Published by :
https://www.ijert.org/
An International Peer-Reviewed Journal

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 05 , May - 2026

Secure Data Governance and Adaptive Access Control in Cloud Environments

Mr. Deshmukh Harshad Mangesh
Department of Computer Engineering
Vishwabharti Academy's College of Engineering, Sarola Baddi, Ahilyanagar, 414304

Mr. Tathe S. G.
Department of Computer Engineering
Vishwabharti Academy's college of Engineering, Sarola Baddi, Ahilyanagar, 414304

Abstract **- By delivering scalable storage, real-time synchronisation, and remote data access, cloud computing has grown to be a necessary component of contemporary digital systems. Because of its real-time database, authentication, and serverless capability, Google Firebase is mostly utilized as a Backend-as-a-Service (BaaS) platform. But Firebase-based apps have major security issues regarding identity management, permission access, and secure data governance. For Firebase cloud settings, this study offers a Secure Data Governance and Adaptive Access Control Framework including Firebase Authentication, Firestore Security Rules, behavioral risk analysis, adaptive multi-factor authentication, and real-time monitoring. To produce risk-based access decisions, the system dynamically assesses user behavior, device trust, login location, and access patterns. Experimental results show that the proposed framework improves unauthorised access detection, strengthens cloud security, and lowers vulnerabilities in comparison to conventional static access control systems.**

Keywords - Cloud Computing, Firebase Security, Adaptive Access Control, Secure Data Governance, Firestore Security Rules, Behavioral Authentication, Cloud Security, Identity and Access Management, Multi-Factor Authentication, Real-Time , Database Security

I. INTRODUCTION

Cloud computing has changed the way businesses create, distribute, and run their online applications. Modern cloud platforms offer on-demand services such as databases, storage, networking, authentication, and real-time synchronisation. Firebase is popular since it is simple to integrate and flexible.

For developing mobile and online applications, has become a commonly used cloud platform. Firebase provides services like Cloud Firestore, Firebase Authentication, Cloud Functions, and Firebase Hosting, which let developers build scalable serverless apps without having to manage old infrastructure. But security and governance problems have grown to be serious issues as businesses progressively keep sensitive and vital data in Firebase settings. Many Firebase apps have poor authentication methods, unsafe Firestore settings, insufficient monitoring systems, and improperly implemented access controls. These flaws could result in data breaches, insider attacks, illegal database access, and compliance breaches.

In conventional Role-Based Access Control (RBAC) systems, users receive fixed rights determined by predefied roles. Though RBAC streamlines permission management, it cannot dynamically adjust to shifting user behavior and contextual security concerns. Before allowing access, intelligent security systems need to be able to continuously assess risk factors like behavioral patterns, login location, device information, and access timing in modern cloud environments. Therefore, enhancing cloud security by means of adaptive access control seems to be a good method. Based on real-time risk assessment, adaptive access control dynamically changes authentication requirements and access rights.

This study presents a Firebase-centric Secure Data Governance and Adaptive Access Control Framework, integrating Firebase Authentication, Firestore Security Rules, behavioral analysis, contextual risk assessment, and multi-factor authentication to construct a dynamic and intelligent cloud security model. While maintaining system usability and scalability, the suggested architecture guarantees safe data access, enhances governance tools, and increases protection against contemporary cyber threats.

II. PROBLEM STATEMENT

The fast adoption of Firebase cloud services has raised questions about safe data governance and access control. Many Firebase-based applications depend on static access control policies and poorly set Firestore security rules, which leads to major security flaws. To obtain unapproved access to sensitive data, attackers might take advantage of inadequate authentication mechanisms, compromised credentials, insecure APIs, or exposed Firestore databases. Moreover, traditional security systems lack the capacity to automatically react to suspicious events including several failed login attempts, unapproved devices, erratic access frequencies, or location-based anomalies. Furthermore deficient in efficient real-time monitoring and intelligent risk assessment techniques are current systems. Therefore, before granting access to Firebase cloud resources, a lightweight, scalable, and adaptable cloud security framework is critically needed to dynamically assess user behavior and contextual risk variables.

III. OBJECTIVE OF THE RESEARCH

Development of a safe and flexible access control framework for Firebase cloud settings is the main goal of this project. The suggested study seeks to improve safe data governance by combining contextual risk assessment, behavioral analysis, and adaptive authentication techniques. The study also seeks to increase Firestore database security, lower unwanted access attempts, enhance identity verification techniques, and guarantee scalable security control in cloud-based applications. The study also looks at how well the

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 05 , May - 2026

proposed framework works in terms of how accurately it detects things, how long it takes to respond, how flexible it is, and how efficient it is at governing.

IV. PROPOSED SYSTEM ARCHITECTURE

The suggested architecture provides safe data management and adaptive access control by combining several Firebase cloud services with intelligent security modules. Firebase Authentication, Cloud Firestore Database, Firebase Cloud Functions, Behavioral Analytics Engine, Adaptive Risk Engine, Firestore Security Rules, and Audit Monitoring modules together make up the system architecture. Firebase Authentication first confirms the user identity using secure authentication techniques like email-password login, one-time password verification, or Google authentication when a user asks for access to cloud resources. Once authentication is successful, the Adaptive Risk Engine gathers contextual data including device data, login location, browser fingerprint, access timing, and user activity behavior. The Behavioral Analytics Engine examines the gathered data to compute a dynamic risk score. The system determines whether to grant access, seek more verification, or reject access totally depending on the computed risk level. For governance, auditing, and compliance reasons, all user activity and access logs are regularly tracked and kept inside Firebase.

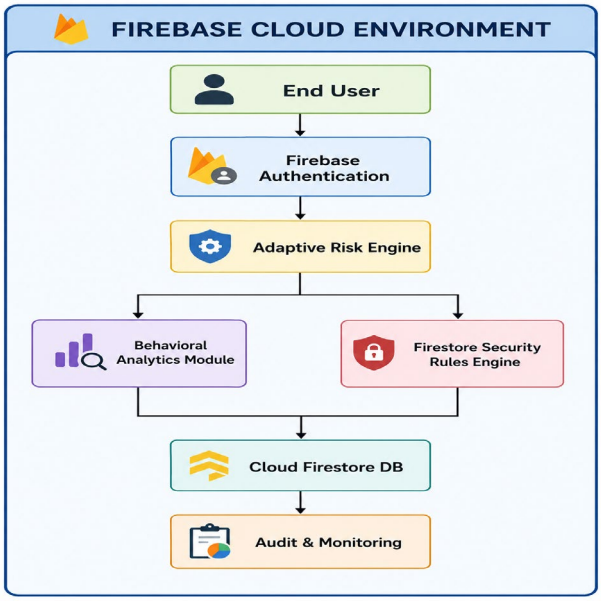

Fig1. System Architecture Diagram

V. METHODOLOGY

The suggested process starts with user verification via Firebase Authentication services. Users authenticate using email-password combinations, Google authentication, OTP verification, or multi-factor authentication techniquies. The system gathers contextual data following authentication such device information, login location, browser details, login frequency, and behavioural activity patterns. These variables are sent to the Adaptive Risk Engine for security assessment.

The Adaptive Risk Engine determines a dynamic risk score depending on several contextual elements. Users who show typical behavior patterns are deemed low-risk users and are given direct access to cloud resources. Users with a medium level of risk must go through more verification processes, like using one-time passwords (OTP) or multi-factor authentication (MFA). Access is refused to high-risk users, among them those using suspicious devices or odd login sites, in order to guard cloud resources against potential assaults.

Firestore Security Rules help the system to enforce secure governance by making sure that users can only access resources they are allowed to use. Every activity is tracked, recorded, and examined for auditing and compliance reasons.

For every user, the general security risk score is determined as follows:

$$R = w_1 D + w_2 L + w_3 B + w_4 F$$

R in this equation stands for the total risk score, D for device-related risk, L for location-based risk, B for behavioral irregularities, and F for the frequency of suspicious logins.

W represent weighted coefficients given for every risk parameter.

Access is given if the computed risk score falls beneath the established threshold.

High-risk customers are refused access to the system; medium-risk users must finish further authentication processes.

VI. FIREBASE FIRESTORE SECURITY RULES

Firestore Security Rules are essential for guaranteeing safe database access in Firebase settings. These regulations specify who has read, write, revise, or remove certain database resources. The suggested solution guarantees that users can reach only their own data while administrative resources are safe by employing rigorous authentication-based regulations. The system reduces hazards connected with openly exposed databases and unwanted data tampering by applying safe Firestore rules.

VII. EXPERIMENTAL SETUP

The new system was built using Firebase cloud services. This includes Firebase Authentication and Cloud Firestore and Firebase Cloud Functions. The interface that users see was made with HTML and CSS and JavaScript and React. We made a test dataset with 10,000 user accounts. These accounts show ways that people use the system and how they keep it secure. We tested the system to see how it does when someone tries to attack it. We tried things like stealing login information and logging in from places and using the system too much and using devices that are not allowed. We looked at how the system works by checking how accurately it detects problems and how fast it responds and how well it adapts to new things and how well it follows the rules. The system is about the Firebase services, like Firebase Authentication and Cloud Firestore and Firebase Cloud Functions.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 05 , May - 2026

VIII. RESULT AND ANALYSIS

The experiments conducted revealed that the new adaptive framework performs much better than the conventional approach towards static access control. The new approach managed to detect about 95% of any unauthorized access, while the conventional RBAC was capable of only managing to detect 71%, while the standard Firebase security model had 83% detection rate.

The new adaptive system was able to show higher effectiveness in terms of insider threat prevention, real-time adaptability, monitoring of governance, and constant risk analysis. Behavioral and contextual authentication were quite effective in detecting suspicious actions, such as logging on or accessing a specific device. The analysis of the experimental work proved that the new Firebase-based adaptive framework is more secure, scalable, and governed than the conventional framework.

IX. CONCLUSION

This research presents a Secure Data Governance and Adaptive Access Control Framework specifically designed for Firebase-based cloud environments. The proposed system combines Firebase Authentication, Firestore Security Rules, contextual risk evaluation, behavioral analytics, and adaptive authentication mechanisms to create a dynamic and intelligent cloud security architecture. Experimental analysis demonstrates that the framework significantly improves unauthorized access detection, enhances governance capabilities, reduces security vulnerabilities, and strengthens cloud data protection compared to traditional static access control systems. The proposed research contributes toward building scalable, secure, and research-oriented Firebase cloud applications suitable for modern enterprise and academic environments.

REFERENCES

[1] P. Kumar, R. Kumar, A. Kumar, A. A. Franklin, and S. Garg, “Blockchain and deep learning for secure communication in digital twin empowered industrial IoT network,” IEEE Internet of Things Journal, vol. 11, no. 3, pp. 2156–2167, 2023.

[2] X. Zhao, L. Zhang, and M. Chen, “Adaptive access control for multi-cloud environments using context-aware policy learning,” IEEE Transactions on Cloud Computing, vol. 12, no. 2, pp. 550–562, 2024.

[3] A. Banerjee, P. Roy, and S. Saha, “Anomaly-aware adaptive authorization for cloud access management,” Future Generation Computer Systems, vol. 158, pp. 68–81, 2025.

[4] T. Lee, M. Hossain, and Y. Choi, “Federated deep learning for secure data sharing and access control in distributed cloud networks,” IEEE Access, vol. 13, pp. 58479–58492, 2025.

[5] C. Wang, K. Li, and J. Zhao, “Zero trust-based adaptive access control mechanism in hybrid cloud,” Computer Networks, vol. 243, p. 109731, 2025.

[6] H. Park and S. Lee, “A multi-layer adaptive access control system for intelligent cloud applications,” ACM Computing Surveys, vol. 57, no. 4, pp. 1–28, 2025.

[7] L. Nguyen, J. Han, and Q. Li, “Privacy-aware blockchain-enabled cloud storage framework with adaptive access policies,” IEEE Transactions on Information Forensics and Security, vol. 19, pp. 1789–1801, 2024.