2023 4th International Conference for Emerging Technology (INCET)
Belgaum, India. May 26-28, 2023

Enhancing Data Privacy of IoT Healthcare with Keylogger Attack Mitigation

Atul Kumar
Chitkara University Institute of Engineering and Technology
Chitkara University
Punjab, India
kumar.atul@chitkara.edu.in
Orcid Id – 0000-0003-2548-1173

Ishu Sharma
Chitkara University Institute of Engineering and Technology
Chitkara University
Punjab, India
ishu.sharma@chitkara.edu.in
Orcid Id - 0000-003-1669-3393

2023 4th International Conference for Emerging Technology (INCET) | 979-8-3503-3575-0/23/$31.00 ©2023 IEEE | DOI: 10.1109/INCET57972.2023.10170531

***Abstract*— The healthcare industry has been revolutionized by the Internet of Things (IoT), which has made it possible to develop various applications to monitor patients' health conditions and provide customized care. One of the ways in which IoT is being used in healthcare is through remote patient monitoring. This involves collecting real-time data from IoT-enabled devices such as blood pressure monitors, thermometers, and heart rate monitors, which can help healthcare professionals detect and respond to changes in a patient's health condition before they become critical. Despite the numerous benefits of IoT healthcare applications, there are critical security concerns that need to be addressed. One such concern is data privacy, as IoT devices collect a significant amount of sensitive patient information that needs to be protected from unauthorized access, hacking, and breaches. Another issue is the vulnerability of IoT devices to malware and hacking attacks due to inadequate security protections and outdated software. IoT devices can be utilized by cyber attackers to remotely get the patent's data by causing keylogger attacks. The harm caused by keylogger attacks is significant, as they compromise private information such as patients' private details, leading to identity theft and other crimes. These attacks can also cause operational problems such as degraded response time of IoT healthcare, system crashes, and corrupted files. Keyloggers can be difficult to detect as they run covertly in the background. In this paper, a methodology is proposed for early detection of keylogger attacks in IoT healthcare to preserve the patient's identity from cyber attackers using the machine learning-based approach. The proposed framework is experimented on IoT healthcare dataset for comparing the performance of LightGBM, CNN, and ANN machine learning models.**

Keywords*— *Healthcare, Keylogger Attack, Deep Learning, Internet of Things Healthcare, Security, Patient Monitoring

I. INTRODUCTION

Internet of Things (IoT) healthcare is the use of IoT technology to enhance patient care and results in the healthcare business. It entails collecting, transmitting, and analyzing health data in real time via networked devices, sensors, and networks. These gadgets and sensors may be incorporated in medical equipment, wearables, or even the patient's body to monitor health issues, measure vital signs, and inform healthcare professionals automatically. The utilization of the Internet of Things has the potential to revolutionize the healthcare sector by increasing effectiveness, minimizing expenses, and elevating the quality of care received by patients. IoT devices, for example, may be used to remotely monitor patients' health problems, enabling healthcare personnel to respond early if the patient's health state changes. IoT healthcare may also offer personalized care by using patient data to develop individualized treatment regimens based on their specific health requirements. Because healthcare data is very sensitive and must be safeguarded against unauthorized access or abuse, the introduction of IoT healthcare raises issues about data privacy and security [1].

IoT healthcare with blockchain technology has the potential to recover security, interoperability, and data privacy. Blockchain technology offers a safe and decentralized platform for healthcare data management. It stores and tracks data transactions via a distributed ledger, resulting in an immutable and tamper-proof record of all healthcare data. This makes it impossible for any unauthorized entity to tamper with the data or obtain unauthorized access to it. Blockchain technology may also assist IoT devices by using its smart contract feature. When particular criteria are satisfied, smart contracts may be designed to do certain activities, like as sending an alarm to healthcare personnel when a patient's vital signs fall outside of typical ranges. Another advantage of merging IoT healthcare with blockchain is the possibility of interoperability. Healthcare providers and patients may securely communicate data across diverse systems and devices, regardless of origin or location, by using a standardized blockchain network. IoT healthcare and blockchain technologies have the potential to improve patient outcomes, increase data privacy and security, and allow more efficient and cost-effective healthcare delivery [2].

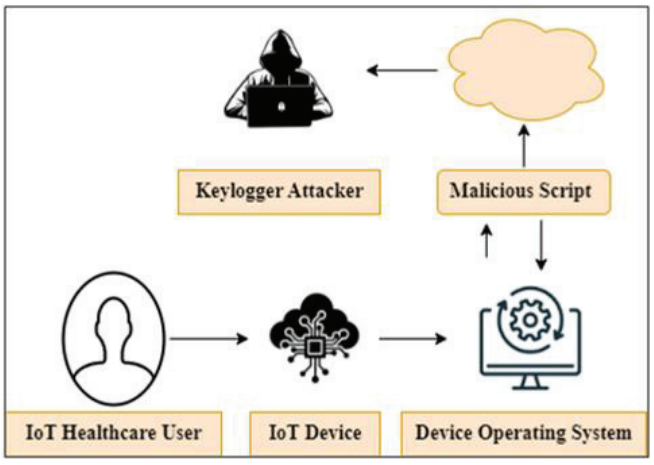

Fig. 1. Working of Keylogger Attack

Figure 1, depicts the occupied of keylogger Attacks, Keystroke loggers, also known as keyloggers, are devices that record an individual's input on a device. Although there are legitimate uses for keyloggers, they are frequently used for malicious purposes. The keylogger program records all keystrokes on the target's device and sends them to the attacker in a keylogger attack.

A keylogger attack is a sort of cyberattack where a bad actor installs software or hardware on the computer or mobile device of a victim to record all of the victim's keystrokes, including passwords, credit card numbers, and other sensitive data. Typically, a keylogger assault aims to steal the victim's financial or personal information so that it can be exploited for fraud or other harmful activities. Keyloggers can be set up in a number of ways, including via malicious email attachments, corrupt software downloads, or even direct physical access to the victim's device. The keylogger can be installed and then operated in the background, secretly recording all keystrokes without the victim's knowledge or consent [3].

In the field of healthcare, blockchain technology has various benefits, including A safe and decentralized platform for handling healthcare data is provided by blockchain technology. Healthcare data is shielded against illegal access and manipulation via encryption. It is challenging for any unauthorized entity to alter the data or access it without the right authority since data kept on a blockchain is dispersed throughout a network of computers. Blockchain technology makes it possible to store healthcare data in a standardized format, making it simpler to exchange and access data across various systems and devices. This might enhance the data interoperability across various healthcare systems and providers. Blockchain technology offers a transparent and unchangeable record of all transactions involving healthcare data [4].

This promotes more openness and accountability by making it simpler to monitor and audit the flow of healthcare data. Patients now have more control over their medical data because to blockchain technology. Patients may manage who gets access to their healthcare data by storing it on a blockchain. This aids in preserving patient privacy and preventing illegal access to private medical information. Blockchain technology can handle tasks like managing the supply chain for drugs, processing insurance claims, and invoicing for medical services. This lowers expenses, increases effectiveness, and decreases administrative overhead. Blockchain technology has several benefits for the healthcare industry, including better patient privacy, higher transparency, improved data interoperability, and increased security. Healthcare providers may enhance patient care and outcomes while lowering costs and increasing efficiency by taking advantage of these advantages. IoT healthcare refers to the application of IoT technology in the healthcare industry to improve patient outcomes and make healthcare more efficient. IoT healthcare devices typically involve a network of interconnected medical devices, sensors, and software applications that collect and transmit patient data in real-time [5].

II. Literature review

In this paper, the authors have discussed article how the Lamport Merkle Digital Signature (LMDS) works and aims to achieve security needs autonomously, without relying on a trusted third party. It achieves this by utilizing a cloud-based Internet of Things (IoT) network based on blockchain technology, which connects healthcare data of both patients and hospitals. The method simplifies the deployment of cloud IoT applications, signature creation, and signature verification. Authentication mechanisms, LMDSG, and LMDSV were used to safeguard sensitive medical data in the IoT network. The approach has the advantage of lowering the Computational Time and Computational Overhead by employing a Lamport Signature [6].

The article suggests the use of the FID Chain Intrusion Detection System (IDS) to ensure the protection of sensitive healthcare information. This system employs a lightweight artificial neural network (ANN) in a supervised learning approach called Federated Learning (FL). The authors also highlight the advancements of blockchain technology, which provides a distributed ledger for gathering local weights and then updating global weights by averaging them. This technique reduces the risk of data tampering and ensures complete transparency and data integrity across the distributed network, all with minimal overhead. The IDS blocks data from reaching the cloud's gateway, providing faster detection times and requiring less processing power. Using the detection model at the edge of the network offers defense against potential attacks on the cloud [7].

In this paper, the authors have discussed about the application of IoT in healthcare address these issues enhances patient care performance while cutting costs by effectively allocating healthcare resources. IoT devices, however, are susceptible to a number of hazards from different attackers. Blockchain technology has been found to be the most efficient way to keep control systems secure and secret in real-time in order to avoid these issues. By producing the hash of every piece of information, this should provide a security architecture for healthcare multimedia content using blockchain technology, enabling any transition or modification in the information as well as any drug security breaches to be documented across the entire blockchain platform [8].

In this paper, the authors have discussed about the propose a review in this article that provides a comprehensive overview of the application of the internet of things and blockchain technology in the healthcare sector. In addition, the study analyses the main complications in implementing Blockchain in IoT-based healthcare applications. Also, it provides certain potential research lines that, by fusing a number of cutting-edge and potent technologies, could change the healthcare sector [9].

In this paper, the authors have discussed the essay compares and contrasts existing security procedures in order to classify the security threats in six layers of blockchain technology related to healthcare. Additionally, it investigates and specifies the various safety threats and difficulties that arise while using blockchain technology, fostering theoretical investigation and the creation of strong security protocols in both the present and the future of distributed work environments [10] .

This study aims to elaborate on the advantages and important features of utilizing blockchain in the IoT environment. This article specifically examines numerous IoT applications using blockchain. The report also describes the underlying research obstacles and makes distinctions between various technical issues. Finally, based on the knowledge gained, potential future areas for research are discussed [11].

In this article, the authors suggest gathering data from the planned IoT blockchain network's smart health and fitness gadgets. The employment of these tools enables to extract a substantial amount of extremely valuable health data from electronic health records that have been filtered, analyzed,

and stored. With the help of coaches, patients, and doctors, the platform's multiple actors work together to quickly and affordably diagnose and treat a variety of ailments. Authors primary goal is to use Ethereum blockchain technology to give distributed, safe, and authorized access to these sensitive data [12].

In this study, the authors talked about a ground-breaking approach to blockchain technology that is intended for use with IoT devices. They gave an example of remote patient monitoring to show how this approach can be used to enable medical facilities to communicate with patients in their homes, rather than only in a clinical setting. Wearable IoT devices are worn by patients, and they can send data to medical professionals about a patient's blood sugar level, blood pressure, breathing pattern, and the Internet of Things [13].

In this study, the authors propose a blockchain solution called Practical Byzantine Fault Tolerance that is designed for healthcare applications. This consensus-based and lightweight approach involves highly trusted nodes taking part in the consensus process, with the use of the Eigen Trust model and Verifiable Random Function to select a random primary node from a group of trusted consensus nodes to support PBFT consensus. The researchers evaluate the proposed method against the traditional consensus algorithm in a virtual environment, taking into account factors such as throughput, latency, and fault tolerance of the random function [14].

In this paper, the authors have discussed a work that includes a security analysis and an assessment of secure keyboard software, both of which are supported by the discussion of various keyboard attack tactics, some of which are new. The researchers use this information to develop sample malicious code. Testing is carried out, and the results show that when the resend command utilization attack strategy is employed, keyboard information is exposed in 7 out of 10 attacks, but only the company's solution is able to identify it. The researchers attribute this vulnerability to the absence of adequate security features in the hardware chip connected to the PS/2 interface of the keyboard. [15].

In this paper, the Authors have discussed about the This study focuses primarily on various software Keyloggers and their implications on computer systems. Keyloggers capture all keystrokes and user activity on the computer, stealing credit card numbers, passwords, and other confidential information and sending it to the attacker. Hence, many detection strategies are discussed here, with each technique's advantages and disadvantages. All of these methods improve consumer privacy and security [16].

III. Proposed Work

This study proposes a method for enhancing the safety and reliability of IoT healthcare systems. The suggested approach is centered around the capability of IoT healthcare monitoring to detect keylogger attacks in IoT devices employed for recording patients' data or any other medical record at an early stage. To protect the entire IoT healthcare process from such attacks, a Nano-Integrated Circuit (NIC) can be embedded in the IoT devices. This NIC would be responsible for determining whether a packet is malicious or not with the help of keylogger attack detection trained machine learning models. According to the suggested framework, every IoT device in healthcare monitoring should be equipped with a NIC that supports machine learning. The NIC would have a pre-trained model for detecting keylogger attacks based on information obtained from the traffic logs. As soon as a data packet is received by an IoT device, it is immediately sent to the ML-trained NIC for analysis and detection. The proposed ML-trained NIC acts as the receiver of the data packet with the identical hardware configuration of a real IoT healthcare device. Once the ML-trained NIC collects traffic logs for the received data packet, it uses a decision on the received data packet if the packet is malicious or can be allowed for communication by analyzing the packet's attribute. IoT healthcare devices are vulnerable to cyberattacks that exploit information about vulnerable applications, the proposed framework can identify harmful data packets early on. While most security strategies focus on enhancing server-side controls in IoT healthcare, hackers can use vulnerable applications or ports to infect IoT healthcare systems and launch keylogger attacks to steal the data of patients for numerous reasons. Therefore, it is essential to prevent such malicious network packets from entering devices utilized for healthcare monitoring. The integration of machine learning-based NIC can be a major game-changer for patient monitoring applications without compromising data privacy.

IV. Materials and Methods

The proposed methodology experiments on IoT healthcare keylogger attack dataset taken from Kaggle. The proposed approach is utilized for keylogger attack detection with machine learning algorithms Light Gradient Boosting Machine (LightGBM), Convolutional Neural Network (CNN) and ANN. CNN is an abbreviation for Convolutional Neural Network. It is a sort of ANN that is frequently employed in computer vision tasks such as picture categorization and object recognition. Each layer of a CNN is meant to accomplish a particular function. Typically, the first layer of a CNN performs convolution, which extracts data from the input image by applying a filter. The following layers execute pooling to reduce the dimensionality of the features, followed by subsequent convolutional layers that extract progressively complicated information from the pooled output. The output is then flattened and supplied to a conventional neural network for categorization. CNNs have been demonstrated to be highly successful for image recognition tasks, achieving state-of-the-art performance on numerous benchmark datasets. They are also utilized extensively in other fields, including natural language processing and speech recognition [17].

The term Artificial Neural Network is referred to by its acronym. It is a machine-learning algorithm that imitates the composition and operation of the human brain. An ANN is a network of artificial neurons or nodes that are connected and process information in a manner comparable to that of biological neurons. Typically, an ANN comprises numerous layers of artificial neurons, each layer performing a distinct function. The first layer of an ANN is the input, which is responsible for receiving input data. Following the visible layers are the hidden layers, which handle input data processing. The output layer is the final layer, which generates output based on the processing of the hidden levels. ANNs are utilized in numerous applications, including image and audio recognition, natural language processing, financial modelling, and prescriptive analytics. They are renowned for their ability to learn and identify

complicated data patterns, as well as their capacity to adapt to new data over time [18].

Light Gradient Boosting Machine (LightGBM) is an open-source Extreme Gradient Boosting (XGBoost) framework that is optimized for efficiency, scalability, and accuracy. It is based on the gradient boosting process, which works by iteratively adding additional models to increase the main model's prediction accuracy. Light GBM employs a novel method of gradient boosting known as Gradient-based One-Side Sampling (GOSS), which decreases the number of examples analyzed for splitting. As a result, training time is reduced and memory utilization is reduced. Further features supported by Lite GBM include categorical feature support, cross-validation, early halting, and parallel learning. In terms of training time and prediction accuracy, LightGBM has been proven to beat other common gradient-boosting frameworks, particularly on big and sparse datasets. It's frequently used in industry and academia for image classification, text categorization, and recommendation systems, among other things.

V. Results And Discussion

The dataset for the IoT Keylogger Attack contains more than 5,00000 log observations that pertain to both harmful and benign keylogger attacks. This dataset contains 85 features for keylogger traffic observations and related features are selected for building the machine learning model. Features like Flow duration, Total Forward Packets, Total Backward Packets, Total Length of Forward. Packets, Total Length of Backward Packets, Flow Bytes per second, Packet Length Minimum, and Packet Length Variance plays major role in the detection of keylogger occurrences. In this research work, CNN, ANN, LightGBM are utilized for detecting keylogger attack. The results of attack detection are discussed below:

A. AUC

AUC is a contraction for "Area Under the Curve." It usually refers to the space beneath of the Receiver Operating Characteristic (ROC) curve in the context of data science. The total performance of the classification model is measured by the AUC of the ROC curve, which ranges from 0 to 1. with 1 indicating perfect classification performance and 0.5 indicating a random guess. AUC is a popular evaluation metric in machine learning and data science, especially for binary classification problems. AUC is a performance statistic that employs integral calculus to assess the complete area under the ROC curve from (0,0) to (1,1). This measure accounts for how well the model performs at every classification level. AUC can be thought of as the likelihood that a positive example will be given a higher ranking by the model than a negative example.

Figure 2, represents the comparative analysis of the AUC of CNN, ANN, and LightGBM. LightGBM comes with a feature importance measurement feature that assists in recognizing the most significant features that impact the classification task. This can assist in both selecting features and comprehending the underlying patterns in the data. LightGBM comes with a feature measurement tool based on correlation that can assist you in recognizing the most significant features that impact the classification task. This can assist in both selecting features and comprehending the underlying patterns in the data. The result achieved shows that LightGBM gives better results for detecting keylogger attacks in IoT Healthcare as compared to CNN and ANN.

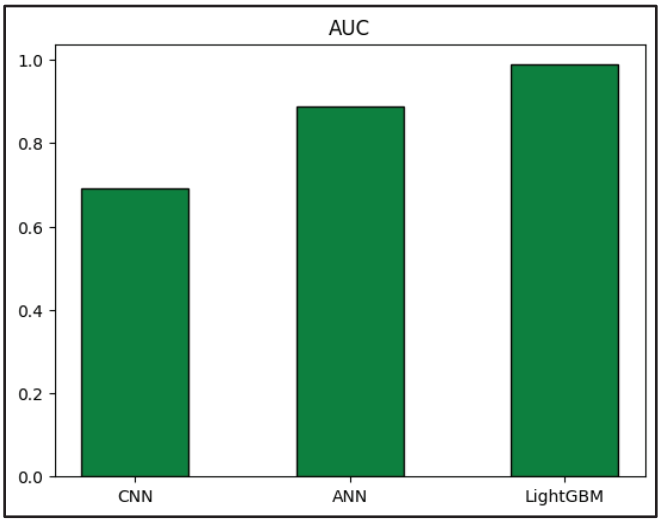

Fig. 2. Comparative Analysis of AUC of CNN, ANN, And LightGBM

B. ROC

A binary classification model's "Receiver Operating Characteristic," or ROC, is a graphical indicator of how well it performs. It is a figure that contrasts different threshold levels' true positive rates (TPR) and false positive rates (FPR). The model determines whether an observation belongs to the positive or negative class in a binary classification problem. The TPR and FPR are calculated at each level while varying the threshold level for identifying an observation as positive or negative to produce the ROC curve. The true positive rate (TPR) is the percentage of real positive cases that the model correctly classifies as positive, whereas the false positive rate (FPR) is the percentage of real negative cases that the model incorrectly classifies as positive. The ROC curve represents each point on the curve as a separate threshold value and graphs TPR on the y-axis and FPR on the x-axis. The effectiveness of a classification model over all threshold values is depicted graphically via the ROC curve. The computing method for determining true positive rate and false positive rate is provided in equations 1 and 2.

$$TPR_{KAD} = \frac{TP_{KAD}}{TP_{KAD}+FN_{KAD}} \quad (1)$$

In Equation 1, TP_{KAD} illustrate the True positive of Keylogger Attack Detection and FN_{KAD} illustrate the False Negative Attack of Keylogger Attack Detection.

$$FPR_{KAD} = \frac{FP_{KAD}}{FP_{KAD}+TN_{KAD}} \quad (2)$$

In Equation 2, FP_{KAD} illustrates the False positive of Keylogger Attack Detection and TN_{KAD} illustrates the True Negative Attack of Keylogger Attack Detection. TPR is synonymous with recall and is thus defined as the following is the definition of the FPR. TPR and FPR at different categorization criteria are compared using a ROC curve. False positives and true positives rise as a result of lowering the classification threshold since more things are labeled as positive. A typical ROC curve is depicted in the figure below.

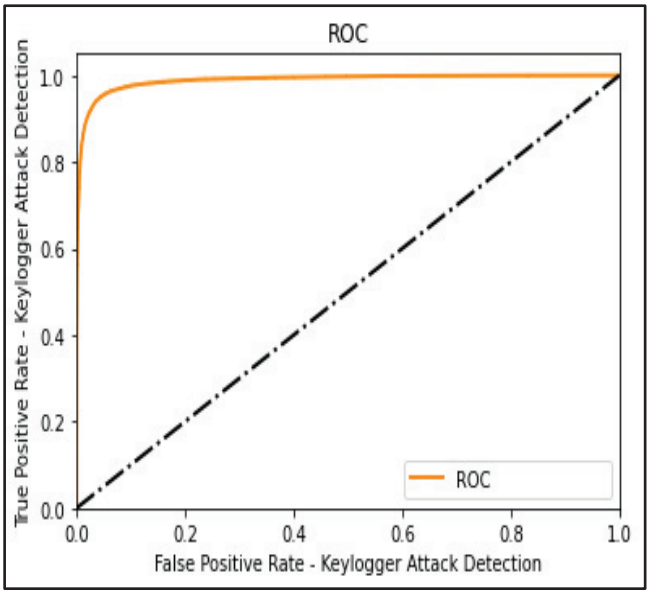

Fig. 3. ROC Curve of LightGBM

Figure 3, depicts ROC Curve of detecting Keylogger attack with LightGBM method. Figure 4, and Figure 5, shows the ROC curve of detecting keylogger attack with CNN Method and ANN method respectively.

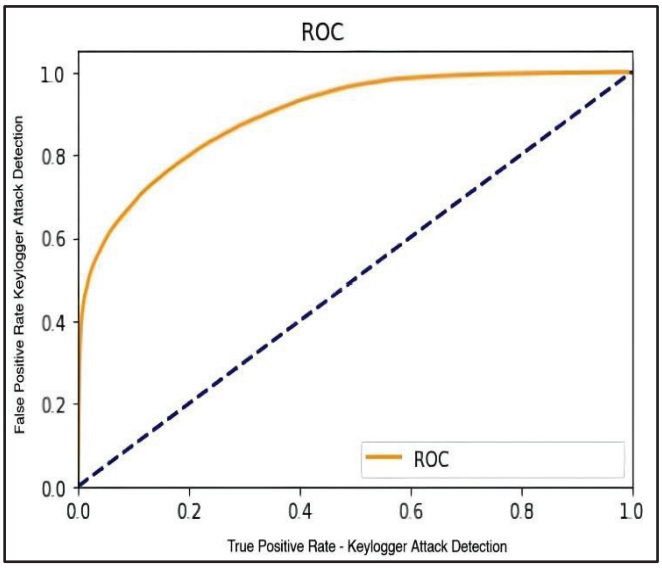

Fig. 4. ROC Curve of ANN

The false FPR is shown by the x-axis on the ROC curve, while the TPR is represented by the y-axis. The ratio of true positives to total positives is known as the TPR, whereas the FPR measures the ratio of false positives to all negatives. Typically, the ROC curve rises sharply at first before leveling out as it approaches the top left corner. The classifier performs better as the curve gets steeper. A diagonal line from the bottom left to the top right denotes speculation, while a curve that hugs the top left corner symbolizes an ideal classifier. The ideal threshold is the location on the curve where the TPR is maximized and the FPR is minimized. This is typically the graphing element that is closest to the top left corner. The decision threshold for the classifier can be set using the optimal threshold. The result achieved by building artificial intelligence-based techniques for keylogger attack detection proves that LightGBM outperforms in comparison to CNN and ANN.

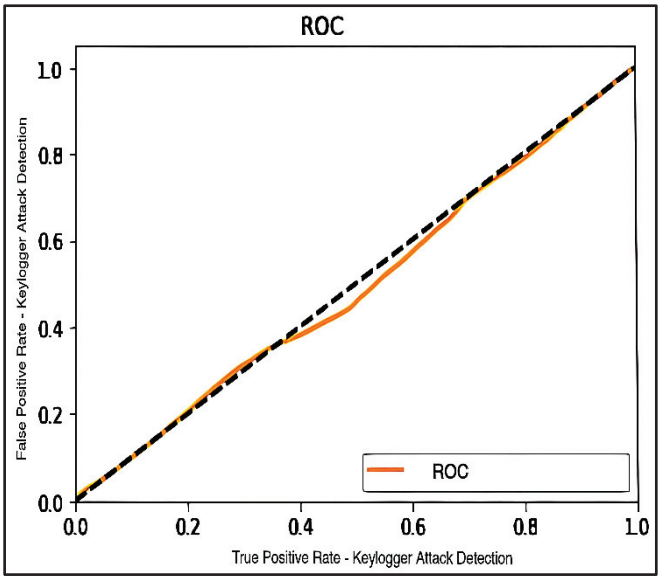

Fig. 5. ROC Curve of CNN

VI. Conclusion And Future Direction

IoT healthcare devices that manage sensitive patient information are at risk of various security vulnerabilities, including data breaches, malware attacks, weak authentication, and insecure software and firmware. This article recommends a framework for improving the security and reliability of IoT healthcare systems by Detecting keylogger attacks. The methodology involves the early detection of IoT keylogger attacks in healthcare monitoring through the use of machine learning algorithms and with the employment of Nano-Integrated Circuits conjected with IoT devices. The proposed work ensures the data privacy of the entire IoT healthcare process from keylogger attacks.

References

[1] A. Haleem, M. Javaid, R. P. Singh, R. Suman, and S. Rab, "Blockchain technology applications in healthcare: An overview," International Journal of Intelligent Networks, vol. 2. KeAi Communications Co., pp. 130–139, Jan. 01, 2021. doi: 10.1016/j.ijin.2021.09.005.

[2] P. P. Ray, Di. Dash, K. Salah, and N. Kumar, "Blockchain for IoT-Based Healthcare: Background, Consensus, Platforms, and Use Cases," IEEE Syst J, vol. 15, no. 1, pp. 85–94, Mar. 2021, doi: 10.1109/JSYST.2020.2963840.

[3] K. Lee and K. Yim, "Vulnerability Analysis and Security Assessment of Secure Keyboard Software to Prevent PS/2 Interface Keyboard Sniffing," Sensors, vol. 23, no. 7, p. 3501, Mar. 2023, doi: 10.3390/s23073501.

[4] F. Hussain et al., "A framework for malicious traffic detection in iot healthcare environment," Sensors, vol. 21, no. 9, May 2021, doi: 10.3390/s21093025.

[5] S. Zaman, M. R. A. Khandaker, R. T. Khan, F. Tariq, and K. K. Wong, "Thinking Out of the Blocks: Holochain for Distributed Security in IoT Healthcare," IEEE Access, vol. 10, pp. 37064–37081, 2022, doi: 10.1109/ACCESS.2022.3163580.

[6] J. A. Alzubi, "Blockchain-based Lamport Merkle Digital Signature: Authentication tool in IoT healthcare," Comput Commun, vol. 170, pp. 200–208, Mar. 2021, doi: 10.1016/j.comcom.2021.02.002.

[7] E. Ashraf, N. F. F. Areed, H. Salem, E. H. Abdelhay, and A. Farouk, "FIDChain: Federated Intrusion Detection System for Blockchain-Enabled IoT Healthcare Applications," Healthcare (Switzerland), vol. 10, no. 6, Jun. 2022, doi: 10.3390/healthcare10061110.

[8] A. I. Taloba et al., "A blockchain-based hybrid platform for multimedia data processing in IoT-Healthcare," Alexandria Engineering Journal, vol. 65, pp. 263–274, Feb. 2023, doi: 10.1016/j.aej.2022.09.031.

[9] K. Azbeg, O. Ouchetto, S. J. Andaloussi, and L. Fetjah, "A Taxonomic Review of the Use of IoT and Blockchain in Healthcare Applications," IRBM, vol. 43, no. 5. Elsevier Masson s.r.l., pp. 511–519, Oct. 01, 2022. doi: 10.1016/j.irbm.2021.05.003.

[10] Z. Wenhua, F. Qamar, T. A. N. Abdali, R. Hassan, S. T. A. Jafri, and Q. N. Nguyen, "Blockchain Technology: Security Issues, Healthcare Applications, Challenges and Future Trends," Electronics (Switzerland), vol. 12, no. 3. MDPI, Feb. 01, 2023. doi: 10.3390/electronics12030546.

[11] S. Mathur, A. Kalla, G. Gür, M. K. Bohra, and M. Liyanage, "A Survey on Role of Blockchain for IoT: Applications and Technical Aspects," Computer Networks, vol. 227. Elsevier B.V., May 01, 2023. doi: 10.1016/j.comnet.2023.109726.

[12] T. Frikha, A. Chaari, F. Chaabane, O. Cheikhrouhou, and A. Zaguia, "Healthcare and Fitness Data Management Using the IoT-Based Blockchain Platform," J Healthc Eng, vol. 2021, 2021, doi: 10.1155/2021/9978863.

[13] A. D. Dwivedi, L. Malina, P. Dzurenda, and G. Srivastava, "Optimized blockchain model for internet of things based healthcare applications," in 2019 42nd international conference on telecommunications and signal processing (TSP), 2019, pp. 135–139.

[14] P. Hegde and P. K. R. Maddikunta, "Secure PBFT Consensus-Based Lightweight Blockchain for Healthcare Application," Applied Sciences, vol. 13, no. 6, p. 3757, Mar. 2023, doi: 10.3390/app13063757.

[15] A. Singh, P. Choudhary, and others, "Keylogger detection and prevention," in Journal of Physics: Conference Series, 2021, p. 12005.

[16] A. Solairaj, S. C. Prabanand, J. Mathalairaj, C. Prathap, and L. S. Vignesh, "Keyloggers software detection techniques," in Proceedings of the 10th International Conference on Intelligent Systems and Control, ISCO 2016, Institute of Electrical and Electronics Engineers Inc., Oct. 2016. doi: 10.1109/ISCO.2016.7726880.

[17] V. Tanwar, S. Lamba, and B. Sharma, "Deep Learning-based Hybrid Model for Severity Prediction of Leaf Smut Sugarcane Infection," in 2023 Third International Conference on Artificial Intelligence and Smart Energy (ICAIS), 2023, pp. 1004–1009.

[18] A. Sharma, H. Babbar, and A. Sharma, "TON-IoT: Detection of Attacks on Internet of Things in Vehicular Networks," in 2022 6th International Conference on Electronics, Communication and Aerospace Technology, 2022, pp. 539–545.