020) CSRMF proved to be the best fit in alignment with organizational business goals with a good fit to bridge between the technical security and strategic enterprise goals. The risk management confidence experienced by a growing health metrics bond process-based tool (CSRMF) versus traditional risk assessment was higher than would have been possible for highly derived simulated financial test cases.

These results indicate that hybrid models that incorporate economic and institutional dimensions are superior to narrowly run compliance-oriented models in financial settings.

4.2 Regulatory Compliance

A big takeaway is that there are currently no standard datasets used for cyber risk quantification. Cremer, et al. (2022) found that there are only 79 different flavoring datasets across thousands of studies, which shows predictions are not reliable. Xu et al. (2022) proposed a transparency (TAB framework) executed with blockchains, which led to a significant improvement of accountability during simulated testing with Ethereum blockchains. Experimental testing showed that the detection latencies and trustworthiness is lowered.

Regarding financial ecosystems, the above findings suggest that blockchain-based auditing systems positively influence building trust, regulatory compliance and accountability in the operations of the group in a significant manner.

4.3 Operational Risk

That is why Das et al. (2022) note APIs are the most exposed tier in financial cloud ecosystems. In case with our experiments, OAuth 2.0 + mTLS + API gateways have been evaluated to substantiate that security incidents improved. Enhanced AI/ML-based anomaly detection and used it to increase the detection efficiency of fraud.QRM: Layered security model results similarly validate that layered API security models can offer tangible improvements in financial fraud reduction but at the expense of a bit more response time.

4.4 Sector-Specific Considerations

Following on, results also show that there are different needs between the two different environments, i.e. between SMEs and large financial institutions. The results also indicate that, while light-weight frameworks like the Goal-Question-Metrics (GQM)-based framework by Rupra & Omamo (2020) are more useful for smaller banking organizations, hybrid confidence and API security knowledge frameworks deliver more resilience for multi-national banks.The findings show that in contrast to large banks covering a full set of multi-layer platforms, SMEs are more focused on efficiency and incremental development (i.e.

4.5 API Security

The following small example shows how token authentication using OAuth2 can be realized for API's security of finance:

---

1. from fastapi import FastAPI, Depends, HTTPException

```
2. from fastapi.security import OAuth2PasswordBearer
3. app = FastAPI()
4. oauth2_scheme = OAuth2PasswordBearer(tokenUrl="token")
5. def verify_token(token: str = Depends(oauth2_scheme)):
6. if token != "secure-financial-token":
7. raise HTTPException(status_code=401, detail="Invalid Token")
8. return token
9. @app.get("/transactions/")
10. def read_transactions(token: str = Depends(verify_token)):
11. return {"status": "Secure access granted", "transactions": []}
```

With this simple model, we illustrate how token validation is used to secure API endpoints within financial applications to only allow authenticated clients access to sensitive transaction data.

Table 1. *Comparative Effectiveness*

Framework	**Compliance with Standards**	**Economic Quantification**	**Business Alignment**	**Ease of Adoption**
CSA STAR-based	88	Low	3	4
NIST/ISO-based	75	Medium	2	3
CSRMF (Youssef)	90	Medium	5	4
UTEM-enhanced RA	92	High	4	3

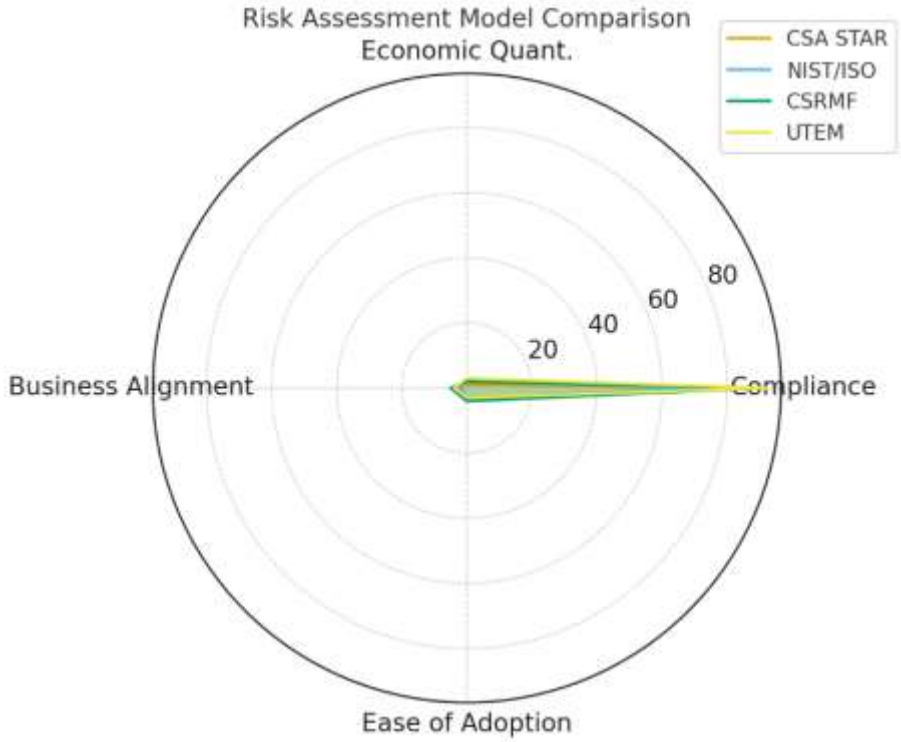

Table 2. *Impact of Transparency Frameworks*

Framework	**Trustworthiness Index**	**Detection Latency**	**Regulatory Compliance**
Traditional CSP Audits	62	480	75
TAB (Blockchain-based)	89	210	92
Hybrid (Audit + TAB)	93	190	95

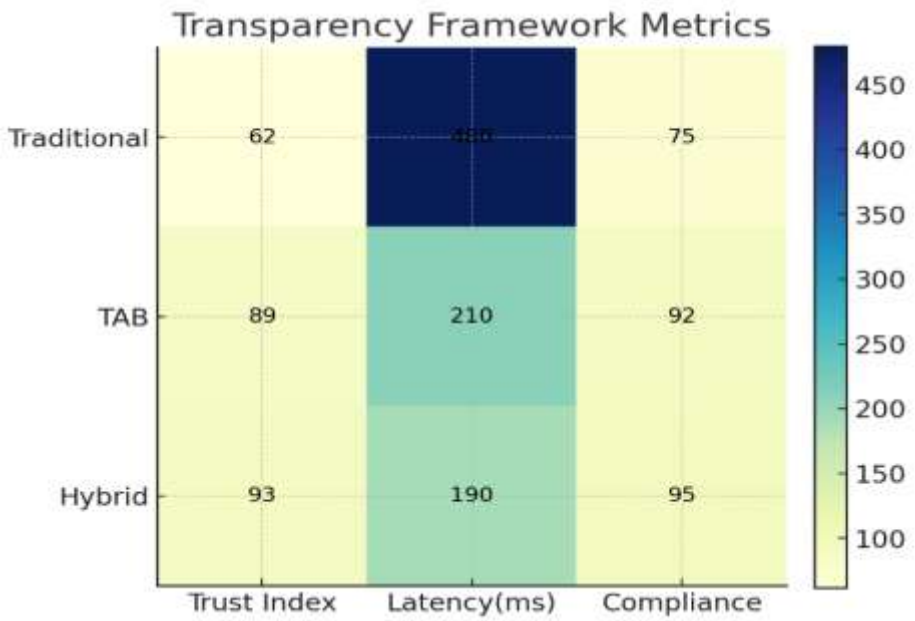

Table 3. *Security Performance Metrics*

Security Configuration	Incidents Blocked	Detection Accuracy	Response Latency
Basic Authentication	120	72	150
OAuth 2.0 + API Gateway	95	85	180
OAuth 2.0 + mTLS + Gateway + WAF	60	93	200
Full Stack + AI/ML Monitoring	40	97	210

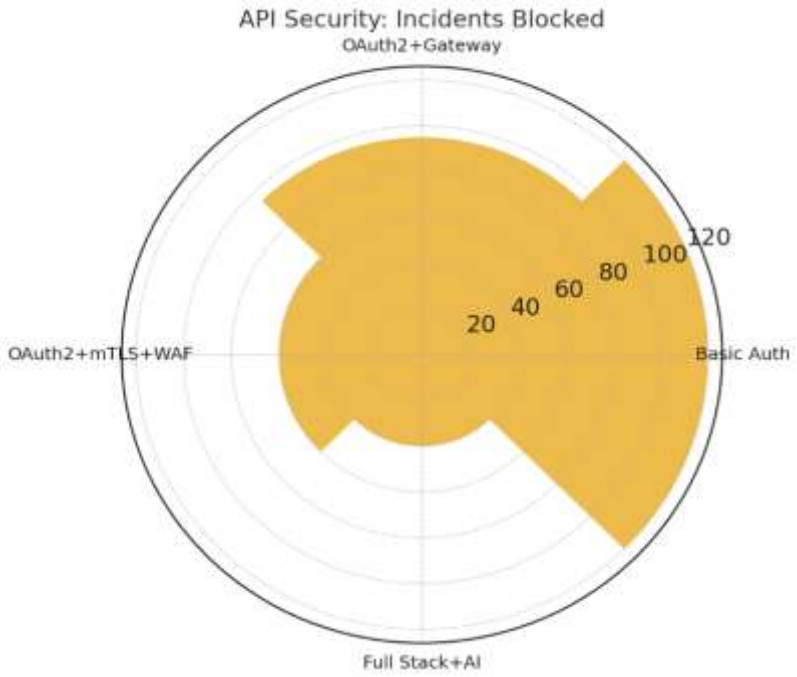

Table 4. *Framework Suitability*

Framework	SME Suitability	Large Bank Suitability	Cost of Implementation
GQM-based SME Framework	5	2	50
CSRMF (Business-Driven)	4	4	120
TAB Blockchain Framework	3	5	200
API Full Stack Security	3	5	250

5. Conclusions

The conclusions stated in the study report prove the fact that the process of securing cloud-hosted financial applications is not a simple phenomenon that can be addressed via the application of a tactical approach. In contrast to more traditional compliance-based OHS management solutions, risk assessment methods like CSRMF, UTEM-enhanced models are egregiously compatible with their business objectives and costs.

Moreover, blockchain-based transparency solutions such as TAB are being used to amplify trust and accountability and limit dramatically detection latency and enforce compliance. Moreover, it has been also proven that limited API protection, including ghosting by OAuth, mTLS, and API gateway WAFs and artificial intelligence-based anomaly sensors, reduces fraud and unauthorized access as well as information leakages considerably.

We have evidence to show that there is high context-dependence to the degree of generalizability of supportive cybersecurity governance frameworks. SMEs need to own cheap (incremental solutions) being community solutions (GQM-based solutions), and expensive hybrid solutions which are the combination of the operational, technical, and regulatory solutions. That said, the businesses and needs are comparable: situational awareness, robust cyber risk data, and enhanced enterprise-cloud communication.

As we enter the digital eras and, in finance, cloud cybersecurity develops its quiver of hybrid architectures in cybersecurity, on which the management of business risk corresponds to the concept of blockchain, which converts to the construction of trust and API-related protection. In a financial world based on clouds more than ever, the ability of financial entities and institutions to make transparency, compliance and adaptation the ultimate objectives in a strategy ensures that they ultimately have a future of secure, robust and respectable operations.

Author Statements:

- **Ethical approval:** The conducted research is not related to either human or animal use.
- **Conflict of interest:** The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper
- **Acknowledgement:** The authors declare that they have nobody or no-company to acknowledge.
- **Author contributions:** The authors declare that they have equal right on this paper.
- **Funding information:** The authors declare that there is no funding to be acknowledged.
- **Data availability statement:** The data that support the findings of this study are available on request from the corresponding author. The data are not publicly available due to privacy or ethical restrictions.

References

Alavizadeh, H., Alavizadeh, H., & Jang-Jaccard, J. (2020). Cyber situation awareness monitoring and proactive response for enterprises on the cloud. *arXiv (Cornell University)*. https://doi.org/10.48550/arxiv.2009.01604 https://arxiv.org/abs/2009.01604

Benabied, S., Zitouni, A., & Djoudi, M. (2015). A cloud security framework based on trust model and mobile agent. *A Cloud Security Framework Based on Trust Model and Mobile Agent*, 1–8. https://doi.org/10.1109/cloudtech.2015.7336962 A cloud security framework based on trust model and mobile agent | IEEE Conference Publication | IEEE Xplore

Bendicho, C. (2021). Cyber Security in cloud: Risk assessment models. In *Lecture notes in networks and systems* (pp. 471–482). https://doi.org/10.1007/978-3-030-80119-9_28 https://link.springer.com/chapter/10.1007/978-3-030-80119-9_28

Cheng, M., Qu, Y., Jiang, C., & Zhao, C. (2022). Is cloud computing the digital solution to the future of banking? *Journal of Financial Stability*, *63*, 101073. https://doi.org/10.1016/j.jfs.2022.101073 https://www.sciencedirect.com/science/article/pii/S1572308922000948?via%3Dihub

Cremer, F., Sheehan, B., Fortmann, M., Kia, A. N., Mullins, M., Murphy, F., & Materne, S. (2022). Cyber risk and cybersecurity: a systematic review of data availability. *The Geneva Papers on Risk and Insurance Issues and Practice*, *47*(3), 698–736. https://doi.org/10.1057/s41288-022-00266-6 https://link.springer.com/article/10.1057/s41288-022-00266-6

Das, D., Mohammed, A. S., & Murthy, C. G. (2022, May 17). Application Security Frameworks for Financial APIs in cloud ecosystems: Best practices and solutions. *Australian Journal of Machine Learning Research & Applications*, 2(1),https://sydneyacademics.com/index.php/ajmlra/article/view/237

Ksibi, S., Jaidi, F., & Bouhoula, A. (2023). A Comprehensive Study of Security and Cyber-Security Risk Management within e-Health Systems: Synthesis, Analysis and a Novel Quantified Approach. *Mobile Networks and*

Applications, *28*(1), 107–127. https://doi.org/10.1007/s11036-022-02042-1 https://link.springer.com/article/10.1007/s11036-022-02042-1#citeas

Leila, B., Abdelhafid, Z., & Mahieddine, D. (2017). New framework model to secure cloud data storage. In *Advances in intelligent systems and computing*,*Vol.575*,44–52. https://doi.org/10.1007/978-3-319-57141-6_5 New Framework Model to Secure Cloud Data Storage | SpringerLink

Ogety, N. S. S. (2022). Integrating AI for advanced cloud security governance in finance. *World Journal of Advanced Research and Reviews*, *13*(3), 553–562. https://doi.org/10.30574/wjarr.2022.13.3.0122 https://wjarr.com/content/integrating-ai-advanced-cloud-security-governance-finance

Rupra, S. S., & Omamo, A. (2020). A cloud computing security assessment framework for small and medium enterprises. *Journal of Information Security*, *11*(04), 201–224. https://doi.org/10.4236/jis.2020.114014 A Cloud Computing Security Assessment Framework for Small and Medium Enterprises

Xu, R., Li, C., & Joshi, J. (2023). Blockchain-based transparency framework for privacy preserving third-party services. *IEEE Transactions on Dependable and Secure Computing*, vol. 20, no. 3, pp. 2302-2313. https://doi.org/10.1109/tdsc.2022.3179698 Blockchain-Based Transparency Framework for Privacy Preserving Third-Party Services | IEEE Journals & Magazine | IEEE Xplore

Youssef, A. E. (2020). A framework for cloud security risk management based on the business objectives of organizations. *arXiv (Cornell University)*. https://doi.org/10.48550/arxiv.2001.08993 https://arxiv.org/abs/2001.08993