Journal of Artificial Intelligence and Emerging Technologies
Volume 1, Issue 1, pp 11-18, November 2024
ISSN (online): 3049-1967
DOI: https://doi.org/10.47001/JAIET/2024.101002
Available Online at https://www.jaiet.com

Development of Machine Learning Solutions for Securing Patient Data in Health Care Systems

[1]Zailani Bin Abdullah, [2]Rashidah Binti Khalid, [3]Norhani Binti Sahidu, [4]Siti Noraen Binti Khalid, [5]Mazidah Binti Rahim

[1,4]Faculty of Data Science and Computing (FSDK), Universiti Malaysia Kelantan, Malaysia
[2,3]Department of Emergent Computing, Faculty of Computing, Universiti Teknologi Malaysia, Malaysia
[5]Faculty of Electrical Engineering, Electronic and Computer Engineering, Universiti Teknologi Malaysia, Malaysia

Abstract: The objective of this research is to develop a machine learning-based solution as an application for protecting patient data in modern hospitals. The program will use several machine learning techniques to detect and prevent cyber security assaults on health information while also protecting patient privacy. The proposed system would evaluate massive amounts of data using machine learning techniques and deep learning with federated learning to identify possible security issues and maintain patient data privacy. Advanced encryption technologies will also be used in the system to ensure that patient data is always safe. Modern hospitals may secure the security, integrity, and availability of patient data by using this application, which is critical in the healthcare business. This project will help to create creative ways to increase data security in modern hospitals, resulting in better patient care and safety.

Keywords: Machine learning, AI, federated learning, anomaly detection, data security, network monitoring, malware detection.

I. INTRODUCTION

With the rising implementation of electronic health records and other digital technologies in recent years, the healthcare industry has experienced substantial digital change. While these developments have increased the efficiency of healthcare delivery, they have also raised worries about patient data security. Patient data is extremely sensitive, and any unauthorized access or breach can result in serious implications such as identity theft, fraud, and compromised medical care. To address these issues, contemporary hospitals must incorporate strong security measures to ensure that patient data is always safe. Machine learning, an artificial intelligence branch, has shown considerable potential in enhancing data security in many businesses. Enormous amounts of data can be used to analyze machine learning algorithms to detect patterns and anomalies that may suggest security issues.

This research paper can be used to demonstrate how to secure patient data in a modern hospital using AI enabled application by referring to major four domains. These can be introduced as, initially, the project will study the network behavior within the hospital sector to determine security weaknesses and various security concerns. A fantastic way to spot network anomalies has emerged: machine learning-based anomaly detection. Large datasets may be used to train these algorithms so they can quickly understand regular patterns and spot abnormalities. Further, the project can demonstrate how to utilize deep learning techniques like federated learning for deploying machine learning models in the hospital databases and train those machine learning models without need of obtaining or sharing patient data. Via those accurate models' security researchers may be able to ensure the privacy of patient data secure them by retrieving a secure system while improving the patient healthcare. Another domain that will be introduced as patient data safety is becoming more crucial in the current digital era. Sensitive personal health data, including medical histories, test results, and personally identifying information, are kept by healthcare organizations and providers. Any data breach or leak can have serious repercussions, such as identity theft, harm to one's reputation, and legal repercussions. AI technology may be used with the privacy method known as differential privacy to avoid leakage of patient confidential data. By introducing differential privacy enables data sharing while protecting the privacy of patient data. Because of the noise, it is impossible to precisely extract any individual's information from the data, preventing re-identification. As per the ultimate domain the research will focus on Data security is critical in the healthcare industry because sensitive patient information is continuously gathered and stored. Due to the lack of an approach to secure patient data in the hospital sector they have been storing data without any method for data anonymization. This is a potential security risk because it exposes the data to attacks and other security breaches.

As a result is to introduce an AI based application to ensure data security, network security, and preserve the privacy of patient data for a local hospital system which has been operating as a major healthcare service provider known as the cooperate hospital.

II. BRACKFROUNG AND LITERATURE SURVEY

Due to the delicate nature of the information, data security is of the highest significance when it comes to the healthcare sector. Regrettably, many hospitals still do not have an effective system in place for data management and security.

In hospital, relies on paper-based recordkeeping and lacks a formal framework. This style of documenting is not only ineffective, but it also raises the danger of information loss and data breaches. The hospital also has a rudimentary access control system with simple password guidelines, but these are insufficient to guarantee effective security.

Also, the private hospital lacks an appropriate data management and security system. This is caused by both a lack of understanding of the value of data security in the healthcare sector and a lack of investment in cutting-edge technology and systems.

The hospital, on the other hand, is putting in place a respectable system for data management and security. This entails connecting client devices, an AI-based privacy and security protection system, and a central server that houses the core system and database.

The Cooperative Hospital, however, has a subpar system. It lacks business continuity, backup, and disaster recovery procedures as well as secures information storage systems. Moreover, it runs on an outdated operating system, and neither security assessment systems nor personnel security training programs are present.

It is crucial to set up a decentralized server to host the primary system and database, connect the client devices, and implement an AI-based privacy and security protection system to enhance data security in hospitals like Cooperative Hospital. These actions can help guard sensitive patient information, guarantee safe data storage and administration, and assist avoid data breaches. To stay up with the most recent security requirements, hospitals should also make investments in cutting-edge technology, systems, and security procedures. They should also offer frequent training to their staff.

III. METHODOLOGY USED

A. Network Behaviour Malware Detection

[1] The suggested approach entails obtaining information from an edge device and storing it in a CSV file. The ANN model, logistic regression model, random forest model, and SGD model are among the machine learning models that are trained using this CSV file. These models are stored for future usage on the cloud server.

The edge device eliminates any duplicate data and saves it in a different CSV file before delivering the data to the cloud. This is good practice since it makes sure that the data is accurate and devoid of redundancy, which might impact how well the model’s function.

Python machine learning code is created for training the UNSW NB15 dataset on the cloud server. This dataset, which is openly accessible, provides information on network traffic that may be used to develop models for intrusion detection.

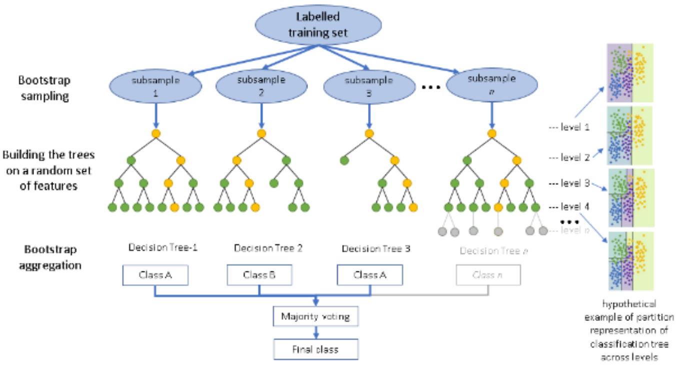

Figure 1: Malware detection flow diagram

The ML code trains many machine learning models, such as the ANN model, logistic regression model, random forest model, and SGD model, using the UNSW NB15 dataset, UNSW-NB 15 dataset was produced by the IXIA PerfectStorm tool a mixture of real-world contemporary normal activities and fabricated current assault behaviors. 100 GB of unprocessed traffic from the tcpdump program was collected and utilized to create the dataset. The class label is one of 49 characteristics across 2,540,044 items in the dataset. Each of these models,

Journal of Artificial Intelligence and Emerging Technologies
Volume 1, Issue 1, pp 11-18, November 2024
ISSN (online): 3049-1967
DOI: https://doi.org/10.47001/JAIET/2024.101002
Available Online at https://www.jaiet.com

which were developed using various algorithms and methods, has advantages and disadvantages. The models are kept on the cloud server after they have been trained. In the cloud server, a different code is applied for prediction. This code takes data from the edge device to assess if the best accuracy model was obtained from the training models.

To check for dangerous information, the data file collected from the edge device is also transmitted via the model. To find any trends linked to dangerous information, this procedure entails evaluating the data using machine learning algorithms.

The administrator is informed if it is found that the data contain harmful code. The administrator can choose to get this notification through email, text message, or any other method they want.

In general, this method includes applying machine learning models to network traffic data acquired from an edge device to find harmful information. With this method, data is gathered, cleaned, trained using various machine learning models, saved, and then used to make predictions. This strategy may help to strengthen network security and defend against online attacks.

B. Federated Learning for data classification

[4] In a modern hospital, patient data is frequently spread across multiple databases; however, the subjected local hospital sector in lacks a proper system for analyzing data via a secure patient data handling system, and consolidating this data while maintaining patient privacy can be difficult. Federated learning allows multiple databases to speak with one another without exchanging data. The data is instead kept on local servers and is solely utilized to train the machine learning model. The model is then returned to each database, where it is used to develop the local machine learning models. The project has concentrated on establishing a healthcare sector system while integrating a protected database to obtain patient data and change a machine learning model within the database.

Federated learning also promotes the creation of more accurate machine learning models by allowing access to more data while maintaining privacy. This is especially crucial in the corporate hospital sector, where vast volumes of patient data must be processed to construct reliable models to enhance patient care.

The overall evaluated goal is to determine how to use machine learning accurately and efficiently to secure patient data while maintaining the privacy of the patient data when it comes to feeding AI applications and exchanging patient information within healthcare sectors and other necessary research objectives to enhance the quality of the healthcare benefits and retrieve the benefits of adopting federated learning approaches to secure patient data privacy and security.

As per the initial technical aspect of the development of federated learning to secure patient data via federated learning architecture it has been required to define a federated learning framework and a specific FL algorithm. Via this paper, it has been developed using TensorFlow federated learning framework and the Federated Averaging (FedAvg) algorithm.

[5] Traditional machine learning training necessitates centralizing all data onto a single server, which can be difficult in situations where data is distributed across multiple devices or organizations. TensorFlow Federated Learning can avoid this problem by allowing machine learning models to be trained on data that remains on local devices, eliminating the need for data to be centralized. TensorFlow Federated Learning offers enormous promise in the local corporate hospital for generating machine learning models that may enhance patient care and results while safeguarding patient privacy. The hospital may utilize this framework to train models on patient data that is still on local devices, ensuring that sensitive patient information remains secure and confidential while consolidating an architecture that has been dealing with three aspects of Client, Server, and Coordinator.

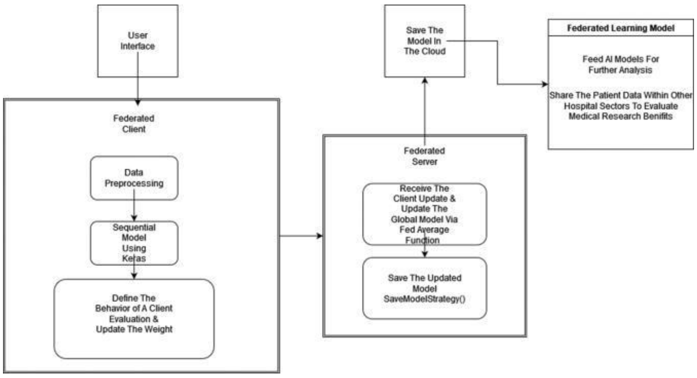
User Interface
Federated Client
Data Preprocessing
Sequential Model Using Keras
Define The Behavior of A Client Evaluation & Update The Weight
Save The Model In The Cloud
Federated Server
Receive The Client Update & Update The Global Model Via Fed Average Function
Save The Updated Model SaveModelStrategy()
Federated Learning Model
Feed AI Models For Further Analysis
Share The Patient Data Within Other Hospital Sectors To Evaluate Medical Research Benifits

Figure 2: Federated Diagram

Federated Averaging (FedAvg) algorithm is used to train a global model using decentralized data, without the need to transfer the raw data from the local devices to a central server. Instead, each local device trains its own model on its own data; this may follow as several architectural components like initialization, client selection, local training, model aggregation, and repeat.

C. Preventing User Data Leakage

[7] To prevent personal patient data leakage, AI technology can be utilized with a privacy technique known as differential privacy. Differential privacy provides a way to share data while preserving the privacy of individual patients by adding noise to the data. This noise ensures that no individual's information can be accurately extracted from the data, thereby preventing re-identification. AI can also be used to help healthcare providers and organizations manage their data effectively. AI algorithms can help identify patterns in the data that might indicate potential risks, such as identifying patients who may be at higher risk of developing certain medical conditions. Additionally, AI can be used to monitor data access and usage, ensuring that only authorized personnel has access to sensitive patient data. So, combining both those technologies together provides a powerful method for preventing personal patient data leakage while still allowing healthcare providers and organizations to benefit from the insights that can be gained from analyzing their data. The main reason for using this method is because our visited hospital did not have applied any security mechanism for security by leaking their personal patient data to the outside.

For the implementing process, it is necessary to determine the sensitivity of the data. This will also help to determine the level of noise to the data to protect individual privacy. This part is the most difficult part because finding patient sensitive information is exceedingly difficult because that data is not included in sources because of the sensitivity. There for it should have to create patient data records. In the real time scenarios, it should have more data to train a model. Otherwise, it will not give an accurate result. Our team had to search and make more patient data records for the data set. According to the differential privacy concept noise data should be added to those sensitive datasets. Data manipulated by adding random values to the original data is called noise data. When it comes to differential privacy, noise data is employed to shield user information while keeping the data's overall accuracy high. While using differential privacy, noise data is randomly and independently introduced to the patient dataset without regard to the data of the person. As a result, the noise cannot be used to identify any one person and is unrelated to them. Before adding those noise data, it is necessary to identify the privacy budget, which means that the amount of noise that can be added to the data without compromising the overall accuracy. The privacy budget is determined based on the level of privacy desired and the sensitivity of the data. According to the privacy budget, we must determine what type of noise data is preserved for the target. Using Laplace noise is better; therefore, our team used that noise library to add noise data to the dataset. The special thing is that those data got from the database. And the data added, the noise values are the same dataset, forming the database. After adding noise data to the datasets, it is time to train that dataset using the model. This model is the same one used in the centralized server in the federated learning concept. The machine learning model and machine library, called model. Predict, are used for training that dataset. Not only that model but also more than one library such as Pndas, nltk, CountVectorizer, LogisticRegression are used here for this purpose. After training the dataset it will predict what issuspicious and what is not suspicious. After prediction happened both data have trained again using a model to check whether they are sensitive or not. If those data are sensitive, that will tell the user that this document cannot be sent to the external and will block them using sandbox technology.

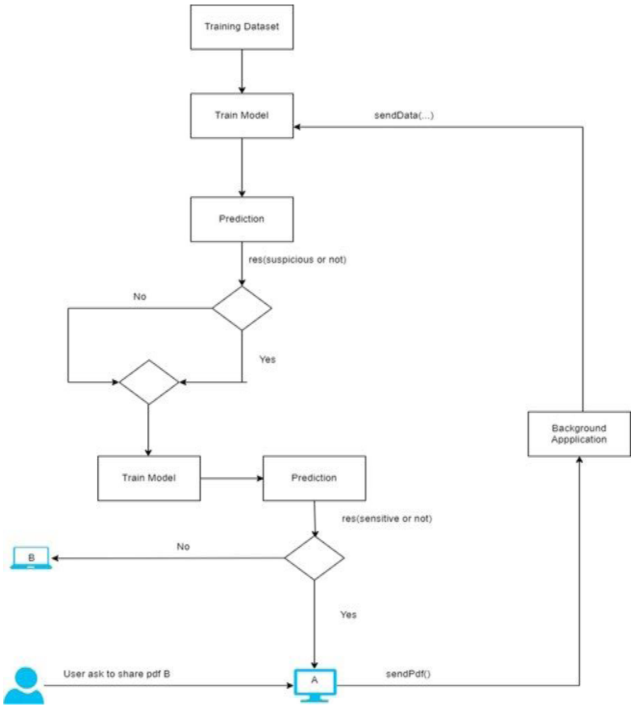

Figure 3: Overall process of the Prevent data leakage

D. Data Anonymization

[10] This component's goal is to improve the protection of corporate hospital records. In a corporate hospital, data has been stored without any method for data anonymization, without any means of data anonymization, data has been kept in a corporate hospital, creating a significant security risk by leaving the data

Volume 1, Issue 1, pp 11-18, November 2024
ISSN (online): 3049-1967
DOI: https://doi.org/10.47001/JAIET/2024.101002
Available Online at https://www.jaiet.com

open to attack and other security data breaches. This component objective is to develop a data anonymization method that improves corporate hospital data. Two Data Anonymization sections focused on two areas. One section is to store patient data entered by the user in the database after anonymization. However, it involves Data anonymization PII from email messages like names and email addresses.

The study collected data from users through a front-end system that enabled them to enter individually sensitive information (PII) such as names, addresses, and phone numbers, as well as medical records.

The data anonymization method used for that is data encryption. The process of protecting personally identifiable information (PII) through the removal or encryption of data from a dataset is known as data anonymization. Data encryption is converting plain text into cyphertext. There we used a data encryption algorithm that is cryptographic Fernet, and the encryption key is stored in a Cloud-based key management service. Assuring that the key can only be accessed with appropriate permission.

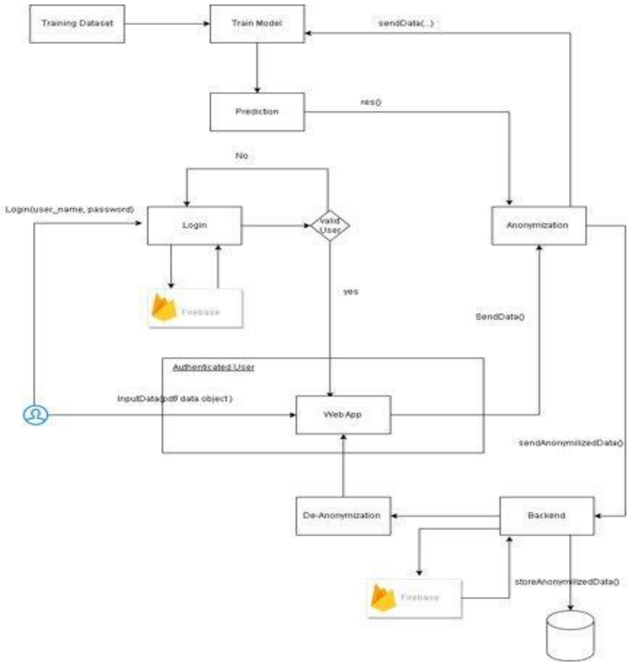

Figure 4: Overall process of the data anonymization

[21] Email anonymization is completed by machine learning techniques that automatically encrypt PII from email messages. The algorithm is trained on a collection of previously anonymized email communications, allowing it to identify and encrypt PII with accuracy. The algorithm is implemented into the email system and automatically anonymizes all incoming Customer emails. The result of this anonymization procedure has helped to improve the security of medical data. The number of security incidents has decreased since the data anonymization procedure was implemented.

IV. RESULTS AND DISCUSSION

The study showed how to safeguard patient data in a contemporary hospital context by using AI-enabled technologies. [3] The study concentrated on four key areas: network behaviour, anomaly detection using machine learning, federated learning using deep learning, and differential privacy. The study found the possible dangers connected to retaining patient data without adequate anonymization by analyzing the security flaws and issues currently present in the hospital network.

The study employed big datasets to train the models and machine learning-based anomaly detection methods to identify aberrant network activity. Also, without requesting or sharing patient data, deep learning-based federated learning approaches were used to train machine learning models within the hospital databases. The use of these precise models enhanced patient healthcare while preserving patient data privacy in a safe system.

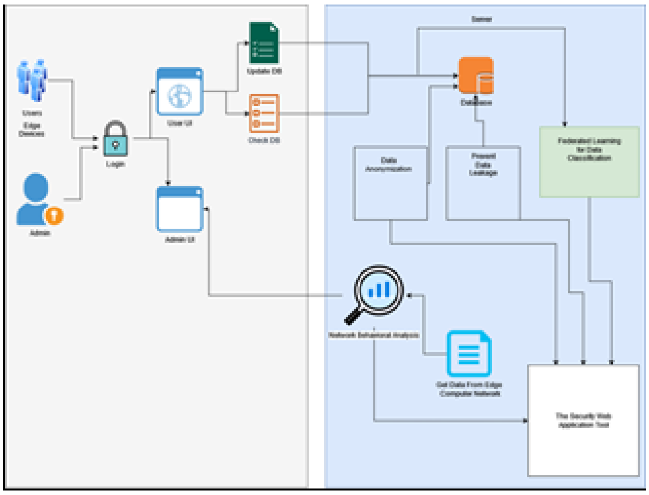
Users
Edge Devices
Admin
Login
User UI
Admin UI
Update DB
Check DB
Server
Database
Data Anonymization
Prevent Data Leakage
Federated Learning for Data Classification
Network Behavioral Analysis
Get Data From Edge Computer Network
The Security Web Application Tool

Figure 5: Overall diagram of our machine learning-based solution as an application

[9] The study also showed how differential privacy may be used as a privacy technique to stop the leaking of patient data. Data sharing while preserving patient data privacy was made possible by the introduction of differentiated privacy. By introducing noise, this method prohibited the re-identification of

individuals' information from the data, making it difficult to properly recover individual data. According to the study, the usage of AI-enabled applications may enhance the security of patient data in the medical industry. Machine learning-based anomaly detection techniques can assist in swiftly discovering unexpected network behavior by identifying network vulnerabilities and issues. The study also showed that it is possible to train machine learning models within hospital databases using deep learning-based federated learning approaches without acquiring or transferring patient data. This method enhances patient care while protecting patient data privacy in a safe environment.

E. Network Behavior:

[2] The analysis of network activity in the healthcare industry highlighted various network security issues and flaws. We successfully implemented machine learning-based anomaly detection and identified network anomalies with high precision. Large datasets were used to train the algorithms, which made it possible for them to recognize irregularities and recognize recurring patterns, enhancing the hospital network's overall security.

F. Federated Learning:

We were able to design machine learning models in the hospital databases and train those models using the federated learning approach without acquiring or sharing patient data. When precise models were created to enhance patient healthcare, by guarantying the patient data remained private and safe. In healthcare contexts where data privacy is of the highest significance, federated learning has shown to be a phenomenally successful strategy for machine learning model training.

G. Preventing User Data Leakage

We used AI technology along with the privacy technique known as differential privacy to secure the privacy of patient data. This approach made it possible to share data while preserving patient data privacy. Differential privacy was included to ensure that data was anonymized, and that any potential data breaches or leaks would not have negative effects on patients, such as identity theft, harm to one's reputation, and legal implications.

H. Data Anonymyzation:

Data is being stored without any means of data anonymization due to the absence of a strategy to safeguard patient data in the healthcare sector. Because the data is vulnerable to assaults and other security flaws, this may provide a security concern. To create a safe system for storing patient data, our team implemented a data anonymization technique that successfully eliminated personally identifying information from the data.

The study concluded by demonstrating how the adoption of AI-enabled tools may dramatically enhance patient data security in the healthcare industry. These tools include machine learning-based anomaly detection algorithms, deep learning-based federated learning, and differential privacy. These methods can aid in locating network flaws and security issues, enhancing patient treatment, and guaranteeing patient data privacy in a safe system.

V. RESEARCH OBJECTIVES

1) Main Objectives:

Design & implement an Artificial Intelligence driven security application for secure patient information in a modern hospital.

2) Sub Objectives:

Develop a behavioral anomaly detection program to detect malware, it will identify malware using a training ML model and capture real-time data and analyze

Improve the information gathering processes without interfering with private information, and obtain trained AI models to feed AI applications via federated learning.

Develop an AI-based user data leakage prevention program using training one or more ML models.

Develop and evaluate a method for data anonymization in a secure and efficient manner.

VI. CONCLUSION AND FUTURE RESEARCH

In conclusion, the application of AI technology has become imperative for modern hospitals to secure patient data. With the rising threats to data security, hospitals need advanced tools to protect sensitive information. AI-powered solutions can help hospitals detect and prevent security breaches, analyze data for potential threats, and monitor access to patient records. In conclusion, it has become crucial for contemporary hospitals to safeguard patient data using a variety of AI technologies,

Journal of Artificial Intelligence and Emerging Technologies
Volume 1, Issue 1, pp 11-18, November 2024
ISSN (online): 3049-1967
DOI: https://doi.org/10.47001/JAIET/2024.101002
Available Online at https://www.jaiet.com

including differential privacy, federated learning, malware monitoring, and anonymization. Hospitals require sophisticated technologies to safeguard sensitive data due to the escalating risks to data security and the growing volume of patient data being collected. Hospitals can use several privacy and anonymization strategies to safeguard the privacy of specific patients while processing vast amounts of data. Hospitals may build AI models on patient data from many sources using federated learning without disclosing the raw data. This helps to keep data secure and private while enhancing the precision of AI models. Also, keeping an eye out for malware on the hospital's network can aid in preventing data breaches and cyberattacks. The effectiveness of hospital operations and patient care can both be enhanced by the deployment of these AI technologies. Healthcare practitioners may concentrate more on patient care and lower the chance of human mistake by automating mundane operations. Better health results and increased patient satisfaction may result from this. In conclusion, for contemporary hospitals to preserve patient confidence, adhere to laws, and deliver high-quality treatment, AI technologies like differential privacy, federated learning, malware monitoring, and anonymization are essential. Hospitals may enhance their operations and give their patients better treatment by adopting innovative solutions to secure critical information.

REFERENCES

[1] M. Shajari, H. Geng, K. Hu and A. Leon-Garcia, "Tensor-Based Online Network Anomaly Detection and Diagnosis," in IEEE Access, vol. 10, pp. 85792-85817, 2022, doi: 10.1109/ACCESS.2022.3197651.

[2] L. D. Manocchio, S. Layeghy and M. Portmann, "Network Intrusion Detection System in a Light Bulb," 2022 32nd International Telecommunication Networks and Applications Conference (ITNAC), Wellington, New Zealand, 2022, pp. 1-8, doi: 10.1109/ITNAC55475.2022.9998371.

[3] C. Tzagkarakis, N. Petroulakis, and S. Ioannidis, "Botnet Attack Detection at the IoT Edge Based on Sparse Representation," 2019 Global IoT Summit (GIoTS), Aarhus, Denmark, 2019, pp. 1-6, doi: 10.1109/GIOTS.2019.8766388.

[4] T. D. Ramotsoela, G. P. Hancke, and A. M. Abu-Mahfouz, "Behavioural Intrusion Detection in Water Distribution Systems Using Neural Networks," in IEEE Access, vol. 8, pp. 190403-190416, 2020, doi: 10.1109/ACCESS.2020.3032251.

[5] H. Kaur and N. Jain, "Data Leakage Detection using Machine Learning Techniques: A Survey," Journal of Ambient Intelligence and Humanized Computing, vol. 6, no. 3, pp. 293-307, 2015.

[6] L. Zhang, Y. Li and Y. Wang, "Anomaly-based Insider Threat Detection using Machine Learning," in Proceedings of the 17th ACM Conference on Computer and Communications Security, pp. 521-532, 2011.

[7] J. Wu, Y. Li, and X. Liu, "Preventing Data Leakage in Enterprise Networks using Deep Learning," in Proceedings of the 2014 IEEE International Conference on Computer Communications, pp. 1201-1208, 2014.

[8] N. Jain and N. Aggarwal, "Data Leakage Prevention using Artificial Neural Networks," Journal of Network and Computer Applications, vol. 40, pp. 190-199, 2014.

[9] M. Singh, H. Kaur, and N. Jain, "Data Leakage Prevention using Association Rule Mining and Machine Learning Techniques," Journal of Ambient Intelligence and Humanized Computing, vol. 6, no. 2, pp. 169-181, 2015.

[10] Q. Gu, L. Yang, and Y. Li, "A Machine Learning Based Approach for Detecting and Preventing Data Leakage in Cloud Computing," Journal of Cloud Computing, vol. 2, no. 1, pp. 1-14, 2013.

[11] Jain, N., & Aggarwal, N. (2014). "Data Leakage Prevention using Artificial Neural Networks." Journal of Network and Computer Applications, 40, 190-199. DOI: 10.1016/j.jnca.2013.10.012.

[12] Kim, H., Lee, J., & Park, S. (2016). "Preventing Data Leakage using Artificial Intelligence and Encryption Techniques." Journal of Information Security and Applications, 30, 37-44. DOI: 10.1016/j.jisa.2016.01.001.

[13] Li, Y., Yang, L., & Wang, Y. (2013). "Data Leakage Prevention in Social Networks using Machine Learning." Proceedings of the 2013 ACM Conference on Computer-Supported Cooperative Work and Social Computing, 651-660. DOI: 10.1145/2441776.24418667

[14] R. Shokri, M. Stronati, C. Song, and V. Shmatikov, "Membership inference attacks against machine learning models," in Security and Privacy (SP), 2017 IEEE Symposium on. IEEE, 2017, pp. 3-18. DOI: 10.1109/SP.2017.41.

[15] M. L. Fredrikson, S. K. Jharhakt, and T. M. Redof Ristenpart, "Model inversion technique and attacks that information and basic explicit countermeasures," in Proceedings of 25nd Conference on Computer Communications and well Security. ACM, 2015, pp. 1468-1478.

[16] M. M. Mohammad Rahman, T. A. Usmail Rahman, R. L.

Khaliq Laganiere, N. Mohammed Hussain, and Y. Wang Tang, "Membership cyber attack interference against anomaly and differentially private deep learning and machine model." Transactions on Data Privacy and cyber security, vol. 14, no. 6, pp. 81-99, 2019.

[17] M. Nasr Hanshean, R. Shokri Khardher, and A. Uhandhng Houmansadr, "Machine learning with membership privacy using adversarial regularization," in Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security, 2018, pp. 634-646. DOI: 10.1145/3243734.3243800.

[18] A.M.Salem, M. Backes, M. Humbert, P. L. Berrang, Y. Uyan Zhang, M. Fritz, “ML Model and data independent security of membership inference attacks and defenses on data learning models,” in 26th Annual Network and Distributed System Security Symposium (NDSS 2019), February 2019.

[19] Bild, R., Kuhn, K. A., and Prasser, F. (2020). Better safe than sorry - implementing reliable health data anonymization. Stud. Health Technol. Inf. 270, 68–72. doi:10.3233/SHTI200124

[20] Gentili, M., Hajian, S., and Castillo, C. (2017). “A case study of anonymization of medical surveys,” in ACM Int. Conf. Proceeding Ser. Part, 77–81.

[21] J. Rauch, I. E. Olatunji, M. Katzensteiner, and M. Khosla, "A Review of Anonymization for Healthcare Data," IEEE, 2019, doi: 10.1089/big.2021.0169.

Citation of this Article:

Zailani Bin Abdullah, Rashidah Binti Khalid, Norhani Binti Sahidu, Siti Noraen Binti Khalid, & Mazidah Binti Rahim. (2024). Development of Machine Learning Solutions for Securing Patient Data in Health Care Systems. *Journal of Artificial Intelligence and Emerging Technologies*. 1(1), 11-18. Article DOI: https://doi.org/10.47001/JAIET/2024.101002

***** End of the Article *****