

Anomaly – Based Threat Detection in Smart Health Using Machine Learning

C. SENTHILKUMARAN, MCA., (Ph.D)

[Dean & Head, Associate Professor, Department of Master of computer applications]

A. VJAYALAKSHMI., MCA

[Christ College of Engineering and Technology Moolakulam, Oulgaret Municipality, Puducherry-605010]

Abstract- The Anomaly Based Threat Detection in Smart Health Using Machine Learning system is designed to improve healthcare security and patient monitoring by identifying abnormal health conditions using intelligent prediction techniques. In healthcare environments, delayed detection of critical patient conditions can lead to serious consequences. This project utilizes machine learning algorithms to analyze patient health data and detect anomalies at an early stage. The system provides secure user authentication through OTP verification and role-based access control, ensuring that only authorized healthcare personnel can access sensitive patient information.

The application is developed using HTML, CSS, JavaScript, Flask, Python, and MongoDB. Patient records are securely stored and processed by the machine learning model to predict potential health threats. When abnormal conditions are detected, the system generates alert notifications and maintains anomaly logs for monitoring and future analysis. The proposed system enhances patient safety, improves healthcare decision-making, reduces manual monitoring efforts, and provides a reliable platform for intelligent healthcare threat detection and management.

I.INTRODUCTION

Healthcare systems generate a large amount of patient data every day, including medical records, vital signs, laboratory results, and treatment information. Monitoring this data manually is often difficult and time-consuming, which may lead to delays in identifying critical health conditions. With the rapid growth of digital healthcare technologies, there is a need for intelligent systems that can analyze healthcare data efficiently and provide timely alerts for abnormal

situations. Machine Learning has emerged as a powerful technology for detecting hidden patterns and predicting potential risks in healthcare environments.

The Anomaly Based Threat Detection in Smart Health Using Machine Learning project is designed to identify abnormal patient conditions and potential healthcare threats automatically. The system collects and processes patient-related information, analyzes the data using machine learning algorithms, and detects unusual patterns that may indicate health risks. Secure authentication mechanisms such as OTP verification and role-based access control are implemented to protect sensitive healthcare information and ensure that only authorized users can access the system.

II.MAIN OBJECTIVES

The primary objective of the Anomaly Based Threat Detection in Smart Health Using Machine Learning project is to develop an intelligent healthcare monitoring system capable of identifying abnormal patient conditions at an early stage. The system aims to analyze healthcare data using machine learning techniques and detect anomalies that may indicate potential health threats. By providing timely alerts and accurate predictions, the system helps healthcare professionals take preventive actions and improve patient safety. Another important objective is to reduce manual monitoring efforts and enhance the efficiency of healthcare services through automated analysis and decision support.

The project also focuses on ensuring data security and controlled access to sensitive healthcare information. Features such as OTP-based authentication, role-based access control, patient record management, and anomaly logging are implemented to maintain confidentiality and system integrity. Additionally, the

system aims to provide a user-friendly platform for healthcare staff to monitor patient data, receive threat notifications, and manage records effectively. Through the integration of machine learning and secure healthcare management, the project seeks to deliver a reliable, scalable, and intelligent smart health solution.

III.SYSTEM OVERVIEW

The Anomaly Based Threat Detection in Smart Health Using Machine Learning system is a web-based healthcare monitoring platform developed to identify abnormal patient conditions and potential health threats automatically. The system allows authorized users such as administrators, doctors, nurses, lab technicians, and pharmacy staff to access healthcare information based on their roles. It provides secure authentication through login credentials and OTP verification to ensure data confidentiality and system security.

The system stores patient records in MongoDB and uses machine learning algorithms to analyze healthcare data and detect anomalies. Whenever abnormal conditions are identified, the system generates alert notifications and records the event in anomaly logs for future analysis. Developed using HTML, CSS, JavaScript, Flask, Python, and MongoDB, the system provides an efficient and secure environment for healthcare monitoring, helping medical professionals make timely decisions and improve patient safety.

IV.SYSTEM ARCHITECTURE

The Anomaly Based Threat Detection in Smart Health Using Machine Learning system follows a multi-layer architecture that integrates user interfaces, application services, machine learning models, and database management. The architecture is designed to provide secure access, efficient data processing, and real-time threat detection in healthcare environments. Each layer performs a specific function and communicates with other components through well-defined interfaces.

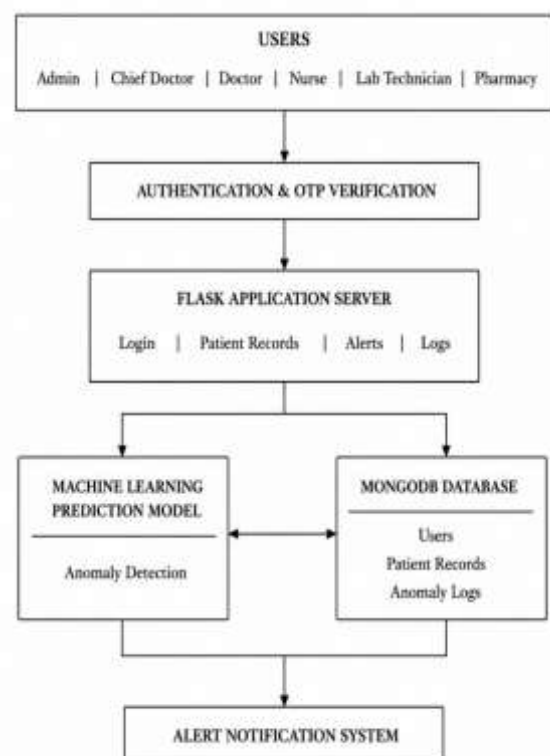
The first layer is the User Interface Layer, which allows users such as Admin, Chief Doctor, Doctor, Nurse, Lab Technician, and Pharmacy staff to interact with the system. This layer is developed using HTML, CSS, and JavaScript. Users can log in, manage patient records, view anomaly alerts, and access reports according to their assigned roles.

The second layer is the Authentication and Access Control Layer. This layer handles user login, OTP verification, session management, and role-based access control. It ensures that only authorized healthcare personnel can access sensitive patient information and perform specific operations within the system.

The third layer is the Application Layer, which is developed using Flask and Python. This layer acts as the bridge between the frontend and backend components. It processes user requests, manages patient records, handles anomaly logs, and coordinates communication between the machine learning model and the database.

The fourth layer is the Machine Learning Layer, which is responsible for analyzing healthcare data and detecting abnormal patient conditions. Patient health information is processed through the machine learning model to identify anomalies and potential threats. When abnormal conditions are detected, the system generates alerts and records the detected threats for further monitoring.

The final layer is the Database Layer, which uses MongoDB for storing user information, patient records, anomaly logs, and system data. The database provides secure and efficient data management while supporting real-time access and retrieval. Together, all layers work collaboratively to provide a secure, intelligent, and reliable healthcare threat detection system.



V. ALGORITHM

Isolation Forest

The Isolation Forest Algorithm is used in the proposed system to detect anomalies in healthcare data and user activities. It works by randomly partitioning data points and isolating observations that significantly differ from normal patterns. Anomalous records require fewer partitions to be isolated compared to normal records, making them easier to identify. The algorithm analyzes patient information and system activities to detect unusual behavior, generate threat alerts, and improve healthcare security. Due to its high efficiency and accuracy in handling large datasets, Isolation Forest is well suited for anomaly-based threat detection in smart healthcare environments.

VI. RESULT AND DISCUSSION

The Anomaly Based Threat Detection in Smart Health Using Machine Learning system was successfully developed and tested using healthcare data. The system effectively performed user authentication through OTP verification, managed patient records, monitored user activities, and detected abnormal patterns using the Isolation Forest machine learning algorithm. The prediction results demonstrated that the model could accurately identify suspicious activities and potential healthcare threats. Detected anomalies were stored in the anomaly logs database, and alert notifications were generated for authorized users, enabling timely monitoring and response.

The overall performance of the system was found to be reliable, secure, and efficient. Role-based access control ensured that only authorized healthcare staff could access sensitive patient information. The machine learning model produced accurate anomaly detection results with minimal processing time, improving the effectiveness of healthcare monitoring. The generated alerts, patient records management, and anomaly logs helped enhance system security and data integrity. The results confirm that the proposed system successfully achieves its objective of providing intelligent threat detection and secure healthcare data management in a smart health environment.

VII. BENEFITS

The proposed Anomaly Based Threat Detection in Smart Health Using Machine Learning system provides

early detection of abnormal patient conditions and suspicious healthcare activities. By using the Isolation Forest algorithm, the system can identify unusual patterns in healthcare data and generate alerts before critical situations occur. This helps healthcare professionals take timely actions, improving patient safety and reducing the risk of severe health complications.

Another major benefit of the system is enhanced security and data protection. Features such as OTP verification, role-based access control, and secure database management ensure that sensitive healthcare information is accessed only by authorized users. The system also maintains anomaly logs, which help administrators monitor activities and investigate suspicious events effectively.

The system improves overall healthcare efficiency by automating patient monitoring and anomaly detection processes. It reduces manual workload, minimizes human errors, and provides accurate prediction results in a short time. The alert notification mechanism enables quick response to potential threats, while the centralized database allows efficient management of patient records. These advantages make the system reliable, scalable, and suitable for modern smart healthcare environments.

VIII. DIFFICULTIES AND CHALLENGES FACED

During the development of the Anomaly Based Threat Detection in Smart Health Using Machine Learning system, several challenges were encountered. Collecting and preprocessing healthcare data required significant effort to ensure data quality and consistency. Integrating the machine learning model with the Flask backend and MongoDB database was also challenging. Implementing secure OTP authentication and role-based access control required careful testing. Additionally, improving anomaly detection accuracy and reducing false alerts were important challenges faced during the project development.

IX. CONCLUSION

The Anomaly Based Threat Detection in Smart Health Using Machine Learning system successfully provides an intelligent and secure solution for monitoring healthcare data and detecting abnormal activities. By utilizing the Isolation Forest algorithm, the system can identify anomalies efficiently and generate timely alerts

for healthcare professionals. Features such as OTP verification, role-based access control, patient record management, and anomaly logging enhance both security and reliability. The developed system reduces manual monitoring efforts, improves patient safety, and supports better healthcare decision-making. Overall, the project demonstrates the effective application of machine learning techniques in creating a secure, reliable, and efficient smart healthcare threat detection system.

X. FUTURE ENHANCEMENTS

The proposed Anomaly Based Threat Detection in Smart Health Using Machine Learning system can be further enhanced by integrating advanced machine learning and deep learning techniques to improve prediction accuracy and threat detection capabilities. Future developments may include real-time patient monitoring using IoT-based healthcare devices, mobile application support for remote access, and cloud-based deployment for improved scalability and data availability. Additional features such as automated emergency response systems, advanced data visualization dashboards, and integration with electronic health record (EHR) systems can further enhance healthcare management. These improvements will make the system more intelligent, efficient, and capable of supporting next-generation smart healthcare environments.

XI. REFERENCES

1. Ian Goodfellow, Yoshua Bengio, and Aaron Courville, *Deep Learning*, MIT Press, 2016.
2. Aurélien Géron, *Hands-On Machine Learning with Scikit-Learn, Keras, and TensorFlow*, O'Reilly Media, 2022.
3. Ethem Alpaydin, *Introduction to Machine Learning*, MIT Press, 2020.
4. Christopher M. Bishop, *Pattern Recognition and Machine Learning*, Springer, 2006.
5. Jiawei Han, Micheline Kamber, and Jian Pei, *Data Mining: Concepts and Techniques*, Morgan Kaufmann, 2011.
6. Trevor Hastie, Robert Tibshirani, and Jerome Friedman, *The Elements of Statistical Learning*, Springer, 2017.
7. Jake VanderPlas, *Python Data Science Handbook*, O'Reilly Media, 2016.
8. Wes McKinney, *Python for Data Analysis*, O'Reilly Media, 2022.
9. Grady Booch, James Rumbaugh, and Ivar Jacobson, *The Unified Modeling Language User Guide*, Addison-Wesley, 2005.
10. Roger S. Pressman and Bruce R. Maxim, *Software Engineering: A Practitioner's Approach*, McGraw-Hill, 2020.
11. Ian Sommerville, *Software Engineering*, Pearson Education, 2016.
12. Flask Documentation, *Flask Web Development Framework*, Available at: <https://flask.palletsprojects.com>
13. Python Software Foundation, *Python Documentation*, Available at: <https://www.python.org>
14. MongoDB Inc., *MongoDB Documentation*, Available at: <https://www.mongodb.com/docs>
15. Scikit-Learn Developers, *Scikit-Learn Documentation*, Available at: <https://scikit-learn.org>
16. NumPy Developers, *NumPy Documentation*, Available at: <https://numpy.org>
17. Pandas Development Team, *Pandas Documentation*, Available at: <https://pandas.pydata.org>
18. Twilio Inc., *Twilio SMS API Documentation*, Available at: <https://www.twilio.com/docs>
19. IEEE Xplore Digital Library, *Machine Learning and Healthcare Research Articles*, Available at: <https://ieeexplore.ieee.org>
20. Springer Link, *Healthcare Analytics and Anomaly Detection Research Papers*, Available at: <https://link.springer.com>.