e-ISSN:2582-7219

INTERNATIONAL JOURNAL OF MULTIDISCIPLINARY RESEARCH IN SCIENCE, ENGINEERING AND TECHNOLOGY

Volume 7, Issue 11, November 2024

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 7.521

© 2024 IJMRSET | Volume 7, Issue 11, November 2024| DOI: 10.15680/IJMRSET.2024.0711070

ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 7.521| ESTD Year: 2018|

International Journal of Multidisciplinary Research in Science, Engineering and Technology (IJMRSET)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

Secure Student Information Management System with Real-Time Anomaly Detection Using Machine Learning

V.Mohana Priya, Dr.D.Rajinigirinath

PG Student, Department of CSE, Sri Muthukumaran Institute of Technology, Chennai, India

Professor, Department of CSE, Sri Muthukumaran Institute of Technology, Chennai, India

ABSTRACT: This paper presents a secure student information management system (SIMS) that incorporates real-time anomaly detection through advanced machine learning techniques for enhanced security and data integrity. The system utilizes Firebase for its backend infrastructure, ensuring seamless authentication, database management, and secure hosting. Autoencoder-GAN models are trained to detect and classify anomalous behaviour, thereby protecting sensitive information like attendance records, marks, placement details, and textbook resources. The frontend, designed using HTML, CSS, and JavaScript with optional frameworks like React.js or Vue.js, provides user-friendly interfaces tailored for students, staff, and administrators. The solution emphasizes secure role-based access, real-time data updates, and intuitive dashboards for users. By integrating a robust anomaly detection mechanism and leveraging Firebase's scalability, this system sets a benchmark for secure, efficient, and intelligent student management platforms.

I. INTRODUCTION

Modern educational institutions face challenges in managing sensitive student data, which includes academic records, attendance, placement details, and learning resources. Traditional systems often suffer from security vulnerabilities, inefficiencies, and a lack of real-time anomaly detection mechanisms. With the rise of cyber threats and data breaches, there is a pressing need for a **secure and intelligent student information management system**.

This paper introduces a **multi-role platform** designed for students, staff, and administrators. It integrates machine learning-based anomaly detection models (Autoencoder-GAN) to identify and mitigate unusual activities or unauthorized access in real time. The Firebase backend ensures scalability and security with role-based access controls, while the frontend offers seamless user experiences across various roles. The system is optimized for real-time operations and scalable deployments, making it an ideal solution for academic institutions aiming to modernize their data management processes.

II. EXISTING SYSTEM

Current student information management systems typically operate as isolated platforms with limited capabilities:

- **Manual Processes**: Many institutions still rely on manual methods or standalone systems for data entry and retrieval, leading to errors and inefficiencies.
- **Lack of Security**: Traditional systems often lack robust security measures, making them vulnerable to data breaches and unauthorized access.
- **No Anomaly Detection**: These systems fail to monitor or identify unusual patterns of activity, such as suspicious login attempts or data modifications.
- **Inefficient Updates**: Real-time updates and synchronization between users are often missing, leading to outdated information being displayed.

© 2024 IJMRSET | Volume 7, Issue 11, November 2024| DOI: 10.15680/IJMRSET.2024.0711070

ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 7.521| ESTD Year: 2018|

International Journal of Multidisciplinary Research in Science, Engineering and Technology (IJMRSET)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

III. PROPOSED SYSTEM

The proposed system addresses these shortcomings by introducing:

1. **Secure Backend Infrastructure**: Utilizing Firebase for role-based authentication, real-time database updates, and secure hosting.
2. **Machine Learning Integration**: Employing Autoencoder-GAN models for real-time anomaly detection and classification of security threats.
3. **User-Friendly Frontend**: Customizable interfaces for students, staff, and administrators, ensuring a smooth user experience.
4. **Role-Based Access Control**: Implementing fine-grained Firebase security rules to restrict access based on user roles.
5. **Real-Time Synchronization**: Leveraging Firestore listeners for instantaneous updates across all user interfaces.

IV. ARCHITECTURE DIAGRAM

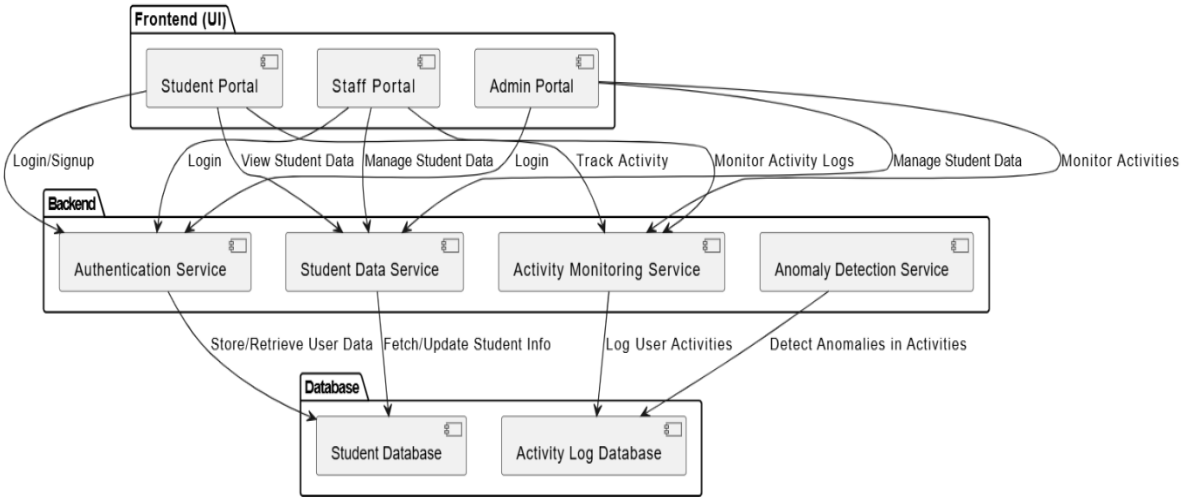

Fig 1. Architecture Diagram

V. METHODOLOGY

Requirements Analysis:
The first phase involves identifying the system's functional and non-functional requirements. Stakeholders, including students, staff, and administrators, are consulted to gather input on the desired features. System specifications such as data management, role-based access, and anomaly detection are defined. Constraints like platform compatibility, scalability, and security are also addressed. Technologies are selected based on their suitability, such as Firebase for backend services, Autoencoder-GAN for anomaly detection, and React.js or Vue.js for the frontend. This phase ensures a clear understanding of paper goals and aligns them with technical feasibility.

System Design:
This phase focuses on creating a detailed blueprint for the system. An architecture diagram outlines the interaction between the frontend, backend, database, and machine learning components. Firestore database structures are designed with collections like users, marks, and resources. UI/UX prototypes are developed to ensure an intuitive interface for all user roles. Security is integrated into the design, with role-based Firebase security rules and secure APIs for model deployment. By addressing both functionality and security, this phase establishes a solid foundation for the development process.

ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 7.521| ESTD Year: 2018|

International Journal of Multidisciplinary Research in Science, Engineering and Technology (IJMRSET)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

Backend Development:
Backend development involves building a secure and scalable infrastructure using Firebase. A Firestore database or Realtime Database is configured to handle dynamic data storage, and Firebase Authentication is implemented for secure login and role-based access. Serverless Firebase Functions manage backend logic, including triggers for alerts on anomalies or critical events. Storage for files like textbooks and resources is managed with Firebase Storage, ensuring security and access control. This phase emphasizes secure data handling and seamless integration of backend services to support real-time functionality.

Frontend Development:
Frontend development focuses on creating responsive and user-friendly interfaces for students, staff, and administrators. Technologies like HTML, CSS, and JavaScript, along with React.js or Vue.js, are used to build dynamic dashboards and forms. Firebase SDKs are integrated for authentication, database access, and file storage operations. Features like real-time data synchronization using Firestore listeners ensure updates are reflected instantly. Modular UI components enable flexibility and reusability across the application, enhancing maintainability. This phase delivers an engaging and accessible platform for all users.

Machine Learning Model Development:
Machine learning models, particularly Autoencoder-GANs, are developed to detect anomalies in user behaviour and system activities. Historical data is pre-processed to train models that identify suspicious activities, such as unauthorized access attempts. Separate models are trained for students, staff, and admin roles to improve detection accuracy. Trained models are saved as serialized files and deployed using Flask or Django APIs. These models are integrated with Firebase Functions for real-time anomaly detection, ensuring the system remains secure and adaptive to potential threats.

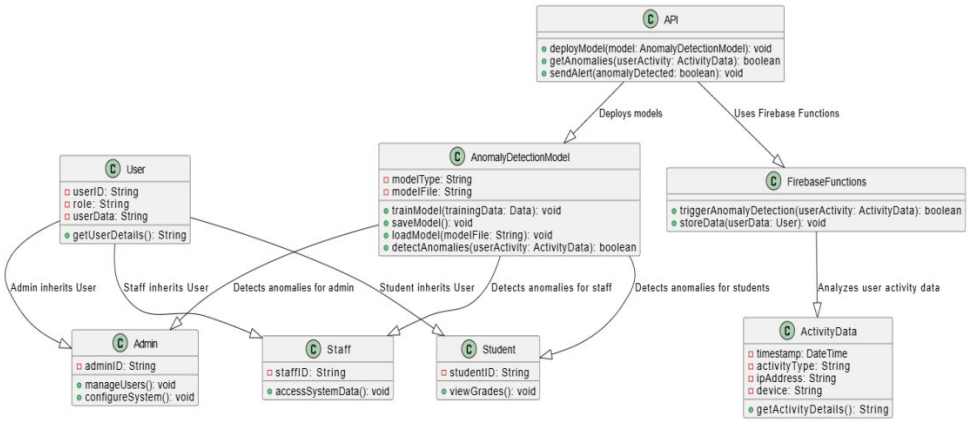

Figure 2. Machine Learning Model Development Class Diagram

Integration and Testing:
In this phase, the system's components are integrated and rigorously tested. Unit tests validate the functionality of individual modules, while integration tests ensure seamless interaction between the frontend, backend, and machine learning models. Security tests address vulnerabilities like unauthorized access, and performance tests assess the system under varying loads. Machine learning models are validated with test datasets to ensure accurate anomaly detection. This comprehensive testing ensures the system is reliable, secure, and ready for deployment.

Deployment:
The deployment phase involves making the system operational for real-world use. The frontend is hosted on Firebase Hosting with CDN integration for optimized performance, while Firebase Functions handle backend operations. Machine learning models are deployed via Flask/Django APIs on platforms like Heroku or AWS. Firebase ML Kit may

ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 7.521| ESTD Year: 2018|

International Journal of Multidisciplinary Research in Science, Engineering and Technology (IJMRSET)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

be used for native model integration if needed. This phase ensures that the system is accessible, scalable, and performs efficiently under real-world conditions.

Monitoring and Maintenance:
Post-deployment, the system is monitored and maintained to ensure smooth operation. Firebase Analytics tracks user activity and system performance, while logs are reviewed for anomalies or potential improvements. Security rules and machine learning models are periodically updated to address evolving threats. Regular backups of Firestore data and user logs ensure data integrity. Feedback from users is collected to refine features and enhance usability, ensuring the system remains relevant and secure over time.

VI. CONCLUSION

The Secure Student Information Management System ensures efficient, scalable, and secure data handling for educational institutions. By integrating machine learning techniques for real-time anomaly detection and leveraging Firebase's backend capabilities, the system offers robust protection against unauthorized access and threats. Its user-friendly interface and real-time updates make it a practical solution for modern educational environments.

VII. FUTURE WORK

Enhanced machine learning models incorporating federated learning can enable privacy-preserving anomaly detection by processing data locally on user devices without centralized storage. Advanced analytics can be introduced to provide predictive insights, such as forecasting student performance trends and placement outcomes, aiding staff in decision-making. Cross-platform integration with Learning Management Systems (LMS) and other educational tools would create a seamless ecosystem for academic and administrative processes. Additionally, implementing blockchain technology can bolster security by providing a tamper-proof ledger for sensitive student data, ensuring transparency and enhanced protection against unauthorized access.

REFERENCES

1. Ilias Siniosoglou, Panagiotis Radoglou-Grammatikis, Georgios Efstathopoulos, Panagiotis Fouliras , and Panagiotis Sarigiannidis " A Unified Deep Learning Anomaly Detection and Classification Approach for Smart Grid Environments"IEEE transactions on network and service management, vol. 18, no. 2, june 2021
2. M. M. Elsaid Khoudier *et al*., "Prediction of student performance using machine learning techniques," *2023 5th Novel Intelligent and Leading Emerging Sciences Conference (NILES)*, Giza, Egypt, 2023, pp. 333-338.
3. R. Sharma, T. U. Bux, B. Varshney and K. Tomar, "Real-time Student Management Application Using Google Firebase and Android Studio," *2021 International Conference on Intelligent Technologies (CONIT)*, Hubli, India, 2021, pp. 1-6.
4. S. Tharsha, J. Dilogera, B. Mohanashiyaam, S. Kirushan, K. B. A. B. Chathurika and N. H. P. R. S. Swarnakantha, "Machine Learning-based Prediction Model for Academic Performance," *2021 3rd International Conference on Advancements in Computing (ICAC)*, Colombo, Sri Lanka, 2021, pp. 305-310.
5. L. Zheng, C. Wang, X. Chen, Y. Song, Z. Meng and R. Zhang, "Evolutionary machine learning builds smart education big data platform: Data-driven higher education", *Applied Soft Computing*, vol. 136, pp. 110114, 2023.
6. H. T. H. Duong, L. T. M. Tran, H. Q. To and K. Van Nguyen, "Academic performance warning system based on data driven for higher education", *Neural Computing and Applications*, vol. 35, no. 8, pp. 5819-5837, 2023.
7. G. S. Kumar, D. De la Cruz-Cámaco, M. Ravichand, K. Joshi, Z. Gupta and S. Gupta, "Monitoring and Predicting Performance of Students in Degree Programs using Machine Learning", *2023 10th International Conference on Computing for Sustainable Global Development (INDIACom)*, pp. 1311-1315, 2023, March.
8. K. Bala, Mukesh Kumar, Sayali Hulawale and Sahil Pandita, "ChatBot For College Management System Using A.I", *International Research Journal of Engineering and Technology (IRJET)*, vol. 04, no. 11, November 2017.
9. Amirah Mohamed Shahiria, Wahidah Husaina, Nur'aini and Abdul Rashida, "A Review on Predicting Student's Performance using Data Mining Techniques", *Procedia Computer Science*, vol. 72, pp. 414-422, 2015.
10. Havan Agrawal and Harshil Mavani, "Student Performance Prediction using Machine Learning", *International Journal of Engineering Research & Technology (IJERT)*, vol. 04, no. 03, March 2015.

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

INTERNATIONAL JOURNAL OF MULTIDISCIPLINARY RESEARCH

IN SCIENCE, ENGINEERING AND TECHNOLOGY

| Mobile No: +91-6381907438 | Whatsapp: +91-6381907438 | ijmrset@gmail.com |

www.ijmrset.com