International Journal on Science and Technology (IJSAT)
E-ISSN: 2229-7677 ● Website: www.ijsat.org ● Email: editor@ijsat.org

Context-Aware Federated Learning for Regulatory Risk Assessment in Financial Applications

Sri Rama Chandra Charan Teja Tadi

Lead Software Developer
Nueve Solutions LLC

Abstract

Federated learning facilitates model training scaling in distributed financial systems with data locality and regulatory compliance. Context-awareness integration increases model flexibility in terms of jurisdictional rules, transactional semantics, and user-level risk indicators. In the design of contemporary banking and finance applications, this integration can be facilitated by the modularity of services, secure APIs, and client-side execution patterns supportive of enterprise-class infrastructure. Context metadata, including time-stamped milestones, geographic compliance stamps, and activity signals, provides robustness to regional inference and facilitates global model convergence. Dynamic aggregation processes and adaptable participation mechanisms further enhance system flexibility and performance. The final product is an interpretive, privacy-aware regulatory risk assessment model deployable in institutionally segmented systems in real time.

Keywords: Federated Learning, Context Awareness, Regulatory Compliance, Risk Assessment, Financial Systems, Client-Side Execution, Secure Aggregation, Distributed Modeling

1. Federated Learning Architectures for Financial Applications

Federated learning (FL) offers a great evolution in strategy to financial institutions for data processing and risk management. FL enables the training of a model on multiple decentralized data sources with the guarantee of data privacy, which is appropriate for the stringent regulatory compliance in the banking industry. With this decentralized model architecture, organizations can train machine learning models cooperatively without even sharing individual customer information directly with each other. For example, the use of privacy-protecting federated learning methods specifically designed to detect financial transaction fraud has been outlined, emphasizing model selection via local gradient values from individual banks [1]. The design optimizes model performance with shared knowledge while maintaining privacy requirements, a key factor to obtain regulatory regimes.

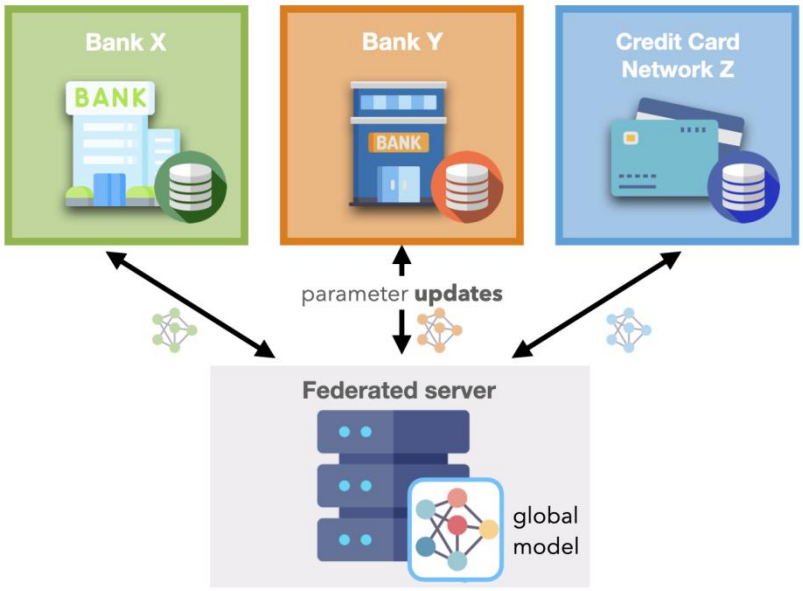

Figure 1: A workflow of an inter-company federated learning use case in Banking
Source: Adapted from [21]

In addition, the introduction of federated learning into traditional banking culture can facilitate a multi-tenant data atmosphere that can strengthen cooperation between financial institutions within a data localisation setting. It is useful mainly because it can make several stakeholders, including regulators and banks, share collective knowledge when dealing with fraud detection or risk measurement without making confidentiality lose meaning in terms of independent datasets. The incorporation of context-aware federated learning makes this approach even more robust by adding contextual metadata, which facilitates comprehension of jurisdictional subtleties and user-specific risk profiles [4]. This adaptive architecture can be utilized by financial institutions to meet various regulatory demands and improve predictive accuracies in financial transaction monitoring [18].

Moreover, the scalability that federated learning provides for financial use cases is critical to sustaining the boom data culture in banking, whose assets have grown from $25 trillion in 2000 to approximately $124 trillion in 2020 [4]. With institutions going ahead and implementing digital banking platforms, leveraging federated learning structures enables them to continuously evolve their risk evaluation modules with the aid of gigantic transaction data sets that are inherently time-sensitive in scope. Using dynamic aggregation techniques for model parameter tuning based on observations from local data, financial institutions can enable real-time support of their strategic positions against dynamically changing threats while maintaining compliance with established regulatory environments intended to mitigate risk [10]. Concisely, federated learning systems are a game-changing solution to the financial sector by integrating model sharing among disseminated data stores, addressing the needs of privacy, and inducing collective efforts toward the field of risk assessment. The incorporation of contextual metadata in such systems improves the resilience of models as well as facilitates alignment to various regulation requirements, hence making these finance systems robust and adaptive to the changing risk landscapes.

Figure 2: Advantages of Federated Learning

Source: Adapted from [22]

2. Contextual Adaptation to Regulatory and Transactional Signals

Regulatory and contextual adaptation of federated learning models plays a crucial role in creating effective risk assessment mechanisms for financial applications. Contextual adaptation ensures the use of appropriate data that mirrors transactional behavior, user trends, and regulatory environments to improve model performance and readability. Imbibing local context enables financial institutions to ensure their risk assessment models strongly adhere to jurisdictional regulations and client-specific risk features. The application of distributed computing in federated learning architectures has been seen to assist banks in handling compliance cost-effectively while at the same time setting up responses to varied risk scenarios [11].

Following its origin back to what is essentially an adaptive process is contextual metadata such as date-stamped milestones, geographic flags of compliance, and transaction-associated activity signals. Any fact about the context can dramatically boost model performance through enabling the model to acquire regulatory compliance subtleties and the monetary behavior of a desired set of user segments. For example, user-level risk indicators that identify individual transaction volumes can be imbued in learning algorithms to provide for customized risk assessment output. This tailored flexibility also reflects the complexity of real-life financial transactions, in which tendencies might be determined by market need and tailor-made client profiles [4][3].

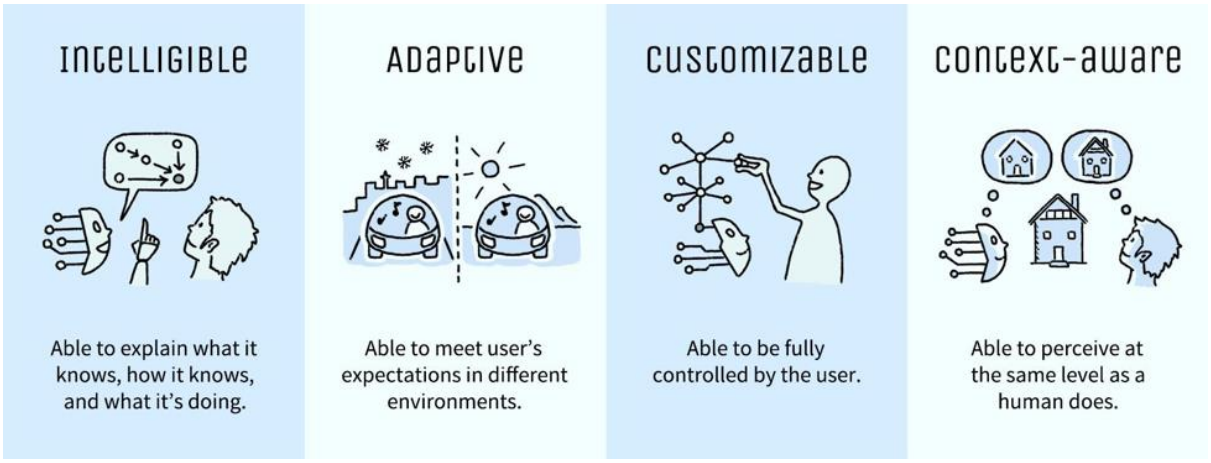

Figure 3: Pillars of Contextual AI

Source: Adapted from [23]

Moreover, compliance in financial services is on the move; thus, adaptable capabilities are more relevant. In response to changing regulatory environments, federated formats within federated learning networks might flex dynamically under the change of demand of regulation or transaction complexities. With that, institutions are capable of fixing compliance gaps ahead of time. This is of utmost importance in the context of more regulation faced by banking institutions around the world and the necessity for real-time monitoring systems capable of leveraging cutting-edge machine learning approaches to avoid the risk inherent in financial transactions [10]. Through the introduction of contextual adaptation along with federated architectures, richer interpretability and faster responsiveness in models of risk analysis are achievable.

In addition, the use of rule-awareness in adaptation at the context level also facilitates the straightforward integration of customary compliance rules in model operations. Such functionalities may provide insights about which transactions could possibly result in alerts against regulatory thresholds, enabling the institutions to move quickly towards dealing with prospective risks. Beginning a rule-based approach with machine learning methods provides end-to-end knowledge of risk contexts in different jurisdictions as well as a user-friendly interface for financial institutions [10][12]. Overall, context adaptation in federated learning frameworks enables the timeliness and responsiveness of financial institutions to regulatory cues and altered patterns of users' transaction behavior. By using local context and rule-awareness in combination, these systems promote more stringent compliance, allowing institutions to successfully navigate the regulatory environment while improving their risk-assessment processes.

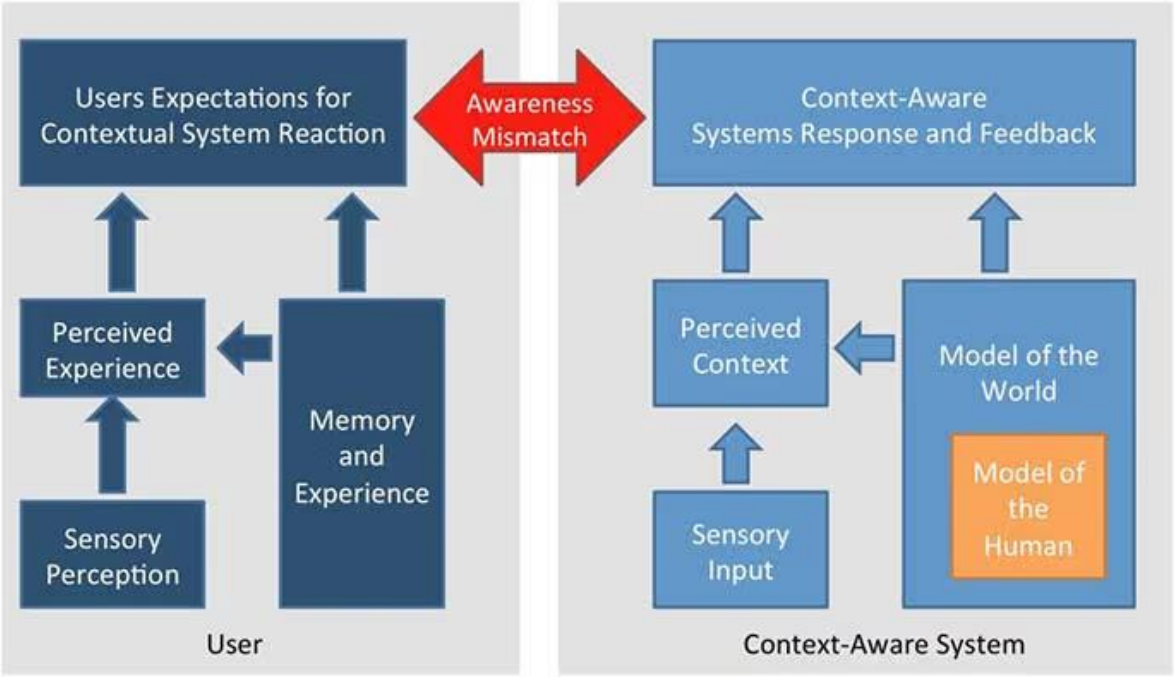

Figure 4: User-System Interaction in Context-Aware Computing

Source: Adapted from [24]

3. Modular Service Composition in Risk-Aware Systems

The use of modular service architectures has become more and more critical to the creation of scalable, maintainable risk assessment platforms in financial applications. With a modular design enabled by APIs and microservices, interoperability is improved, and financial institutions can better respond to changing regulatory environments and market conditions. With applications broken down into separate, manageable pieces, organizations can gain more flexibility in constructing, deploying, and maintaining risk management systems [17]. Such modularity allows incrementally adding sophisticated functionality, as financial institutions are able to respond quickly to the evolving compliance issues or risk dimensions due to varying regulations or changing customer needs [4].

APIs have an essential role within such modular architecture, serving to act as bridging elements between different service constituents so that communication is seamless. They enable heterogeneous systems, like CRM applications and analytics engines, to interact in real time, hence facilitating improved data sharing and operational alignment. This feature is specifically useful in risk assessment processes where prompt access to various data sources is crucial. For instance, in anti-money laundering (AML) activities, APIs can retrieve the transaction records from different databases to build broad client behavior profiles and improve the precision of risk assessment [11]. The availability of microservices also allows institutions to introduce individual risk management features as independent components, which can be scaled or altered without affecting the overall structure.

Also, modular service composition will assist greatly with maintainability because groups are in a position to develop autonomous segments without affecting the entire system. The independent development of these components ensures optimal efficiency in implementing upgrades, patches, and

regulatory modifications. Financial institutions face significant pressure to maintain compliance; therefore, the ability to segment and host individual compliance-related services enables them to keep their systems current and fully aligned with regulatory mandates. Modular composition, in turn, not only streamlines processes but also improves system reliability and resilience to unexpected risk.

Furthermore, the composition of services as modular blocks puts institutions in a good position to leverage their risk monitoring capability. By applying statistical operations and machine learning algorithms as interchangeable analytics modules, banks can execute real-time monitoring of transactions scripted to address exacting regulatory requirements [9]. Such granularity allows for distinct identification of anomalies or fraudulent activities, along with compliance, and safeguards the organization from reputation loss [3]. The module-based integration of analytics to respond to local data inputs renders risk assessment context-aware and effective in an environment where financial transactions become increasingly complex and multi-dimensional. Modular service composition as a whole provides financial institutions with a powerful tool to enhance their risk management systems. By leveraging APIs and microservices, organizations can create scalable architecture, enhance maintainability, and add specialized risk management functions that react to compliance needs. This strategic solution enables financial institutions to remain agile, responsive, and well-placed to meet the dynamic regulatory challenges they encounter in the current financial landscape.

4. Client-Side Execution Frameworks for Local Model Training

The use of client-side execution frameworks for local model training represents a foundational shift in how financial applications analyze data and evaluate risk. The frameworks support the real-time processing of data, and the machine learning model runs on the users' devices, such as desktops, mobile devices, or browsers. By conducting inference and model training on the device, financial institutions are able to keep sensitive user data on-device, which is all the more valuable as a result of strict data privacy regulations such as the GDPR. Client-side execution not only ensures user trust but also enables institutions to react to regulatory requirements that call for data minimization [4][11].

The on-device execution of machine learning models facilitates diverse operations in financial apps. For example, on-device machine learning can be employed for risk evaluations done at transaction time. When a user initiates a transaction, the local model is able to inspect the transaction features against past behavior patterns and define regulatory thresholds. This enables real-time feedback to the user, e.g., alerts or compliance messages, hence providing a level of security and reactivity demanded in high-risk financial environments [3]. Moreover, this feature minimizes dependency on continuous connectivity to central servers for security reasons, hence improving user experience and performance, particularly in scenarios where internet connectivity is slow or unreliable.

Secondly, client-side execution platforms enable one to easily imagine the idea of federated learning in which models are training in parallel on various data locally but in a manner that maintains privacy. User devices may mimic interactions on context-specific data while adding up to a global model [20]. This decentralized architecture permits the derivation of useful patterns out of aggregated neighborhood knowledge without any loss of the anonymity of data at the level of individuals, thus preserving rules of compliance while improving the overall risk assessment model performance [10][19]. Client-side computation is the decentralization component supporting personalized banking experience, which

dynamically adjusts itself in accordance with specific financial behavior and risk profiles of users based upon context information present on their systems.

In addition, client-side runtime platforms play a vital role in implementing policies and controls at the time of service delivery. Client-side runtime platforms are able to modify the risk assessment thresholds dynamically based on real-time user behavior or external regulatory modifications. For example, if a new compliance rule is implemented that requires more stringent assessment criteria for specific types of transactions, the client-side runtime can instantly apply these modifications without requiring the total redesign of central systems. This adaptability allows financial companies to stay in compliance ahead of time and stay within the limits of changing regulatory environments [13].

Overall, client-side execution frameworks are a key factor in the success of financial applications for local model training and inference. With on-device computation, financial companies can improve user experience, optimize operational efficiency, and keep up with changing regulations. The integration of local computation with federated learning principles enables a secure platform for financial services personalization that doesn't compromise sensitive user information. Ultimately, these technologies place financial institutions on a level playing field in a time of aggressive regulatory oversight and increased customer expectations.

5. Integration of Temporal, Spatial, and Behavioral Context

The incorporation of metadata like temporal, spatial, and behavioral context in risk assessment models improves accuracy as well as interpretability. Temporal context is the incorporation of time-stamped information to understand the temporal dynamics of financial behavior and transactions. It is necessary for the detection of timing-dependent anomalies, like unusual spikes in volumes of transactions during non-peak hours or pattern disruption in certain economic events. It has been established that timely information, if recorded and analyzed properly, can provide rich insights into customers' behavior and transaction feasibility, thus contributing greatly to credit risk decisions [8]. Advanced temporal analytics allow financial institutions to draw meaningful insights that inform their decision-making.

Spatial context is also a key element that, when added, increases the accuracy of risk judgments. Geographic location influences other such things as market tendencies, regulatory needs, and even sociopolitical risk. Spatial analysis enables financial institutions to make their risk management more location-based. User behavior can be compared to the past experience of similar areas so that the risk approximation becomes sophisticated with an eye toward localized forces of economics as well as consumer behavior. Spatial modeling enables one to identify possible dangers through tensions and geopolitical or domestic market instability [13]. As such, financial institutions can institute focused interventions to keep risks geographically isolated.

Contextual behavior, like patterns in user behavior, habits in outlay, and transactional history, adds precision to models. It enables the personalized measuring of risk in response to individual user characteristics, which is more critical in an era of tailored financial services. By monitoring behavioral signals, banks are able to recognize anomalies indicative of fraud or another risk before such become substantial concerns. Proactiveness of this nature can form a cornerstone for loss prevention, compliance, and customer confidence-building [5]. Further, with the combination of behavioral data and

temporal and spatial contexts, richer datasets are obtained, which enhance model training protocols and make them more adaptable and predictive.

In addition, since federated learning systems perform better when decentralized clients are cooperative, integrating those various contexts enables the creation of models that can learn from local data never exchanged, with no privacy loss. Integrating temporal, spatial, and behavioral contexts helps financial institutions take advantage of information from individual user data without losing the individuality of such data, within acceptable regulatory limits [6]. This integrated comprehension guarantees that models will react not just to the threat but also to forecast and anticipate threats in the assessment. In general, incorporating temporal, spatial, and behavioral contexts into risk assessment models makes them more accurate and interpretable to a great degree. Such dimensions of context allow financial institutions to best fit their risk management policies, thereby contributing to better decision-making abilities. It develops resiliency to upcoming and emerging threats while enhancing compliance and customer relationships via customized services.

6. Secure Update Propagation and Aggregation Mechanisms

Secure update propagation and aggregation operations are essential to the integrity and reliability of federated learning systems, particularly in finance, where regulatory compliance and data sensitivity are of high value. The effectiveness of such operations depends on how securely the operations can be shared around encrypted on distributed nodes and remain synchronized and consistent throughout the aggregation process. Since financial institutions deal with confidential information, the utilization of strong encryption techniques during update transfer is the most important part of intellectual property protection and customer information defense against encroachment [16].

The mechanism starts with every customer device keeping local model updates after training on their respective data sets. These updates, including perhaps gradients or the model's weights, are subsequently encrypted such that even if intercepted, the information would be useless to unauthorized users. Through the use of encryption methods like homomorphic encryption or secure multi-party computation (MPC), clients can compute and share computations without unveiling sensitive information to the central server or other clients, providing strong privacy guarantees within a federated learning system and thus satisfying regulation demands [7].

After preparing the encrypted updates, they are sent to the central server to be aggregated. The server's function here is to aggregate data from a number of clients to improve the global model without ever seeing individual datasets. This has to be accompanied by advanced aggregation algorithms that are able to process and merge the encrypted updates in an efficient manner to correctly represent the collective learning from diverse data sources. Methods like Federated Averaging (FedAvg) are usually utilized for computing model parameters as an average over the received updates from the clients that participate to ensure that the resultant global model still represents all the participating datasets [6].

Alignment at the aggregation step is highlighted as observed with heterogeneous models produced by heterogeneous environments. The system needs to be developed in federated learning architecture that can tackle system heterogeneity so that the updates are cohesive irrespective of having varying data distribution among various clients [15]. It is necessary not only for performance but also to ensure fairness in the process when users from varying populations are engaged in federated learning. Having

processes that account for contribution from every update with regard to local model performance can increase risk assessment systems' robustness in real-time contexts.

To summarize, solid update propagation and aggregation methods make up the foundation of fruitful federated learning operations in the finance sector. Protecting the encryption of updates sent, as well as their aggregation, allows banks and other financial organizations to create robust machine learning algorithms that firmly shield user data while meeting strong requirements for regulatory compliance. This secure framework becomes pivotal to user and stakeholder trust, as well as opening innovation in banking and financial products to innovation.

7. Cross-Institution Deployment of Privacy-Preserving Risk Models

Deploying privacy-fair risk models across financial institutions involves crossing intricate terrains of data silos, compliance zones, and organizational boundaries. Financial institutions are typically in data silo environments with intricate compliance demands and organizational policies governing the usage and access of the data. Federated learning models represent a very appropriate solution under such a scenario because they facilitate collaboration across institutions while subjecting individual data to strict privacy and security measures [14]. The models were trained under federated configurations whereby institutions can apply collective learning insight without directly divulging sensitive data, thereby keeping the integrity and confidentiality of an institution's data intact.

To be specific, cross-institution deployment enables collective risk models based on contextual information from diverse data sources, therefore enabling more substantial risk assessment potential. For example, companies can exchange historical transaction information highlighting customer trends and associated risks of different financial products without compromising geographical and compliance needs. This greatly improves the strength of models learned from heterogeneous data without compromising the sovereignty of sensitive data [11]. With financial institutions putting more emphasis on collaboration to fight fraud and enhance risk management, privacy-preserving federated models are a key go-between that is institutionally aware but enables cooperative progress in risk evaluation.

Furthermore, the success of cross-institutional deployments also depends significantly on good governance mechanisms that provide assurance of compliance with regulatory frameworks. Legislative data protection laws like GDPR in the EU or CCPA in California require institutions to do regular audits on data-sharing behaviors [2]. Aware of such regulations, financial institutions adopting federated learning can have well-defined contractual agreements for when and where data may be utilized, thereby aligning risks and rewards accordingly. Moreover, technologies such as secure multiparty computation (MPC) or differential privacy can be incorporated into the training phases of models in a way that learning derived from collaborations does not violate the data privacy of individual institutions [15].

Practically, the deployment of these models is done by setting up secure communication channels through which model updates are sent by institutions without exposing data to leaks or breaches. Secure transmission ensures that the sensitive customer data is not revealed during the model update process, safeguarding the integrity of the respective organizations and customer privacy. The institutions should have technology solutions in place that allow secure communication, updating, and review procedures used on an ongoing basis to support future vulnerabilities [8]. Besides, companies can utilize new-generation cryptography techniques like lattice-based cryptography or homomorphic cryptography in a

bid to guarantee security while carrying out collaborative modeling activities. Generally, the cross-institutional adoption of privacy-preserving risk models in financial applications offers a framework to augment risk management processes without being in violation of regulatory standards. Harmonization with the possibility of not disclosing confidential information is notably important in ensuring innovation, considering the advent of new threats to the financial system. By offering secure and compliant collaboration, organizations are able to optimize their risk assessment processes and tap into collective intelligence in order to stay ahead of emerging risks.

8. Operationalizing Regulatory Risk Intelligence at Scale

When banks implement regulatory risk intelligence at scale, there are a number of crucial points to take into account, such as monitoring, compliance verification, model refreshing, and system scalability as a whole. Maintaining processes under real-time observation is critical to discovering upcoming risks, regulation conformity, and precision in forecasts of risk. Real-time monitoring controls can cause institutions to respond to anomalies or deviations in real-time so that they can respond quickly to mitigate risks, such as by modelled adjustments or by exploring anomalous patterns of transactions [15].

Compliance validation must be integrated at every operational level within risk intelligence systems. Institutions should have strong validation processes in place that guarantee that models are consistent with regulation, including auditing the output of analytics, transaction logging, and monitoring the performance of models against defined compliance measures. Clear mechanisms for reporting help to convey risk analysis and position of compliance properly to stakeholders so that governance obligations are met. Systematic checks for model soundness and regulatory compliance with changing regulations guarantee that institutions not only keep pace with current compliance needs but also keep up with changing regulatory issues.

The fine-tuning of the model is crucial for reacting and performing in a business environment. When there is a financial application, information and regulatory contexts are always changing and require constant fine-tuning and updating of risk models using new data. A periodic refresh mechanism includes automatic model retraining on the basis of new inputs of data as well as continuous feedback from surveillance systems. Dynamic management of models ensures that risk analysis is current and in line with the prevailing market environment as well as regulatory requirements [7].

Operationalizing regulatory risk intelligence also has scalability at its core. Risk assessment system architecture has to scale at a fast rate to support increased volumes of data and users without affecting performance. Microservices and cloud computing facilitate financial institutions to scale their compute power on demand and introduce more functionalities as and when required. In addition, the application of a service-based modular architecture enables scalability, such that organizations are able to introduce or replace modules independently based on business needs [13].

For financial institutions and banks to effectively implement regulatory risk intelligence, they need to have a collaborative and improvement-oriented culture in which intelligence gathered from risk analysis is used to inform strategic decision-making and operational processes. The harmonious integration of all the components - monitoring, compliance verification, model refreshment, and scalability - utilizes technology to enable organizations to respond effectively to regulatory issues while preserving sound risk management practices. Finally, winning at scaling regulatory risk intelligence is about having strong

systems, processes, and a collaborative culture grounded firmly in the institution. Through a focus on continuous monitoring, verification of compliance, model maintenance in a flexible manner, and scalability, financial institutions are able to create a firm foundation that encourages effective risk management, enabling compliance with applicable regulations while being flexible in the presence of the complexities of the financial environment.

9. Conclusion

In conclusion, the use of context-aware federated learning models in financial systems presents a revolutionary solution for regulatory risk analysis, which helps institutions navigate successfully through the complexities of contemporary financial environments while strictly following compliance guidelines. With the use of modular service compositions, client-side execution environments, and integration of temporal, spatial, and behavioral context, organizations can develop robust, responsive risk assessment models that adapt to the fast-changing market circumstances and regulatory requirements. In addition, crossing institutional boundaries with privacy-preserving risk models facilitates cooperative risk management while maintaining data security. As the financial institutions deploy these systems in volume, ongoing monitoring, compliance verification, and model updating based on new threats will be key to sustaining resilience and agility in responding to emerging threats. This end-to-end approach not only builds the accuracy and interpretability of risk models but also enhances trust and transparency among stakeholders, ultimately resulting in more resilient and robust financial ecosystems. The continued evolution of federated learning and risk intelligence promises a brighter future, one where organizations are better able to defend their assets, stay in compliance with the law, and treat their customers well in an increasingly complex regulatory landscape.

10. References

[1] S. Kanamori et al., "Privacy-preserving federated learning for detecting fraudulent financial transactions in Japanese banks." [Online]. Available: https://doi.org/10.2197/ipsjjip.30.789

[2] Q. Yang et al., "Federated machine learning: concept and applications." [Online]. Available: https://doi.org/10.48550/arxiv.1902.04885

[3] W. Du et al., "Fairness-aware agnostic federated learning." [Online]. Available: https://doi.org/10.48550/arxiv.2010.05057

[4] M. Jiao, "Big data analytics for anti-money laundering compliance in the banking industry." [Online]. Available: https://doi.org/10.54097/hset.v49i.8522

[5] E. Alotaibi, "Risk assessment using predictive analytics." [Online]. Available: https://doi.org/10.26668/businessreview/2023.v8i5.1723

[6] K. Hu et al., "Federated learning: a distributed shared machine learning method." [Online]. Available: https://doi.org/10.1155/2021/8261663

[7] M. Ersai, "Research on risk management and risk prevention measures of internet financial." [Online]. Available: https://doi.org/10.23977/ferm.2023.061008

[8] D. Mhlanga, "Financial inclusion in emerging economies: the application of machine learning and artificial intelligence in credit risk assessment." [Online]. Available: https://doi.org/10.3390/ijfs9030039

[9] M. Lokanan and V. Maddhesia, "Predicting suspicious money laundering transactions using machine learning algorithms." [Online]. Available: https://doi.org/10.21203/rs.3.rs-2530874/v1

[10] C. Singh, "Artificial intelligence and deep learning: considerations for financial institutions for compliance with the regulatory burden in the United Kingdom." [Online]. Available: https://doi.org/10.1108/jfc-01-2023-0011
[11] A. Shende, "Leveraging distributed computing for enhanced risk management and compliance in banking: a pathway to financial success." [Online]. Available: https://doi.org/10.47363/jaicc/2022(1)199
[12] Y. Sun and J. Li, "Deep learning for intelligent assessment of financial investment risk prediction." [Online]. Available: https://doi.org/10.1155/2022/3062566
[13] Z. Ji et al., "Computation offloading for edge-assisted federated learning." [Online]. Available: https://doi.org/10.1109/tvt.2021.3098022
[14] Z. Gao et al., "A method for improving the robustness of federal learning systems based on input transformation." [Online]. Available: https://doi.org/10.1117/12.2661042
[15] S. Bharati et al., "Federated learning: applications, challenges and future directions." [Online]. Available: https://doi.org/10.3233/his-220006
[16] K. Wakil and D. N.A., "Extracting the features of modern web applications based on web engineering methods." [Online]. Available: https://doi.org/10.14569/ijacsa.2019.0100209
[17] H. Supriati and H. Supriatna, "Designing a web-based credit application information system." [Online]. Available: https://doi.org/10.55208/jeme.v1i1.93
[18] L. Vasconcelos et al., "An approach to support the construction of adaptive web applications." [Online]. Available: https://doi.org/10.1108/ijwis-12-2018-0089
[19] S. Yasin and S. Ismail, "A review on fault taxonomies for web testing." [Online]. Available: https://doi.org/10.30534/ijeter/2020/2681.22020
[20] M. Joo and W. Lee, "Webprofiler: user interaction prediction framework for web applications." [Online]. Available: https://doi.org/10.1109/access.2019.2949077
[21] A. Brundyn, E. Scoullos, and D. Williams, "Using Federated Learning to Bridge Data Silos in Financial Services," *NVIDIA Developer Blog*, 2022. [Online]. Available: https://developer.nvidia.com/blog/using-federated-learning-to-bridge-data-silos-in-financial-services/
[22] L. Wrobel, "Federated Learning – Efficient Machine Learning That Respects Privacy?" *cc-bei.news*, 2022. [Online]. Available: https://cc-bei.news/en/federated-learning-efficient-machine-learning-that-respects-privacy/
[23] O. Brdiczka, "Contextual AI: The next frontier of artificial intelligence," *Digiday*, 2019. [Online]. Available: https://digiday.com/sponsored/adobesbl-contextual-ai-the-next-frontier-of-artificial-intelligence/
[24] A. Schmidt, "Context-Aware Computing," *The Encyclopedia of Human-Computer Interaction*, 2nd ed., Interaction Design Foundation, 2014. [Online]. Available: https://www.interaction-design.org/literature/book/the-encyclopedia-of-human-computer-interaction-2nd-ed/context-aware-computing-context-awareness-context-aware-user-interfaces-and-implicit-interaction