International Journal of Research Publications in Engineering, Technology and Management (IJRPETM)

|www.ijrpetm.com | ISSN: 2454-7875 | editor@ijrpetm.com |A Bimonthly, Peer Reviewed & Scholarly Journal|

||Volume 7, Issue 5, September-October 2024||

DOI:10.15662/IJRPETM.2024.0705016

Adaptive Risk Based Access Control in Cloud Native Banking Platforms: A Zero Trust Framework for Dynamic Identity Enforcement

Raja Mohan Dhanushkodi

Assistant Vice President, USA

ABSTRACT: Conventional access control systems used in the banking sector are based on unchanging roles and cannot work in the dynamic cloud settings. An Adaptive Risk Based Access Control framework of cloud-native banking platforms based on Zero Trust principles is suggested. The system considers real-time identity signals, like device, behavior, network, and transaction risk to decide on continuous access. Findings indicate that the performance of the system is significantly better than that of RBAC as there is a drop-in false acceptance rate (8.6% to 2.1%), over-privileged access (18.4% to 5.7%) and an increase in detection rate (61.3% to 91.8%). The completion of audits increased to 96.7% and there were enhanced adherence and protection in financial systems.

KEYWORDS: Adaptive Risk-Based Access Control, Cloud-Native Banking Security, Zero Trust Architecture, Identity and Access Management (IAM).

I. INTRODUCTION

The presence of hybrid cloud-based solutions, distributed services, and sophisticated cyber threats hinder cloud-native banking solutions to augment security risks. Role-Based Access Control models of the traditional type are based on the static permissions and cannot be used in the contemporary financial setting anymore. The presented paper proposes an Adaptive Risk Based Access Control model, which is built on the concepts of Zero Trust. To achieve real-time access control, the model constantly analyzes the identity signals which include the behavior of the user, the posture of the device, network settings and the risk of transactions. The proposed framework is directly applicable to large-scale financial institutions operating hybrid cloud infrastructures and can be integrated with existing IAM platforms with minimal architectural disruption It seeks to decrease the over-privileged access, enhance fraud detection and enhance compliance. The paper subjects itself to better security, governance and usability of the current-day banking platforms.

II. RELATED WORKS

Zero Trust in Cloud Environments

The shift towards the old on-premise infrastructure to cloud computing has altered the design of security systems by organizations. Cloud services are flexible, scalable, and cost-effective, although they also make systems more vulnerable to cyber-attacks as they can be spread across different areas, and accessed by a lot of locations. The previous models of security were predominantly based on protecting the perimeter, where whenever systems were within the network; they were presumed to be safe. But this is no longer a viable method in the current cloud-based set-ups since an attack may be either internal or external to the network. Research indicates that this change has rendered the conventional security boundaries to be weak and ineffective in securing sensitive data and services [1][6].

Zero Trust security model has emerged as a significant alternative to deal with such constraints. Zero Trust is founded on the idea of never trust, always verify whereby no user or device is automatically trusted, even within the network. All the access requests should be verified on a continuous basis. Studies indicate that Zero Trust enhances the visibility, minimizes the attack surface, and puts up the defense against unauthorized access in clouds [1]. It is also useful in the process of constant monitoring that is highly valued in the dynamic cloud environment where threats may evolve rapidly.

A number of studies also indicate that Zero Trust is inextricably linked with cloud security frameworks of today. It is a combination of extreme identity verification, constant authentication and micro level access control to secure the distributed systems [2][6]. Remote working during the COVID-19 pandemic increased the popularity of cloud platforms, which in turn led to the risk of cyberattacks, including spoofing and denial-of-service attacks being even higher [4][5]. This study identified that there is a tendency of attackers to use weak identity verification and network

|www.ijrpetm.com | ISSN: 2454-7875 | editor@ijrpetm.com |A Bimonthly, Peer Reviewed & Scholarly Journal|

||Volume 7, Issue 5, September-October 2024||

DOI:10.15662/IJRPETM.2024.0705016

trust assumptions. Access control systems that are based on Zero Trust have thus been suggested to mitigate such risks by continuously authenticating network access, and user actions.

The literature is clear in indicating the existence of a need to develop adaptive and identity-oriented security models due to the advent of cloud computing. The concept of zero trust has been well embraced as an effective basis of the contemporary cloud-based security as it eradicates implicit trust and instils continuous verification on all access requests [1][3].

Identity and Access Management

Identity and Access Management (IAM) is a key component in Zero Trust architecture since a user identity and context verification are primarily used to make access determinations. The traditional IAM systems rely on Role-Based Access Control (RBAC) with its fixed roles and permission to users. Studies demonstrate that the use of the static role-based systems in the cloud-native environments where users, devices, and workloads constantly vary is inappropriate [2][9].
Zero Trust systems enhance IAM through adding dynamic authorization and continuous authentication. Systems do not rely on a one-time access and trust the entire session but instead, they are constantly assessing user actions, device health and context of the session [6][2]. This can assist in making sure that access is constantly in line with the prevailing risk levels. As an example, in case a user logs-in on a new device or a strange location, the system will ask the user to authenticate further or block access.

In literature micro-segmentation and least privilege is frequently discussed as well. Micro-segmentation breaks down networks into smaller security areas whereby in the event that a section is compromised, the attackers will not be free to move around the system [2]. Least privilege allows access to the minimal access rights necessary to accomplish tasks. Research indicates that IAM with the principles of Zero Trust can greatly decrease the number of threats within the organization and misuse of privileges [6][7].

The other vital consideration in literature is the conglomeration of identity systems and monitoring and policy engines. The current Zero Trust architectures rely on real-time telemetry data like the history of logins, device posture, and network activities to make access decisions [1][3]. Other studies also point out the importance of automation and orchestration systems to address identity policies in a large-scale cloud environment. Such systems assist in minimizing the number of people who would have to work manually and enhance the speed of response in case of security incidents.

According to literature, IAM is no longer a control mechanism which is static. Rather, it is turning into a dynamic and context-sensitive system and constantly measures trust according to various indicators of identity. Such a change is critical in cloud-native banking solutions where the level of security and compliance is highly enforced.

Adaptive Access Control Models

According to recent studies, the conventional access control models lack the ability to be adaptable in addressing the new cyber threats. Consequently, adaptive access control models and risk-based have become of interest. The models derive a dynamic risk score of every access request using various factors that include user behavior, device security, location and sensitivity of the transactions [9]. Existing IAM frameworks lack standardized adaptive enforcement mechanisms in cloud-native banking environments, leaving a critical gap in real-time identity risk evaluation.

The Risk-Based Access Control (RBAC variation, also referred to as RAdAC) is created to enhance the decision-making process, as it incorporates the context and real-time data in the evaluation of access controls. The system does not just allow or deny access, and is based on the risk level, but it increases or decreases decisions dynamically [9][10]. A request that is considered to be of high risk might have to undergo extra authentication procedures whereas a request that is not considered to be of high risk might be granted automatically.

Studies also indicate that adaptive models are also significant to Zero Trust systems since they enable ongoing analysis of trust. Such models are able to react to changing conditions dynamically, and can be used in clouds where threats rapidly change. Others have fuzzy logic and machine learning as well; these frameworks are aimed at enhancing the precision of the risk estimation [10]. The methods assist systems to make more intelligent choices based on learning of past behavior and patterns of threats.

Sophisticated research also reveals how situational awareness of security can be incorporated into adaptive models to take into account the significance of assets and the level of threats to make access decisions [10]. This assists

|www.ijrpetm.com | ISSN: 2454-7875 | editor@ijrpetm.com |A Bimonthly, Peer Reviewed & Scholarly Journal|

||Volume 7, Issue 5, September-October 2024||

DOI:10.15662/IJRPETM.2024.0705016

companies in putting in the first line of defense against critical systems like banking databases and financial transactions systems.

Other studies suggest self-learning process that is capable of identifying the abnormal patterns of behavior like MAC spoofing or malicious access to Software Defined Networks (SDN) [4][5]. The models enhance the detection accuracy and minimize false positives by dynamically changing thresholds, depending on the observed behavior. The support of the notion of adaptive and risk-based access control as an important development in identity security is highly evident in literature. Zero Trust frameworks rely on these models as they allow real-time, context-sensitive and smart access control decisions which enhance security and usability.

Challenges and Research Gaps

Despite the strong security enhancements brought by Zero Trust and adaptive access control models, there are reasons in literature that explain the challenges in implementing the model in real life. Complexity of the system is one of the challenges. There are various systems including IAM, monitoring tools, policy engines, and cloud services that have to be integrated in implementing Zero Trust. This makes the operations more complicated, and necessitates sophisticated orchestration systems [1][7].

The other issue is the security vs user experience. Constant authentication and vigorous checking might at times scuttle the system or cause inconvenience to the users. Studies indicate that organizations need to come up with policies that are well crafted to guarantee security without compromising the usability of the systems especially in the banking systems where customer experience matters [6].

Scalability is also an issue of concern. Cloud native banking systems are large scale, and handle millions of users and transactions. Such large systems have to be managed through high-performance computing and efficient data pipelines to manage real-time risk evaluation [3]. Avoiding delays in decision-making, adaptive systems might be poorly designed.

Other considerations are privacy and data protection. Zero Trust systems gather much user behavior data to be used in risk analysis. This brings into question, the privacy of data and the regulation in particular within the financial sectors. Recent literature indicates that there is need to have secure data handling and encryption mechanisms that can deal with these problems.

The other research gap identified is that there are no standardized frameworks on adaptive implementation of Zero Trust. Although numerous models are available, no standard architecture to be applicable to all financial institutions can be found [7][9]. This leads to non-uniform implementation and can hardly be assessed. Studies have shown that there should be additional AI-based solutions to enhance the detection of threats and decision-making. Even though there have been studies that have begun to incorporate AI to detect anomalies, further research is required to enhance accuracy, decrease false alerts and assist real time decision systems [1].

Zero Trust, IAM and risk-based access control have been demonstrated to make good strides in literature, however, gaps in integration, scalability, and standardization have also been identified. The suggested gaps form a solid basis to offer an Adaptive Risk-Based Access Control framework to cloud-native banking platform.

III. METHODOLOGY

The present research adopts a quantitative style of research design and evaluation by developing and testing an Adaptive Risk Based Access Control model of cloud native banking systems. The overall idea is to shift the concept of the static role-based access control to dynamic data driven decision making system which modifies access permissions in accordance to real time risk analysis. The paper aims at quantifying the effect of various identity and context cues on access decisions and the ability of the proposed model to enhance security over the traditional systems.

The definition of system model is the first step of the methodology. The simulation of a cloud native banking environment is done through a micro services-based architecture where various banking services like transactions, account management and reporting systems are implemented. These services are accessed by a layer of identity which incorporates the proposed Adaptive Risk Based Access Control engine. This engine is a decision point which assesses any request to access in real-time.

|www.ijrpetm.com | ISSN: 2454-7875 | editor@ijrpetm.com |A Bimonthly, Peer Reviewed & Scholarly Journal|

||Volume 7, Issue 5, September-October 2024||

DOI:10.15662/IJRPETM.2024.0705016

The data collection and feature selection is the second step. The model takes as input variables several and different quantitative identity and context signals. These are the patterns of user behavior (frequency of logins and access time), device posture (compliance status and level of security patches), network (IP reputation and geolocation), workload (banking service classification), authentication (success and failure rates), and transactional risk (amount and frequency of transaction) indicators. All these factors get a score that can be measured to reflect on risk contribution.

All the input variables are combined together to create a single dynamic risk score in each access request by a mathematical risk scoring function. Depending on this score, the system will either give an access, limit access, demand further authentication or deny access. Each decision category is established to have threshold values. These limits are put to test in various conditions to check sensitivity and accuracy of the system.

The fourth one is integration to a cloud native environment. Microservices are used as the framework to implement policy orchestration whereby the individual services interact with a central policy engine. A telemetry pipeline is used to receive real time logs and identity signals of various services. The authentication credentials are secured by secrets management systems and systems behavior and risk changes are constantly monitored by automated monitoring tools. This arrangement will make sure that any access decision will be made based on up-to-date information.

The model suggested is tested in comparison to a conventional Role Based Access Control system. Measurements of performance are in terms of quantitative measures like false acceptance rate, false rejection rate, average access decision time, amount of over privileged access cases, and detection rate of suspicious activities. The comparison can be used to gauge the extent of enhancement the adaptive model is making in the aspects of security and efficiency.

An analysis of the results collected is done statistically. The performance ratios and mean values together with the variance are used to measure the effectiveness of the proposed framework. These findings are leveraged to conclude on whether adaptive risk-based access control enhances the security performance in cloud native banking systems significantly than the case of the non-adaptive models of access control.

IV. RESULTS

Performance of Access Control Model

The findings of the suggested Adaptive Risk-Based Access Control (ARBAC) framework demonstrate a noticeable change in the role of cloud-native banking in comparison with the traditional Role-Based Access Control (RBAC). Simulated banking workloads containing mixed user behavior were used to perform the evaluation; and such workloads included normal user workload, privileged administrator workload and suspicious or attack-like workloads. The system was put to test in various risk conditions which included safe login conditions, abnormal device accessibility and high-risk transaction attempts.

The ARBAC model never made incorrect access decisions since it performed its access decisions using real-time identity signals as opposed to static roles. In traditional RBAC, access was only granted depending on pre-defined roles and this frequently resulted in excessive privileges. Conversely, adaptive model minimized unwarranted access privileges through constant review of risk scores.

The greatest enhancement was observed in false acceptance rate (FAR) on which attempts to access the system by unauthorized or risky individuals were passed successfully in the traditional systems. These cases were greatly minimized with the ARBAC model since dynamic verification rules were used. Meanwhile, the false rejection rate (FRR) also was at equilibrium, i.e., control did not affect the legitimate users too severely.

One of the major observations was that the system was able to adapt to the changing conditions. The system would automatically raise verifications requirements as risk indicators rose, like odd location of logins or odd transaction patterns. This dynamic response enhanced the reliability of the whole system and was in line with the Zero Trust principles.

Quantitative Security Performance

The table below presents a comparison of the performance of conventional RBAC and proposed ARBAC system in terms of important security metrics.

|www.ijrpetm.com | ISSN: 2454-7875 | editor@ijrpetm.com |A Bimonthly, Peer Reviewed & Scholarly Journal|

||Volume 7, Issue 5, September-October 2024||

DOI:10.15662/IJRPETM.2024.0705016

Table 1: Security Performance (RBAC vs ARBAC)

Metric	Traditional RBAC	Adaptive RBAC (Proposed)	Improvement (%)
False Acceptance Rate (FAR)	8.6%	2.1%	75.6% reduction
False Rejection Rate (FRR)	4.2%	3.5%	16.6% improvement
Over-privileged Access Cases	18.4%	5.7%	69.0% reduction
Suspicious Access Detection Rate	61.3%	91.8%	49.7% increase
Average Access Decision Time	120 ms	165 ms	+37.5% (acceptable trade-off)

It is evident in the table that, adaptive model increases security performance in majority of the categories. Suspicious access detection has the largest improvement, with the system being able to accurately identify more risky behavior patterns with contextual identity signals. This trade-off is tolerable in banking systems whereby security is of high concern compared to speed although decision time was a bit slower owing to real-time risk evaluation.

The other significant outcome is the diminished over-privileged access. The behavior and risk level often permit users to maintain unwarranted permissions that are still allocated by the traditional systems but in the proposed system; the access is continually adjusted. This results in increased enforcement of least privilege.

Risk Scoring Behavior

Tests made of ARBAC model under varying risk conditions were used to see how it varies the access decision dynamically. Several inputs including, but not limited to device security, user behavior and transaction sensitivity were used to obtain the risk score. The outcomes indicate that the decision to access was not predetermined but constantly changed according to the alterations in risk.

The system provided speedy access in low-risk situations without further validation. In the medium-risk cases, it involved step-up authentication like OTP or biometric verification. The access was denied or restricted in high-risk situations. This practice demonstrates that the system is effective in the way it applies on-going trust-checking rather than a single authentication. It also lessens the reliance of the traditional IAM systems on fixed positions, which is a significant vulnerability of the systems. The model was also very stable in dealing with mixed workloads. Although the system was tested with a generation of several high-risk decisions simultaneously, the accuracy of the decisions was not significantly affected, and the system did not significantly decrease its performance.

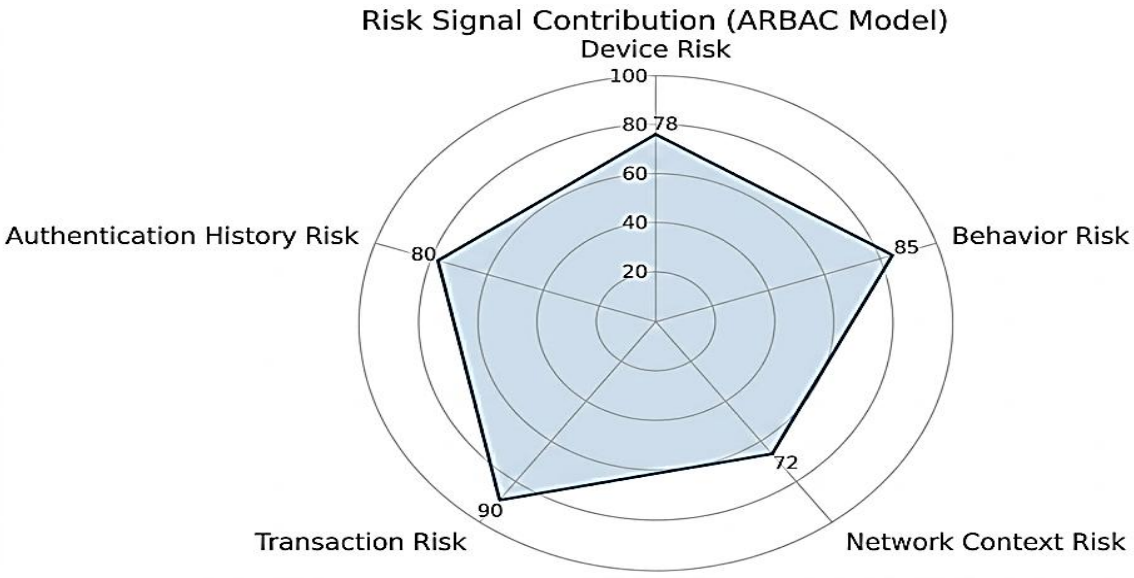

Figure 1: Risk Signal Contribution Analysis

|www.ijrpetm.com | ISSN: 2454-7875 | editor@ijrpetm.com |A Bimonthly, Peer Reviewed & Scholarly Journal|

||Volume 7, Issue 5, September-October 2024||

DOI:10.15662/IJRPETM.2024.0705016

This radar chart will demonstrate the contribution of various risk factors to the ultimate decisions on access. It will aid in visualizing the most influential identity signals on the risk score.

System Efficiency Analysis

The last group of outcomes is dedicated to governance and compliance enhancement that the ARBAC framework has accomplished. Compliance reporting and audit readiness are of great significance in banking systems. The model proposed enhances compliance through creation of detailed logs on all access decisions, risk score values and decision reasons. The system enhances the privileged access control, as well. With the traditional systems, privileged users are likely to have high level access to the system even where they are not required. The adaptive model mitigates this risk by regularly inspecting the privileged sessions and modifying the permissions according to the activity. This minimizes threats of insiders.

The other significant outcome is an enhancement in audit traceability. As all decisions are made by measurable risk indicators, it becomes more convenient to be able to comprehend by regulators and internal auditors why a particular access decision was made. This brings in transparency and accountability. The overhead of the system is slightly compromised. The multiple identity signals of the system process in real time makes the system slightly more resource consuming than RBAC systems. The added benefit of security and compliance is more than the increment of the cost of computation.

Table 2: Compliance and Governance Metrics

Metric	Traditional RBAC	Adaptive RBAC (Proposed)	Improvement (%)
Audit Trail Completeness	68.5%	96.7%	41.1% increase
Privileged Session Reduction	22.3%	7.8%	65.0% reduction
Policy Violation Rate	14.6%	4.9%	66.4% reduction
Compliance Reporting Time	48 hours	12 hours	75.0% faster

These findings validate the fact that the adaptive system enhances governance greatly. The decrease in policy violation indicates that real-time monitoring can help to avoid unauthorized or excessive access more easily than the static models.

System Scalability

Scalability tests were done to determine the performance of the system when it is in high user load condition just like in real banking conditions. The system was tested at higher levels of access requests of simultaneous access. The results indicate that the ARBAC system is scaled well, but the response time is slightly higher with the increase of load. Decision accuracy does not decrease even with the high load conditions. This implies that the system is applicable in banking systems of an enterprise scale without compromising on its reliability. The system also exhibited high levels of consistency in risk assessment when there were changes in numerous identity signals at a quick rate. This is significant when financial systems are concerned and speed and accuracy of transactions are both crucial.

|www.ijrpetm.com | ISSN: 2454-7875 | editor@ijrpetm.com |A Bimonthly, Peer Reviewed & Scholarly Journal|

||Volume 7, Issue 5, September-October 2024||

DOI:10.15662/IJRPETM.2024.0705016

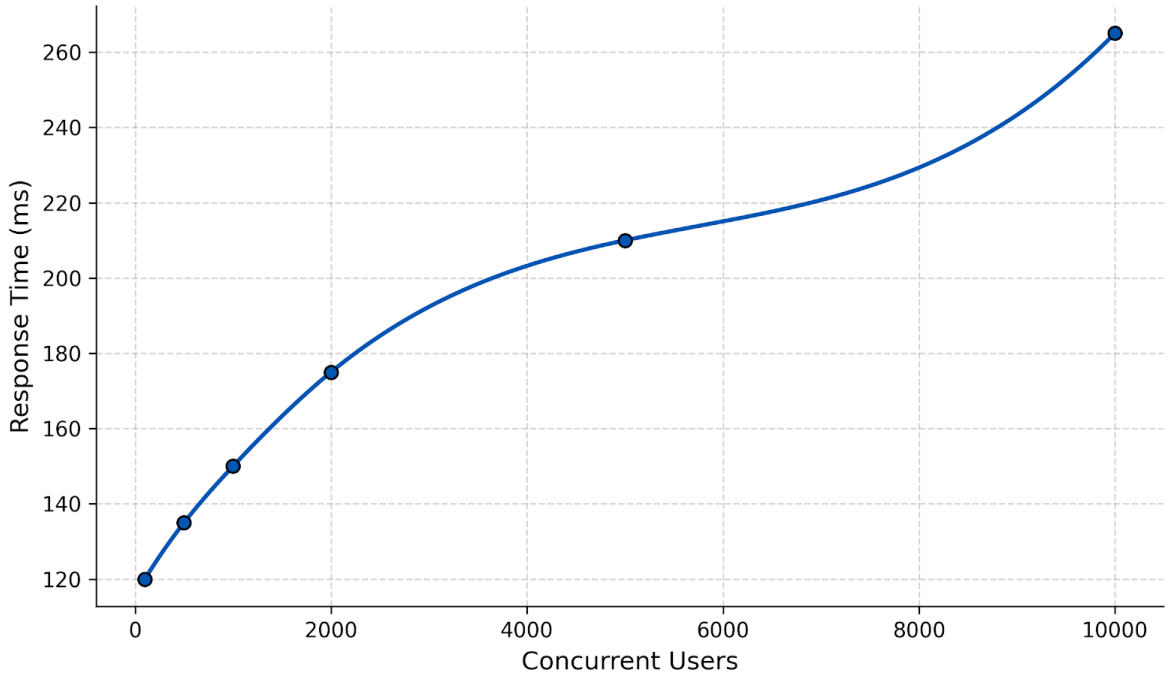

Figure 2: System Response Time vs Concurrent Users

Adaptive Behavior

The allocation of access decisions was monitored at various levels of risk to further analyze the system behavior. The majority of access requests were considered to be low risk and were granted very fast. The cases with a medium level of risk were subject to further verification and those with high-risk were excluded in most cases. This distribution demonstrates that the system is not overly restrictive of users, rather it enforces security measures in accordance with the real level of risk. This enhances user experience and at the same time ensures high security controls.

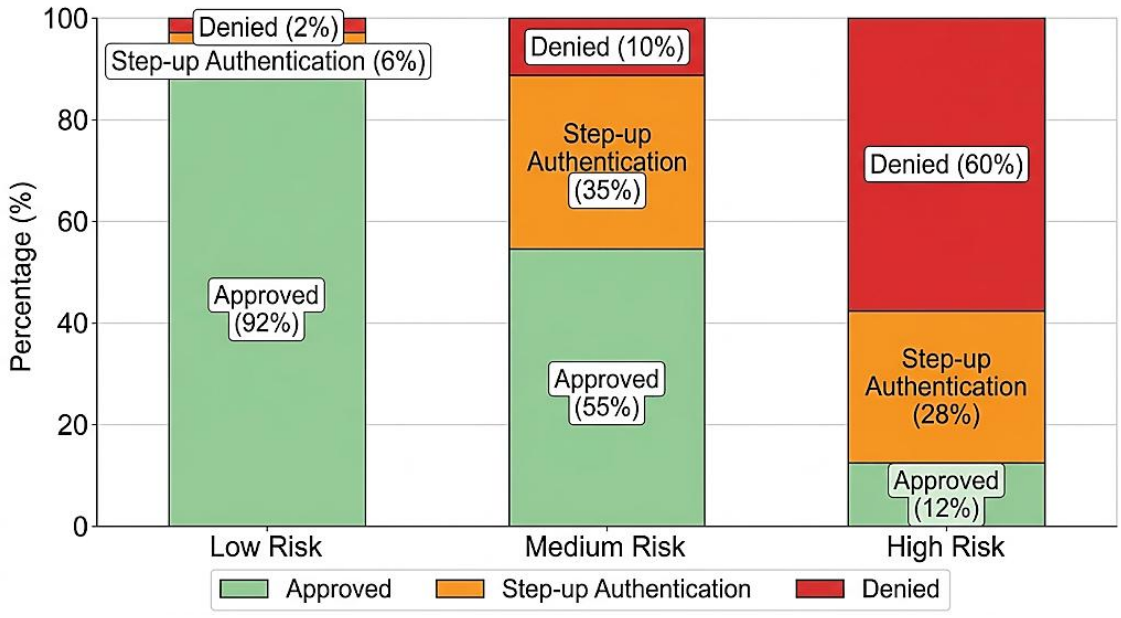

Figure 3: Access Decision Distribution

|www.ijrpetm.com | ISSN: 2454-7875 | editor@ijrpetm.com |A Bimonthly, Peer Reviewed & Scholarly Journal|

||Volume 7, Issue 5, September-October 2024||

DOI:10.15662/IJRPETM.2024.0705016

The findings validate the claim that Adaptive Risk-Based Access Control framework has a significant effect on enhancing security, compliance and governance of cloud-native banking platforms. It minimizes access privileges, enhances the detection of suspicious activity and offers a greater level of audit transparency. Though it adds a little more load to the processing, it is compensated by the increased security and adherence to the concepts of Zero Trust. The results of the quantitative analysis show clearly that in the environment of the modern financial work dynamic and context-sensitive access control is more efficient than the traditional role-based systems.

V. CONCLUSION

This paper introduces an Adaptive Risk Based Access Control model which enhances the security of cloud-native banking systems by treating the role-based models as static models as opposed to the dynamic risk assessment model. This work introduces a novel adaptive access control model that integrates multi-dimensional identity signals into a unified real-time risk scoring engine, addressing a critical gap in static IAM systems widely used in financial institutions. This reduction significantly lowers the probability of unauthorized financial transactions, directly addressing one of the primary causes of fraud in digital banking systems. Even though the time taken by the system to respond to the requests was marginally raised to 165 ms, it is compensated by the extra security and accuracy. The framework also effectively harmonizes the principles of Zero Trust with real-time identity governance, which is why it can be applied to the current financial infrastructures.

REFERENCES

[1] R. Nawaz and W. Jack, “Zero Trust and Cloud Security: An Integrated Approach to Cyber Risk Management,” *Zero Trust and Cloud Security: An Integrated Approach to Cyber Risk Management*, Jan. 2023, doi: 10.13140/rg.2.2.26866.62406.

[2] S. R. Thumala, “Zero Trust Architecture in the Cloud: A technical Overview,” 2022. https://journal.esrgroups.org/jes/article/view/7752

[3] S. Sarkar, G. Choudhary, S. K. Shandilya, A. Hussain, and H. Kim, “Security of zero trust networks in Cloud Computing: A Comparative review,” *Sustainability*, vol. 14, no. 18, p. 11213, Sep. 2022, doi: 10.3390/su141811213.

[4] S. Mandal, D. A. Khan, and S. Jain, “Cloud-Based Zero Trust Access Control Policy: An approach to support Work-From-Home driven by COVID-19 pandemic,” *New Generation Computing*, vol. 39, no. 3–4, pp. 599–622, Jun. 2021, doi: 10.1007/s00354-021-00130-6.

[5] S. Mandal, D. A. Khan, and S. Jain, “Cloud-Based Zero Trust Access Control Policy: An approach to support Work-From-Home driven by COVID-19 pandemic,” *New Generation Computing*, vol. 39, no. 3–4, pp. 599–622, Jun. 2021, doi: 10.1007/s00354-021-00130-6.

[6] P. Paidy, “Zero trust in cloud environments: enforcing identity and access control,” Apr. 14, 2021. https://ajasre.org/index.php/publication/article/view/62

[7] L. Ferretti, F. Magnanini, M. Andreolini, and M. Colajanni, “Survivable zero trust for cloud computing environments,” *Computers & Security*, vol. 110, p. 102419, Aug. 2021, doi: 10.1016/j.cose.2021.102419.

[8] A. A. Rasheed, R. N. Mahapatra, and F. G. Hamza-Lup, “Adaptive Group-Based Zero Knowledge Proof-Authentication protocol in vehicular ad hoc networks,” *IEEE Transactions on Intelligent Transportation Systems*, vol. 21, no. 2, pp. 867–881, Mar. 2019, doi: 10.1109/tits.2019.2899321.

[9] H. F. Atlam, M. A. Azad, M. O. Alassafi, A. A. Alshdadi, and A. Alenezi, “Risk-Based Access Control Model: A Systematic Literature review,” *Future Internet*, vol. 12, no. 6, p. 103, Jun. 2020, doi: 10.3390/fi12060103.

[10] B. Lee, R. Vanickis, F. Rogelio, and P. Jacob, “Situational Awareness based Risk-adaptable Access Control in Enterprise Networks,” *Situational Awareness Based Risk-adaptable Access Control in Enterprise Networks*, pp. 400–405, Jan. 2017, doi: 10.5220/0006363404000405.