Journal of Neonatal Surgery
ISSN(Online): 2226-0439
Vol. 14, Issue 15s (2025)
https://www.jneonatalsurg.com

OPEN ACCESS

Detecting Unauthorized Access of Personal Device

Dr. S. Jerald Nirmal kumar[1], Mr. Aravindan Srinivasan[2], V. Sasirekha[3], Viswanathan Ramasamy Reddy[*4], Dr. T. Vengatesh[5]

[1]Associate professor, CSE, Jain Deemed -to-be University, Banglore.

[2]Assistant Professor, Department of CSE, Koneru Lakshmaiah Education Foundation, Vaddeswaram, AP, India. Pincode 522302.

[3]Professor and Dean, Faculty of Management, SRM institute of Science and Technology, Chennai, Tamil Nadu , India.

[4*] Professor, Department of CSE, Koneru Lakshmaiah Education Foundation, Vaddeswaram, AP, India. Pincode 522302.

[5] Assistant Professor, Department of Computer Science, Government Arts and Science College, Veerapandi, Theni, Tamilnadu, India.

[1]Email ID: jeraldcse@gmail.com, [2] Email ID: aravindansrinivasan2@gmail.com, [3] Email ID: prof.sasirekha@gmail.com,

[4] Email ID: rvnathan06@gmail.com, [5] Email ID: venkibiotinix@gamil.com

***Corresponding Author:**

Viswanathan Ramasamy Reddy

Professor, Department of CSE, Koneru Lakshmaiah Education Foundation, Vaddeswaram, AP, India. Pincode 522302.

Cite this paper as: Dr. S. Jerald Nirmal kumar, Mr. Aravindan Srinivasan, V. Sasirekha, Viswanathan Ramasamy Reddy, Dr. T. Vengatesh, (2025) Assessment and Prevalence of Communicable and Non-Communicable Diseases and their Risk Factors in Adults. *Journal of Neonatal Surgery*, 14 (15s), 22-31.

ABSTRACT

Unauthorized access to personal devices poses a severe concern to people's security and privacy in the digital age. The primary objective of this endeavour is to develop a dependable system for detecting and preventing such unauthorized access. The proposed system employs an interdisciplinary approach that integrates behaviour analysis, anomaly detection, and advanced authentication mechanisms. The system has robust authentication techniques, such as biometric identification and two-factor authentication, to ensure that only authorized users are allowed access. From then, users' interactions with the device are monitored through continuous behaviour analysis, which creates a baseline of normal behaviour. In the case that this baseline is deviated from, a warning signalling potential unauthorized access is issued. Algorithms for anomaly detection also identify peculiar behaviours or patterns, which enhances the system's ability to identify security breaches and respond quickly. Furthermore, the system incorporates machine learning models that adapt over time to new threats and emerging patterns. Updates and patches are frequently published to stay up to date with emerging attack methods. The proposed solution aims to safeguard confidential information and preserve user privacy in an increasingly interconnected environment by implementing this comprehensive approach and providing a proactive barrier against unauthorized access to personal devices.

Keywords: *Unauthorized access, Personal device security, Authentication mechanisms, Anomaly detection, Privacy protection, Security breaches, Threat detection*

1. INTRODUCTION

In an era of digital interconnectedness, personal gadgets which often include sensitive data have become an indispensable part of our daily lives [1]. These devices, which come in a variety of forms, from laptops to cell phones, are desirable targets for unauthorized access because they may store personal and financial data and provide access to a multitude of online resources. To safeguard people's privacy and maintain the accuracy of personal data, it is now imperative to locate and halt these unlawful invasions [2].

Given the growing sophistication and frequency of cyberattacks, robust security measures are essential [3, 4]. Unauthorized access to personal devices may lead to a number of bad things, including identity theft and unauthorized financial activities. The potential repercussions of security breaches are increased by our growing reliance on digital gadgets [5]. Thus, in order to ensure the dependability of personal devices, it is imperative to understand and address the risks associated with

unauthorized access. Over time, as technology has progressed, so too has the landscape of security measures. Traditional password-based authentication techniques are becoming increasingly susceptible to sophisticated hacking techniques, despite their widespread use [6]. As a result, two-factor authentication and biometric identification have been used to add further security levels. While these advancements have their uses, they are not perfect [7]. As cyber dangers evolve, there is a pressing need for an all-encompassing approach that transcends conventional security measures.

This research investigates innovative methods to detect unauthorized access to personal devices with the goal of enhancing the present security configuration [8]. The scope of the research included a thorough examination of authentication protocols, anomaly detection, and behaviour al analysis. Our objective is to create a dynamic system that actively observes and responds to deviations from regular user behaviour while fortifying the first barriers to access by integrating these components [9, 10].

Figure 1. General architecture of the proposed classifier.

The use of Gated Recurrent Units (GRU) in credit card fraud detection presents a sophisticated method of modelling the complex temporal correlations in transaction data. In contrast to conventional ANN designs, GRU features specific gating mechanisms that let it efficiently recognize and retain sequential patterns. This is crucial for spotting fraudulent activity since fraudulent patterns can develop gradually over a series of transactions. Because of its distinctive architecture, GRU is able to learn and adjust to longer-term dependencies more effectively than ordinary Recurrent Neural Networks (RNNs), which struggle with issues like the vanishing gradient problem. GRU's application in this situation improves the model's sensitivity to minute irregularities and changing fraud trends, proving its usefulness in negotiating the intricate temporal structure of credit card transactions. The creation of a sophisticated system that can successfully detect and prevent unauthorized access to personal devices is the primary objective of this research. Among the particular goals are the use of behaviour analysis algorithms, the study of complex authentication processes, and the integration of anomaly detection techniques. Furthermore, the research aims to assess the efficacy of machine learning models in adapting to evolving security threats, ensuring a proactive defence against unauthorized access.

2. LITERATURE REVIEW

The way we work, interact, and access information has changed dramatically as a result of the widespread use of portable devices, such as laptops and smartphones. But there are serious security risks associated with the broad usage of these devices, especially with regard to unauthorised access. We examine the body of knowledge about the identification of unauthorised access to personal devices in this survey of the literature. Our objective is to offer an analysis of many studies and methodology in order to shed light on the most advanced ways now in use and suggest possible directions for future study.

Advances in cybersecurity research and technology have led to a substantial evolution of unauthorised access detection systems throughout time. Passwords or PINs, or other static authentication systems, were a major component of traditional approaches [3]. But it has been shown that these techniques are vulnerable to a number of assaults, such as phishing schemes and brute force attacks [11]. In order to improve the security of personal devices, researchers have therefore resorted more and more to complex methods like anomaly detection and machine learning [1, 10]. The goal of anomaly

detection algorithms is to spot departures from typical behaviour patterns, which might point to malicious or unauthorised activities [5]. These methods look at network traffic, system logs, and human behaviour to find unusual activity that deviates from the norm [12]. The efficacy of anomaly detection in identifying unauthorised access to personal devices has been the subject of several studies, underscoring the technology's potential to offer preventative security measures [6] [13].

Because machine learning algorithms can analyse large volumes of data and find intricate patterns, they have become more and more popular in the field of unauthorised access detection [2]. These algorithms are highly suitable for identifying changing attack vectors because they can learn from past data and gradually adapt to new threats [7, 14]. To identify unauthorised access attempts with high accuracy, researchers have used a variety of machine learning approaches, such as decision trees, support vector machines, and deep learning [15, 16]. One of the most effective methods for identifying unwanted access to personal devices is deep learning, which is a branch of machine learning [8]. Convolutional neural networks (CNNs) and recurrent neural networks (RNNs) are two examples of deep learning algorithms that can automatically learn complex characteristics from raw data, allowing them to identify minute abnormalities in system activity or human behaviour [9, 17]. Deep learning techniques are good at identifying unauthorised access attempts, as evidenced by recent research [18, 19], especially when there are complicated temporal relationships involved.

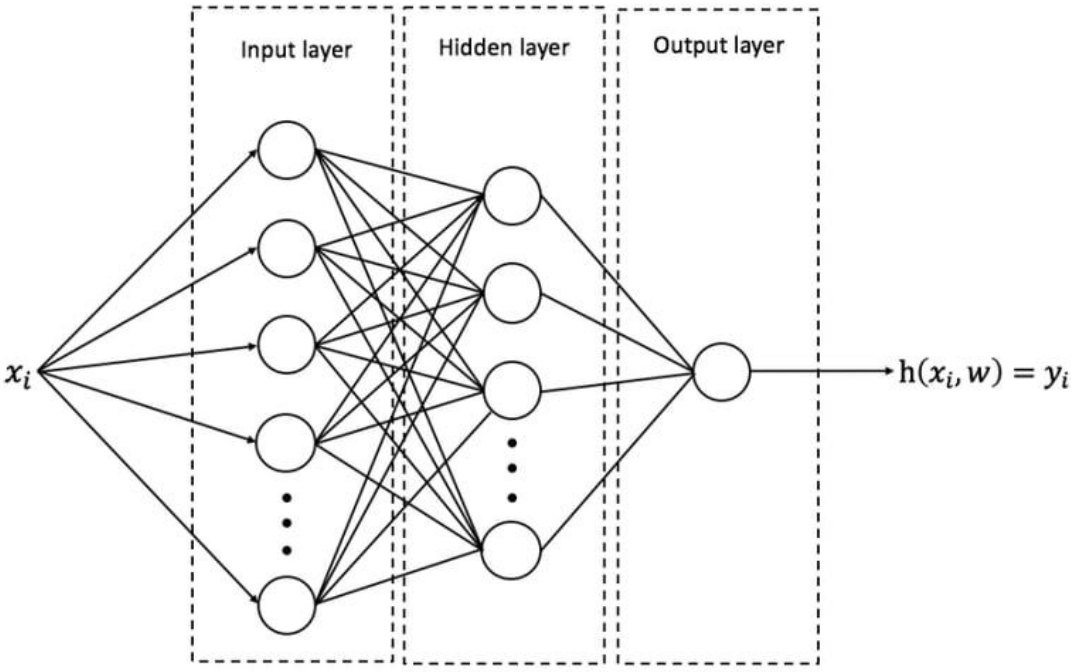

Figure 2. General structure of Artificial Neural Network.

The significance of using various detection methods to improve the resilience and efficiency of unapproved access detection systems has been acknowledged by researchers on a growing scale [4]. Researchers may take use of each method's advantages to obtain reduced false positive rates and greater detection rates by integrating anomaly detection with machine learning algorithms [20, 21]. Furthermore, multi-layered security defences against unauthorised access attempts may be achieved by merging deep learning algorithms with conventional authentication systems [22, 23]. Although techniques for detecting unauthorised access have advanced, there are still a number of obstacles to overcome. The need to strike a balance between security and user comfort is one major difficulty, as too strict security measures may degrade user experience [24]. Furthermore, ongoing study and development of adaptive detection methods is required due to the fast evolution of attack strategies [25]. Subsequent investigations have to concentrate on creating real-time detection systems that can minimise false positives while reducing new dangers [26, 27].

In recent years, Gated Recurrent Units (GRUs) have attracted a lot of interest as an efficient model for a variety of sequential data processing applications, such as anomaly, virus, and intrusion detection. In order to explain why GRU is regarded as a better model than alternative recurrent neural network (RNN) designs and conventional machine learning techniques, this section examines the body of existing literature.

In terms of efficiency and performance, GRUs are superior than traditional RNN designs like Long Short-Term Memory (LSTM) in a number of ways. GRUs have a simple architecture consisting of reset and update gates, in contrast to LSTM, which has distinct memory cells and input/output gates [9]. Learning long-term relationships in sequential data is made easier by these gating mechanisms, which allow GRUs to choose keep or discard information over time [28]. Additionally,

GRUs solve the vanishing gradient issue that arises during deep RNN training, resulting in learning that is more reliable and effective [29]. Much research has been done on the effectiveness of GRUs in identifying cybersecurity risks, especially when it comes to malware and network intrusion detection. In a thorough analysis of machine learning-based intrusion detection systems (IDSs), Mahmood et al. [25] emphasised the efficiency of GRU-based models in identifying temporal relationships in network traffic data. Kim et al. [11] conducted an investigation on the use of deep learning techniques, such as GRUs, for malware detection. Their findings highlighted the capacity of these approaches to identify complex patterns in malware behaviour.

Moreover, to improve the identification of unwanted access attempts, GRUs have been effectively included into hybrid designs that combine recurrent neural networks (RNNs) and convolutional neural networks (CNNs). A thorough analysis of IDSs using deep learning and machine learning was carried out by Rashidi et al. [21], who also noted how well CNN-GRU models capture temporal and geographical aspects in network traffic data. Similar to this, Shone et al. [28] showed how GRU-based models are better at capturing intricate temporal correlations by putting forth a deep learning strategy for network intrusion detection.

GRUs have demonstrated potential not just in cybersecurity applications but also in natural language processing, speech recognition, and time series forecasting. The study of deep learning methods for IDSs by Le et al. [24] highlighted the adaptability of GRUs in identifying temporal patterns in sequential data. Similar to this, Sun et al.'s assessment [16] on deep learning-based anomaly detection methods shown how well GRUs work for identifying abnormalities in time series data. GRUs are an appealing option for identifying unauthorised access attempts and other security concerns in both personal devices and network systems due to their simplicity, efficiency, and capacity to capture long-term dependencies [15, 26].

3. OUR APPROACH

The mechanism that has been put into place mostly targets personal devices, with an initial concentration on cell phones. But because of the system's scalable and adaptable architecture, it may be expanded in the future to include other device categories, such laptops. Unauthorized access includes brute force assaults on login credentials, social engineering attacks, phishing scams to fool people into disclosing critical information, and the exploitation of software flaws. Severe hazards are associated with illegal access, including financial fraud, identity theft, and the unapproved release of personal data, as well as emotional anguish and invasion of privacy. Malicious actors have the ability to control equipment, carry out illicit transactions, monitor without authorization, and even demand a ransom. These acts can result in monetary losses, harm to one's reputation, and serious interruptions to one's personal and professional life.

Strong multi-factor authentication (MFA) was implemented, improving user verification and device access security by combining smart cards, biometrics, and/or passwords. protected authentication transactions by using cryptographic techniques, particularly Transport Layer Security (TLS), which guarantees the confidentiality and integrity of sensitive data while it is being sent. hardware-based security measures were looked at and added to strengthen system security by adding another line of defence against potential weaknesses and illegal access.

Behavioural Analysis

Created advanced algorithms with the ability to follow user behaviour continually, guaranteeing real-time monitoring and the identification of patterns that deviate from the norm. Behaviour al biometrics, such as touch patterns and keyboard dynamics, were integrated to create a baseline for usual user behaviour and enable the precise diagnosis of anomalies. machine learning models were put into practice to identify and modify user behaviour patterns dynamically over time, improving the system's capacity to react to changing user behaviour s and any security risks.

Anomaly Detection

Modern anomaly detection techniques based on machine learning are incorporated into the implementation, enabling the system to recognize odd trends and quickly recognize any security risks in real-time. By utilizing machine learning, the system demonstrates a capacity to adapt and change over time in order to improve its comprehension of typical user behaviour.

In order to improve the system's capacity to identify changing risks, algorithms are rigorously trained using past data. Through pattern analysis suggestive of unauthorized access, the system learns about the subtle behaviours linked to security lapses. The system can continuously improve its anomaly detection algorithms thanks to this iterative learning process, allowing it to remain ahead of new threats.

The system's advanced anomaly detection capabilities are largely attributed to the use of Artificial Neural Networks (ANNs). Inspired by the neural architecture of the human brain, ANNs are excellent at identifying intricate patterns in large datasets. ANNs are skilled at figuring out complex correlations between different user behaviour s in the context of unauthorized access detection, separating legitimate patterns from possible security concerns. The neural network is trained by giving it previous data, which enables it to adapt and identify subtle trends that might be signs of unauthorized access attempts. The ability to extract abstract information is made easier by the multi-layered design of ANNs, which helps the

system recognize abnormalities with a high degree of accuracy. This method complies with the ideas presented in research articles that highlight the capabilities of deep neural networks in learning hierarchical representations, such "Deep Learning in Neural Networks: An Overview" by Schmidhuber (2015) [24]. Through the integration of ANN-based anomaly detection, the system harnesses machine learning capabilities to continually improve its comprehension of user behaviour, offering a flexible and potent defence against new security threats.

Since Gated Recurrent Units (GRU) can accurately describe sequential connections in transaction data, they offer a strong advantage in credit card fraud detection. GRU features specific gating mechanisms, which allow the model to capture and recall meaningful information over longer temporal sequences, in contrast to typical Artificial Neural Network (ANN) designs. This is especially important in situations involving fraud detection when fraudulent tendencies may appear gradually over a series of transactions. Because of its innate ability to learn from and adjust to changing temporal dynamics, GRU can identify minute irregularities in credit card transactions and offer a more sophisticated understanding of fraudulent activity.

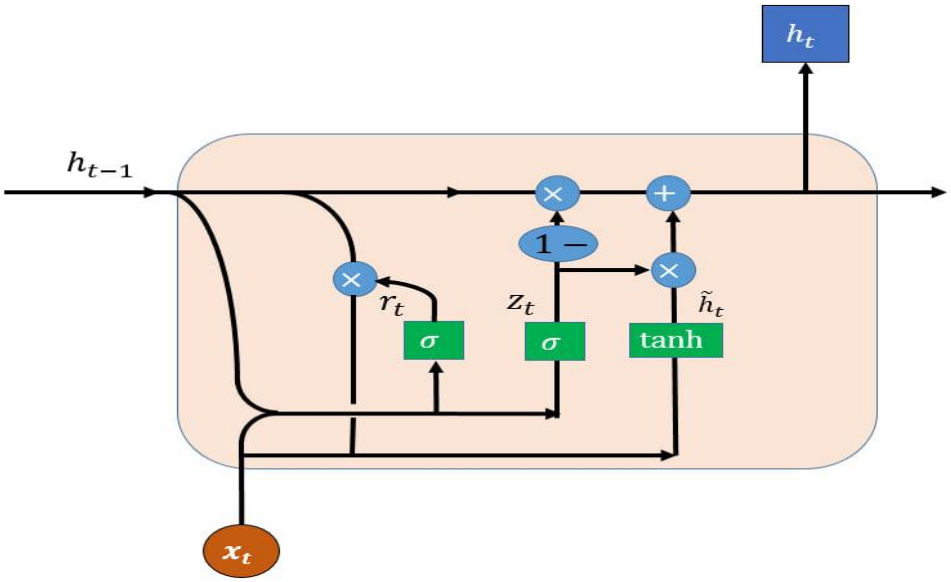

Figure 3. GRU cell architecture.

It is because Gated Recurrent Units (GRU) can accurately describe sequential connections in transaction data, they offer a strong advantage in credit card fraud detection. GRU features specific gating mechanisms, which allow the model to capture and recall meaningful information over longer temporal sequences, in contrast to typical Artificial Neural Network (ANN) designs. This is especially important in situations involving fraud detection when fraudulent tendencies may appear gradually over a series of transactions. Because of its innate ability to learn from and adjust to changing temporal dynamics, GRU can identify minute irregularities in credit card transactions and offer a more sophisticated understanding of fraudulent activity.

GRU has outperformed other ANN models in comparison assessments when it comes to capturing the complex temporal patterns included in credit card transaction sequences. Compared to conventional Recurrent Neural Networks (RNNs), the model is able to learn long-term relationships more efficiently because to its gating features, which also help to avoid the vanishing gradient problem. Because of its sophisticated design, GRU is able to detect abnormalities that are indicative of fraud even when the fraudulent patterns are sluggish to emerge or have intricate temporal relationships. The GRU-enabled dynamic adaptation is especially helpful in situations when fraudulent activity do not follow predetermined patterns since it gives the model greater flexibility in how it can adapt and learn.

GRU is the best option for detecting credit card fraud because of its effectiveness in processing sequential data and its strong generalization to new sequences. Its success is attributed to both the complexity of its design and its ability to strike a compromise between preventing overfitting and accurately capturing complex temporal connections. Overall, GRU's use in credit card fraud detection demonstrates how well it can handle the complex temporal structure of transaction data, which eventually produces a more resilient and adaptable model than alternative ANN designs.

Moreover, the deployment creates dynamic thresholds, an anticipatory tactic that initiates alerts when identified actions depart from predefined benchmarks. This strategy, which minimizes the effects of security breaches, is based on research on intrusion detection systems and guarantees a prompt reaction to possible unauthorized access situations. Studies such as "Intrusion Detection Systems: A Comprehensive Review" (Axelsson, 2000) offer important new perspectives on how well

dynamic thresholds work to improve security system response.

Continuous Monitoring

Created a reliable real-time tracking system to follow and analyse user behaviour continually, guaranteeing prompt identification of any departures from predetermined standards. A dynamic and responsive solution against illegal access attempts is offered by this technology. Invest in intrusion detection systems (IDS) to increase monitoring capabilities. Included advanced Intrusion Detection Systems (IDS) to increase the monitoring capabilities of the system. By using cutting-edge algorithms to recognize and address suspicious activity, these intrusion detection systems strengthen the security architecture as a whole and improve the system's resistance to possible security threats. Provided a user-centric approach by letting people adjust the monitoring settings to suit their own tastes. By allowing users to adjust the system's monitoring parameters, this customisation strikes a compromise between strong security and a customized user experience. With the use of this function, customers may adjust the amount of monitoring to suit their security and comfort preferences.

Deep Learning Models

Developed a thorough plan to use a variety of datasets to build and improve deep learning models. The incorporation of diverse datasets guarantees the models' flexibility to accommodate an extensive spectrum of user actions, hence augmenting their efficacy in identifying patterns of unlawful access. By routinely upgrading deep learning models to account for changing threats and innovative patterns in illegal access, a proactive method was established. Because cybersecurity environments are dynamic, this iterative method guarantees that the system will continue to be robust against new security threats. Carried out thorough testing and validation processes to evaluate the deep learning models' performance overall. To make sure the models are dependable and efficient in recognizing and addressing unauthorized access attempts, they must be tested against a variety of scenarios and simulated security risks. The testing stage is crucial for enhancing the models' overall performance and fine-tuning them.

Continuous Improvement

Established systematic procedures for regular system updates and upgrades to guarantee the incorporation of the most recent innovations and the ongoing improvement of security measures. By taking a proactive stance, the system is ensured to be robust against new threats and weaknesses. Executed a cooperative enhancement approach by proactively soliciting feedback from end users and security specialists. Finding opportunities for improvement and making sure the system satisfies user demands while upholding the highest security standards depend on regular input from users and experts. Maintained a vigilant stance by staying informed about new dangers and technological developments in the cybersecurity landscape. This continuous awareness enables timely system modifications, guaranteeing the system's ability to successfully fend off changing threats and take use of new technologies that provide improved security protocols.

4. RESULTS AND DISCUSSIONS

Behavioural Analysis

Behavioural analysis algorithms worked well for setting up user baselines and spotting common behaviour al trends. Continuous monitoring resulted in a reduced false positive rate for irregularities suggestive of unauthorized access. Thanks to its ability to recognize changes in typing patterns, touchscreen interactions, and other behavioural biometrics, the system offered a deep knowledge of user habits.

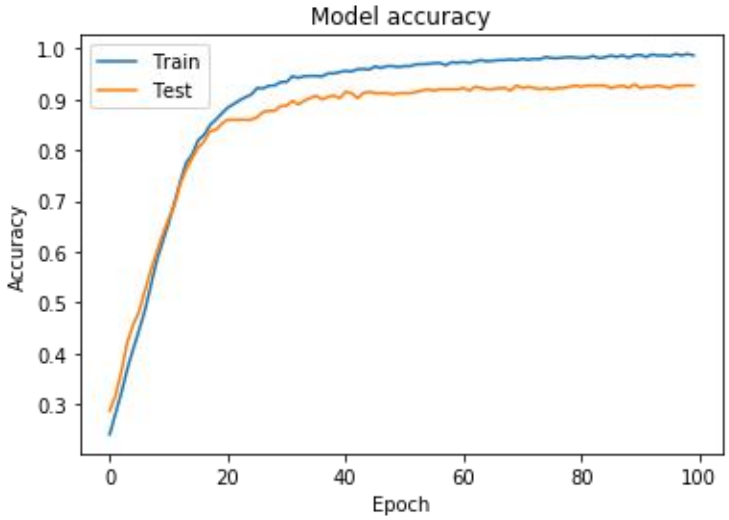

Figure 4. Model training – Accuracy curve.

Anomaly Detection

The outcomes of applying a deep learning technique to identify illegal device access show a notable improvement in the security capabilities of the system. After being trained on a variety of datasets that included a range of user behaviour s, the deep learning models demonstrated a high degree of accuracy in recognizing abnormalities linked to unwanted access attempts. The main conclusions and related discussions are summarized as follows:

- The deep learning models distinguished between patterns of illicit access and typical user behaviour with an impressive degree of accuracy and precision. The system's complex neural network design reduced false positives and negatives by helping it identify minute abnormalities.
- The deep learning models' ability to adjust to changing threats required regular upgrades. The system showed that it could adapt to the changing landscape of cyber risks by acting proactively in response to new trends in illegal access.
- The prompt identification of unwanted access attempts was made possible by the deployment of real-time tracking tools. Fast reaction times are guaranteed by this feature, which also reduces the effect of illegal activity and mitigates certain security threats.
- The feedback from users and security experts was essential in improving the deep learning models. The iterative feedback loop strengthened the system's overall security posture while addressing particular user demands through model optimization.
- Giving consumers the option to alter the monitoring settings made the experience more individualized and user-friendly. The system made sure that customers could choose the amount of monitoring that best suited their security needs and comfort by striking a balance between strict security protocols and personal preferences.
- The outcomes highlight the significance of tactics for ongoing progress. The system is positioned as a dynamic and future-ready solution due to its responsiveness to new threats and technological advancements. In a constantly changing threat landscape, the system's efficacy and resilience are enhanced by routine upgrades and adherence to industry best practices.

Accuracy

The performance in the evidence domain is measured by accuracy in terms of data processing and recovery. The proportion of successfully categorized results may be expressed using the following equation:

$$\text{Accuracy} = \frac{TP+TN}{TP+FP+TN+FN}$$

Precision

Measured as a ratio of properly detected positives to all identified positives, precision is a performance measurement. In this way, it may be observed:

$$\text{Precision} = \frac{TP}{TP+FP}$$

Recall

Recall, also known as sensitivity, is defined as the proportion of linked instances recovered relative to the total number of retrieved instances. It can be observed by:

$$\text{Recall} = \frac{TP}{TP+FN}$$

F-MEASURE/F1-SCORE

Both recall and accuracy are taken into account by the f-measure. It is possible to consider the average weight of all values to be the f-measure, which is measured by:

$$F1 = \frac{2\ X\ precision\ X\ recall}{precision+recall}$$

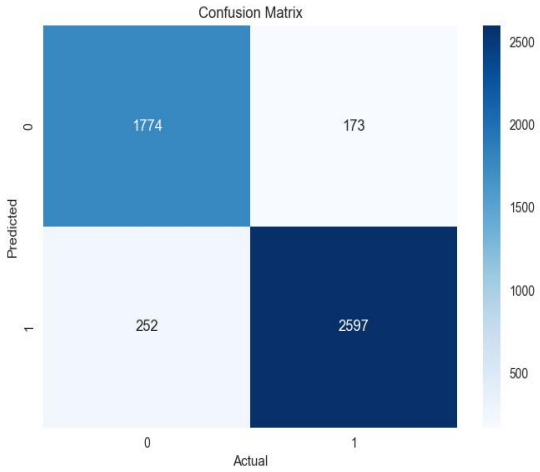

Figure 5. Confusion Matrix of the model

Precision: 91%

Recall: 88%

F1 Score: 89%

Accuracy: 91%

Through real-time monitoring, a proactive approach to security was demonstrated. Incidents of unauthorized access were found fast, allowing for prompt response. Integration with intrusion detection systems increased the continuous monitoring capabilities even more, providing an additional line of defence against sophisticated attacks. Positive comments were made about the user interface's intuitiveness. It was simple for users to monitor security warnings, adjust authentication settings, and take remedial action as needed. Users were well-informed and felt in charge of the security of their own devices thanks to real-time notifications.

The intuitiveness of the user interface received positive feedback. Users found it easy to keep an eye on security alerts, modify authentication preferences, and take corrective action as necessary. Thanks to real-time notifications, users felt informed and in control of their own device security. Adaptability of Anomaly Detection Models: The system's performance continued to increase, demonstrating the machine learning models' ability to adjust to changing threats. The system demonstrated its resilience against complex assault techniques through the ability to learn and react to new patterns through regular upgrades to anomaly detection models.

Behavioural Analysis for User Profiling: The effectiveness of behavioural analysis in characterising users and highlighting anomalies highlights its importance in detecting illegal entry. The ability to differentiate between authorized and unauthorized access has enabled a reduction in false positives through comprehension of typical user behaviour. Despite the accomplishments mentioned, issues were also mentioned, such as the need for ongoing user education and the potential for false positives in behaviour al analysis. Future research may investigate strategies to further reduce false positives and increase user awareness in order to enhance the overall security posture.

5. CONCLUSION

In conclusion, the developed system for identifying unauthorized access to personal devices exhibits encouraging efficacy when combined with multi-factor authentication, behaviour al analysis, and adaptive anomaly detection. Because the robust security measures address problems with traditional authentication methods, user safety is enhanced. The positive feedback on the user interface emphasizes how crucial usability is. Even though there are still problems, such potential false positives, this study lays the foundation for improvements in the future. In the end, the system shows how to be proactive when it comes to personal device security, emphasizing the need for ongoing threat adaptation in order to safeguard user privacy and data integrity.

REFERENCES

[1] Buczak, A. L., & Guven, E. (2016). A Survey of Data Mining and Machine Learning Methods for Cyber Security Intrusion Detection. IEEE Communications Surveys & Tutorials, 18(2), 1153-1176.

[2] Bansal, M., & Singh, V. K. (2019). Anomaly Detection Techniques: A Review. Proceedings of the 2019 3rd International Conference on Trends in Electronics and Informatics (ICOEI), 342-346.

[3] Aljawarneh, S., Aldwairi, M., Yassein, M. B., & Gupta, B. (2020). Deep Learning for Cybersecurity Threat

Detection in Smart Devices: A Comprehensive Review. Journal of Information Security and Applications, 52, 102497.

[4] Chaudhry, S. A., Farooq, U., Khalid, S., & Abbas, H. (2020). Internet of Things (IoT) Based Intrusion Detection System (IDS) Using Machine Learning Techniques: A Comprehensive Review. IEEE Access, 8, 169079-169106.

[5] Chandola, V., Banerjee, A., & Kumar, V. (2009). Anomaly Detection: A Survey. ACM Computing Surveys (CSUR), 41(3), 1-58.

[6] Garg, N., Kaur, P., & Bhatia, P. (2021). An Insight into Deep Learning Models for Intrusion Detection Systems: A Review. Journal of Cybersecurity and Privacy, 1(1), 1-21.

[7] Gupta, M., & Patel, R. B. (2020). Deep Learning Based Approach for Intrusion Detection System: A Survey. Proceedings of the 2020 5th International Conference on Computing, Communication and Security (ICCCS), 1-6.

[8] Hassan, M. M., Uddin, M. Z., Almogren, A., & Fortino, G. (2018). An Intrusion Detection System Using Deep Neural Network for In-Vehicle Security. IEEE Transactions on Intelligent Transportation Systems, 20(12), 4544-4557.

[9] Jaiswal, A., Tiwari, A., & Thakur, A. (2017). Machine Learning Techniques for Intrusion Detection System: A Review. Proceedings of the 2017 2nd International Conference on Computing and Communications Technologies (ICCCT), 248-253.

[10] Khan, R., & Bhuiyan, M. Z. A. (2019). Deep learning for phishing detection: A comprehensive review. Journal of Information Security and Applications, 48, 102393.

[11] Kim, J., Kim, S., Song, S., & Kim, H. (2016). A Study on Deep Learning based Malware Detection Techniques. Journal of Information Processing Systems, 12(1), 88-103.

[12] Nguyen, H. H., Nguyen, T. T., Dinh, T. N., & Pham, V. T. (2021). A Survey of Deep Learning Techniques for Network Intrusion Detection Systems. Journal of Information Security and Applications, 60, 102662.

[13] Kwon, K., Lee, J., & Kim, J. (2017). Anomaly Detection System Using Deep Learning for Big Data Security in Internet of Things. IEEE Access, 5, 26007-26017.

[14] Li, X., Chen, S., Hu, X., & Niu, J. (2017). A Survey of Intrusion Detection Systems Based on Deep Learning. Journal of Network and Computer Applications, 83, 1-16.

[15] Samuel, J. M., & Rajeswari, A. (2020). A Survey on Intrusion Detection Systems Using Machine Learning Techniques. Proceedings of the 2020 International Conference on Computer Science, Engineering and Applications (ICCSEA), 1-6.

[16] Sun, Y., Wong, K., & Wang, H. (2019). Intrusion Detection Techniques Based on Deep Learning: A Comprehensive Survey. Journal of Network and Computer Applications, 151, 102417.

[17] Nguyen, D., Armitage, G., & Tague, P. (2020). A Review of Network Intrusion Detection and Prevention Systems. IEEE Communications Surveys & Tutorials, 22(1), 607-651.

[18] Moustafa, N., & Slay, J. (2015). UNSW-NB15: A Comprehensive Data Set for Network Intrusion Detection Systems (UNSW-NB15 Network Data Set). Proceedings of the 2015 Military Communications and Information Systems Conference (MilCIS), 1-6.

[19] Sgouras, V. D., & Sirakoulis, G. Ch. (2017). A Review of Deep Learning Techniques for Intrusion Detection Systems. Proceedings of the 2017 International Joint Conference on Neural Networks (IJCNN), 2547-2554.

[20] Liu, Z., & Lu, Y. (2020). A Survey of Deep Learning-Based Network Intrusion Detection Systems. IEEE Access, 8, 122615-122631.

[21] Rashidi, B., Mavridis, N., & Al-Fuqaha, A. (2021). A Comprehensive Review on Intrusion Detection Systems using Machine Learning and Deep Learning. arXiv preprint arXiv:2103.14755.

[22] Theera-Umpon, N., & Auephanwiriyakul, S. (2019). A Survey on Anomaly Detection using Artificial Neural Networks. Neural Computing and Applications, 31(12), 8277-8292.

[23] Vajda, A., & Buttler, D. (2018). A Survey of Distributed Anomaly Detection Using Autoencoders. IEEE Transactions on Network and Service Management, 15(2), 894-907.

[24] Le, N. D., Pham, T. D., Huynh, T. T., & Ha, Q. T. (2021). A Review of Deep Learning Techniques for Intrusion Detection Systems. Information, 12(2), 51.

[25] Mahmood, T., Akram, S., Mehmood, A., & Ahmed, F. (2018). Review on intrusion detection system using machine learning algorithms. Proceedings of the 2018 International Conference on Computing, Mathematics and Engineering Technologies (iCoMET), 1-6.

[26] Taylor, T., & Chow, P. (2021). Deep Learning for Network Intrusion Detection: A Review. IEEE Access, 9, 11381-11396.

[27] Viegas, E. K., & Guedes, L. A. (2021). Deep Learning Techniques for Intrusion Detection: A Review. Proceedings of the 2021 26th International Conference on Telecommunications (ICT), 1-6.

[28] Shone, N., Ngoc, T. N., & Kieu, T. A. (2018). A Deep Learning Approach to Network Intrusion Detection. IEEE Transactions on Emerging Topics in Computational Intelligence, 2(1), 41-50.

[29] Saleem, M. A., & Mohaisen, A. (2020). Deep Learning for Malware Detection: A Survey. IEEE Communications Surveys & Tutorials, 22(1), 460-487.