Expert System for Detection of Intrusion in Healthcare Sector

Sonal Shukla, Piyush Singh, Shailesh Pratap Singh, Shivang Krishn
Senior Guide, Author, Author, Author.
Galgotia College of Engineering and Technology,
Knowledge Park, Greater Noida, U.P., India
sonal.shukla@gmail.com, piyushsingh2429@gmail.com, shaileshpratapsingh21@gmail.com, shivangkrishn@gmail.com

Abstract—Because healthcare organizations are becoming dependent on digital systems for maintaining for storing and maintaining patient data and offering services due to which they have become the prime targets for cyberattacks. Healthcare providers face a significant challenge in protecting patient security and privacy because threats have become more advanced through data breaches and unauthorized network intrusions. This study shows how some of the Artificial Intelligence technologies can improve the functionality of IDS functionality in the healthcare industry.

AI uses advanced ML and some basic DL algos such as SVM, RF, Autoencoders, RNN, and NLP to effectively detect anomalies and prevent unauthorized data injections while accurately identifying spoofed data. Through real-time anomaly detection combined with predictive modelling and adaptive learning strategies this proposed method enhances healthcare systems' defences against advanced cyber threats.

AI based intrusion detection system can also enhance the protection of data which helps in increasing the trust in digital healthcare platforms while maintaining and keeping patient data confidentiality and handles medical operations.

Keywords—: **Expert System, Intrusion Detection, Data Injection, Data Spoofing, Cyber Threats, Healthcare Security.**

1. INTRODUCTION

AI uses advanced ML and some basic DL algos such as SVM, RF, Autoencoders, RNN, and NLP to effectively detect anomalies and prevent unauthorized data injections while accurately identifying spoofed data. Through real-time anomaly detection combined with predictive modelling and adaptive learning strategies this proposed method enhances healthcare systems' defences against advanced cyber threats.

AI based intrusion detection system can also enhance the protection of data which helps in increasing the trust in digital healthcare platforms while maintaining and keeping patient data confidentiality and handles medical operations.

[I] Problem Understanding

The healthcare sector works as the complicated ecosystem intended to provide major medical services, such as patient care management, and the promotion of public health in general. It encompasses to the various stakeholders.

Lately, the digital technology is used for its efficiency and data-driven insights with better patient records management.

a. Risks Associated with Healthcare Data

The sector of healthcare is exposed to some of the several major risks, including privacy, data security, and operational continuity, among others. The most important concern is the threat of cyberattacks [1] such as data breaches or ransomware, due to which sensitive patient information it can also ruin the essential services. These attacks may compromise Electronic Health Records (EHRs), exposing personal or financial data of patients, leading to potential identity theft or fraud.

b. Why Healthcare Needs Robust Safety Measures?

The current industry of healthcare requires brilliant security to protect the most personal patient information, maintain business continuity and to retain trust. In this regard, robust security measures are essential to prevent breaches in the data and ransomware attacks and maintain privacy and avoid major threats such as unauthorized access besides maintaining compliance with legal regulations.

Expert systems for detection of intrusion in healthcare explains this need as they provide automated, intelligent mechanisms helps to detect or respond to suspicious activities accordingly in real-time. Sometimes the systems employ the combination of some pre-defined rules, historical data, or monitoring network traffic, user behaviour, and system anomalies, expert systems can improve major security problems of health and welfare institutes and minimize the risk of severe violations of data activities.

[II] Literature review

Summary of some of the reported studies on intrusion, access control or to detection of any malware.

Intrusion detection has evolved from simple rule-based systems to an advanced solutions leveraging machine learning and AI. The early systems focused on predefined signatures, but modern approaches emphasize anomaly detection, behaviour analysis, and real-time threat mitigation. These advancements address sophisticated threats like zero-day attacks particularly in sensitive domains like healthcare, where protecting critical data is essential.

Table 1: Summary of the studies and their conclusions

AUTHOR OF PAPER	DESCRIPTION OF STUDIES	TYPES OF INTRUSION DETECTED	TOOLS	USEFUL FEATURES	GAP OR LIMITATION
1. Begli M, Derakhshan F, Karimipour H. 2019. [1]	Layer system for detection of any intrusion with the help of some machine learning algos.	Anomaly or signature based	R- Program	Detection accuracy is high, Detection time is satisfied.	Detection rate is low during misuse analysis, very high memory overhead
2. Rathore H, Fu C, Mohamed A, Al-Ali A, Du X, Guizani M, Yu Z. 2018b." [8]	Using Multi-layer scheme of security for medical devices which are implantable.	Legendre approximation or MLP	MATLAB, Keras, Theano	Testing accuracy is high.	unknown attacks are tough to detect.
3. Schneble W, Thamilarasu G. 2019b [3]	Optimal selection of feature for the detection of intrusion in medical cyber-physical systems.	Injection of false data, Changing forms of data, DoS IDS	Sci-kit Learn's on Raspberry Pi's, using MATLAB	Simultaneous multiple attack can be detected, accuracy is high, FPR Flexible is lower.	Accuracy is reduced and FPR is increased, weak against some cases that are adversarial.
4. Alrashdi I, Alqazzaz A, Alharthi R, Aloufi E, Zohdy MA, Ming H. 2019 [4]	FBAD: Detection of Fog-based attack for the IoT in healthcare for smart cities.	Anomaly based NIDS	Python (scikitlearn, Tensorflow, Keras, Numpy)	Very Low latency when compared to cloud-based.	Memory or CPU usage is not considered
5. Swarna Priya RM, Maddikunta PKR, Parimala M, Koppu S, 2020.[5]	DNN used in IoMT for intrusion detection using the hybrid PCA-GWO.	Signature based IDS NIDS	Not mentioned	Very high accuracy rate and also low time of testing.	Memory and CPU overhead is high, can only be used for IP based devices
6. Landau O, Cohen A, Gordon S, Nissim N. 2020 [6].	Mind your privacy: Privacy leakage through BCI applications using machine learning methods	Detection of privacy attack	Not mentioned	Performance is improved, larger datasets can be used.	High error rate, Accuracy is still low.

[III] Problem formulation

Intrusion detection in healthcare is critical due to the sensitive nature of patient data, reliance on interconnected medical devices, and stringent regulatory requirements. Some of the important healthcare problems that can be dealt with by intrusion detection are:

1. Protecting the Electronic Health Records (EHRs)

Unauthorized access resulting theft of EHRs may lead to some breaching of data, compromising privacy of patient and major regulations like HIPAA.

2. Protection from ransomware attacks

Ransomware attacks are very common against healthcare organizations.

3. Monitoring the network traffic in different hospital systems

Hospital networks which are large are very prone and susceptible to attacks.

4. Identifying insider threats

Legitimate insiders can abuse their access to data and can misuse the stolen data.

5. Addressing the real-time response challenges

Intrusion detection is often post-event, and responses are late which leads to dangerous circumstances.

[IV] Technologies and Techniques to Use

Intrusion detection in healthcare uses various technologies such as machine learning (SVM, Random Forest, KNN) for accurate detection of threat, AI for identifying anomaly, and blockchain for ensuring data integrity. Along with encryption, IoT security, and cloud-based monitoring, the security is robust enough for the protection against evolving cyber threats.

Machine Learning (ML): For anomaly detection and behavioral analysis.

Signature-based Detection: For identifying known threats and patterns.

Deep Packet Inspection: To predict network of traffic for granular level.

Threat Intelligence Integration: Use threat databases to improve detection accuracy.

[V] Proposed Work:

Such algorithms can learn patterns and identify anomalies as a result of spoofing attempts.

a. Support Vector Machines (SVM): SVM are the algorithms of ML which can use taken for the classification: linear may be for the nonlinear. It can also be used in regression or detection of outlier tasks.

b. Trees and Random Forests: These algorithms excel at making clear decisions used on defined features, as suspicion in some of IP addresses or unusual login times.

c. K-Nearest Neighbours (KNN): Ideal for detecting anomalies by comparing new data points with known legitimate data.

These algorithms helps in improving the detection accuracy, learn complex patterns from malicious activities, and provide robust defence against evolving cyberattacks, therefore providing stronger protection to the sensitive healthcare data.

Table 2: Data breaches in healthcare with different types of disclosure.

Years	Data Breaches Number	Theft or Loss of data	Hacking or reported IT Incidents	Unauthorized Access	Unknown	Exposed Records in Millions
2018	365	55	158	143	0	33.200
2019	505	51	274	142	31	41.200
2020	393	37	262	77	4	18.57
2021	734	134	387	198	20	57.120
2022	542	85	264	147	9	42.780
2023	573	83	276	183	16	49.862

Some of the major problems in healthcare related to intrusion detection solutions are as follows:

There are basic solutions to major problems in healthcare:

1. Defending the Electronic Health Records (EHRs)

The intrusion detection systems\can be developed that can monitor the access patterns to EHR databases, to identify suspicious behaviours such as unauthorized queries.

2. Identifying insider threats

Implementing some behavioural-based IDS to identify differences from normal activity.

3. Securing Medical Devices (IoMT - Internet of Medical Things)

Utilize IDS which tracks communication between devices for any unusual traffic, malware, or unauthorized access attempts.

4. Preventing major ransomware attacks

Identify ransomware activity by scanning for any pattern of unusual file encryption patterns or sudden increased in data access, to prevent attacks.

5. Addressing real-time response challenges

Integrate real-time IDS with response automation devices to immediately isolate affected systems and minimize the damage instantly.

[VI] Conclusion

This paper of research shows some valuable estimation of the correctness of ML models used to the detection of intrusion in the field of IoMT, resulting to strengthening into the security fields measures and to protect the data which is very sensitive. This paper is mainly foccuses on the learnning techniques such as: boosting and stacking of data using the RF and the SVM as the base models, and helps to evaluate some of the approaches to help the WIUSTL-REHMS-2022 dataset.

The study of the performance, including acccuracy of algos, precizion of algos, recall of algos, due the f1-score of algos, which shows that the Sttacking algo achieved high acccuracy and high reliability, with a brilliant rate of accuracy that is 97.63%. Bagging is very close with a rate of accuracy of 95.17%, while boostting is realizable and effective, but observed some lower rate of accuracy of 85.73%.

This paper showcase some better performance of the stacking or the bagging in detection and classification of some cyber-attacks occurrence and also showcasing their true potential to greatly improve the security of IoMT services.

REFERENCES

1. Begli M, Derakhshan F, Karimipour H. 2019. "A layered intrusion detection system for critical infrastructure using machine learning".

2. Itten A, Vadakkumcheril GT. 2016. "Enhanced intrusion detection system in medical cyber physical systems using multivariate correlation analysis"

3. Schneble W, Thamilarasu G. 2019b "Optimal feature selection for intrusion detection in medical cyber-physical systems."

4. Swarna Priya RM, Maddikunta PKR, Parimala M, Koppu S, Reddy T, Alazab M. 2020. "An effective feature engineering for DNN using hybrid PCA-GWO for intrusion detection in IoMT architecture".

5. Landau O, Cohen A, Gordon S, Nissim N. 2020. "Mind your privacy: Privacy leakage through BCI applications using machine learning methods."

6. Alrashdi I, Alqazzaz A, Alharthi R, Aloufi E, Zohdy MA, Ming H. 2019. "FBAD: Fog-based attack detection for IoT healthcare in smart cities."

7. Mohsen NR, Ying B, Nayak A. 2019. "Authentication protocol for real-time wearable medical sensor networks using biometrics and continuous monitoring."

8. Rathore H, Fu C, Mohamed A, Al-Ali A, Du X, Guizani M, Yu Z. 2018b. "Multi-layer security scheme for implantable medical devices."

9. Al-Garadi, M.A.; Mohamed, A.; Al-Ali, A.K.; Du, X.; Ali, I.; Guizani, M. A survey of machine and deep learning methods for internet of things (IoT) security.

10. Alalhareth, M.; Hong, S.C. An improved mutual information feature selection technique for intrusion detection systems in the Internet of Medical Things.