



ORIGINAL

## Efficient intrusion detection model based on health care sector using lstm based rnn

### Modelo eficiente de detección de intrusos en el sector sanitario mediante rnn basado en lstm

Salim Davlatov<sup>1</sup>  , Akhtam Akramov<sup>2</sup>  , Ibodat Kamarova<sup>2</sup>  , Farida Azizova<sup>3</sup>  , Feruza Bakaeva<sup>4</sup>  , Muborak Turayeva<sup>5</sup>  , Bakhtigul Mamadaminova<sup>4</sup>  

<sup>1</sup>Bukhara State Medical Institute named after Abu Ali ibn Sino. Bukhara, Uzbekistan.

<sup>2</sup>Samarkand State Medical University. Samarkand, Uzbekistan.

<sup>3</sup>Center for the Development of Professional Qualifications of Medical Workers of the Ministry of Health of the Republic of Uzbekistan. Uzbekistan.

<sup>4</sup>Tashkent Institute of Irrigation and Agricultural Mechanization Engineers National Research University. Tashkent, Uzbekistan.

<sup>5</sup>Jizzakh State Pedagogical University. Uzbekistan.


**Cite as:** Davlatov S, Akramov A, Kamarova I, Azizova F, Bakaeva F, Turayeva M, et al. Efficient intrusion detection model based on health care sector using lstm based rnn. Health Leadership and Quality of Life. 2024; 3:191. <https://doi.org/10.56294/hl2024.191>

Submitted: 01-03-2024

Revised: 20-06-2024

Accepted: 15-10-2024

Published: 16-10-2024

Editor: PhD. Prof. Neela Satheesh 

Corresponding Author: Salim Davlatov 

#### ABSTRACT

Almost all real-world operations have moved online in recent years, with computers interacting with one another over the Internet. Consequently, there is an increase in network security vulnerabilities, making it difficult for network managers to protect their networks against all types of cyberattacks. Numerous methods for detecting network intrusions have also been created. However, they face critical difficulties from the continuous rise of new weaknesses that are outside the ability to understand of existing frameworks. We present an astute and effective Profound Learning (DL)- based network interruption discovery framework (NIDS), motivated by deep learning's outstanding performance in a variety of detection and identification tasks. We investigate an RNN-based prediction model for the detection of intrusions in industrial IoT networks. For intrusion detection, we use anomaly detection algorithms to identify if a packet is normal or abnormal. These methods quantify and assess the distance measurement in actual packets, as well as predict the following packet. The cyber security community has access to a wide range of malware datasets for use in public domain research. Furthermore, to the best of our knowledge, no study has offered a thorough evaluation of how well different machine learning techniques perform across a range of publicly accessible datasets. In this paper, we investigate novel hybrid deep learning model, with the aim of building an adaptable and efficient intrusion detection system that can identify and categorise unexpected and cyber-attacks. The results of this type of research make it easier to select the optimal algorithm for use in anticipating and stopping impending cyberattacks. Finally, to perform anomaly identification, a cosine similarity boundary that is thought of as a typical packet was provided. Then, a scoring function based on cosine similarity was applied.

**Keywords:** Attacks; LSTM; Health Care; Deep Learning.

#### RESUMEN

Casi todas las operaciones del mundo real se han trasladado a la red en los últimos años, con ordenadores que interactúan entre sí a través de Internet. En consecuencia, aumentan las vulnerabilidades de la seguridad de las redes, lo que dificulta a los gestores de las mismas la protección contra todo tipo de ciberataques. También se han creado numerosos métodos para detectar intrusiones en la red. Sin embargo, se enfrentan a dificultades

críticas derivadas del aumento continuo de nuevas debilidades que escapan a la capacidad de comprensión de los marcos existentes. Presentamos un marco de descubrimiento de interrupciones de red (NIDS) basado en el aprendizaje profundo (DL), astuto y eficaz, motivado por el extraordinario rendimiento del aprendizaje profundo en diversas tareas de detección e identificación. Investigamos un modelo de predicción basado en RNN para la detección de intrusiones en redes IoT industriales. Para la detección de intrusiones, utilizamos algoritmos de detección de anomalías para identificar si un paquete es normal o anormal. Estos métodos cuantifican y evalúan la medida de distancia en paquetes reales, además de predecir el siguiente paquete. La comunidad de ciberseguridad tiene acceso a una amplia gama de conjuntos de datos de malware para su uso en investigaciones de dominio público. Además, hasta donde sabemos, ningún estudio ha ofrecido una evaluación exhaustiva del rendimiento de diferentes técnicas de aprendizaje automático en una serie de conjuntos de datos de acceso público. En este artículo, investigamos un novedoso modelo híbrido de aprendizaje profundo, con el objetivo de construir un sistema de detección de intrusiones adaptable y eficiente que pueda identificar y categorizar ataques inesperados y cibernéticos. Los resultados de este tipo de investigación facilitan la selección del algoritmo óptimo para su uso en la anticipación y detención de ciberataques inminentes. Por último, para realizar la identificación de anomalías, se proporcionó un límite de similitud coseno que se considera un paquete típico. A continuación, se aplicó una función de puntuación basada en la similitud del coseno.

**Palabras clave:** Ataques; LSTM; Atención Sanitaria; Deep Learning.

## INTRODUCTION

Various counter measures for getting information saved in records on a PC kept up with on variants of windows may be tracked down in reference section. Conventional interruption discovery strategies, then again, didn't work well when utilized in that frame of mind to forestall awful tasks and virtualization interruption endeavors. Subsequently, creative security approaches are important to increment client trust in cloud administrations. To defeat the security issues, cloud sellers presently utilize cryptographic methods, consents, and mimicked firewalls. Notwithstanding, wellbeing safety net providers' configurable and secure arrangements couldn't handle creative sorts of dangers. For example, to forestall an aggressor, for example, for a SQL proclamation, this has the ability to impact the host machine. Thus, a mix of frameworks and programming level standards were expected for the web-based capacity framework. As of now, involved gatherings' security highlights didn't matter weakness filtering, requiring the utilization of additional ways of expanding security of cloud server. Furthermore, in recent years, there has been an increase in cyberattacks against computer networks.<sup>(1)</sup> Many techniques are being developed all the time to identify suspicious network behaviour that shows signs of intrusion, like obscurity, variety, entanglement, and fluctuating tendency. The accuracy of the intrusion detection and prevention system has significantly increased recently as a result of the application of artificial intelligence-based algorithms.<sup>(2)</sup> An intrusion detection system (IDS) is a system that monitors network traffic, detects anomalous or questionable activity, and then proactively neutralises intrusion risks. Based on how they work, intrusion detection systems are separated into two groups: (1) NIDS and (2) HIDS. In a society that is becoming more digital and diverse, it is incredibly difficult to protect private information with basic security measures. Network Infiltration Detection Systems (NIDS) are usually deployed or positioned at crucial network nodes to ensure that they monitor traffic that is more susceptible to infiltration, while HIDS systems function on any networked device with an Internet connection. The two main methods for identifying intrusion are intrusion detection systems (IDS) based on anomalies and IDS based on signatures.<sup>(3)</sup> Because it constantly refreshes the signature database with the most recent trends and zero-day attack methods, signature-based intrusion detection is the best option. Finding {{signature}\ patterns of incursion occurrence is its main focus. The anomaly-based intrusion detection system (IDS), sometimes referred to as behavior-based detection, compares consistent behavioural patterns with anomalous behaviours based on routine activity monitoring. In an increasingly digitised and diverse world, protecting private information with conventional means can be quite difficult. Administrators utilise Intrusion Prevention Systems (IPS) in reaction to IDS system notifications to prevent threats such as DDoS attacks and Trojan horses, among other things.

Developing an effective network intrusion detection system is one of the most crucial tasks for network security (NIDS). Despite significant developments in the industry, the majority of NIDS systems in use today are focused on signature-based strategies rather than anomaly detection methods.<sup>(4)</sup> Anomaly detection techniques are not commonly employed for a variety of reasons, including systems behavioural dynamics, training data lifetime, dependable training data collection, high costs, and mistake rates resulting from the dynamic nature of the data. Current approaches may give rise to inaccurate and inefficient NIDS verification methodologies and solutions.<sup>(5)</sup> The only thing that can fix the flaws in today's most advanced networks is an effective intrusion detection system.

### Literature Review

Over the past three decades, a number of anomaly detection approaches have been released in an attempt to develop effective network intrusion detection systems (NIDS), with the objectives of increasing the speed at which network packets are sent over the network and reaching a high level of prediction accuracy in recognising attacks.<sup>(6)</sup> All of these tactics begin with a fundamental statistical learning system and go from classical machine learning approaches to more contemporary deep learning-based strategies. Most of these techniques attempted to find a pattern inside the network so that malicious activity could be separated from regular traffic .

These days, regulated learning methods like Irregular timberland (RF), K-closest neighbor (KNN),<sup>(8)</sup> Backing vector machines (SVM), and so forth, are utilized to construct most ID frameworks. Be that as it may, these methods produce a ton of misleading problems and have a low location rate for assaults in IDS.<sup>(9)</sup> Presented a mixture interruption identification framework that utilizes the SVM and C4 decision tree (DT) grouping calculations, separately, to recognize bizarre attacks and distinguish harmful assaults. They tried their half breed IDS utilizing the NSL-KDD dataset.<sup>(10)</sup> assessed the Gullible Bayes (NB) calculation for irregularity identification utilizing the KDD Cup dataset. It was found that the NB procedure beat a few different IDS as far as low phony problem rate, short calculation times, and minimal expense.<sup>(11)</sup> utilized an improved strategy called the Help Vector Choice Capability (ESVDF). On the DARPA dataset, their IDS beat other traditional procedures.

Researchers also proposed further hybrid and parallel categorisation methodologies using the C4.classifier in conjunction with the Self-Organization Map (SOM).<sup>(12)</sup> This method views the SOM-based component as regularizing model behavior, with any deviation from this regular behavior being recognized as an incursion. Misuse detection is carried out via the C4 classifier-based section. The final choice was made by the decision support system (DSS) module, which may be utilized to classify the intrusion type data into the appropriate attack category. By combining inputs from each module, the DSS was assessed, and using the KDD dataset, it was able to detect attacks with a maximum accuracy of 99,8 % and a false alarm rate of 12,5 %.

Although the above described techniques have shown some degree of effectiveness in detecting security issues, there is always space for improvement, especially when it comes to increasing accuracy and reducing the quantity of false alarms. Deep learning-based techniques are therefore growing in popularity. The neural network (NN), which is at the core of these techniques, provides extraordinarily powerful answers for a range of issues in domains such as cybersecurity, natural language processing (NLP), computer vision, and speech recognition.<sup>(13)</sup>

### METHOD

One kind of repetitive neural network that is ordinarily utilized for succession expectation issues is known as a Long Transient Memory organization.<sup>(14)</sup>

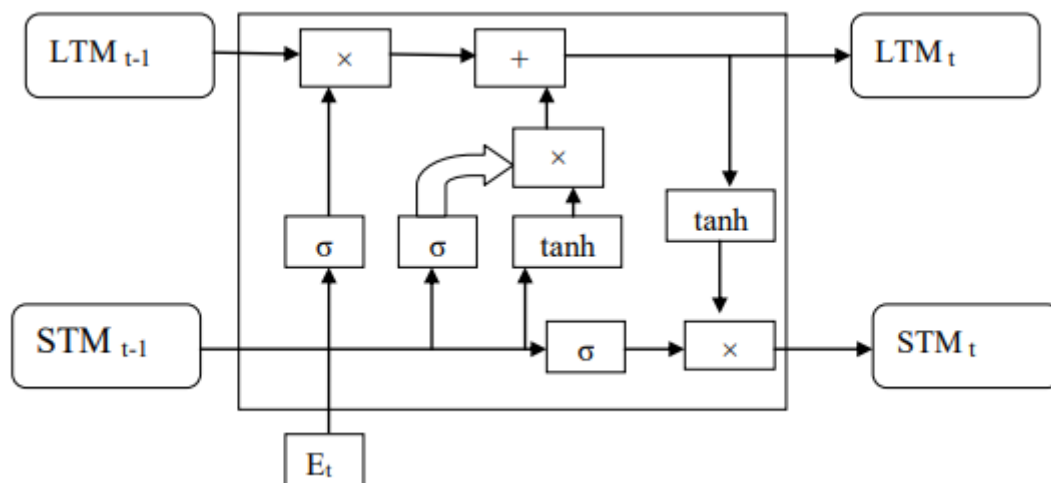


Figure 1. LSTM architecture

It is realized that cells have long transient memory (LSTM) that permits them to hold values across time.<sup>(15)</sup> Take  $x_t$  as an input. The hidden layer's output is  $h_t$ , and it was previously  $h_{t-1}$ . The cell's input and output states are  $C_t$  and  $G_t$ , respectively, and their previous values are  $G_{t-1}$  and  $T_0$ , respectively.<sup>(16)</sup> According to figure 1, the construction of the LSTM cell shows that  $G_t$  and  $h_t$  are moved to the following brain network in Remaining Organization building blocks (RNN).<sup>(17)</sup> The result and neglect entryways don't refresh the memory all through the LSTM's blend of the result from the former unit and the ongoing info state. The accompanying recipes are

utilized to get  $G_t$  and  $h_t$ .<sup>(18)</sup> The cell input state, input entryway, and three doors should not entirely set in stone. Long short-term memory flow prediction is given in figure 2.

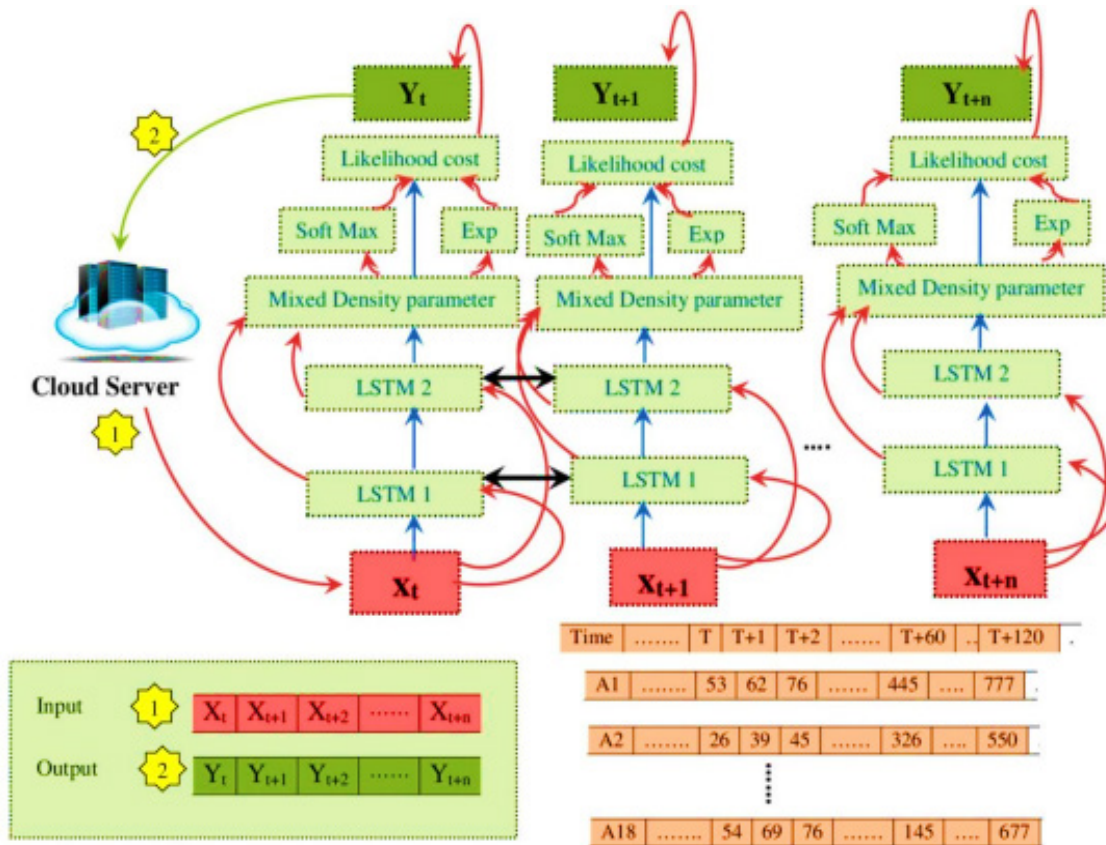


Figure 2. Long Short-Term Memory Flow Prediction

### Filter Tuning

Below is a discussion of the suggested LSTM's training method. A hybrid ensemble learning method is created by fusing Ada-Boost learning algorithms with LSTM networks.<sup>(19)</sup> The Ada-Lift strategy changes the loads of the classifiers to reinforce and upgrade the more vulnerable classifiers.<sup>(20)</sup> Until a serious level of characterization/expectation exactness is to be achieved, the proposed Cross breed Models gatherings the Ada-Lift with the LSTM to deal with the video groupings really with higher forecast precision.<sup>(21)</sup> Dk(i), which addresses highlights from the managed channel layers of the convolutional networks, is utilized to prepare the LSTM network after the elements from the pruned layers have been gathered. D(i) are first set uniformly, with  $D1(i) = 1/n$ , where n is the quantity of preparing tests.<sup>(22)</sup>

### RESULTS AND DISCUSSION

This segment presents the discoveries of the investigation, which was directed utilizing the two recently referenced datasets, alongside a clarification.<sup>(23)</sup> For each dataset, two primary investigations are completed to assess the adequacy of the proposed calculation, ILSTM. In the principal analyze, the proposed strategy is assessed for double characterization (i.e., typical or malignant traffic), and in the subsequent examination, it is assessed for multi-class grouping (i.e., to separate between typical, dos, prob, U2R, or R2L). Each trial likewise contained two fundamental components: The calculation's pertinence will be exhibited by<sup>(1)</sup> a measurable investigation (Wilcoxon test) and a study<sup>(2)</sup> a correlation of the ILSTM calculation's presentation with other profound learning and AI techniques.<sup>(24)</sup>

This analysis expects to test the proposed ILSTM's exhibition for interruption identification with regards to parallel arrangement – that is, distinguishing whether organization traffic is typical or unusual.<sup>(25)</sup> This was finished utilizing the KDDTest+ and KDDTest-21 datasets, as demonstrated underneath. The proposed ILSTM is contrasted and the first LSTM and two LSTM adaptations that have been improved utilizing BOA and CBOA to assess its exhibition.<sup>(26)</sup> These outcomes were accomplished after a normal of ten runs with the KDDTest+ dataset.<sup>(27)</sup> This information unambiguously shows that, with a 91,31 % precision, 96,46 % explicitness, and 3,51 % FAR – a basic incentive for interruption recognition frameworks – the suggested ILSTM calculation produced the best outcomes.<sup>(28)</sup> Striking text demonstrates other top results in this table.<sup>(29)</sup> For more itemized data, allude to figure 3, which shows the disarray framework for this trial.



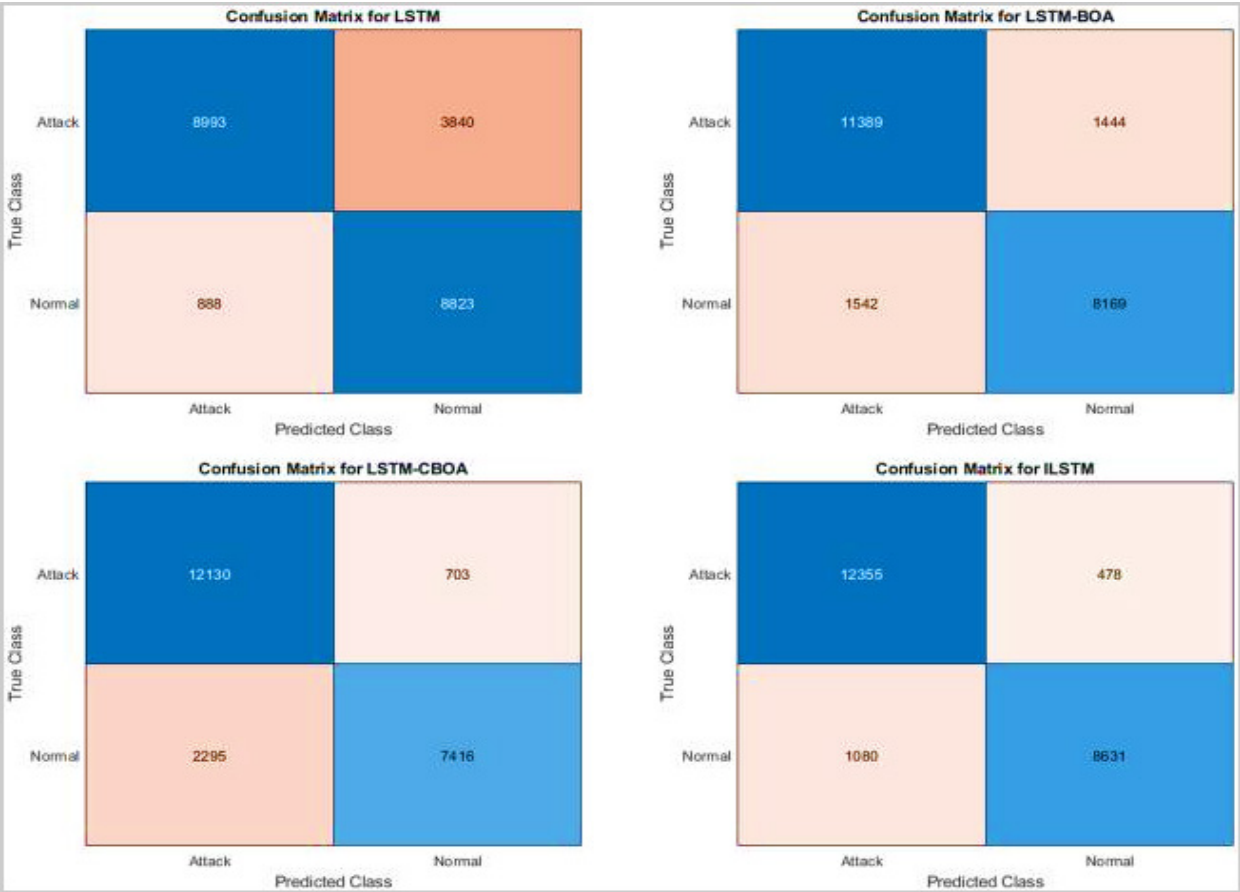
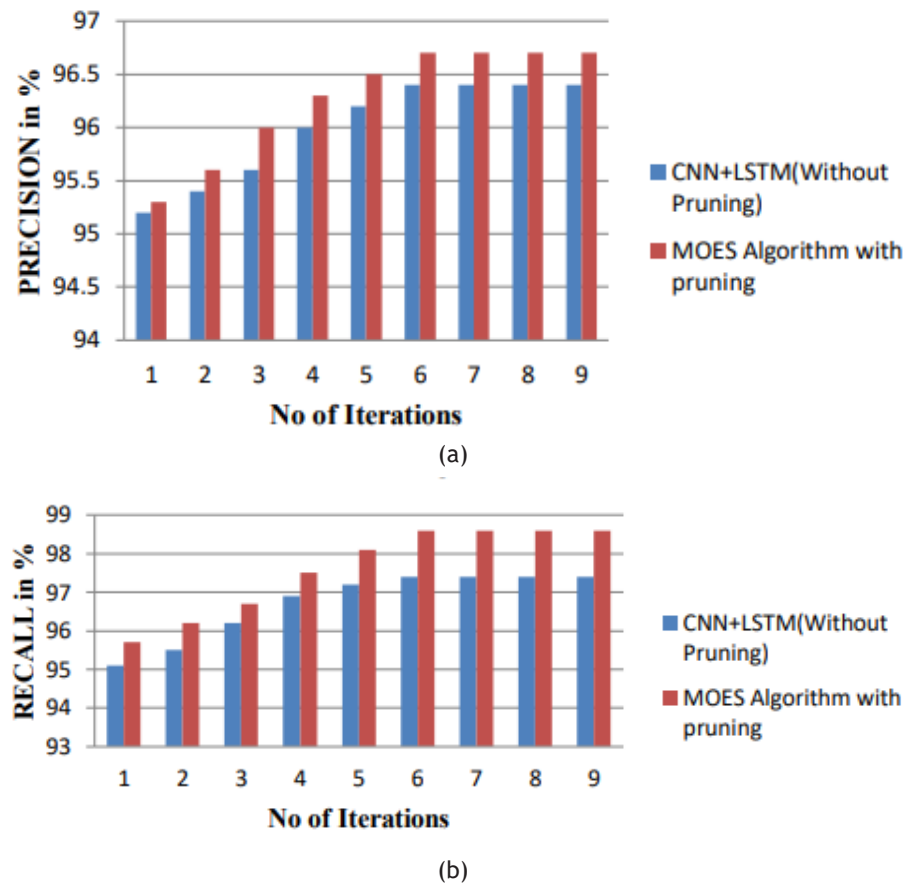


Figure 3. Confusion matrices for KDDTest+ in binary classification

Following figure 4 shows the performance comparison of proposed models.



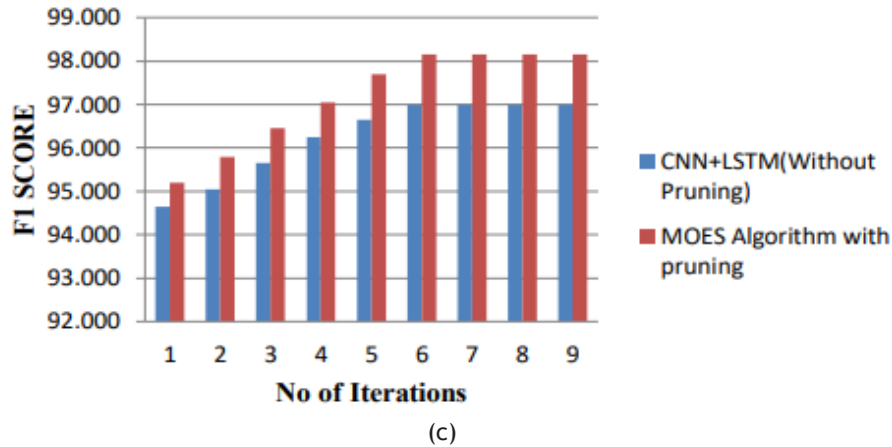


Figure 4. Performance comparison

## CONCLUSIONS

The purpose of this work was to introduce a revolutionary approach based on learning algorithms that allows for attack prevention, detection, and response in order to prevent the same aggression from occurring in the future. Through detection, a particular trait that violates security policies can be found. As was already noted, the RNN layers can operate in parallel to improve performance and capture local correlations of sequence patterns. In the wake of being prepared on normal call successions, the model predicts a likelihood circulation for the following number in a call grouping. Thusly, Host-based Interruption Discovery Framework with Consolidated RNN Model 9 is expected to use this. A likelihood for the whole succession and a limit for classication are looked over the scope of negative log probability values. We have kept up with close to best in class execution for brain network models with an impressive decrease in preparing times contrasted with LSTM models. It is not really shocking that our presentation doesn't match that of the gathering models. Our model ought to be a significant piece of a greater gathering model, perhaps joined with a KNN-based model and an encoder-decoder model.

## BIBLIOGRAPHIC REFERENCES

1. S. Forrest, S. A. Hofmeyr, A. Somayaji, T. A. Longsta\_: A Sense of Self for Unix Processes, Proceedings. In: 1996 IEEE Symposium on Security and Privacy, Oak- land, CA, pp. 120-128 (1996)
2. Gideon Creech and Jiankun Hu, Generation of a new IDS Test Dataset: Time to Retire the KDD Collection
3. Ilya Sutskever, Oriol Vinyals, Quoc V. Le: Sequence to Sequence Learning with Neural Networks
4. Jan Chorowski, Dzmitry Bahdanau, Dmitriy Serdyuk, Kyunghyun Cho, Yoshua Bengio: Attention-Based Models for Speech Recognition, NIPS 2014 Deep Learning Workshop.
5. Alexander M. Rush, Sumit Chopra, Jason Weston: A Neural Attention Model for Abstractive Sentence Summarization
6. Ramesh Nallapati, Bowen Zhou, Cicero Nogueira dos santos, Caglar Gulcehre, Bing Xiang: Abstractive Text Summarization Using Sequence-to-Sequence RNNs and Beyond
7. Yelong Shen, Po-Sen Huang, Jianfeng Gao, Weizhu Chen: ReasoNet: Learning to Stop Reading in Machine Comprehension, Microsoft Research
8. Yin, C.; Zhu, Y.; Fei, J.; He, X. A Deep Learning Approach for Intrusion Detection Using Recurrent Neural Networks. IEEE Access 2017, 5, 21954-21961. [Google Scholar] [CrossRef]
9. Kuang, F.; Xu, W.; Zhang, S. A novel hybrid KPCA and SVM with GA model for intrusion detection. Appl. Soft Comput. 2014, 18, 178-184. [Google Scholar] [CrossRef]
10. Reddy, R.R.; Ramadevi, Y.; Sunitha, K.V.N. Effective discriminant function for intrusion detection using SVM. In Proceedings of the International Conference on Advances in Computing, Communications and Informatics (ICACCI), Jaipur, India, 21-24 Septembert 2016; pp. 1148-1153. [Google Scholar]

11. Li, W.; Yi, P.; Wu, Y.; Pan, L.; Li, J. A new intrusion detection system based on KNN classification algorithm in wireless sensor network. *J. Electr. Comput. Eng.* 2014, 2014, 240217. [Google Scholar] [CrossRef]
12. Farnaaz, N.; Jabbar, M.A. Random forest modeling for network intrusion detection system. *Procedia Comput. Sci.* 2016, 89, 213-217. [Google Scholar] [CrossRef]
13. Zhang, J.; Zulkernine, M.; Haque, A. Random-Forests-Based Network Intrusion Detection Systems. *IEEE Trans. Syst. Man Cybern. Part C Appl. Rev.* 2008, 38, 649-659. [Google Scholar] [CrossRef]
14. Çiftçi, N., Ayas, D., & Bakan, M. (2021). First Report on the Elemental Composition of the Largest Bony Fishes in the World, the Ocean Sunfish (*Mola mola*) from the Mediterranean Sea. *Natural and Engineering Sciences*, 6(3), 166-177. <http://doi.org/10.28978/nesciences.1036846>
15. Mitra, S., & Acharya, S. C. (2024). Socio-Emotional Well-Being and its Determinants in School Students: A Comprehensive Review. *Indian Journal of Information Sources and Services*, 14(4), 108-116. <https://doi.org/10.51983/ijiss-2024.14.4.17>
16. Menniti, M. A., & Vella, A. (2022). Sighting of risso's dolphin (*Grampus griseus*) during scientific research of the calabrian southern Ionian Sea (Central Eastern Mediterranean). *Natural and Engineering Sciences*, 7(3), 248-259. <http://doi.org/10.28978/nesciences.1206056>
17. Manikandan, V., Ramakrishnan, P. R., & Shanmugam, H. (2024). The Advantages of Adopting the ISO/IEC 17025: 2017 Lab Management System in Calibration and Testing Laboratories. *Indian Journal of Information Sources and Services*, 14(4), 131-135. <https://doi.org/10.51983/ijiss-2024.14.4.20>
18. Saidov, A., Yakhshieva, Z., Makhkamova, N., Gudalov, M., Djuraeva, N., Umirzaqov, o., Adilova, o., & Juraev, A. (2024). Examining environmental impact through geological interactions and earth's layers. *Archives for Technical Sciences*, 2(31), 230-239. <https://doi.org/10.70102/afts.2024.1631.230>
19. Yanar, A., Turan, C., & Doğdu, S. A. (2022). Report of *Nerocila bivittata* (Risso, 1816) (Isopoda: Cymothoidae) Parasitic on Alien Fish, *Pterois miles* (Bennett, 1828) from the Aegean and Mediterranean Sea. *Natural and Engineering Sciences*, 7(2), 169-181. <http://doi.org/10.28978/nesciences.1159261>
20. Patel, V., & Shivarama Rao, K. (2023). Research and Publications Productivity of the Malaviya National Institute of Technology, Jaipur: A Scientometric Study. *Indian Journal of Information Sources and Services*, 13(1), 59-64. <https://doi.org/10.51983/ijiss-2023.13.1.3428>
21. Ilić, P., Nešković Markić, D., & Stojanović Bjelić, L. (2018). Variation Concentration of Sulfur Dioxide and Correlation with Meteorological Parameters. *Archives for Technical Sciences*, 1(18), 81-88.
22. Turan, F., Ergenler, A., & Bardakcı, F. (2022). Monitoring DNA damage in Suez pufferfish (*Lagocephalus suezensis*) from the northeastern Mediterranean. *Natural and Engineering Sciences*, 7(2), 190-199. <http://doi.org/10.28978/nesciences.1159286>
23. Priyanka, J., Poorani, T. R., & Ramya, M. (2023). An Investigation of Fluid Flow Simulation in Bioprinting Inkjet Nozzles Based on Internet of Things. *Indian Journal of Information Sources and Services*, 13(2), 46-52. <https://doi.org/10.51983/ijiss-2023.13.2.3845>
24. Singh, N., & Katiyar, S. K. (2024). Assessment of black spots in urban bhopal with the aid of weighted severity index and kernal density estimation methods. *Archives for Technical Sciences*, 2(31), 201-212. <https://doi.org/10.70102/afts.2024.1631.201>
25. Uyan, A. (2022). A Review on the Potential Usage of Lionfishes (*Pterois* spp.) in Biomedical and Bioinspired Applications. *Natural and Engineering Sciences*, 7(2), 214-227. <http://doi.org/10.28978/nesciences.1159313>
26. Bazarova, N. and et.al. (2024). Determination of the relationship between the polymorphic genes of metalloproteinases MMP9 (A-8202G) RS11697325 and the level of cystatin C in children with chronic nephritic syndrome. *BIO Web of Conferences*, 121, 03011. <https://doi.org/10.1051/bioconf/202412103011>

27. Karimov, B. K., et al. (2020). Relationship between the concentrations of nitrogen compounds and the water discharge in the Chirchiq River, Uzbekistan. IOP Conference Series: Earth and Environmental Science, 614, 012154. <https://doi.org/10.1088/1755-1315/614/1/012154>

28. Karimov, N., et al. (2024). Exploring food processing in natural science education: Practical applications and pedagogical techniques. Natural and Engineering Sciences, 9(2), 359-375. <https://doi.org/10.28978/nesciences.1574453>

29. Ebenezar, U.S., Vennila, G., Balakrishnan, T.S. and Krishnan, P., 2024, June. Optimizing Healthcare Delivery through CloudBased Clinical Decision Support Systems. In 2024 OPJU International Technology Conference (OTCON) on Smart Computing for Innovation and Advancement in Industry 4.0 (pp. 1-6). IEEE.

#### **FINANCING**

No financing.

#### **CONFLICT OF INTEREST**

The authors declare that there is no conflict of interest.

#### **AUTHORSHIP CONTRIBUTION**

*Data curation:* Salim Davlatov, Akhtam Akramov, Ibodat Kamarova, Farida Azizova, Feruza Bakaeva, Muborak Turayeva, Bakhtigul Mamadaminova.

*Methodology:* Salim Davlatov, Akhtam Akramov, Ibodat Kamarova, Farida Azizova, Feruza Bakaeva, Muborak Turayeva, Bakhtigul Mamadaminova.

*Software:* Salim Davlatov, Akhtam Akramov, Ibodat Kamarova, Farida Azizova, Feruza Bakaeva, Muborak Turayeva, Bakhtigul Mamadaminova.

*Drafting - original draft:* Salim Davlatov, Akhtam Akramov, Ibodat Kamarova, Farida Azizova, Feruza Bakaeva, Muborak Turayeva, Bakhtigul Mamadaminova.

*Writing - proofreading and editing:* Salim Davlatov, Akhtam Akramov, Ibodat Kamarova, Farida Azizova, Feruza Bakaeva, Muborak Turayeva, Bakhtigul Mamadaminova.