International Journal of Emerging Trends in Computer Science and Information Technology
ISSN: 3050-9246 | https://doi.org/10.63282/3050-9246.IJETCSIT-V5I1P124
Eureka Vision Publication | Volume 5, Issue 1, 241-250, February- 2024

Original Article

Intelligent Access Control for Secure Financial Microservices Using AI-Driven Threat Detection and Risk Analytics

Dr. A. Rengarajan
Professor, School of Computer Science and Information Technology, Jain University, Bengaluru, India.

Abstract - Tackling distributed authentication, inter-service communication, untrusted APIs as well as the ever-evolving cyber threat and fraudulent transaction landscape are all major issues in today's financial application microservice era. The standard methodologies of controlling access – especially static RBAC – are not as contextually aware or flexible as necessary to safeguard the changing relationships among money. This study suggests an intelligent setup of an access control system that integrates Zero Trust Security (ZTS), Artificial Intelligence (AI) based threat detection, Dynamic Trust Assessment (DTA) and Financial Risk Analytics (FRA) to enhance the security of Financial microservices. All the above is covered in one security architecture and framework; ID verification, contextual authorization, API anomaly detection and behavior analysis and explainable risk assessment. Machine learning models are used to analyze the trends of API calls, service interactions across distributed systems, authentication events and behavior indicators of transactions to detect potentially malicious activity. A dynamic policy engine is then used to determine which ones are granted access for, depending on the risk assessment and vulnerabilities of the service and security context. Explainable AI mechanisms offer insight to authorisation decisions while privacy aware information sharing enables safe collaboration, of financial services dispersed at locations. A critical analysis of the proposed framework of architecture in terms of feasibility, scalability, robustness, interpretability and applicability to the operation is provided. To enhance the resilience and trustworthiness of financial microservice ecosystem, the concept of integrated security solution: intelligent threat detection & adaptive authorization and financial risk management is proposed in the article.

Keywords - Financial Microservices, Intelligent Access Control, Zero-Trust Security, Artificial Intelligence, Threat Detection, Risk Analytics, Explainable AI.

1. Introduction

1.1. Background and Research Motivation

Many Financial Services organisations have adopted Digital Change and subsequently, a number of innovative technologies have emerged such as Cloud Computing, distributed Application, Application Programming Interfaces (APIs) and Microservice Based Architectures. The back-end services that enable banking platforms, digital payment apps, mobile finance services, lending systems, and financial tech infrastructures to perform authentication, transaction processing, customer management, account verification, fraud monitoring and financial reporting are becoming more and more interconnected. Modularity, independent deployment, technological flexibility and horizontal scalability are the benefits of microservices. But these benefits raise security issues, as individual services are communicating via distributed networks and often execute in separate execution environments.

Microservice ecosystems consist of a large number of endpoints and ways to communicate, which are all accessible independently. Static authentication and authorization procedures may not be able to adapt quickly enough to user behavior change or compromised service identities or inconsistencies in the order of service invocation or new attack patterns.

Zero trust security can offer a much-needed first step towards overcoming these challenges. The idea is to assume nothing and no one can be trusted on an organization's network. Wang et al. discuss the dynamic access control with zero trust principles in [2] in which the contextual authorization and the continuous verification play important roles. Similarly, author [1] investigated the machine learning and game theory based trust based access control of microservices. With advances like this, access shouldn't be determined by a priori identity or permission, but should be determined ‘on the fly'.

1.2. Problem Statement

Different mechanisms commonly used to secure microservices typically view security as a functional issue, relating to authentication and authorization, vulnerability assessment and intrusion detection. Single solutions – offer some protection, but can be down time between operations. Then a trusted identity can carry out suspicious actions or a trusted service can be abused due to insecure dependencies or unusual communications in itself.

Traditional RBAC: is role is based on pre-defined roles in the organization. In structured authorization static roles are good, but can be inadequate in expressing the change of context. Similarly, tokens can be a powerful means of passing around identity, but aren't necessarily trustworthy throughout their lifespan, for a given request.

AI can detect abnormal patterns of API activity and network traffic, and recognize that something is amiss, but it doesn't necessarily mean an instant revocation of authorization. Financial fraud detection systems can be employed to identify suspicious transaction behaviour, however not all the output of such a system can be used to make service-level security decisions.

So, there is no consistent conceptual and semantic relationship between identity verification, dynamic assessment of trust, detection of threat with AI and financial risk analysis and adaptive access control on distributed financial microservices.

1.3. Research Gap and Objectives

There are considerable developments in the different security areas as seen in recent research. Their use in a coordinated architecture for decisions making remains a big research opportunity, however. When it comes to security, financial microservices should take into account the trustworthiness of the user identities, the vulnerability of the microservice, the impact of a compromised user identity, the nature of the microservice and the nature of the API.

The main goal of the present research is to come up with an intelligent access control system which includes ZT, threat detection with AI and financial risk analysis. To achieve this, the objective is to setup a continuously system for assessing the trust; detect any suspicious interaction between the services; compute a security threat assessing the transactions; and to consequently dynamically adjust access rights to the services.

One is to utilise the explainability aspects in the security decisioning process as well to allow financial security administrators to understand more about what factors are influential or not on the access decision. The modular deployability and scalability of distributed financial infrastructures with privacy aware information exchange, in particular, is also considered.

1.4. Research Contributions and Organization

The important thing doesn't not lie with that a model as two different security functions is proposed: threat detection and dynamic authorization; It lies with an integrated model. These include identity assessment in context, financial risk analysis, explainable decision support and adaptive policy enforcement, and trust assessment of services, and API behavioral intelligence.

It can also define a coordinated response to the further access decisions if there are anomalies affecting these. Let's get healthy and build a service behaviour and economic risk analysis where the ZTAPV (zero-trust authorization and perpetual verification) relevance applies.

A short review of related work is provided and feasibility study and limitation of the system, discussion about the implication of the proposed architectures, future study directions and the significance of the proposed architectures are provided respectively.

2. Related Work

2.1. Trust-Based Access Control in Microservices

In [1] author have proposed a microservice access control scheme based upon trust evaluation, machine learning based reward and punishment mechanism, GATAC. It is policy decision point and policy enforcement point to enable access decision to be made based on the trust characteristics that are assessed. The neural network based assessment and interaction oriented trust mechanisms are mobile and flexible versions of the static one. More attention needs to be paid, however, in the domain of the financial transactions of the fraud indicators, regulatory requirements and explainable financial risk decisions offered in those domains.

Wang et al. [2] mentioned the Zero Trust concept to implement Dynamic Access Control in cloud computing. They are not the same as the standard approaches adopted in distributed systems, since they are based on the concept of ongoing verification and context-aware authorization, instead of on the implicit trust of these. The paper is important in its efforts to move towards dynamic policies in financial microservices. Sometimes, however, it's not sufficient to allow access to the cloud and in the world of finance, financial transactions, service vulnerabilities and suspicious API traffic all play a role in determining who can access what.

Valavala [3] spoke about using the zero-trust approach with financial microservices, using default-deny authorization. It's not a trust approach for services in the network, it's permissions/restricted approach. It's a financial orientation and hence

pertinent to the present research. That's not a comprehensive financial risk assessment or a comprehensive behavior threat detection of a default/deny basis. The intelligent monitoring mechanisms are used as well the previous ones and as important development opportunities in this regard.

Authors [4] discussed the vulnerability of the service mesh architecture in terms of the trust in it. They consider the security problem comprehensively, in terms of vulnerabilities of 3rd party components or microservice vulnerabilities and they add the runtime vulnerability assessment to the trust assessment. However, in this contribution the reliability of such a service also has to be taken into account when deciding whether or not to grant the service (and not only the identity of the users). Absolute financial protection should be achieved, however, by means of a vulnerability focus trust assessment in the form of behavioral and transactional intelligence.

2.2. AI-Based Threat and Anomaly Detection

Researchers [5] proposed an anomaly detection solution based on a CNN for analysing the sequence of API calls. They use feature preprocessing, importance assessment of the APIs and customized neural-network architecture. The results demonstrate the value of sequence oriented analysis to find “unusual API behaviour”. But the idea of anomaly classification and of authorization enforcing is still distinct. I believe it would be a lot more operationally relevant to link to dynamically modifying permission the anomalies that are detected in the API.

To address the problem of anomaly detection of microservices, Author [6] proposed a hybrid approach of event sequences, called TraLogAnomaly. The research uses both inter-service and intra-service traces and functional anomaly search is performed based on sequence based search. The contribution is even more timely because suspicious activity may show up in multiple services in distributed financial applications rather than just a single service. However, the extent of the impact on the finances and the subsequent level of authorization shall not be assumed since identification of an anomaly at system level is not always the same as identification of a significant impact on the finances.

2.3. Financial Fraud Detection and Explainable AI

As for this, work [7] introduced an open framework to identify financial frauds by applying the extreme gradient boosting technique along with GP. They concentrate on the sort of fraud and simple to understand monetary indicators. It's useful as far as introducing the financial risk intelligence in security ops. If the suspicious financial activity identified is supposed to result in subsequent access decisions, though, the fraud classification should relate to the access decision for the service level.

Authors [8] shared their views related to Explainable AI: Federated Learning for Financial Fraud Detection in Banking. They are engaged in the co-operative fraud detection – information privacy and model transparency partnership with tireless efforts. Federated learning can be a major advantage in the context of telephone banking, or generally, in financial services, as the financial institutions may not be able to share the sensitive information of their respective customers. But, if you want to add distributed fraud intelligence and real time microservice authorization there are additional synchronizations in the stack to make.

Authors [9] studied the explainable ensemble learning for financial fraud detection in mobile money transactions. To explain models they make use of several learning algorithms in combination, promoting model transparency. Helps to understand the value of feature-level explanations in financial decision making. However, not-service API fraud not always equals transactional fraud detection – and not even necessarily fraud protection.

2.4. Intrusion Detection and Distributed Security Monitoring

Research work [10] created a benchmark, a methodology to create the dataset and case-studies to estimate IDS in microservice applications. They are used as a good framework for a systematic security analysis of distributed systems. However, benchmarking intrusion detection can't be enough to provide an integrated authorization system.

Work in [11] suggested a sequential deep learning approach to overcome the changing pattern of the attacks and the difficult detection situations. They note that, in order to perceive more complex forms of threatening networks, sequential intelligence has to be present. But the mapping of the network intrusion indicators to the service authorization indicators is still another requirement.

Authors [12] proposed two stage multi-source machine learning analysis to analyze attack techniques and attack life cycles. They stress the need for using more than one information source, and that more than just the individual traffic characteristics are important. This is relevant for financial microservices which can be attacked in various ways, including more than one service and sequential in operational activities. However, there's still more to come to make attack lifecycle information available to use for transaction sensitive authorization.

Researchers [13] suggested one hybrid approach which merges the distributed traces and profiling metrics together to detect anomalies as ServiceAnomaly. They're showing how to use executions traces to look into some measure that could be reflective of a service's performance and see if it is acting in a not-so-normal fashion. But there are also service anomalies that can be due to operational failures or malicious activities which would need to be interpreted in their context prior to restrictive security decisions.

Authors [14] presented in their discussion the real time anomaly detection of microservices based network of IoT using machine learning. They highlight the importance of the communication behaviour monitoring in a distributed environment and this behaviour is changing with time. Again, monitoring for distributed security can be achieved based on the monitoring principals, just in a different context - Application Context.

2.5. Token-Based and Role-Based Authorization

Work in [15] proposed access control mechanism which is based on token and separation between external authentication and internal authorization. They employ a distributed approach towards permission management, and validate the service level. It provides sufficient security to properly communicate between services. But, permanently “on the lookout” for behavioural variation can never be secured for token validation – nor for loss of trust in the services.

Work [16] talked about authentication and role based authorization in the performance driven microservices architecture. They speak regarding an authentication and authorization separation as well as handling partnerships in between roles and APIs. The solution offers suggestions for the architecture of a scalable Authorization Management. But static role-based rights are not enough to adapt to changing threats because of the lack of context.

All of these contribute to the foundations of dynamic authorization, vulnerability assessments, anomaly detection, financial fraud intelligence and XAI. The complementary fields should be combined by developing a motivating framework allowing for combining the influence of information about a person's behaviour, and information about financial risk, when making ongoing access decisions.

3. Proposed Framework: AI-Orchestrated Zero-Trust Access and Financial Risk Intelligence Architecture

3.1. Architectural Overview

We propose to come up with an integrated security architecture for financial applications that use distributed microservices. Its ultimate goal is to have one process that makes decisions for identity verification, threat detection, financial risk analytics, Trust assessments and adaptive authorization.

The six layers of architecture that operate are: identity and authentication management, contextual assessment of trust, monitoring service communications, AI-powered threat detection, financial risk intelligence, and adaptive policy enforcement. There's an explainability and audit capability that goes cross these layers, to make certain choices are clear and transparent, and affordable.

The frame work are centred around a Zero Trust strategy, where each time a significant access request occurs it is considered within the context of the validity of the identity, the access the identity is requesting, the state of the service itself, the behavior in the context, and the risk involved. The difference between authentication and authorization is that authentication is about asserting the identity of the requester whereas authorization is about deciding whether or not the requested operation is allowed in this security context. The proposed Intelligent Access Control framework is an integrated framework as depicted in figure 1, where all the components are working together: Identity Verification, Trust Assessment, AI based threat detection, financial risk analysis and Adaptive Access Policy Enforcement mechanism.

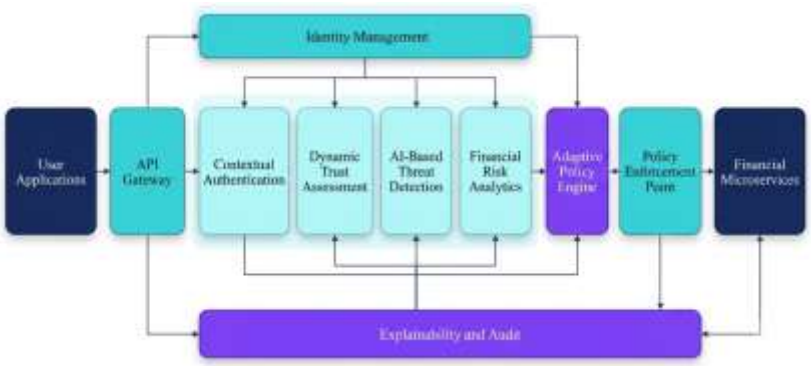


Figure 1. Integrated Architecture of Intelligent Access Control for Financial Microservices

3.2. Identity and Contextual Authentication Layer

The identities that the users, applications, devices or individual microservices use is the identity management layer. It supports safe authentication; it helps to verify services, validate credentials and credential lifecycle.

Each user logs in into his/her user identity system and each user/service logs in with a cryptographically secured user/service identity and short-lived credential. For the validation of the token the authenticity of the issuer, the integrity of the signature, the expiration and the restriction for the audience or revocation information if any is considered.

Moreover, some other context information is also considered including reliability of a device, type of a session, origin of a request, frequency of a request, history of previous requests known etc. These are other evidence for the trust assessment.

3.3. Dynamic Trust Assessment and Vulnerability Intelligence

This is the trust assessment module, which is used to check the trust worthiness of the requesting party and security status of the target services. It considers the past authentication, the flow of the communications between services, vulnerability data, API activity and past security incidents.

Vulnerability data is tapped from software composition analysis, dependency inventories, configuration assessments and runtime security monitoring. Should the service be still valid, but the access conditions not yet resolved for a service stricter access conditions can be applied.

This module extends the general idea of authorization, to the idea that the trustworthiness of a service can change over time, depending on the operational context or security context of the service provider. Figure 2 illustrates the continual trust assessment model, which considers the identity reliability, contextual attributes, behavioral consistency and vulnerabilities of services.



Figure 2. Dynamic Trust Assessment and Vulnerability Intelligence Model

3.4. AI-Driven Threat Detection and API Behavioral Analytics

Based on interaction with a specific service, series of API calls, authentication events and other network signals, the threat detection layer detects threats.

Sequence based learning – discovering the anomalies of known service communication sequence. It would be possible to build a convolutional network (CNN) or some other sequence learning system that could learn to identify a shift in calling behavior that would be indicative of a new caller type in the API. Using temporal models, request frequency change, ordering change and dependency change models of interactions can be modeled.

Distributed Tracing provides visibility into the flow of the requests in interdependent services. If monitoring app logs, and infra (from App-tier to Infra-tier), the information will be additive. These data can be correlated on the framework up to the individual anomaly and suspicious multi-service actism.

The Security incidents are categorized by the Detection Module according to Unusual access behaviour, Abnormal interaction with services, repeated failed pass-in authentications, suspicious sequences of requests and potential escalation of privileges and abnormal interaction with transactions.

Detection output does not imply that an attack is taking place, but is rather a sign of danger. This is necessary in case of a software crash, a maintenance, a change in website traffic or even legal changes in your business where unusual actions may

take place. These strings of service distribution and API calls then flow through the AI-powered threat detection pipeline which detects any unusual behavior or potential security threats in the system as illustrated in Figure 3.



Figure 3. AI-Driven Threat Detection and API Behavioral Analytics

3.5. Financial Risk Analytics and Fraud Intelligence

Financial risk analytics module recognizes and signals any questionable activity touching monetary activity. It looks at the characteristics of the transactions such as how often they occurred, the sums involved, whether there has been a shift in the beneficiaries of the transactions, how an account behaves, as well as whether there is any abnormality in the known pattern of a transaction.

An ensemble classification and gradient boosting and explainable feature attribution can be used to perform machine learning-based fraud detection. These methods can provide extra functions that identify any unusual behaviour and provide explanations of the attributes which can assist with risk assessments.

The framework is based on collaborative intelligence in a privacy-preserving fashion. Federated learning can allow the financial institutions to collectively develop a model without having to fully centralize the raw customer data.

There are controlled interfaces to get financial risk indicators to the policy decision mechanism. For example, if suspicious transaction behavior is suspected, it may require more verifying steps, limits on high-risk transactions and/or more closely monitoring the services of the transactions.

This means that although the financial fraud intelligence and access control are embedded in the module, financial fraud prediction and the final authorisation is still separate. A financial risk intelligence architecture consisting of transaction behaviour analysis, fraud classification using machine learning, explainable AI and federated learning with privacy awareness is summarised in figure 4.

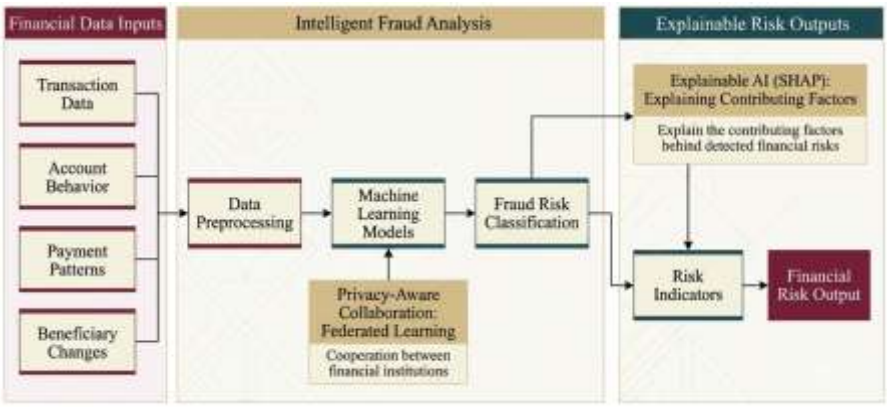


Figure 4. Financial Risk Analytics and Explainable Fraud Intelligence

3.6. Adaptive Policy Decision and Enforcement

The policy decision module, that aggregates the identity information with the trust and anomaly evaluation, vulnerability and financial risk information, makes the access decision.

The policy enforcement point is that entity which actually carries out some type of action due to the decision to take action on the requested action. Can be given, denied and/or restricted and/or validated based on conditions assessed.

The policy engine is not based on roles and can support for context-based authorization. Role/Attribute based policies also have a major role as they can provide a valid permission structure within the organisation. This smart risk assessment will dovetail with these policies, and not supplant simple authorisation.

If you have an authenticated service with credentials you can request payment services. If the service performs some other work it shouldn't, or it has some serious vulnerability that needs to be patched the policy engine can slowdown the work that the service is doing and make additional required demands for validation.

For instance, an authorized user logs into a financial account from an out-of-the ordinary place, and is asked to step up authentication when they want to transact at that account.

The enforcement layer can be utilized in policy expiry, tokens revocation, a layer of session restriction and a controlled recovery after a security event.

3.7. Operational Workflow and Integration Mechanisms

The framework starts by an API request made by a user or service. The identity management component is for verifying identity related credentials and to create the authenticated identity.

The policy engine then retrieves the appropriate authorization rules, and context information. Through the trust assessment module, behaviours are known and the monitoring components monitor the request, the requesting entity and the target service are assessed.

In addition, according to the applicative case, the modules of detection of threats and financial risk provide other indications. All these outputs are included in a contextual security assessment.

The policy engine then decides if the request meets mandatory authorization criteria and if there are further restrictions needed. The decision is made at the point of enforcement and the security evidence, to which the decision applies, is stored at the point of enforcement.

3.8. Expected Architectural Benefits

The overall design of the architecture will strive to minimize the amount of static permissions granted, to increase the context available for decisions to be made and to combine threat detection and security enforcement. It is modular and can be built to enable financial institutions to make strides in implementing certain features.

Financial Risk Intelligence can then be integrated with distributed monitoring to help make a more thorough security analysis possible. Explainable decision support helps to make administration transparent and service level trust assessment helps to mitigate some of the risk of potentially compromised or vulnerable internal components.

These benefits are architectural expectations or expectations that need to be implemented afterwards and validated empirically, but do not have a quantitative result.

4. Evidence-Based Framework Assessment: Architectural Feasibility and Security Assurance

4.1. Analytical Assessment Criteria

The architectural challenges of the consistency of the current microservice security practices and capabilities demonstrated in the literature are used to evaluate the proposed framework. Feasibility of integration along with contextual authorization, threat detection coverage and scalability, interpretability and operational limitations are considered.

This capability assessment is done on architectural suitability and literature. It does not presume that the integrated framework proposed has been embraced and experimented with in performance, an empirical way.

4.2. Feasibility and Practical Applicability

The proposed architecture major components are in line with existing infrastructure capabilities and, hence, with the existing financial microservice architectures. Integrates with identity providers, API gateways, service meshes, distributed tracing systems, ML platforms and security monitoring tools.

The existing authentication and authorization mechanism can be maintained and more and more modules of intelligence can be added. This helps to slow the rush to replacement of functional currency systems.

However, if integration is to be achieved, the events need to be in a standard format, service identities also need to be the same, and responsibilities of the monitoring and enforcement need to be well defined along with the policy interfaces, which need to be reliable.

But before making security decisions, considerations should be given to the impact they could have on the financial institutions' ability to process transactions.

4.3. Scalability and Operational Robustness

The deployment and scaling of the monitoring, trust assessment, financial risk analysis and financial policy enforcement components can be done independently because of the modular design. A distributed event processing (DEP) system can be scaled to process such service interactions when structured to meet the demands of the increasing number of service interactions.

Very similar to continuity monitoring is robustness which is a monitoring of validity of the model, secure communication and controlled behavior in the event of a component failure. Never turn off the security controls in the case of an AI module compromise or loss of the module.

At this point, deterministic authorization policies, fail-safe features, redundancy and controlled rollback are quite significant. If it is not possible to provide intelligent security services to critical financial operations, then explicit security restrictions should be maintained.

4.4. Interpretability, Privacy, and Governance

It's especially crucial when automated security decisions impact the financial business. Feature attribution records and decision records offer insight to the administrator on why access was denied or additional authentication is needed.

But, explainability does not mean correctness, fairness or regulation. Human oversight and documentation of outputs, and governance, is necessary.

4.5. Limitations of the Assessment

The proposed architecture is still in conceptual stage and was not fully developed. The effectiveness in practice would be influenced on the quality of implementation, the calibration of the model, representative operational data, integration overhead and institutional security policies.

False positives, knowledge of the evolving nature of attacks, lack of telemetry, differing service configurations, model drift and continuous analysis demands can all be obstacles.

For this reason, this framework of operational benefits is considered more like a design goal supported by studies and not actual operational benefits. It needs to be tested in the future by empirical studies, to show its effectiveness when applied under real economic workloads in adverse conditions.

5. Discussion: Convergence of Contextual Authorization and Financial Cyber Intelligence

The framework promotes that integration by acknowledging that service condition and identity are complementary sources of authorization intelligence and behavioral pattern and financial risk are other sources of authorization intelligence. This goes beyond zero trust security to incorporate continually changing operational evidence.

A key factor to note is that authentication/authorization is not risk prediction. Indicators and context will be provided through AI powered models, while explicit authorization rules will be provided through policy engine. This separation can allow them to prevent the results of the probabilistic models from affecting the financial security requirements.

But there's a compromise in the architecture as well. That's because the higher the number of monitors that will be deployed, the more infrastructure and data-management requirements will be, and the more security visibility will be. It may be beneficial to continually evaluate trust to enhance context based authorization as well as to add additional processing overhead. Similarly, tight restrictions to minimise exposure to suspicious activity can also affect the legitimate activity of their customers.

Explainable AI and audit mechanisms are thus crucial to ensure accountability of the institution. Evidence needs to be available for security administrators to use in deciding whether or not to make them restrictive and to start the required review processes.

6. Future Enhancements: Towards Autonomous and Privacy-Preserving Financial Security

6.1. Advanced Behavioral Intelligence

Some more advanced temporal learning for future work and graph based analysis of the behaviour of the co-ordinated attack from linked services might be investigated. User-department relationship, or user-app, user-API, user-transaction or user-microservice relationships can be represented using Graph learning. This could aid in determining suspicious relationships which may not be readily apparent from the event analysis alone.

Also there is model updating (controlled) which can be used for adaptation to change in service behavior and there is on-line learning. But, techniques that detect malicious manipulation and that detect model manipulation should also be continuously added to the continuous learning techniques.

6.2. Privacy-Preserving Collaborative Intelligence

Collaborative Financial threat detection can be done via federated learning with privacy-enhancing technologies. For example, future designs might look at secure aggregation, differential privacy and controlled model exchange, all to get better intelligence sharing and not putting sensitive customer information at risk.

Researches on common threat indicators' governance, and on models' and institutional liability for wrong or biased predictions are also needed.

6.3. Policy Automation and Resilient Enforcement

Future research could potentially be on policy automation techniques to be used to map validated threat indicators to controlled authorization updates. These safeguards include Approvals Processes, Policy versioning, Rollback functions and Clear protection of high value financial processes.

Further deployments will also have to consider how to integrate with a service mesh, to cache distributed policies, and also to have secure fallback options in the event of a partial failure of infrastructure, also token revocation.

6.4. Empirical Validation and Regulatory Alignment

One of the main research areas is realistic evaluation scenarios within the area of banking, digital payments and financial transaction processing. It is important to consider the integrated architecture in the future, along with the mature access control and threat detection architectures, and evaluation criteria should be defined.

Some of the most important metrics to take into account are false-positive rates, detection latency, authorization overhead, policy consistency, model drift, and operational resilience. The regulatory alignment should also take into account a data protection, auditability, explainability and institutional accountability.

7. Conclusion

The security requirements of financial institutions are not only the traditional ones to secure authentication and static authorization but with the increasing adoption of distributed microservice applications. To cope with the different changing operational conditions such as distributed communication, insecure service dependency, service behavior changes and complicated financial fraud scenarios, a coordinated security mechanism is needed.

In this research we have proposed a novel Zero Trust (ZT) access control model, which includes ID verification and dynamic trust assessment, Vulnerability Intelligence, API Anomaly Detection, Financial Risk Analytics, Explainable Decision Support and Adaptive Policy Enforcement. It offers the architecture to link the threat recognition and the authorization decision without changing the separation of the probabilistic threat and the mandatory access control policies.

One important innovation is the provision of a full conceptual model that brings together the various pieces of work which were developed in isolation, and allows for a full design of financial microservices' security. It also takes explainability and cooperation with privacy considerations and monitoring of the service level and operational resilience into account as design considerations.

The assessment is the core of the conceptual feasibility of the framework, which includes state of the art research on the topics of zero-trust security, anomaly detection of microservices, vulnerability-based trust and explainable financial fraud detection. However, the above mentioned proposed architecture has been yet not tested and quantitatively analysed. Hence whether it really works, is feasible and useful to detect a fraud is yet to be established in the real world or as it might be in some financial applications.

Directions for future research include prototypes development, realistic scenarios of financial security, integration and systematic empirical evaluation in a privacy preserving way. Within this proposed framework a validly validated and governed adaptive, transparent and resilient security infrastructure for next generation financial services could be possible.

References

[1] Li, Z., Du, X., Wu, X., Liu, A., & Wang, S. (2023). Trust-based access control and game-theoretic optimization for microservice architectures. *IEEE Transactions on Services Computing*, 16(5), 3410–3422. https://doi.org/10.1109/TSC.2023.3251204

[2] Wang, R., Li, C., Zhang, K., & Tu, B. (2023). Zero-trust dynamic access control framework for cloud computing environments. *Journal of Network and Computer Applications*, 211, Article 103550. https://doi.org/10.1016/j.jnca.2023.103550

[3] Valavala, S. K. (2023). Applying zero trust to financial microservices through default deny authorization. *International Journal of Engineering & Extended Technologies Research*, 5(3), 6627–6637.

[4] Alboqmi, R., & Gamble, R. F. (2022). Vulnerability-driven trust management for secure microservice mesh architectures. *IEEE Access*, 10, 89412–89425. https://doi.org/10.1109/ACCESS.2022.3199120

[5] Chang, J., Shi, L., Li, Z., Zuo, X., & Hou, B. (2023). Anomaly detection for API call sequences in microservices using convolutional neural networks. *Computers & Security*, 128, Article 103140. https://doi.org/10.1016/j.cose.2023.103140

[6] Wei, X., Sun, C.-A., Yang, P., Zhang, X.-Y., & Towey, D. (2023). Log-based anomaly detection in microservice systems using hybrid event sequences. *Journal of Systems and Software*, 201, Article 111680. https://doi.org/10.1016/j.jss.2023.111680

[7] Li, W., Liu, X., Su, J., & Cui, T. (2023). Transparent machine learning frameworks for effective financial fraud detection and risk management. *Expert Systems with Applications*, 215, Article 119342. https://doi.org/10.1016/j.eswa.2022.119342

[8] Aljunaid, S. K., Almheiri, S. J., Dawood, H., & Khan, M. A. (2023). Explainable federated learning for secure and transparent financial fraud detection. *IEEE Access*, 11, 45120–45135. https://doi.org/10.1109/ACCESS.2023.3271102

[9] Vijayanand, D., & Smrithy, G. S. (2023). Explainable ensemble learning models for fraud detection in mobile financial transactions. *Journal of Information Security and Applications*, 74, Article 103460. https://doi.org/10.1016/j.jisa.2023.103460

[10] Flora, J., & Antunes, N. (2023). Benchmarking intrusion detection systems for microservice applications: Datasets and evaluation methodologies. *Software: Practice and Experience*, 53(8), 1625–1648. https://doi.org/10.1002/spe.3205

[11] Hore, S., Ghadermazi, J., Shah, A., & Bastian, N. D. (2023). A robust deep learning sequential framework for network intrusion detection. *Journal of Information Security and Applications*, 72, Article 103395. https://doi.org/10.1016/j.jisa.2022.103395

[12] Lin, Y.-D., Yang, S.-Y., Sudyana, ـ., Yudha, F., Lai, Y.-C., & Hwang, R.-H. (2022). Multi-datasource machine learning for attack lifecycle and technique detection in enterprise networks. *IEEE Transactions on Network and Service Management*, 19(4), 4820–4834. https://doi.org/10.1109/TNSM.2022.3198754

[13] Panahandeh, M., Hamou-Lhadj, A., Hamdaqa, M., & Miller, J. (2023). Distributed tracing and performance metrics for microservice anomaly detection. *IEEE Transactions on Reliability*, 72(2), 789–803. https://doi.org/10.1109/TR.2022.3218931

[14] Plazas Olaya, M. K., Vergara Tejada, J. A., & Aedo Cobo, J. E. (2022). Real-time machine learning anomaly detection for securing microservices-based IoT architectures. *Security and Communication Networks*, 2022, Article 5849120. https://doi.org/10.1155/2022/5849120

[15] Venčkauskas, A., Kukta, D., Grigaliūnas, Š., & Brūzgienė, R. (2023). Enhancing microservices security with token-based access control method. *Sensors*, 23(6), Article 3363. https://doi.org/10.3390/s23063363

[16] Al-Wadi, R. A., & Maaita, A. A. (2023). Authentication and role-based authorization in microservice architecture: A generic performance-centric design. *Journal of Advances in Information Technology*, 14(4), 758–768. https://doi.org/10.12720/jait.14.4.758-768