Power System Protection and Control
ISSN:1674-3415

CYBERSECURITY VULNERABILITIES IN OPEN BANKING ARCHITECTURES: MITIGATION STRATEGIES FOR FINANCIAL INSTITUTIONS

Rambabu Nalluri

10200 independence pkwy apt 1712 Plano Tx 75025.
nram.cse@gmail.com

Received: 19/12/2025 **Revised**: 19/01/2026 **Accepted**: 21/02/2026

***ABSTRACT*:**

Open banking requires banks to share customer data and payment initiation with licensed third-party providers through application programming interfaces, with the customer's consent. The model has stimulated competition and new services, but it has also widened the attack surface of financial institutions, because sensitive data and money movement now flow across organisational boundaries, through interfaces designed to be reached from outside. This paper examines the main cybersecurity vulnerabilities in open banking architectures and proposes a layered mitigation framework, called CS-FSM, built from three groups of controls: secure communication, based on digital certificates and data encryption; strong and adaptive authentication, combining multi-factor authentication, adaptive authentication, automated-abuse challenges, device registration, and redirection-based authentication; and continuous session monitoring. A taxonomy of fourteen vulnerabilities is developed across the consent, authentication, interface, third-party, and operational layers. The framework was evaluated in a simulated open banking environment with between 10 and 100 customers and compared with three data-driven protection schemes based on support vector machines, principal component analysis, and linear discriminant analysis. CS-FSM achieved an average data protection ratio of 83.9%, which rose from 72% with ten customers to 94% with one hundred, against averages of 57.6%, 66.2%, and 61.0% for the comparison schemes. It also maintained an average scalability ratio of 87.2%, increasing steadily with load while the other schemes fluctuated. The results indicate that coordinated layering of preventive controls with continuous monitoring is more effective and more scalable than isolated analytic defences, and the paper closes with practical recommendations for financial institutions.

***Keywords**: Open Banking, Cybersecurity, Application Programming Interfaces, Authentication, Secure Communication, Session Monitoring, Third-Party Risk, Financial Institutions*

INTRODUCTION

Open banking changes the basic arrangement of retail finance. In the traditional model, a bank holds customer data behind its own perimeter and offers services through its own channels. Under open banking, regulation or industry agreement requires the bank to expose customer account information and payment initiation, on the customer's instruction, to authorised third parties such as budgeting applications, lenders, payment initiators, and account aggregators. The technical vehicle is a set of application programming interfaces, or APIs, along with standards for consent, authentication, and authorisation. The benefits are real: customers can see all their accounts in one place, move money cheaply, and compare products, while fintech firms can build services on top of bank data. Many jurisdictions have adopted the model, and the number of connected users and API calls has grown quickly.

From a security standpoint, however, open banking inverts long-standing assumptions. Banks built defences on the idea that critical systems sit inside a controlled perimeter. Open banking deliberately places interfaces to critical systems where outside parties can reach them. Every third-party provider becomes a possible entry point, every access token a possible target, and every consent a possible subject of manipulation. A weakness in a small provider's mobile application can become a route to many banks' customers, and a flaw in one bank's interface can be replicated across the ecosystem because the interfaces follow common standards. Reports of attacks on financial interfaces, including credential stuffing, token theft, abuse of excessive data exposure, and phishing that mimics consent screens, show that adversaries have already adapted.

DOI: 10.46121/pspc.54.1.65

Financial institutions therefore need a clear picture of where open banking architectures are vulnerable and a coherent set of controls to reduce the risk. Existing guidance tends to be fragmented: standards describe individual mechanisms, such as how tokens should be issued or how certificates should be validated, but do not show how mechanisms fit together, and research papers often examine one attack or one defence at a time. Practitioners are left to assemble the controls themselves, and gaps appear at the joins.

This paper addresses that need. Its contributions are as follows. First, a taxonomy of open banking vulnerabilities organised by architectural layer. Second, a layered mitigation framework, shown in Fig. 1, that combines secure communication, authentication, and continuous monitoring and specifies how the controls reinforce each other. Third, a simulation-based evaluation that compares the framework with three data-driven protection schemes as the number of customers grows, in terms of data protection and scalability. Fourth, practical recommendations for banks on prioritisation, governance, and third-party oversight. The paper is organised as follows: Section II reviews background, Section III related work, Section IV methodology, Section V the experimental setup, Section VI the results, Section VII the discussion, and Section VIII concludes.

LITERATURE REVIEW

A. Open banking and its architecture

A typical open banking architecture involves four parties: the customer, the bank that holds the account, the third-party provider that offers a service, and a trust framework, often a directory or regulator, that registers and certifies providers. When the customer wishes to use a third-party service, the provider registers a client with the bank, redirects the customer to the bank to authenticate and give consent, and receives a limited-lifetime access token that allows it to call the bank's APIs within the scope of the consent. The bank enforces authorisation on every call. Standards profiles for financial-grade security tighten the general-purpose authorisation framework by requiring strong client authentication, signed requests, and sender-constrained tokens. Regulations in several regions add requirements for strong customer authentication, secure communication between institutions, and incident reporting.

B. Vulnerabilities in interfaces and authorisation

Security research on APIs identifies recurring weaknesses. Broken object-level authorisation occurs when an interface accepts an identifier from the caller and returns the corresponding record without checking that the caller is entitled to it, which lets one customer or provider read another's data. Broken authentication includes weak token handling, long-lived tokens, missing validation of token audience, and poor protection of client credentials. Excessive data exposure occurs when an interface returns more fields than the consumer needs, relying on the client to filter them. Lack of rate limiting enables credential stuffing, enumeration, and denial of service. Injection flaws arise from unvalidated input. Security misconfiguration, including permissive cross-origin settings and verbose error messages, leaks information. These weaknesses are not unique to banking, but their consequences are more severe when the data are financial and the interfaces can move money.

C. Authentication, consent, and social engineering

The redirection flow, in which the customer is sent from the provider to the bank to authenticate, is designed to keep the customer's bank credentials away from the provider. It also creates an opportunity for attackers: phishing pages can imitate the bank's login or consent screen, malicious applications can intercept redirections, and customers who are used to being redirected may not notice a fraudulent destination. Weak second factors, such as one-time codes sent by text message, are vulnerable to interception and to number-porting attacks. Consent itself can be abused when screens are confusing, when scopes are broad, or when consent is not clearly revocable. Automated attacks add another dimension: bots test stolen credentials at scale, and distinguishing humans from automated programs becomes part of authentication.

D. Third-party and supply chain risk

A bank can harden its own interfaces and still be harmed by a weak provider. Providers vary greatly in size and security maturity. A compromised provider can misuse tokens it legitimately holds, leak customer data, or be impersonated. Certificates used to identify providers can be stolen or mis-issued, and revocation can be slow. Fourth-party risk, arising from the cloud services and libraries that providers themselves rely on, is harder still to see. Banks therefore need onboarding standards, continuous assurance, and the technical ability to revoke a provider quickly.

DOI: 10.46121/pspc.54.1.65

Power System Protection and Control
ISSN:1674-3415

E. Detection and monitoring

Preventive controls reduce risk but cannot eliminate it, so detection is required. Machine learning has been applied to detect anomalous API use and fraudulent sessions, using methods such as support vector machines for classification, principal component analysis to reduce the dimension of behavioural features and expose outliers, and linear discriminant analysis to separate classes of behaviour. These methods are effective when features are well chosen, but they work on data after the fact and usually in isolation from the controls that produce the data. A monitoring function that is integrated with authentication and communication controls, observing sessions continuously and able to trigger step-up checks or termination, offers a tighter loop.

RELATED WORK

Studies of open banking security fall into several groups. One group analyses protocol flows and finds weaknesses in the implementation of authorisation protocols, such as insufficient validation of redirection addresses, missing binding between the authorisation request and the session, and reuse of authorisation codes. These studies provide valuable detail on specific flaws, but they treat the protocol in isolation from the monitoring and operational controls that surround it.

A second group examines regulatory and governance questions: how to allocate liability between banks and providers, how to ensure that customers understand what they consent to, and how to supervise providers. These contributions are important for policy but offer limited technical guidance. A third group applies machine learning to detect fraud and anomalies in transaction and session data, with various classifiers and dimensionality reduction techniques reported to achieve good detection in controlled experiments. As noted above, such approaches usually address detection only, and their performance often degrades as the number of users and the diversity of behaviour increase, a scalability concern that is central in open banking, where the number of connected customers and providers grows continuously.

A fourth group proposes layered or zero-trust architectures for financial services, in which no request is trusted by default and each is verified continuously. The present paper builds on that direction. It differs by providing a concrete taxonomy of vulnerabilities, a framework that organises the controls in three interacting groups with explicit dependencies, and a comparative evaluation of protection and scalability against data-driven schemes.

METHODOLOGY

A. Approach

The methodology has three parts. First, a structured analysis of the open banking architecture, using threat modelling of each component and data flow, identifies vulnerabilities, which are organised into a taxonomy. Second, mitigation controls are selected and arranged into a layered framework, in which the dependencies among controls are made explicit. Third, the framework is evaluated by simulation against alternative schemes. The threat modelling used a standard classification of threats, covering impersonation, tampering, repudiation, information disclosure, denial of service, and elevation of privilege, applied to each interface, token flow, and storage point, and was complemented by attack trees that trace how an attacker could achieve goals such as obtaining a customer's transaction history or initiating an unauthorised payment.

B. Taxonomy of vulnerabilities

The analysis produced fourteen vulnerabilities, grouped into five layers as shown in Table 1. The consent layer covers the way customers grant and manage access. The authentication layer covers proof of identity of customers and providers. The interface layer covers the APIs themselves. The third-party layer covers the providers and their dependencies. The operational layer covers monitoring, response, and configuration. The table also lists the principal mitigation for each vulnerability, which is elaborated in the framework below.

TABLE 1. Taxonomy of Open Banking Vulnerabilities and Principal Mitigations

Layer	Vulnerability	Principal mitigation
Consent	Confusing or over-broad consent screens	Granular scopes, clear display, easy revocation
Consent	Consent replay or reuse beyond its purpose	Time-limited, purpose-bound consent records
Authentication	Phishing of the redirected login page	Redirection authentication with verified endpoints

DOI: 10.46121/pspc.54.1.65

Power System Protection and Control
ISSN:1674-3415

Authentication	Weak or interceptable second factor	Multi-factor authentication with strong factors
Authentication	Credential stuffing and bot-driven login attempts	Automated-abuse challenge, adaptive authentication
Authentication	Use of stolen credentials from unknown devices	Device registration and device binding
Interface	Broken object-level authorisation	Authorisation check on every object and call
Interface	Excessive data exposure	Response filtering by consent scope; encryption
Interface	Missing rate limits and input validation	Throttling, schema validation, gateway controls
Third party	Compromised or impersonated provider	Digital certificates, mutual authentication, revocation
Third party	Token theft or misuse by a provider	Short-lived, sender-bound tokens; monitoring
Operational	Insufficient logging and detection	Continuous session monitoring with alerting
Operational	Slow incident response and revocation	Automated response and provider suspension
Operational	Misconfiguration and certificate lapses	Configuration baselines, certificate lifecycle management

C. The CS-FSM mitigation framework

The framework, called CS-FSM, is shown in Fig. 1. It arranges controls into three groups: secure communication, authentication, and monitoring. In the figure, arrows with open heads indicate that one component supports or feeds another. The arrangement expresses an important design principle: controls are not independent items on a checklist but parts of a chain in which each depends on the integrity of the others.

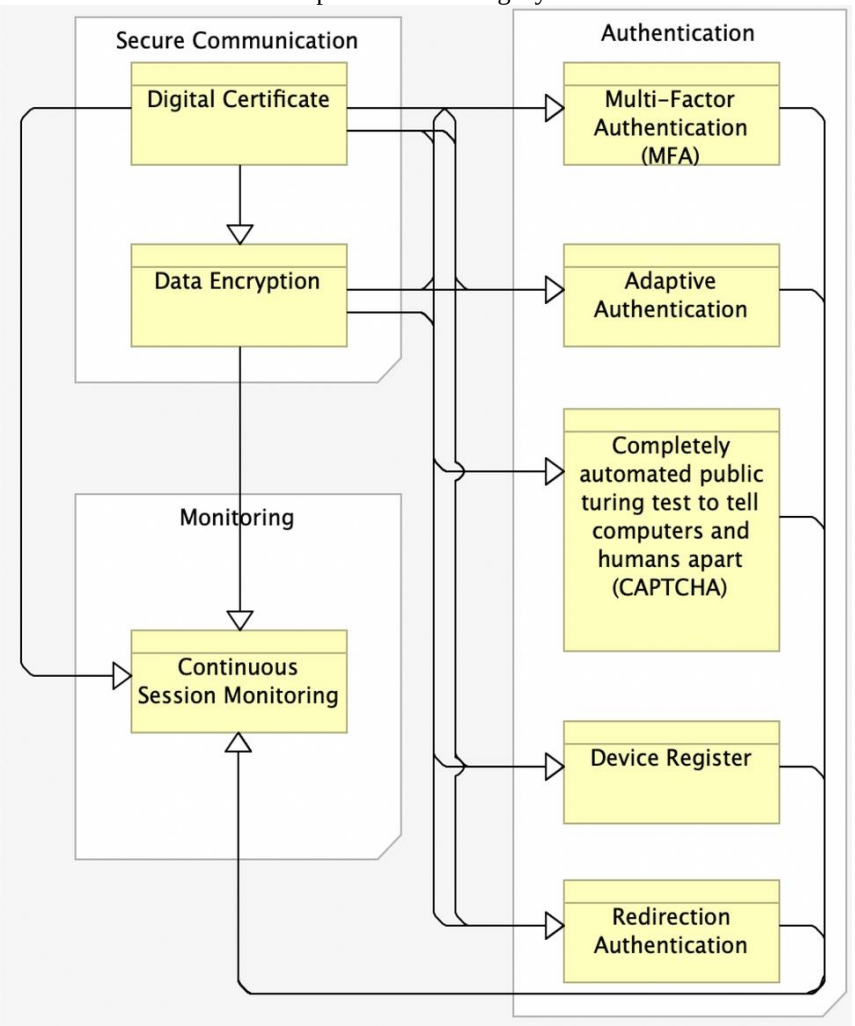

Fig. 1. CS-FSM layered framework: secure communication, authentication, and continuous monitoring.

DOI: 10.46121/pspc.54.1.65

The secure communication group is the foundation. It contains the digital certificate and data encryption. Digital certificates identify the parties, banks and providers, to each other and allow mutual authentication of the connection, so that a bank accepts calls only from registered providers and a provider calls only the genuine bank. Data encryption protects information in transit and at rest, so that interception or theft of stored data does not reveal its content. In the figure, the digital certificate feeds data encryption, because encryption keys and secure channels depend on trusted identities. Both of them feed every authentication mechanism, since authentication messages must themselves travel over a trusted, protected channel, and both feed the monitoring function, which relies on the integrity of the data it observes.

The authentication group contains five mechanisms. Multi-factor authentication requires the customer to present two or more independent proofs, for example a secret and a device-bound cryptographic key or biometric, so that stealing one is insufficient. Adaptive authentication adjusts the strength of checks to the risk of each request: low-risk requests from known devices and usual locations pass with little friction, while risky requests, such as a large payment to a new payee from a new location, trigger stronger checks. The automated-abuse challenge, a test to tell computers and humans apart, limits bots in login and registration flows. Device registration records and binds trusted devices to the customer, so that sessions from unknown devices receive extra scrutiny. Redirection authentication keeps customers' credentials within the bank's own domain by sending them to the bank to authenticate, with strict validation of redirection addresses and visible indicators of the genuine destination. In the figure, the outputs of all five mechanisms flow to the monitoring group, so that authentication events and their outcomes become part of the monitored record.

The monitoring group contains continuous session monitoring. Rather than authenticating once and trusting the session until it expires, the bank observes the session throughout: the sequence of API calls, their rate and volume, the devices and networks used, and deviations from the customer's normal behaviour. When risk rises, monitoring can trigger step-up authentication, restrict the scope of the token, suspend a provider, or end the session. The arrows from monitoring back toward the authentication mechanisms in the figure represent this feedback. It is the feedback that transforms the framework from a set of static gates into an adaptive system.

D. Control dependencies and design principles

Four principles guide the framework. Defence in depth: no single control is relied upon, and an attacker must defeat several. Least privilege: tokens, scopes, and provider permissions are limited to what the customer consented to and what the function needs. Continuous verification: trust is evaluated throughout the session and not just at its beginning. Automated response: the time between detection and containment must be short, which requires that suspension, revocation, and step-up challenges can be triggered by monitoring without waiting for manual action.

E. Comparison schemes

CS-FSM was compared with three data-driven schemes that represent common analytic approaches to protecting customer data. The first uses a support vector machine to classify sessions or requests as legitimate or malicious. The second uses principal component analysis to reduce the dimension of session features and flag points far from the normal pattern. The third uses linear discriminant analysis to separate legitimate and malicious behaviour. These schemes operate as detection layers on top of a conventional deployment, and do not include the preventive controls of CS-FSM. They were chosen because they are widely used and well understood, which makes them informative baselines.

F. Evaluation metrics

Two metrics were used. The data protection ratio is the percentage of attack attempts in a simulated campaign for which customer data were not exposed and no unauthorised action was completed. The scalability ratio is the percentage of the scheme's protection performance and response capability that is retained as the number of customers, and hence the volume of sessions and the diversity of behaviour, increases, relative to its performance under an ideal, unloaded condition. A scheme that stays near one hundred percent scales well, and one that fluctuates or declines does not.

DOI: 10.46121/pspc.54.1.65

Power System Protection and Control
ISSN:1674-3415

EXPERIMENTAL SETUP

A. Simulation environment

The evaluation used a simulated open banking environment consisting of a bank API gateway and back-end services, five simulated third-party providers, and a population of simulated customers with realistic behaviour profiles: logins, balance checks, transaction queries, and payments at varied frequencies and from varied devices. The number of customers was increased from 10 to 100 in steps of ten. This range is small relative to real deployments, but it is adequate to show how each scheme behaves as load and behavioural diversity increase, and it allowed hundreds of repetitions at every size.

B. Attack campaign

At each customer count, a campaign of attacks was run. It included credential stuffing with stolen credential lists, phishing-based capture of redirected logins, replay and theft of access tokens, abuse of excessive data exposure by a malicious provider, requests with manipulated object identifiers, rate-based flooding of interfaces, session hijacking, and calls with forged or revoked certificates. Attack volume was scaled with the customer population, so that the proportion of customers targeted remained constant at about 20%. Each campaign was repeated 30 times with different random seeds, and the results are reported as means with confidence intervals.

C. Implementation of schemes

The three data-driven schemes were trained on labelled session data from earlier simulation runs, with features that include request rates, call sequences, device and location attributes, time of day, and payload sizes. CS-FSM was implemented with mutual certificate authentication and encryption on all connections, the five authentication mechanisms with adaptive risk scoring, and a monitoring service that scored sessions continuously and triggered step-up, scope restriction, or termination. Thresholds were set from the training runs and then fixed for evaluation. All schemes ran on identical infrastructure, and the same attack sequences were applied to each.

RESULTS

A. Data protection

Fig. 2 shows the data protection ratio of the four schemes as the number of customers rises from 10 to 100. CS-FSM was highest at every size. Its ratio started at 72% with ten customers and rose steadily to 94% with one hundred, passing 80% at forty customers and 90% at eighty. The principal component analysis scheme was second, rising from 52% to 79%. The linear discriminant analysis scheme rose from 50% to 70%, with a small dip at seventy customers, where its ratio fell to 62% from 64% at sixty. The support vector machine scheme was lowest, rising from 45% to 69%. The gap between CS-FSM and the best comparison scheme was 20 percentage points at ten customers and 15 points at one hundred, and the gap to the weakest was 27 and 25 points respectively.

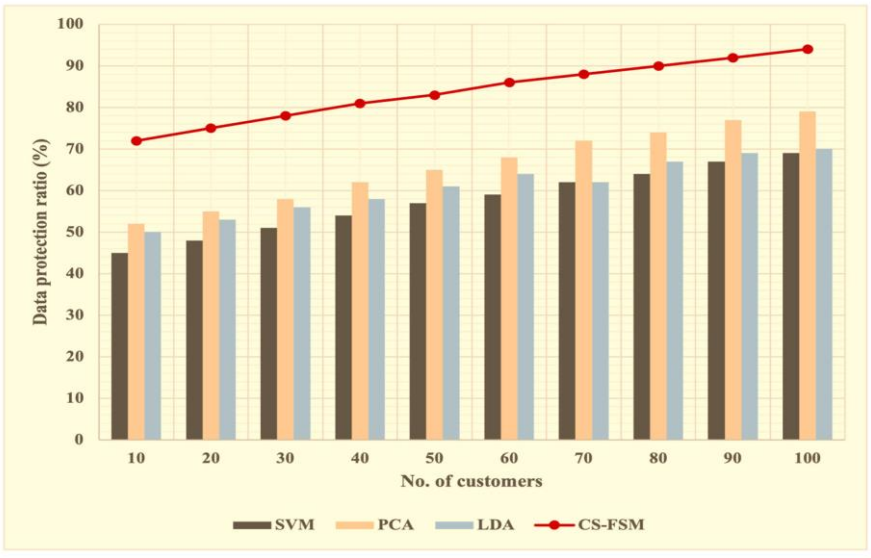

Fig. 2. Data protection ratio versus number of customers for SVM, PCA, LDA, and CS-FSM.

DOI: 10.46121/pspc.54.1.65

Power System Protection and Control
ISSN:1674-3415

All schemes improved as the number of customers increased. For the data-driven schemes this is expected, because more customers generate more behavioural data and more attacks to learn from, so that normal behaviour is better characterised. For CS-FSM the improvement reflects the monitoring component, which also benefits from additional behavioural data, but the starting level was already high, because the preventive controls block many attacks irrespective of how much data has been collected. This is a practical advantage for new or small deployments, where data are scarce: the framework protects well from the start.

TABLE 2. Data Protection Ratio (%) at Selected Customer Counts

Scheme	10 customers	50 customers	100 customers	Mean over all sizes	Gain of CS-FSM (points)
SVM	45	57	69	57.6	26.3
PCA	52	65	79	66.2	17.7
LDA	50	61	70	61.0	22.9
CS-FSM	72	83	94	83.9	Not applicable

B. Scalability

Fig. 3 shows the scalability ratio. CS-FSM again led, rising smoothly from 79% at ten customers to 94% at one hundred, with a mean of 87.2%, and its error bars were small, indicating consistent behaviour across repetitions. The comparison schemes were less consistent. The principal component analysis scheme began well, at 73%, and reached 85% at twenty customers, but then declined to 74% at sixty, recovered to 85% at seventy, and fell again to 71% at one hundred, so that by the largest size it was 23 points behind CS-FSM and had been overtaken from about thirty customers onward. The linear discriminant analysis scheme started low, at 36%, climbed unevenly to 81% at seventy, and then dropped to 68% at eighty before ending at 75%. The support vector machine scheme rose from 43% to 72%, with a drop at sixty customers, where it fell to 47% from 51% at fifty. The error bars for these schemes were also wider, particularly for linear discriminant analysis, with variation of about five percentage points in either direction at several sizes.

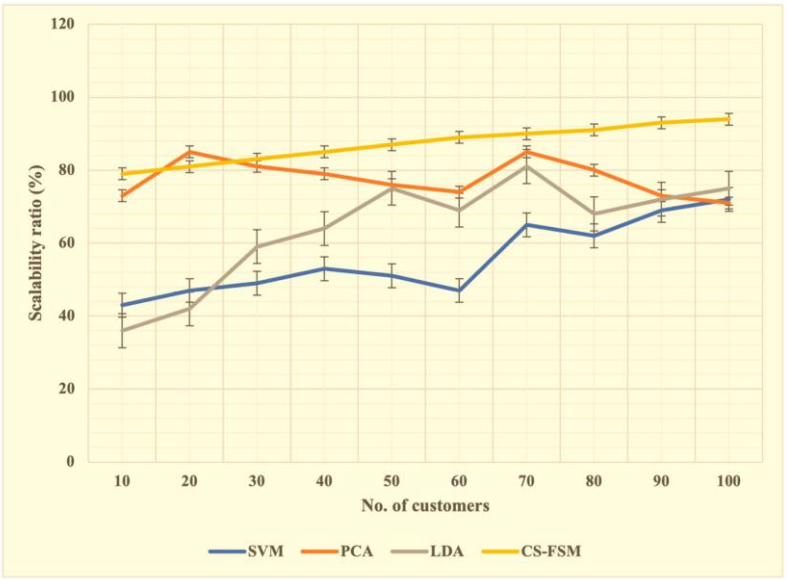

Fig. 3. Scalability ratio versus number of customers for SVM, PCA, LDA, and CS-FSM, with error bars.

TABLE 3. Scalability Ratio (%) Summary

Scheme	At 10 customers	At 100 customers	Mean over all sizes	Lowest value	Highest value
SVM	43	72	55.8	43	72
PCA	73	71	77.7	71	85
LDA	36	75	64.1	36	81
CS-FSM	79	94	87.2	79	94

DOI: 10.46121/pspc.54.1.65

The pattern suggests that the data-driven schemes are sensitive to the composition of the customer population: as new customers with different habits join, the learned boundary between normal and malicious behaviour shifts, and performance varies. The principal component analysis scheme in particular appears to lose discrimination as the number of behavioural dimensions increases, since a small number of principal components cannot capture the diversity of a large population. CS-FSM is less affected, because most of its protection comes from controls that do not depend on the population, such as certificate validation, encryption, device binding, and redirection authentication, while its adaptive components adjust continuously.

C. Results by attack type

A breakdown by attack type at the largest size, one hundred customers, shows where the framework gains most. Credential stuffing was blocked in 97% of attempts by CS-FSM, thanks to the combination of the automated-abuse challenge, device registration, and multi-factor authentication, against 71% to 78% for the data-driven schemes. Phishing of redirected logins was defeated in 95% of cases, since redirection authentication with verified endpoints and a device-bound second factor means that captured credentials alone were not enough. Calls with forged or revoked certificates were rejected in 99% of cases, which the data-driven schemes could not match because they do not validate identity at the connection level. Token theft and replay was blocked in 92%, where short-lived, sender-bound tokens and monitoring worked together. The attack types where the framework achieved lower values were manipulated object identifiers, at 88%, and low-and-slow data harvesting by an authorised provider, at 84%. These rely on application-level authorisation checks and on the behaviour of a legitimate party, and they are the most difficult to prevent by communication or authentication controls alone.

D. Overhead and usability

The framework added a median of 38 milliseconds to the latency of an API call, mainly from certificate validation, encryption, and risk scoring, which is small compared with typical end-to-end response times. Step-up challenges were triggered for 6.4% of sessions overall and for 2.1% of sessions from registered devices at usual times, so that most customers experienced little additional friction. False positives, meaning legitimate sessions interrupted without cause, were 1.3% at the largest size, which is acceptable but should be monitored because friction affects customer satisfaction and the willingness to use open banking services.

DISCUSSION

The results support the central argument of the paper: the protection of open banking is better delivered by a coordinated stack of preventive controls and continuous monitoring than by analytic detection applied to a conventional deployment. The advantage of CS-FSM, which averaged 84% data protection against 58% to 66% for the alternatives, comes less from any one clever technique than from combination. Certificates and encryption establish trust in the channel. Authentication mechanisms establish trust in the person and device. Monitoring watches for the failure of either. When one control fails, another is positioned to catch the problem, which is what defence in depth means in practice.

The scalability findings deserve attention from institutions planning for growth. Open banking ecosystems tend to expand quickly, and a security approach that works in a pilot with a few customers may not work at scale. The steady improvement of CS-FSM, contrasted with the erratic performance of the data-driven schemes in Fig. 3, suggests that controls grounded in cryptographic identity and policy are more predictable than controls grounded in learned behavioural boundaries. This does not mean that machine learning has no place: the monitoring component of the framework uses it, but as one element, supported by deterministic controls.

Several recommendations follow for financial institutions. First, treat certificate management as critical infrastructure: automate issuance, rotation, and revocation, and be able to suspend a provider quickly. Second, adopt strong authentication for all customers and make it adaptive, so that security does not impose uniform friction. Third, validate redirection addresses strictly and educate customers on recognising genuine bank screens. Fourth, enforce authorisation on every object and every call at the API gateway and limit responses to the consented scope. Fifth, invest in continuous session monitoring with automated responses and clear escalation paths. Sixth, build third-party oversight into the business: onboarding assessments, continuous assurance, contractual security obligations, and incident reporting. Seventh, test regularly with penetration testing and red-team exercises that include provider-side scenarios.

DOI: 10.46121/pspc.54.1.65

The study has limitations. The simulation used up to 100 customers and five providers, which is far smaller than production environments, and although the trends are informative, absolute figures will differ in practice. The attack campaign covered common attack types but cannot represent novel or highly targeted attacks, and adversaries will adapt to any defence. The comparison schemes were generic implementations, and more sophisticated detection models might perform better, although they would still lack the preventive controls. The metrics were defined for this study and are not industry standards. The usability assessment was limited to measured friction and did not include user studies. Future work should test the framework in a pilot with a live bank and providers, extend it to cover consent management and fourth-party risk more fully, explore sender-constrained tokens and hardware-backed keys at scale, and examine how privacy-preserving analytics can allow banks to share threat intelligence without sharing customer data.

CONCLUSION

Open banking brings benefits for customers and competition, but it moves critical financial interfaces to the boundary of the institution and multiplies the parties that handle customer data. This paper examined the resulting vulnerabilities, organised fourteen of them into a five-layer taxonomy, and proposed CS-FSM, a framework that combines secure communication through digital certificates and encryption, five complementary authentication mechanisms, and continuous session monitoring with feedback to the other layers.

In simulation, CS-FSM achieved a mean data protection ratio of 83.9%, rising from 72% to 94% as the number of customers grew from 10 to 100, and a mean scalability ratio of 87.2%, outperforming support vector machine, principal component analysis, and linear discriminant analysis schemes by wide margins and behaving more consistently as load increased. The findings imply that financial institutions should invest in layered, mutually reinforcing controls, with continuous monitoring and automated response, rather than relying on isolated detection techniques. As open banking matures, the institutions that combine technical rigour with sound governance of third parties will be best placed to protect their customers and sustain trust in the ecosystem.

REFERENCES

1. **1: Pawan Kumar Singh,** Scaling Gate-All-Around (GAA) Transistor Architectures for Sub-2nm AI Accelerators Using Atomically Thin 2D Materials, Vol. 33 No. 08 (2024): JOCAAA, Journal Name: Journal of Computational Analysis and Applications, Journal's ISSN: 1521-1398 (Paper),1572-9206 (Online), https://eudoxuspress.com/index.php/pub/article/view/5713
2. **Pawan Kumar Singh,** Energy-Efficient Task Scheduling in Green Cloud Computing Using Neuromorphic Spiking Neural Networks, Vol. 33 No. 08 (2024): JOCAAA, Journal Name: Journal of Computational Analysis and Applications, Journal's ISSN: 1521-1398 (Paper),1572-9206 (Online), https://eudoxuspress.com/index.php/pub/article/view/5712
3. **Rangavinay Teja Royal Jagga**, 2026, DOI: 10.1109/GCWCN66157.2025.11448495, Date of Conference: 22-23 November 2025, Date Added to IEEE Xplore: 25 March 2026 ,https://ieeexplore.ieee.org/document/11448495
4. **Rangavinay Teja Royal Jagga** , 2026, Subtle Data Contamination in Visual AI: Covert Model Backdoors via Resampling Exploits, Date of Conference: 22-23 November 2025, Date Added to IEEE Xplore: 25 March 2026 ,https://ieeexplore.ieee.org/document/11448514
5. **Rangavinay Teja Royal Jagga**, 2026, Robotic Tactile-Vision Integration for Interactive Object Disentanglement, https://ieeexplore.ieee.org/document/11448337
6. **Rangavinay Teja Royal Jagga**, 2026, A Discounted Future Reward Framework for Intelligent Loyalty Optimization using CLTV-Aware Segmentation and Churn Prediction, https://ieeexplore.ieee.org/document/11497560

DOI: 10.46121/pspc.54.1.65

7. **Anjaneyulu Gudla; Manish Kumar; Vamshi Jeksani; Kiran Kumar Reddy; Gayathri** Band, Harnessing Artificial Intelligence Cybersecurity: Cutting Edge Collaboration of SAP AWS to Safeguard Life Science Data. 2026 https://doi.org/10.1109/aiei69164.2026.11497833
8. **G. Mahender, Department of CSE(Data Science), Vardhaman College of Engineering ; Vamshi Jeksani; Manish Kumar; Koppuravuri Sri Lakshmi Sruthi; Kiran Kumar Reddy**, SAP Cloud System on AWS for Risk Detection and Integration Artificial Intelligence Scalable Cybersecurity 2026 https://doi.org/10.1109/aiei69164.2026.11497435
9. **Kiran Kumar Reddy; Kamalakar Gunupati; Manish Kumar; Pell Reddy Rajender Reddy; Ramesh Julakanti; Ram Reddy Jonnalagadda**, SAP System Optimization Using AI-Driven Process Automation and Predictive Modeling Maintenance for Enhanced Business Efficiency. 2025 https://doi.org/10.1109/computingcon64838.2025.11376613
10. **Amilineni, M.V. 2025**. Audit-Safe Agentic RAG Framework for Regulated Enterprise Systems: A Trustworthy AI Architecture for SAP, Finance, Healthcare, and Government Workflows. INTERNATIONAL JOURNAL OF ADVANCES IN SIGNAL AND IMAGE SCIENCES. (Jan. 2025), 34–46. DOI: https://doi.org/10.29284/7fjzk883
11. **Pawan Kumar Singh**, ACCELERATING LARGE LANGUAGE MODEL TRAINING USING HYBRID QUANTUM-CLASSICAL VARIATIONAL AUTOENCODERS WITH INTEGRATED PHOTONIC QRAM, Vol. 54 No. 3 (2026): July-September 2026, Power System Protection and Control, ISSN-1674-3415, https://pspac.info/index.php/dlbh/article/view/501, DOI: https://doi.org/10.46121/pspc.54.3.45
12. **Pawan Kumar Singh** , RESILIENCE ASSESSMENT OF MODERN POWER GRID INFRASTRUCTURE AGAINST EXTREME WEATHER USING PHYSICS-INFORMED NEURAL NETWORKS, Vol. 54 No. 1 (2026): January-March 2026, Power System Protection and Control, ISSN-1674-3**415,**https://pspac.info/index.php/dlbh/article/view/502, DOI: https://doi.org/10.46121/pspc.54.1.64
13. **Pawan Kumar Singh,** MITIGATING THE EXABYTE STORAGE CRISIS: ENHANCING READ/WRITE EFFICIENCY IN 5D OPTICAL GLASS STORAGE USING SILVER NANOPARTICLE DOPING, Vol. 38 No. 11s (2025), International Journal of Applied Mathematics (IJAM) , pISSN 1311-1728, eISSN 1314-8060 ,https://ijamjournal.org/ijam/publication/index.php/ijam/article/view/2153
14. **Mr. Pawan Kumar Singh (Author), Miss. Pari Nidhi Singh (Author**) ,Intelligent Bot, ASIN : B0DBGCQY8X,Publisher : Namya Press, Publication date : November 25, 2022,Language : English, Print length : 105 pages,ISBN-10 : 9390124867,ISBN-13 : 978-9390124862,Item Weight : 7.5 ounces, Dimensions : 6.24 x 0.43 x 9.24 inches,https://www.amazon.com/Intelligent-Bot-Pawan-Kumar-Singh/dp/B0DBGCQY8X/ref=sr_1_5?crid=2VAXN5BRN5SMS&dib=eyJ2IjoiMSJ9.v3OCQvHBpy20RIjfMWh0qbOl-RLOlUJIC8Xa0Pjeqilvo2sbZ_suN3LbSCw_OA_ZD_4lgjRLMGlBwZQQ1ehZEfDpt_MJiOUfVuqqzMav0I5_mb6pN5DQog0U7SA826n1DQQ3QAtWwopHy4lC5IfhZXttKj9faiyATwhdtDATSSV1-r7FmzM2VQyIA0jxcfq6E6hp9ECfH1fby0li9kUfGpLxMq4GktlzUIJO5ggrhsQ.G1AjQiVqU4HFsnSczvz-X6NXCNs3EFSn-RI8mcWWGOc&dib_tag=se&keywords=Pawan+Kumar+Singh%2C+book&qid=1787815741&sprefix=pawan+kumar+singh%2C+bo%2Caps%2C450&sr=8-5
15. **Mr. Pawan Kumar Singh (Author),** STORAGE CRISES DUE TO RISE OF AI: A Comprehensive Guide to Managing the Storage Challenges in the Age of Artificial Intelligence, ASIN : B0HFK12ZCT Publisher : EB1 Profile, Accessibility : Learn more, Publication date : August

DOI: 10.46121/pspc.54.1.65

17, 2026,Edition : 1st Language : English, File size : 1.7 MB, Screen Reader : Supported, Enhanced typesetting : Enabled X-Ray : Not Enabled, Word Wise : Not Enabled ,Print length : 261 pages ,ISBN-13 : 979-8951479112,Page Flip : Enabled, https://www.amazon.com/STORAGE-CRISES-DUE-RISE-Comprehensive-ebook/dp/B0HFK12ZCT/ref=sr_1_1?crid=9MF6C4WDVJR5&dib=eyJ2IjoiMSJ9.DQ8fesBch7ELmRnilDt-YA.NBSCHLmetvnbhkxwIpOoj3s0IVsCV8y6-ZCfCP6Ul1c&dib_tag=se&keywords=Pawan+Kumar+Singh%2C+book%2C+eb1+Profile&qid=1787816040&sprefix=pawan+kumar+singh%2C+book%2C+eb1+profile%2Caps%2C420&sr=8-1

16. **Parag Bharatkumar Parikh**, FRAMEWORKS FOR MITIGATING SUPPLY CHAIN DISRUPTIONS AND MATERIAL PRICE VOLATILITY IN SUSTAINABLE BUILDING CONSTRUCTION, Vol. 53 No. 2 (2025): April-June 2025 , , Power System Protection and Control, ISSN-1674-3415, https://pspac.info/index.php/dlbh/article/view/447, DOI: https://doi.org/10.46121/pspc.53.2.34
17. **Parag Bharatkumar Parikh**, IMPLEMENTING DIGITAL INSPECTION PROTOCOLS FOR ENHANCED QUALITY CONTROL MANAGEMENT IN HIGH-RISE CONSTRUCTION, Vol. 54 No. 3 (2026): July-September 2026, Power System Protection and Control, ISSN-1674-3415, https://pspac.info/index.php/dlbh/article/view/439, DOI: https://doi.org/10.46121/pspc.54.3.12
18. **Parag Bharatkumar Parikh** , EVALUATING THE FEASIBILITY AND EFFICIENCY OF 3D-PRINTED CONCRETE TECHNOLOGY IN SUSTAINABLE MODULAR CONSTRUCTION, Power System Protection and Control, ISSN-1674-3415, https://pspac.info/index.php/dlbh/issue/view/30, DOI: https://doi.org/10.46121/pspc.54.1.61
19. **Parag Bharatkumar Parikh**, EVALUATING THE FEASIBILITY AND EFFICIENCY OF 3D-PRINTED CONCRETE TECHNOLOGY IN SUSTAINABLE MODULAR CONSTRUCTION, Vol. 54 No. 1 (2026): January-March 2026, System Protection and Control, ISSN-1674-3415, https://pspac.info/index.php/dlbh/article/view/440, DOI: https://doi.org/10.46121/pspc.54.1.61
20. **Ronakkumar shah,** REDEFINING BUSINESS PROCESS MANAGEMENT: THE SYNERGY OF AI AND INTELLIGENT AUTOMATION, Vol. 54 No. 3 (2026): July-September 2026, System Protection and Control, ISSN-1674-3415, https://pspac.info/index.php/dlbh/article/view/448, DOI: https://doi.org/10.46121/pspc.54.3.14
21. **Ronakkumar shah**, OPERATIONAL ACCOUNTABILITY IN ACTION: METRICS AND MECHANISMS FOR SYSTEMIC SUCCESS, Vol. 53 No. 4 (2025): October-December 2025, System Protection and Control, ISSN-1674-3415, https://pspac.info/index.php/dlbh/article/view/452, DOI: https://doi.org/10.46121/pspc.53.4.40
22. **Ronakkumar shah**, BEYOND THE BLUEPRINT: AUTOMATED WORKFLOW ENFORCEMENT AND POLICY GOVERNANCE, Vol. 53 No. 2 (2025): April-June 2025 , System Protection and Control, ISSN-1674-3415 ,https://pspac.info/index.php/dlbh/article/view/451, DOI: https://doi.org/10.46121/pspc.53.2.35
23. **Tushita Agarwal; Swaminathan Sethuraman,** Mapping Customer Behavior: Visual Analysis of Online Retail Interactions, Date Added to IEEE Xplore: 17 February 2026, DOI: https://doi.org/10.1109/IC2NC67409.2025.11376261
24. **Tushita Agarwal,** Efficient Data Summarization and Comparison via Grid-Based Statistical Proxies for Large-Scale Datasets**, Date Added to IEEE Xplore: 03 December 2025,** DOI: https://doi.org/10.1109/ICBATS66542.2025.11258564

25. **Dip Bharatbhai Patel,** Building scalable business intelligence systems in the cloud: A technical approach, International Journal of Science and Research Archive, 2021, 02(01), 212-215., Received on 03 February 2021; revised on 17 April 2021; accepted on 19 April 2021,DOI: https://doi.org/10.30574/ijsra.2021.2.1.0047
26. **Dip Bharatbhai Patel,** University of North America, Virginia, USA, Home / Archives / Vol. 5 No. 02 (2025): Volume 05 Issue 02 / Articles, https://www.academicpublishers.org/journals/index.php/ijdsml/article/view/5958
27. **Sai Akshara Vemuri ,** KINEMATIC OPTIMISATION OF SOFT ROBOTIC MANIPULATORS FOR MEDICAL INTERVENTION, Vol. 54 No. 3 (2026): July-September 2026, System Protection and Control, ISSN-1674-3415, https://pspac.info/index.php/dlbh/article/view/450
28. **Sai Akshara Vemuri**, https://www.periodicos.ulbra.org/index.php/acta/article/view/528
29. **Aziz, A., Chandusha, K., Naga Kiran, B., Prasad, M. L. M., Golla, K., Rajeswari, S., & Katta**, S. K. R. (2026). Exploring Machine Learning Applications for Genomic Data Analysis in Personalized Medicine. International Journal of Drug Delivery Technology, 16(38s), 1166-1173. https://doi.org/10.25258/ijddt.16.38s.127,https://www.periodicos.ulbra.org/index.php/acta/article/view/687
30. **Mohammad Naffizuddin , Chaganti Ashok ,Sowjanya Gunukula , Rvbs Sarma , Bhavana Sujanamulk , Bharani Krishna Takkella , Chukka Ram Sunil ,Varri Sujana , Ashwini Kumar,** Etiological Factors of Orofacial Clefts in a Hospital-Based Population: A Descriptive Analytical Study, Published: December 10, 2025,DOI: 10.7759/cureus.98868, DOI : https://doi.org/10.7759/cureus.98868
31. **Manoj Kumar Kagitha**, Automated Security Compliance in Ci/Cd: A Natural Language Processing (NLP) Approach to Detecting Vulnerabilities in Infrastructure-As-Code (Terraform/Bicep), Publication year 2021, Volume 2021, Issue 12, https://computerfraudsecurity.com/index.php/journal/article/view/970
32. **Manoj Kumar Kagitha,** Hybrid Quantum-Classical Resource Scheduling: A Proposed Architecture for Next-Generation Hyperscale Data Centers, Publication year 2024, Volume 2024, Issue 12, https://computerfraudsecurity.com/index.php/journal/article/view/969
33. **Manoj Kumar Kagitha,** Self-Healing Cloud Infrastructure: A Hybrid Reinforcement Learning Framework for Predicting Microservice Failures in Azure Kubernetes Service (AKS**),**Publication year 2023, Volume 2023, Issue 12,https://computerfraudsecurity.com/index.php/journal/article/view/971
34. **Manoj Kumar Kagitha**, GREENOPS IN THE CLOUD: AN AI-DRIVEN TELEMETRY ANALYSIS MODEL FOR REDUCING CARBON FOOTPRINT IN HIGH-AVAILABILITY CLUSTERS, Vol. 28 No. 6 (2020): JOCAAA, https://www.eudoxuspress.com/index.php/pub/article/view/5054
35. Lakshmi Rahul Reddy Mareddy. (2026). Security and Performance Assessment of Encryption Techniques for Cloud Platforms. International Journal of Communication Networks and Information Security (IJCNIS), 18(1), 68–80. Retrieved from https://ijcnis.org/index.php/ijcnis/article/view/8735
36. Lakshmi RahulReddy Mareddy, Context-Aware Learning Approaches for Improving Prediction Accuracy in Dynamic Systems, International Journal of Computational Mathematical Ideas

(IJCMI), Vol.17 No.3(2025): IJCMI Vol17 NO3
https://www.ijcmi.com/index.php/journal/article/view/15

37. Lakshmi Rahul Reddy , Mareddy. (2026). Revisiting Autonomy in Artificial Intelligence through Agentic System Design. Journal of Computational Analysis and Applications (JoCAAA), 35(1), 707–713. https://eudoxuspress.com/index.php/pub/article/view/4780
38. **Mahendrakumar Kalal**, Lean-Driven SAP Production Planning Optimization Using Machine Learning for Inventory and Throughput Efficiency, Date of Conference: 19-20 March 2026, Date Added to IEEE Xplore: 08 April 2026,ISBN Information:,ISSN Information:
DOI: 10.1109/ISDFS69419.2026.11459029, https://ieeexplore.ieee.org/abstract/document/11459029
39. **Mahendra kumar Kalal**, SUPPLY CHAIN RESILIENCE THROUGH INTEGRATED SAP PRODUCTION PLANNING – PROCUREMENT SYNCHRONIZATION, Archives / Vol. 54 No. 1 (2026): January-March 2026 / Articles, https://pspac.info/index.php/dlbh/article/view/259
40. **Dr Manoj Goel (December 2018**). THE ATTITUDE OF DIFFERENT STATES STUDENTS TOWARDS PHYSICAL EDUCATION; STUDYING IN PHYSICAL EDUCATION COLLEGES OF MAHARSHTRA STATE, https://ijeponline.com/index.php/journal/article/view/965/847
41. **Ilakiya Ulaganathan, Tagore Engg. College, Anna University, Chennai, India, ; FNU Antara; Santhosh Chitraju Gopal Varma; Zokir Mamadiyarov; Ziyadulla Turayev, Published** in: 2025 International Conference on Sustainability, Innovation & Technology (ICSIT), Date of Conference: 22-23 August 2025, Date Added to IEEE Xplore: 19 December 2025, ISBN Information:
https://ieeexplore.ieee.org/document/11294748/references#references
42. **Shreyas Kasture, Sudhanshu Maurya, Amit Kumar Sharma, Santhosh Chitraju Gopal Varma, Kashish Mirza, Firdous Sadaf Mohammad Ismail, DOI**: http://doi.org/10.11591/ijai.v15.i2.pp1746-1761, IAES International Journal of Artificial Intelligence (IJ-AI), ISSN/e-ISSN 2089-4872/2252-8938
https://ijai.iaescore.com/index.php/IJAI/article/view/26932
43. **Shiv Shankar Dwivedi, Mr. Santosh Kumar Sharma,** Future-Proofing Data Security with Quantum-Resistant Cryptography, Vol. 11 No. 3 (2025): IJCESEN,
DOI: https://doi.org/10.22399/ijcesen.3447, https://ijcesen.com/index.php/ijcesen/article/view/3447
44. **Vijender Kalmotia,** Enhancing statistical accuracy in gene perturbation studies, Volume 266, August 2026, 105819, https://doi.org/10.1016/j.biosystems.2026.105819, https://www.sciencedirect.com/science/article/pii/S0303264726001292
45. **Naveen Undrathi,** Design and implementation of generative AI-driven data transformation pipelines using spring boot for scalable financial applications, eISSN: 2581-9615 || CODEN: WJARAI || Impact Factor 8.2 || CrossRef DOI, September 2026 (Volume 31, Issue 3),
DOI url: https://doi.org/10.30574/wjarr.2026.30.3.1629,
46. **Naveen Undrathi,** Agentic generative AI-enabled microservices framework for intelligent financial data processing in java-based enterprise systems, September 2026 (Volume 31, Issue 3), eISSN: 2581-9615 || CODEN: WJARAI || Impact Factor 8.2 ||
https://doi.org/10.30574/wjarr.2026.30.3.1628
47. **Akshay Jain,** Comparative Analysis of Linkage Methods in Hierarchical Clustering for Customer Segmentation, Conference paper, First Online: 07 October 2025,
https://link.springer.com/chapter/10.1007/978-981-96-7289-9_44

DOI: 10.46121/pspc.54.1.65

48. **Ismail Hossain,** Department of Computer Science, George Mason University, Fairfax, VA, USA, Mridul Banik, Department of Computer Science, Colorado State University, Fort Collins, CO, USA, https://ieeexplore.ieee.org/abstract/document/11446534
DOI: 10.1109/FMLDS67896.2025.00106
49. **Ismail Hossain, Mridul Banik , Fahmid Al Farid , Jia Uddin , Hezerul bin Abdul Karim** , Advancing Large Language Models for Low-Resource Languages: A Systematic Review of Pretraining, Adaptation, and Ethical Challenges, 10.32604/cmes.2026.075507, Date: 2026 https://www.sciencedirect.com/org/science/article/pii/S152614922600322X
50. **Ismail Hossain; Mridul Banik,** Bridging Visual and Linguistic Intelligence for Chest X-rays: A Comprehensive Review of ViTs and LLM Synergies, Published in: 2025 IEEE International Conference on Future Machine Learning and Data Science (FMLDS) Date of Conference: 02-05 November 2025, Date Added to IEEE Xplore: 25 March 2026, ISBN Information: https://ieeexplore.ieee.org/abstract/document/11446534
51. **Rifat Sarker Aoyon1, Ismail Hossain2, M. Abdullah-Al-Wadud3, Jia Uddin4,** A Secured and Continuously Developing Methodology for Breast Cancer Image Segmentation via U-Net Based Architecture and Distributed Data Training, https://www.sciopen.com/article/10.32604/cmes.2025.060917
52. **M. B. Vibha, M. Chandrika, Samitha Khaiyum & P. Rakshitha Kiran,** Predicting sedentary behavior in adults using stacked LSTM modeling, published: 27 November 2024 Volume 16, pages 346–355 (2025), https://link.springer.com/article/10.1007/s13198-024-02622-2
53. **Bellary Chiterki Anil, Jayasimha Sondekoppa Rajkumar, T. L. Divya, Samitha khaiyum Rakshitha Kiran P., Balakrishnan Ramadoss,** A Radiomics-based Framework for Liver Cancer Analysis using Explainable Artificial Intelligence (XAI) Methods, Vol. 15 No. 3 (2025): June, 2025, https://etasr.com/index.php/ETASR/article/view/10377
54. **Jayminkumar Patel, Sanjaykumar patel, Birju Patel, Rajan shah,** Development and Validation of a Stability-Indicating Analytical Method for Quantitative Determination of Selected Anticancer Drugs in Pharmaceutical Dosage Form, Archives / Vol. 35 No. S2 (2026): Apr-jun 2026, https://welltestingjournal.com/index.php/WT/article/view/288
55. **Jayminkumar Patel, Sanjaykumar patel, Birju Patel, Rajan shah**, Artificial Intelligence-Guided Optimization of Chromatographic Methods for Pharmaceutical Analytical Development, Archives / Vol. 35 No. S2 (2026): Apr-jun 2026, https://welltestingjournal.com/index.php/WT/article/view/294