



International Journal of Artificial Intelligence and Machine Learning

Publisher's Home Page: <https://www.svedbergopen.com/>



Research Paper

Open Access

Implementation of a Role-Based Behavioral Access Log Framework for Secure Healthcare Electronic Health Record Systems

Thasleem R¹, Sumathy Kingslin²

¹Research Scholar, Department of Computer Science, Quaid-E-Millath Govt College for Women (A), Chennai, India.

²Associate Professor, Department of Computer Science, Quaid-E-Millath Govt College for Women (A), Chennai, India.

ABSTRACT

Healthcare Electronic Health Record (EHR) systems store sensitive data and are used by people with varying roles and responsibilities. While authentication and role-based access control can help prevent unauthorized access, they can only detect the oddness of authorized users. This study introduces a role-aware behavioral access-log framework for healthcare EHR systems to continuously monitor user activities produce structured behavioral data for future work in data preprocessing, anomaly detection techniques, role-aware analysis and risk assessment. This proposed system will combine role-based authentication, healthcare user management, EHR activity monitoring, automatic behavioral monitoring and dashboard-based monitoring in a controlled healthcare environment. Structured behavioral access logs of user interactions are created during login and logout, viewing or updating of patient records, searching for patient records, laboratory and medication-related activities. The created logs include significant contextual details such as user identification, role assigned to the user, department, date and time of access, patient identifier, user action, session details, user login and accessed healthcare resources. The data set created is not clinical patient data, but rather data on how users are interacting with the EHR system, is appropriate for security analysis. The study shows that controlled environment of EHR can continuously supply structured behavioral access data to develop AI-based security mechanisms to detect abnormal access behavior of authorized users. The proposed framework thus connects the EHR activity monitoring and future intelligent insider-threat detection research. It helps in reproducible behavioral analysis by ensuring consistency in activity records across all roles, departments, sessions and system modules in healthcare.

Keywords: Healthcare Cybersecurity, Electronic Health Record, EHR platform, Insider Threat Detection, Behavioral Access Logs, Role based authentication.

1. Introduction

Healthcare is rapidly evolving into a digital landscape, and the use of Electronic Health Record (EHR) systems has grown significantly to ensure secure storage, management, and sharing of patient data. EHR systems offer advantages over traditional paper-based records, such as increased efficiency in healthcare, decreased manual errors, and better patient care. The rise of digital healthcare systems, however, has brought with it a number of cybersecurity hurdles, as medical information is highly sensitive. Electronic Health Record (EHR) systems are becoming a crucial component of healthcare. Patient information is being heavily relied on by healthcare systems for storage, management and access through Electronic Health Record (EHR) systems. While EHR systems offer significant benefits in terms of improving the efficiency and accessibility of healthcare services, the digital handling of sensitive information also presents substantial cybersecurity challenges. Multiple users of the EHR resources are authorized to access the resources based on their responsibilities, such as doctors, nurses, administrators, laboratory technicians, etc. This is why continuous monitoring of user activities is crucial to safeguarding sensitive healthcare information. While present healthcare security mechanisms, including authentication, access control, encryption and authorization, are good at blocking access by unauthorized users, they are less effective at identifying malicious behavior by users who are authorized. The people who have access to the hospital and know the system inside and out are one of the biggest threats to patient privacy today, as insiders in the healthcare sector are doctors, nurses, hospital administrators and lab technicians. Thus, the identification of malicious activities from regular user activities is still a very difficult task. With the recent development of Artificial Intelligence (AI) and Machine Learning (ML), anomaly detection methods can be used to detect suspicious user access to the healthcare access logs. Unusual access permissions like logging in to a large number of patient records, working beyond working hours, attempts to log in multiple times for the same record, or accessing records from unrelated departments could represent insider threats. But most of the solutions currently available only work on an authentication and access control level, not with continuous monitoring of user activity. Moreover, they frequently fail to take into account the role-specific behavioral traits, which leads to higher false-positive detection rates. To overcome these constraints, the design and implementation of an automated Healthcare Electronic Health Record (EHR) platform that automatically

logs activities of healthcare users and produces structured access logs of user behaviors are presented. The proposed system is designed to integrate role-based authentication, healthcare user management, patient management, and ongoing activity logging to create a realistic dataset of behaviors for future AI-driven insider threat detection. This is the basis for subsequent research on anomaly detection, role-based behavior analysis, and real-time monitoring of cybersecurity of healthcare EHR systems.

1.1 Research objective

The primary objective of this research are as follows:

- To Design and develop a secure Healthcare Electronic Health Record (EHR) platform: offers a realistic environment to manage patient information and healthcare user activities.
- To implement a role-based authentication and access control mechanism: enables different healthcare users to securely access the system according to their assigned responsibilities.
- To continuously track users' activity over healthcare: with automatic generation of structured behavior access logs to exactly capture the interactions between healthcare users and the EHR system.
- To develop a structured behavioral access log dataset: captures user access patterns and supports future behavioral analysis and anomaly detection research.
- To establish a scalable research platform: it can be the basis for future AI-based insider threat detection using anomaly detection techniques and role-aware behavioral analysis.

1.2 contributions of the study:

- Development of an Electronic Health Record (EHR) environment capturing user activities.
- Design of safe role-based authentication and healthcare user management system.
- Structured behavioral access logs automatically generated from healthcare user activities.
- Development of a behavioral dataset for future use in AI based insider threat detection.
- Establishment of a scalable foundation for role-aware behavioral analysis and anomaly detection in healthcare cybersecurity.

2. Related Work And Research Gap

2.1 Related Work

Typical security controls used in electronic health record (EHR) systems include authentication, authorization, role-based access control, and audit logging. These techniques determine access to a resource and maintain logs of system activities. But using the system is not always an acceptable action, especially if the user has permission in the system.

Behavioral monitoring offers another insight by observing the activities of authorized users of the resource within the EHR. Behavioral access events can include things like user logging in, accessing a patient's record, updating a patient's record, searching for patients, making laboratory actions, and performing medication-related activities. A more complete picture of user behavior can be gained by adding information about the user, like role, department, time, session, action, and resource.

Intelligent security analysis means structured behavioral data is of special importance. AI anomaly detection tools can then be used to examine such data to detect deviations from more normal behavior. To support good subsequent analysis of behavior, however, the access logs need to be consistent, complete, and provide context information. Hence, a controlled environment of an EHR system, where interactions of users are systematically recorded, could be used as an appropriate data foundation in building and testing intelligent security mechanisms.

2.2 Research Gap

While authentication and access control mechanisms are crucial tools for safeguarding EHR systems, they focus mainly on access permission and not behavioral deviation. A legitimate healthcare user may be permitted access to the system at the same time as they are engaged in a very different activity from normal. This means there is a need for ongoing behavioral surveillance, in addition to the traditional permission-based security systems.

Another challenge is to have structured, role-associated behavioral access data available for subsequent intelligent analysis. Basic access logs may not contain enough information to be valuable for analysis of user behavior from a role or department perspective, across sessions and EHR resources.

To solve this, the proposed framework proposes an integrated EHR environment where the user's activities in the system are monitored continuously and automatically converted to structured behavioral access logs. The framework links activities recorded with contextual attributes, such as user identity, user role, user department, access time, user action, user session information and accessed healthcare resources. This offers a systematic behavioral baseline on which future anomaly detection and insider threat research can be based.

3. PROPOSED BEHAVIOURAL ACCESS LOG FRAMEWORK

The proposed framework provides for a controlled Electronic Health Record (EHR) environment, which captures and structures activities of healthcare users. It includes secure authentication, role-based access control, real-time monitoring of activities, auto-generation of activity logs, structured dataset construction and

dashboard monitoring. The framework aims to generate uniform behavioral access information which can be leveraged for further AI-driven security analysis.

The framework starts with a healthcare environment with the EHR, which has various operational modules such as patient management, healthcare-user management, department management, medication management, and laboratory management. The users are successfully authenticated and given the right role e.g. Doctor, Nurse, Administrator, or Laboratory Technician. The functions and resources granted to each user is then determined by role-based access control based on the responsibilities of each user.

Once users are authenticated, their activities on the EHR system are constantly tracked and monitored. Behaviors are observed, such as logging in and out, viewing and updating patient records, searching patients, laboratory activities, and medication activities. All events get recorded as a structured access-log entry automatically with relevant contextual attributes such as user identity, role, department, access time, patient identifier, action, session information, logged in or not, accessed healthcare resources etc.

The records created are contained in an organized behavioral dataset, with emphasis on users' interactions with the EHR system instead of patient clinical data. A monitoring dashboard will provide the admin with a summary of activity information and will allow them to review the user activity that was recorded and view the access history. The resulting Dataset provides the future ai integration, risk assessment and real -time insider-threat detection. These analytical stages are not claimed as completed within the framework presented in this study

FIG 1: illustrate the proposed Behavioral Access -Log Framework for developing Healthcare EHR platform. It demonstrates the process of extracting behavioral access logs from healthcare data while providing a basis for future AI-based insider threat detection.

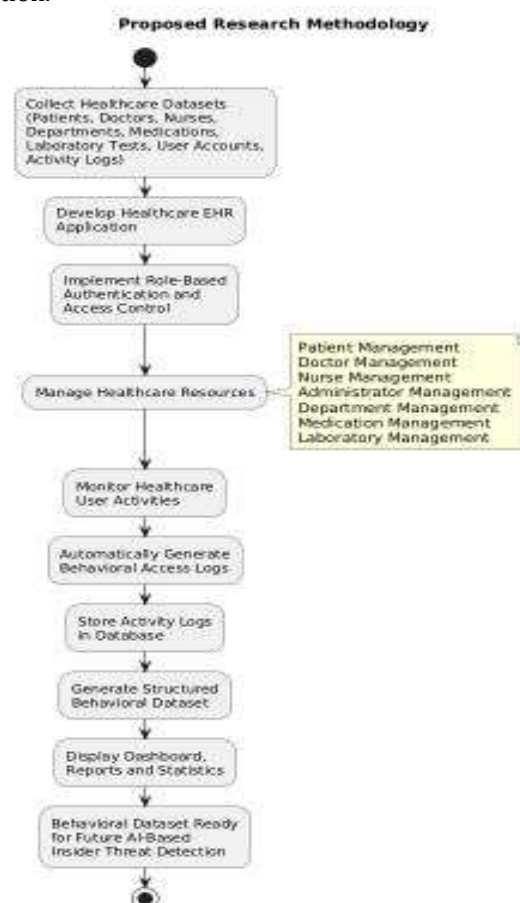


Fig. 1. Proposed Behavioral Access -Log Framework for- Developing a Behavioral access logs Healthcare EHR Platform

4. RESEARCH METHODOLOGY

The research methodology proposed here is to create a Healthcare Electronic Health Record (EHR) system with a realistic hospital environment to handle patient information and track the activities of users of the health care system. The system automatically captures user interactions and creates structured logs of user behavior, which will be the main data source for future insider threat detection based on AI. The methodology includes six steps, starting with the EHR application development and ending with the creation of an AI-ready behavioral access log dataset.

4.1 Healthcare EHR Application Development

The first stage involves designing a Healthcare Electronic Health Record (EHR) application to simulate actual hospital environments. This application includes the handling of patient data and the support of various healthcare users in an integrated web-based environment. It includes patient management, healthcare user management, department management, medication management, laboratory management and secure login modules. The healthcare datasets used for the application include patient records, healthcare users, departments, laboratory information, medications, and user accounts.

4.2 Role-Based Authentication and Access Control: To protect the system from unauthorized users, a secure authentication mechanism is used. Each person who uses the system is given a specific role such as Doctor, Nurse, Administrator, Laboratory Technician. Role based access control allows users to only access functions related to their role, ensuring the safe and organized access of healthcare resources

4.3 User Activity Monitoring and Log Generation: All of the users' interactions with the Healthcare EHR application are constantly tracked after they are authenticated. The system logs regular healthcare operations including login/out, patient record viewing, updating patient information, searching for patients, laboratory report management, medicine update, etc. These monitored activities are the typical behaviors of healthcare users when using the system.

4.4 Behavioral Dataset Generation: Access logs are automatically created for each activity monitored. The logs created provide detailed information about user activity, such as user identity, assigned role, department, access time, patient identifier, user action, session duration, login status, and accessed healthcare resources. These behavioral access logs offer a complete view of how users interact with the EHR system.

4.5 Dashboard Monitoring: A monitoring dashboard is created to visualize the activities, logs of users in the healthcare system, and statistical data usage. The dashboard allows administrators to view user activity and trace user logs with graphical reports and summarized information. The behavioral data produced in this step provides the basis for the next steps of the research, which include data processing, feature engineering, anomaly detection using the Isolation Forest algorithm, behavioral analysis according to the role of the person, calculation of risk score and detection of insider threats in real time.

5. BEHAVIOURAL DATASET AND EXPERIMENTAL ENVIRONMENT

The behavioral dataset contains no specific patient or clinical information, but rather data about users interacting with the EHR system developed. Examples of activities include login/Logout, patient viewing and editing, patient searching, laboratory activities, and medication activities. These records include the users and/or roles involved, department, access time, patient identifier, activity, session information, logs inscribed on sessions, and accessed healthcare resources, all of which provide a foundation for analyzing the patterns of use surging through the roles and the operations of EHRs. The experimental environment comprises of a web-based EHR application, role-based authentication and access control, continuous monitoring of activities, automatic generation of a behavioral-log, and dashboard. It enables the management of patients, healthcare users, departments, medication and lab management. These generated records are processed and aggregated into a structured dataset of behavior, in a controlled setting, to be used to support further studies on behavioral analysis and anomaly detection using AI.

Dataset Statistics

Experimental Setup and Data Generation: The experimental environment was set-up as a web-based Healthcare Electronic Health Record (EHR) system that was based on a controlled healthcare environment. Predefined roles were assigned to authenticated healthcare users, and the allowed activities were carried out in the EHR system. The centralized behavioral activity logging was done automatically by capturing user interactions (identity, role, department, time of access, patient record, action type and session). Behavioral logs were generated and added to the application database as a structured behavioral database. The resulting data set statistics are listed in Table 1.

Table-1 Behavioral dataset statistics computed from the database.

Statistic	Value
Total behavioral-log records	451
Unique users appearing in the logs	6
Total user accounts	11
Roles	10
Departments	18
Hospital branches	10
Distinct patient records referenced	200
Distinct sessions	44
Distinct action types	18
Distinct EHR modules	7

6. Results And Discussion

6.1 EHR implementation

The implemented EHR environment provides authenticated access to healthcare function according to assigned roles. The system successfully supports the activities required for generating user – access behavior.

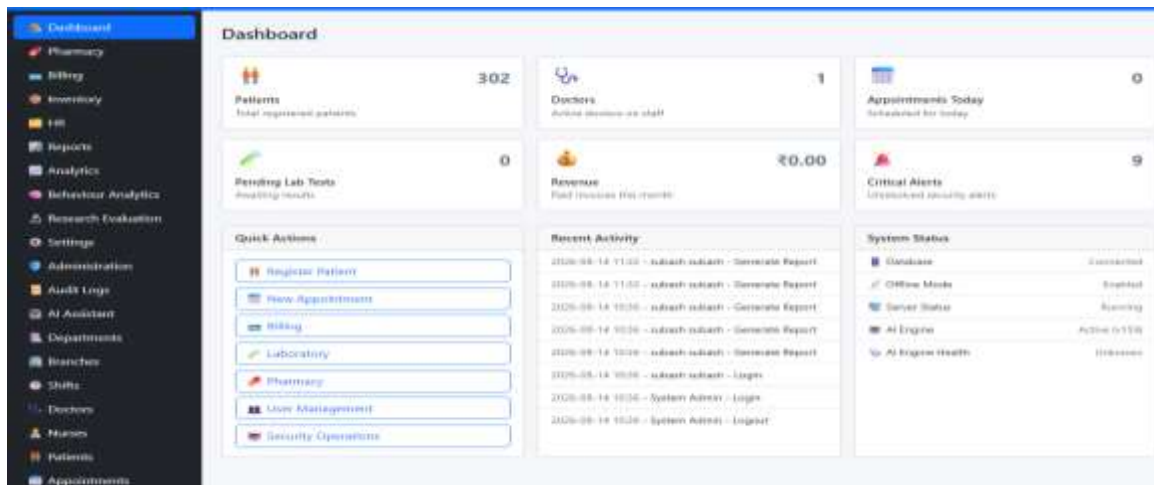


Fig-2: shows the implemented EHR environment

6.2 Behavioral Log Generation

User interaction performed within the EHR environment are automatically recorded as behavioral access logs. The logs capture the activity of each user. During the experimental data collection period, a total of 451 behavioral-log records were generated, for various users, roles, sessions, action types and EHR modules.

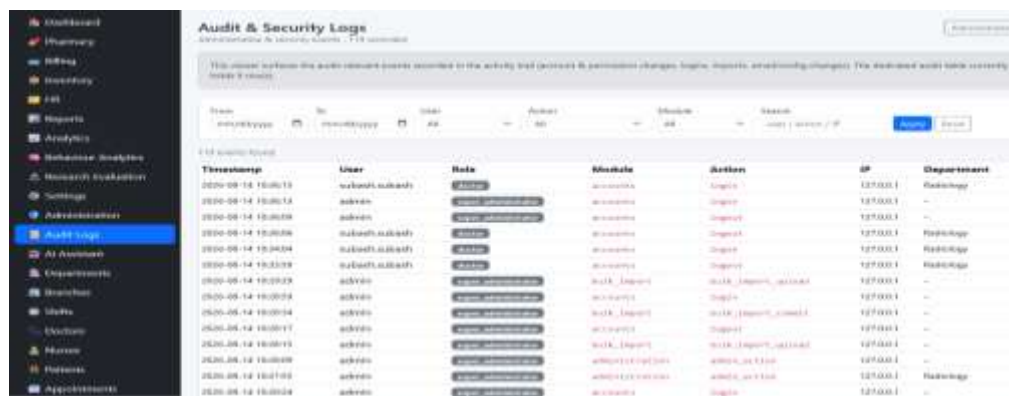


Fig -3 Behavioral Access log -interface

6.3 User/Role/Activity Analysis

The generated record is recorded associates with user activities with their roles and their activity types. This examined the behavioral logs generated according to the user and operational context.



Fig-4 users their Role and Activity types Distribution

The generated behavioral logs were analyzed according to user role and activity type. Table 2 presents the role-wise distribution of the 451 behavioral-log records across the recorded user roles.

Table 2. Role-wise distribution of behavioral-log records

Role	Behavioral-log records	Percentage
Super Administrator	368	81.60%
Doctor	64	14.19%
Nurse	17	3.77%
HR	2	0.44%
Total	451	100%

The generated behavioral logs covered according to Table 3 presents 18 action types, with patient-record updates representing the most frequent activity.

Table 3. Sample access-pattern distribution

Action type	Records	Percentage
Update patient	205	45.45%
Generate report	54	11.97%
View patient	53	11.75%
Login	49	10.86%
Logout	22	4.88%
Admin action	17	3.77%
Create user	13	2.88%
View doctor	13	2.88%
Other recorded activities	45	9.98%
Total	451	100%

The logging capabilities and processing performance were also tested to ensure that the behavioral logs produced are reliable and efficient for processing. Table 4 shows the result

Table 4. Logging Validation and Processing Performance

Evaluation Measure	Result
Total behavioral-log records	451
Duplicate activity-log records	0
Activity timestamp completeness	100%
Activity auto-logging test	PASS
Records processed	448
Average inference time	0.1464 s
Minimum inference time	0.0002 s
Maximum inference time	7.4710 s
Throughput	30.67 events/s
Average processing latency	32.609 ms/event
Degraded events	0

The activity events were recorded by the logging mechanism without an identifier being duplicated, and the performance of the processing pipeline was determined by the measurable degree of inferences and throughput.

The proposed framework achieves both continuous monitoring and automatic log generation of structured behavioral access logs with user, role, activity, temporal and access-related information, which are compared to the conventional access-control mechanisms in EHRs. Table 4 shows the quantitative results, which confirm successful logging and show measurable processing performance, thereby pointing to a reliable basis of data for the following behavior analysis and insider-threat detection within the framework.

Table 5 shows that, unlike conventional EHR security mechanisms that primarily focus on authentication and

access control, the proposed framework extends security monitoring through continuous behavioral logging and structured contextual data generation.

Table 5. Comparison of Conventional EHR Security and the Proposed Behavioral Access-Log Framework

Security/Monitoring Aspect	Conventional EHR Security	Proposed Framework
User authentication	Verifies user identity	Verifies user identity
Access control	Controls access based on permissions/roles	Controls access based on assigned roles
Activity monitoring	Mainly records system access/audit events	Continuously monitors user activities
Behavioral information	Limited behavioral context	Captures user, role, department, time, session and activity context
Behavioral log generation	Not specifically designed for behavioral analysis	Automatically generates structured behavioral access logs
Dataset generation	No dedicated behavioral dataset	Generates a structured behavioral dataset
Future AI analysis	Requires additional data preparation	Provides an AI-ready behavioral data foundation

6.4 Dashboard Analysis

The dashboard provides an administration can view the system activity according to their user roles activity types. It summarizes the behavioral access log information generated by EHR environment.

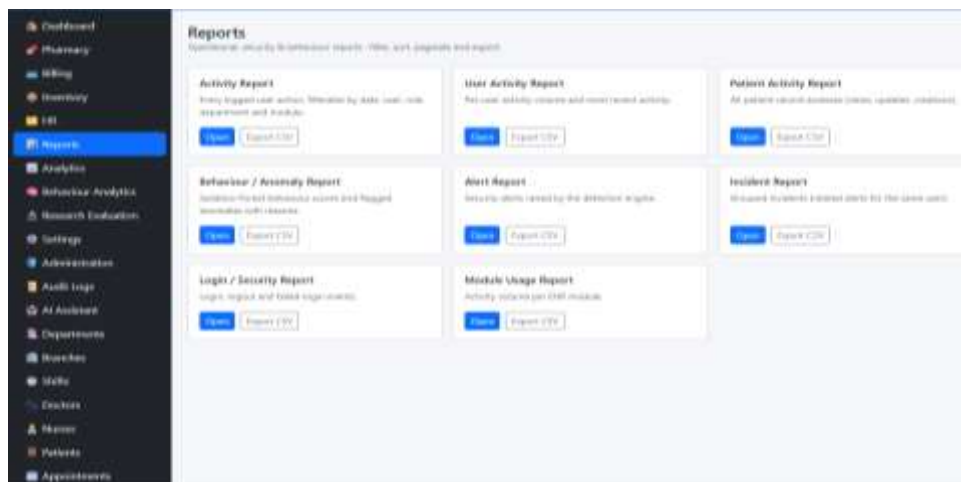


Fig 5- shows the dashboard used to review by the admin about the user activities and access information to be summarized.

6.5 Discussion

The quantitative findings indicate that the framework proposed in this study is effective in generating and structuring behavioral access data from the implemented EHR environment. The data set consists of 451 behavioral-log records from 6 users, within an environment containing 10 configured roles, 44 sessions, 18 action types and 7 EHR modules. The role-wise and activity-wise distributions illustrate that the logging mechanism can include behavioral data of the different user roles and EHR operations. The success of the activity logging validation further validates the automatic activity logging and the processing results in the measured activity further validate that the implemented system can process behavioral events with a measured throughput of 30.67 events per second for the tested configuration. The quantitative results offer measurable evidence of operation and success of the behavioral access-log framework implemented.

7. LIMITATION AND FUTURE RESEARCH

7.1 Limitations

While the proposed framework offers a structured method in capturing the behaviors of the healthcare users, there are some considerations. The data in the study is de-identified healthcare-derived behavior data and a controlled synthetic proxy dataset; hence the behavior observed may not reflect the full scope of behavior across various healthcare institutions. The synthetic environment can also be useful for controlled and repeatable testing, but it is not enough to mimic the complexity of operation environments in hospitals. The current study also focuses on the monitoring of user activities, the generation of behavioral log and the creation of the datasets instead of reporting the performance of the final anomaly detection model. The activities recorded also are not necessarily validated as insider threats without appropriate behavior and ground truthing.

7.2 Future Research

The created behavioral data can be used as a basis to further the research into AI-based detection of insider threats in healthcare EHR systems. Future work will examine and contrast appropriate anomaly-detection methods which can detect deviations from normal authorized-user activity. As part of the analysis, role-aware behavioral modelling will be used, enabling activities to be assessed in terms of role-specific behavioral patterns, rather than using the same expectations for everyone. They will then explore risk scoring and real-time detection as followed by automated alert generation and notification of suspicious behavior. The developed approaches will be assessed using suitable metrics like accuracy, precision, recall, F1-score, ROC-AUC, false positive, and detection time. This will enable the evolution of a more context-aware and practical security mechanism to identify potential insider threats to healthcare EHR environments.

8. CONCLUSION

A role-aware behavioral access-log framework for EHR system was proposed in this study. The framework combines user authentication, role-based access control, continuous activity monitoring, automatic generation of behavioral-log, structured creation of datasets and dashboard-based monitoring. The access logs generated, are structured and contain relevant attributes of the users and the context of their interactions, which is valuable for the healthcare domain. These results illustrate how the framework can systematically capture activities carried out in the EHR context and how they can be arranged into a behavioral data, that is available for security analysis. The framework extends access control to give greater context to understanding the actions of authorized users.

The behavioral dataset generated will serve as a basis for further studies in AI anomaly detection and insider-threats identification, such as role-aware behavioral analysis, risk assessment, real-time detection, and automated alerting. Therefore, the proposed framework provides a structured and controlled foundation for the creation of more intelligent and context-aware security mechanisms in health care EHR environments.

References

1. The American Medical Informatics Association. (n.d.). Information technology and health records. AMIA.
2. Bishop, C. M. (2006). Pattern recognition & machine learning. Springer.
3. Breunig, M. M., Kriegel, H.-P., Ng, R. T., & Sander, J. (2000). LOF: Local Outlier Factor is a method for detecting local outliers. In Proceedings of the 2000 ACM SIGMOD International Conference on Management of Data, pages 93-104.
4. Chandola, V., Banerjee, A., & Kumar, V. (2009). Anomaly detection: A survey. ACM Computing Surveys, 41(3), 1-58.
5. Hochreiter, S., & Schmidhuber, J. (1997). Long short-term memory. Neural Computation, 9(8), 1735-1780.
6. Hurst, W., Tekinerdogan, B., Alskaf, T., Boddy, A., & Shone, N. (2022). Securing electronic health records against insider-threats: A supervised machine learning approach. Smart Health,
7. Kwon, D., Kim, H., Kim, J., Suh, S. C., Kim, I., & Kim, K. J. (2019). Survey of Deep learning-based network anomaly detection. Cluster Computing, 22, 949-961.
8. B., Maschler, B., Sahlab, N., & Weyrich, M. (2021). Survey on Anomaly Detection in Technical Systems based on LSTM Networks. Computers in Industry, 131, 103498.
9. Liu, F. T., Ting, K. M., & Zhou, Z.-H. (2008). Isolation forest. In Eighth IEEE International Conference on Data Mining, 2008.
10. Patcha, A., & Park, J.-M. (2007). Introduction to Anomaly Detection Methods: Current solutions and recent developments in technology. Computer Networks, 51(12), 3448-3470.
11. Sakurada, M. and Yairi, T. (2014). Anomaly detection based on Autoencoders with nonlinear dimensionality reduction. In Proceedings of the ML-SDA 2014 2nd Workshop on Machine Learning for Sensory Data Analysis, 4-11.
12. Shen, J., Deng, C., & Zhou, J. (2019). Security and privacy of EHRs: A review. International Journal of Medical Informatics, 130, 103929.

13. Shin, S. Y., & Hwang, J. (2020). Ethical and privacy issues related to the use of EHRs. *Healthcare Informatics Research*, 26(2), 73–82.
14. Sittig, D. F., & Singh, H. (2010). A new sociotechnical model for studying health information technology in complex adaptive healthcare systems. *Quality & Safety in Health Care*, 19(Suppl 3), i68–i74.
15. Tiwari, B., & Kumar, A. (2015). Access control based on roles and on-demand classification of electronic health record. *International Journal of Electronic Healthcare*, 8(1), 9-24.
16. Zhang, R. (2014). Access and control of EHR data based on roles and time periods. *Security and Communication Networks*, 1–10.
17. Zhang, Y., Qiu, M., Tsai, C.-H., Hassan, M. M., & Alamri, A. (2017). Health-CPS: Healthcare cyber-physical system assisted by cloud and big data. *IEEE Systems Journal*, 11(1), 88–95.