UtilitasMathematica

ISSN 0315-3681 Volume 122, 2025

Deep Learning-Based Intrusion Detection System Using Stacked Autoencoders for Financial Fraud Detection by using ensemble techniques (CNN, LSTM and CNN)

[1] Vishal Lavhaji Lokhande, [2] Vinod Jagannath Kadam, [3] Shahajirao Chinchole, [4] Maryam khalil charfare

[1] Researcher, Dr Babasaheb Ambedkar Technological University, Lonere, Maharashtra, lokhandevishal.it@gmail.com

[2] Assistant Professor, Dr Babasaheb Ambedkar Technological University, Lonere, Maharashtra, vjkadam@dbatu.ac.in

[3] Researcher, Dr Babasaheb Ambedkar Technological University, Lonere, Maharashtra, shahajichinchole@gmail.com

[4] Researcher, Dr Babasaheb Ambedkar Technological University, Lonere, Maharashtra, charfaremaryam@gmail.com

Abstract: This look-in to investigates the mounting threats of cyber security in IoT environments and electronic financial transactions by developing an extensive intrusion detection system (IDS). IDS employs cutting-edge deep gaining knowledge of methods, in addition to an stacked autoencoder (AE) and deep neural network (DNN). The combined AE learns autonomously the basic houses from input network information in unattended, which enhances the effectiveness of future type duties. Then, beneath the supervision of DNN, a deep noble properties come from the proper categorization of the disturbance. Assessment of KDDCUP99 and NSL-KDD facts units reveals incredible overall performance, while the CNN LSTM sets an brilliant accuracy of ninety nine.9%. The following upgrades include the research of extra report methodologies including CNN and CNN LSTM models, resulting in encouragement of accuracy progress. A user-friendly the front-stop interface created the use of a flask body makes it less difficult to have interaction and authenticate customers. This examination enhances cyber security in IoT environments and virtual transactions and demonstrates the effectiveness of deep learning and document techniques in IDS. The intelligent utilization of the device is highlighted through its easy interface, which simplifies adoption in a real environment. Future endeavors are seeking to enhance report strategies and the ability to expand systemic capabilities for a much larger deployment context.

"Index Terms—*Deep neural network (DNN), digital financial service, Internet of Things (IoT), intrusion detection system (IDS), stacked autoencoder (AE)".*

1. INTRODUCTION

Our daily interactions, learning and work have changed as a result of the ubiquity of the Internet. However, this widely penetration on the Internet causes security problems, especially in financial transactions, which is the cornerstone of contemporary life, especially in intelligent digital environments that promote urbanization and industrialization [1].

Financial services are rapidly changing into intelligent digital settings with many IoT devices [1]. Connected networks complicate when developing IoT services. This connection allows easy communication and data sharing, but also represents weaknesses that bad actors could use [1].

Intelligent digital financial services use cable or wireless networks that expose them to several security risks. Due to the volume of data flow, the intruder can simply represent the service provider, while network attacks, especially unexpected, are difficult to detect [1].

Detection and prevention of network intrusionis a prime technical hassle that calls for new solutions. IDSS is decisive in spotting and responding to these threats, whether or not they're current or past [1]. Attacks generated by way of guy and machines grow extra complicated and use hardware, packages and network topologies, which include IoT backups [1].

Bets are huge, as the Yahoo statistics violation indicates, causing full-size monetary losses, and the assault of bitcoins that confirmed the fatal consequences of cyber threats [2]. Advanced algorithms continuously complicate cyber protection and require sturdy and adaptable defense [1].

Both NIDE and host disruption detection (HID) targets for disturbing behavior [3]. NID systems use network devices to analyze behavior and identify risks, while HID systems examine the protocol files locally for intrusion [3].

Traditional ID used detection based totally on signatures and anomalies to become aware of threats. Signature -based totally detection used predetermined formulation and filters, even as detection based totally on anomaly used heuristics to discover odd conduct [3]. Although those strategies were a hit against acquainted threats, they generally lacked fresh or surprising attacks, which brought about a significant fake fantastic extent.

Deep Learning, a subgroup of machine learning, has shown an exceptional ability to learn fine patterns and properties from huge data orchards [4]. The ID has changed to deep learning to overcome these problems. However, the deep -based ID -based ID has significant false positive rates for unknown threats, poor portability between data sets and poor documentation [5].

Due to these troubles, this research shows a deep detection method of disruption based totally on gaining knowledge of by AE and DNN [1]. The proposed IDS uses stacked AE to extract key sieve information and DNN for accurate classification to enhance detection and decrease false positives.

To overcome deep limitation of learning -based ID, this work emphasizes the assessment of common data files and model documentation [1]. The proposed IDS deals with these deficiencies to provide a strong and effective solution to the IoT cyber security and digital financial transactions.

Later parts describe the technique, experimental evaluation and consequences of the proposed ID, as well as its consequences and destiny research.

2. LITERATURE SURVEY

As a result of the complexity, volume and digitization of financial transaction, financial fraud detection has become the main problem in current financial ecosystems. Rules -based systems are often inflexible to the changing tendency of fraud. Contemporary research uses “machine learning (ML), deep learning (DL) and hybrid methods” to increase the durability, scalability and intelligence of fraud detection systems.

Cheng et al. [3] They checked graph neural network (GNN) to detect financial fraud and

emphasized its ability to simulate transactions, accounts and users' connections. GNN can detect suspicious behavior that standard models are missing by capturing graph data relationships. Research shows that GNN can identify network level fraud such as secret or synthetic identity fraud, better than transaction data.

Sudharson et al. [5] They designed a hybrid model of deep learning to detect financial fraud using Bilstm and auto -coder. The Auto -Limits extracts and reduces the size, while the Bilstm component collects contextual information from past and future time steps. The attention technique improves the model by highlighting the key aspects of transactions. This hybrid design solves high -dimensional data and time relations, improves detection accuracy and reduces false positives.

Adejumo and Ogburie [11] tested the involvement of forensic money owed in the detection of economic fraud and growing trends and training practices. Their outcomes emphasize the need to recognize the domain in AI models to growth interpretability and practical usability, although they've no longer centered on algorithmic fashions. According to a scam management time table, forensic accounting and automatic detection systems cooperate.

A thorough study of literature from Chen et al. [13] They examined the application of deep learning to detect financial fraud. They found a transition from conventional machine learning to complicated DL architecture, such as CNN, RNN and transformer -based models. Reviews emphasize hybrid models, attention and learning processes to improve accuracy, generalization and durability. It also shows an increased interest in explaining the AI to increase transparency and trust of the financial institution.

Lee et al. [14] They examined techniques of fraud detection with device mastering through information on Indonesian banking. Their research tested DT, RF, GB and SVM for fraud detection. File -primarily based models passed person classifiers in accuracy and accuracy. Research also emphasizes the want for engineering and records practise, as the pleasant of the enter records influences the performance of the model.

Aljunaid et al. [15] They developed an explained federated teaching architecture for safe detection of financial fraud. Distributed learning without centralization of sensitive client data allows financial institutions to work together to detect fraud. The AI components AI provide transparency of decision -making for consistency with user regulation and confidence. This research emphasizes the equalization of the accuracy of detection, privacy and interpretability in real deployment.

Liu et al. [17] They used latent semantic characteristics from the text of the annual report with accounting indicators to identify fraud. The combination of unstructured text data with structured financial measures allows the program to detect the tendency and irregularities of fraud. Their research shows that NLP in conjunction with numerical analysis can reveal the financial behavior of enterprises.

Al-Dahasi et al. [19] Come the class imbalance in fraud data files. To improve the detection of a minority class (fraudulent). They have found considerable improvements in the recall and F1-Score, indicating that the reduction of imbalances is essential for fraud detection systems.

These research show a trend towards smarter, hybrid and explained financial fraud detection. BiLSTM, GNNs, attention mechanisms, federated learning and semantic analysis show the

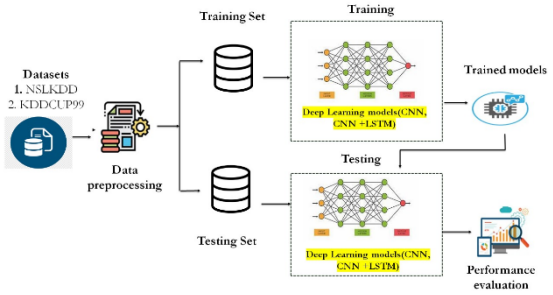
complexity of current fraud detection. These methods solve asymmetry of data, development of fraud strategies, personal data protection and interpretability. AI models, domain knowledge and secure framework can improve fraud detection, scalability and transparency, as financial systems are more connected and digitized.

3. METHODOLOGY

It develops and improves and improves the financial fraud IDS. The system first learns efficiently and reduces the width of the elements using AE. After training beneath the supervision of DNN, it extracts deep studying for class. This included method using AE stacked with latent layers and DNN with or three layers indicates promising in distinguishing ordinary and offensive activities. File procedures such as vote casting classifier and stacking classifier enhance financial fraud detection accuracy. extra classifiers cooperate on developing more unique predictions and attaining 99%accuracy. The flask is used to create a consumer -pleasant front stop as an extension. The IDS is more applicable to monetary establishments and groups for preventing easy interfaces on the queue. consumer authentication permits you to secure IDS and prefers person security whilst detecting financial transaction intrusion.

device structure consists of initial statistics processing and training and assessment of the deep learning version. The machine trains and assessments for NSLKDD and KDDCUP99. records initial processing divides statistics units into education and take a look at package for model training and evaluation. Deep learning models together with CNN and CNN + LSTM are then used to discover disturbances.

Training and testing set compare those fashions. The observed out fashions are saved for future use. The accuracy, precision, recall and score F1 are used to assess the general performance of the model in distinguishing regular and offensive occasions. This methodological technique makes the detection gadget resistant and reliable in figuring out and assuaging threats.



"Fig 1 Proposed Architecture"

i) Dataset collection:

This paintings makes use of three statistics units for training and comparing the proposed detection: KDDCUP99, NSL-KDD and AWID. The KDDCUP99 statistics report is a splendid benchmark facts set of TCP Dump facts from DARPA detection in 1998. It includes two codecs: whole and 10% of subset, together with forty one tendencies and five instructions: "Normal", "DOS", "probe", "R2L" and "U2R". This assessment consists of 9 fundamental factors, thirteen content material competencies, and 19 timeframe capabilities derived from TCP/IP packets. The data report is split into training and check sets, every showing one in all a kind samples for specific sorts of attacks.

	duration	protocol_type	service	flag	src_bytes	dst_bytes	land	wrong_fragment	urgent	hot	...	dst_host_srv_count	dst_host_same_srv_rate	dst_h
0	0	tcp	http	SF	181	5450	0	0	0	0	...	9	1.0	
1	0	tcp	http	SF	239	486	0	0	0	0	...	19	1.0	
2	0	tcp	http	SF	235	1337	0	0	0	0	...	29	1.0	
3	0	tcp	http	SF	219	1337	0	0	0	0	...	39	1.0	
4	0	tcp	http	SF	217	2032	0	0	0	0	...	49	1.0	
...	...	...	...	...	...	...	...	...	...	...	...	...	...	
494016	0	tcp	http	SF	310	1881	0	0	0	0	...	255	1.0	
494017	0	tcp	http	SF	282	2286	0	0	0	0	...	255	1.0	
494018	0	tcp	http	SF	203	1200	0	0	0	0	...	255	1.0	
494019	0	tcp	http	SF	291	1200	0	0	0	0	...	255	1.0	
494020	0	tcp	http	SF	219	1234	0	0	0	0	...	255	1.0	

"Fig 2 KDD CUP 99 Dataset"

NSL-KDD, Effective iteration KDDCUP99, seeks to reduce distortion in machine learning algorithms by removing foreign data. Although it is suitable for detection of abuse, it has real time challenges.

The facts document is divided into training and check units and keeps an identical distribution of samples across assault classes. These facts units offer substantial and diverse information for education and assessment of disturbance detection structures, allowing scientists to evaluate the performance and resistance of their proposed processes across special attack eventualities and network conditions.

	duration	protocol_type	service	flag	src_bytes	dst_bytes	land	wrong_fragment	urgent	hot	...	dst_host_srv_count	dst_host_same_srv_rate	dst_h
0	0	tcp	http	SF	181	5450	0	0	0	0	...	9	1.0	
1	0	tcp	http	SF	239	486	0	0	0	0	...	19	1.0	
2	0	tcp	http	SF	235	1337	0	0	0	0	...	29	1.0	
3	0	tcp	http	SF	219	1337	0	0	0	0	...	39	1.0	
4	0	tcp	http	SF	217	2032	0	0	0	0	...	49	1.0	
...	...	...	...	...	...	...	...	...	...	...	...	...	...	
494016	0	tcp	http	SF	310	1881	0	0	0	0	...	255	1.0	
494017	0	tcp	http	SF	282	2286	0	0	0	0	...	255	1.0	
494018	0	tcp	http	SF	203	1200	0	0	0	0	...	255	1.0	
494019	0	tcp	http	SF	291	1200	0	0	0	0	...	255	1.0	
494020	0	tcp	http	SF	219	1234	0	0	0	0	...	255	1.0	

"Fig 3 NSL KDD Dataset"

ii) Data processing:

Two important facts codecs are frequently used to procedure records to stumble on disturbance via deep studying strategies: Pandas Dataframe in Python and Keres Dataframe to enter the deep getting to know models. Initially, the statistics record is frequently imported into the Pandas data frame, the effective frame of data processing inside the Python. This enables exploration, manipulation and statistics guidance resultseasily. Data Fráme allows scientists to carry out diverse facts cleaning operations, consisting of missing values, removal of duplicates and transformation of variable categories into numerical codecs. After organizing records inside the Pandas records frame, it may be transformed into a format suitable for the input of the deep gaining knowledge of model. For this cause, a records body kerass can be designed, that's fundamentally such as a mill subject, inclusive of input traits and goal labels. This translation is necessary for getting into facts into neural community layout advanced the usage of the Keras Deep Learning Framework. When processing information, it is not unusual to do away with foreign columns that do not drastically assist the classification mission or can add noise to the model. This may be accomplished effortlessly the usage of the Pandas facts body the use of `drop ()` and the column designation for removal. Data processing consists of statistics record imports into Pandas facts body, sporting out the essential cleaning and initial processing processes, transformation of the statistics body right into a Keras well matched layout and casting off foreign columns to optimize enter information for deep learning.

iii) Visualization Using Seaborn & Matplotlib

SEABORN and MATPLOTLIB are two robust Python libraries used to visualise information, each imparting clean features for generating informative and aesthetically excellent graphs. Together they offer a large set of tools for a hit look at and presentation. Seaborn is advanced by means of Matplotlib by way of offering a excessive degree to create visually appealing statistical visuals. It affords a wide variety of predefined themes and color pallets, which makes it less difficult to adapt to the aesthetics of the story. SEABORN offers tools for generating complex visualizations, including distribution charts, paired charts and category graphs, with minimal coding efforts. In addition, SEABORN connects effortlessly with Pandas data frames, which facilitates direct visualization of the data contained in tabular forms. On the contrary, Matplotlib provides low levels for generating different graphs and impromates comprehensive control over all aspects of visualization. Although Matplotlib can be more degrees more than Seaborn, it offers unrivaled versatility and adaptation. Matplotlib allows users to generate a wide range of graphs, from the baseline and scattering charts to three -dimensional

visualizations and animations. The use of SEABORN in conjunction with Matplotlib allows users to merge the user -friendliness of the Seaborn and the visual attraction with detailed control and adaptability of the Matplotlib. This combination facilitates the development of complex visualizations that proficiently express the knowledge derived from data. Together, SEABORN and Matplotlib provide robust solutions to visualize data in Python, whether it examines correlations between variables, distribution visualization, or emphasize formulas in data.

iv) Label Encoding Using Labelencoder

Label coding is a technique used to convert the class data to numerical illustration, which is a prerequisite for several machine mastering strategies. The Labelencoder elegance in the Python's Scikit-Learn module offers an efficient approach for scanning labels on categorical variables. Labelencoder assigns awesome integer labels to every unique category interior express variables. For instance, if the variable includes categories which includes "purple", "inexperienced" and "blue", Labelencoder assigns those labels as zero, 1 and a couple of. This lets in machine gaining knowledge of models to understand categorical facts as numeric values, making it easier to procedure and examine records. Tag encoding is specifically fantastic for ordinal categorical facts, where classes have a natural order or hierarchy. It is vital to understand that the label coding may want to inadvertently create an unexpected serial connection among classes, which might not be greater handy, specifically for nominal categorical variables. In a few cases, one -way coding or other coding techniques can be most popular.

v) Feature Selection

Selectpercentile using the mutual information classifier is a method of selecting functions that prefer the function according to their mutual information with the target variable. It identifies the highest percentile characteristics showing the largest score of mutual information, indicating the most robust correlation with the aim. This approach evaluates the connection between each characteristic and the target class, which represents both linear and non -linear addictions. Selectpercentile increases the performance of the model by minimizing dimension and focusing on the most relevant variables for classification tasks of retention only the most informative attributes.

vi) Training And Testing

In deep learning fashions, the records file is divided into subgroups of schooling and trying out, often the usage of an 80% ratio for training and 20% for testing. The education set is used to teach deep studying models, even as the take a look at kit is used to evaluate their overall performance on new statistics. The education package consists of enter characteristic (X_train) and their related goal labels (y_train), even as the test package carries enter features (x_test) and their corresponding target labels (y_test). This department guarantees that fashions are skilled on a separate statistics file and then tested on unbiased facts to degree their performance.

vii) Algorithms:

"DNN (Deep Neural Network)": DNN is a neural network characterized by numerous layers located between input and output layers. "It contains an inlet layer, one or more hidden layers and an output layer". DNNs are recognized as their ability to obtain complex hierarchical representations from data. DNNs are often used in projects that require complicated patterns recognition and element extraction tasks. This

research is likely to use DNN because of its ability to recognize complex connections in the data file, which is suitable for tasks such as detection of disruption, where it is necessary to recognize fine formulas in network traffic.

"Autoencoder DNN (Deep Neural Network with Autoencoder)": AUTOENCODER is an architecture of a neural network used for DL of unattended. The device consists of an encoder that compresses enter statistics to the representation of the latent area and the decoder that reconstructs the input statistics from this illustration. The integration of the DNN vehicle - gauge means using compressed features acquired by the auto -coder in the later DNN framework. Autoencoder DNNs are proficient in learning and extraction of elements. This research suggests the integration of DNN with an autoencoder and emphasizes the preliminary capture of relevant information. This is particularly advantageous in the detection of disruption, where the inherent network data structure is essential.

"LSTM Autoencoder (Long Short-Term Memory Autoencoder): LSTM is a architecture of the recurrent neural network (RNN) created to capture long -term relations in sequence data. The Autoencoder LSTM integrates the concepts of auto -coder with memory functions of the LSTM network to capture time relations in the sequence input. The LSTM Auto -LSTM is suitable for tasks that include sequential data, including time series and network traffic formulas. This research uses LSTM, emphasizes the capture and reconstruction of sequence patterns in network data necessary for detection of abnormalities or intrusion over time.

"CNN (Convolutional Neural Network): A CNN is a deep learning particularly designed for reading facts just like grids, which include pictures or sequences. It makes use of convolutional layers to self reliant and adaptively collect hierarchical representations of enter facts. CNN might be used inside the mission due to the fact, in step with its robust skills of extraction of functions from established data. In the area of disturbance detection, wherein network site visitors records can display geographical formulation, CNN can simply identify and assimilate these aspects, growing the general accuracy of the machine.

"CNN with LSTM (Convolutional Neural Network with Long Short-Term Memory): This model is a hybrid structure that integrates the abilities of CNN extraction with sequential learning knowledge of information of LSTMS. This is particularly effective for spatial information which include image sequences or time series facts. CNN incorporated with LSTM is used to use the advantages of each frames. This hybrid approach is advantageous in intrusion detection, as network events occur gradually and can show geographical and time formulas. It can collect spatial data via CNN layers and simulate time correlations via LSTM layers, thereby increasing the ability of the system to identify a complex network ingress.

4. EXPERIMENTAL RESULTS

Accuracy: A test capacity towards create a proper difference between healthy & sick cases is a measure of accuracy. We can determine accuracy of a test through calculating proportion of cases undergoing proper positivity & genuine negative. It is possible towards express this mathematically:

$$\text{"Accuracy"} = \frac{\text{"TP + TN"}}{\text{"TP + FP + TN + FN"}} (1)$$

Precision: Precision quantifies the percentage of efficiently identified positive cases or samples. Precision is decided by using the components:

$$"Precision" = \frac{"True\ Positive"}{"True\ Positive\ + False\ Positive"} (2)$$

Recall: ML recall assesses a model's potential to choose out all relevant times of a class. It demonstrates a version's efficacy in encapsulating times of a class by using comparing nicely anticipated high satisfactory observations to the general variety of positives.

$$"Recall" = \frac{"TP"}{"TP\ +\ FN"} (3)$$

F1-Score: The accuracy of a system ML of model is classed the usage of the F1 score. Integrating the precision and do not forget metrics of the model. The accuracy metric quantifies the frequency of proper predictions made through a model at some level inside the dataset.

$$"F1\ Score" = "2" * \frac{"Recall\ X\ Precision"}{"Recall + Precision"} * "100" (4)$$

Tables 1 and 2 assess the "performance metrics—accuracy, precision, recall, and F1 score"—for each method. The CNN routinely surpasses all other algorithms across all measures. The tables provide a comparative examination of the metrics for the alternative methods.

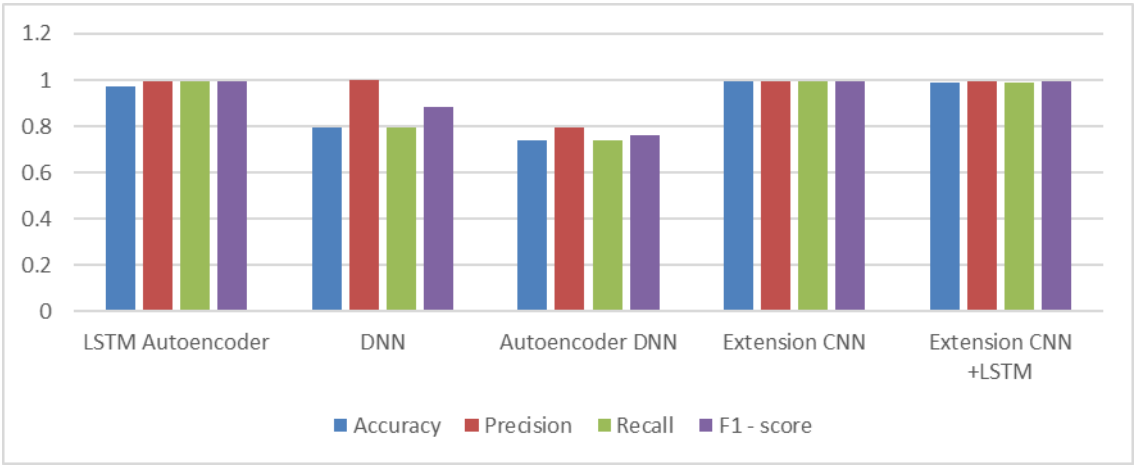
"Table.1 Performance Evaluation Table - KDDCUP99"

ML Model	Accuracy	Precision	Recall	F1 - score
LSTM Autoencoder	0.971	0.996	0.995	0.996
DNN	0.793	1.000	0.793	0.885
Autoencoder DNN	0.737	0.793	0.737	0.760
Extension CNN	**0.995**	**0.996**	**0.995**	**0.996**
Extension CNN +LSTM	0.991	0.993	0.991	0.992

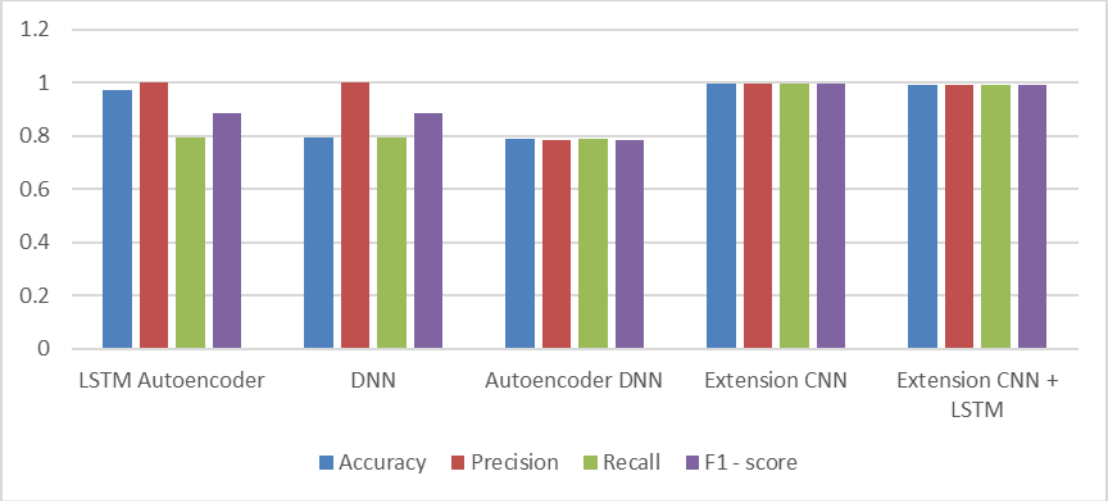
"Table.2 Performance Evaluation Table – NSLKDD"

ML Model	Accuracy	Precision	Recall	F1 - score
LSTM Autoencoder	0.974	1.000	0.793	0.885
DNN	0.793	1.000	0.793	0.885
Autoencoder DNN	0.791	0.783	0.791	0.784
Extension CNN	**0.995**	**0.997**	**0.995**	**0.996**
Extension CNN + LSTM	0.990	0.991	0.990	0.991

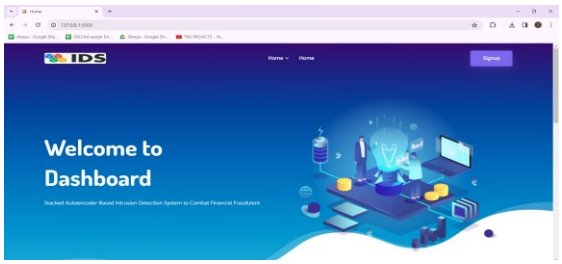
"Graph.1 Comparison Graphs - KDDCUP99"



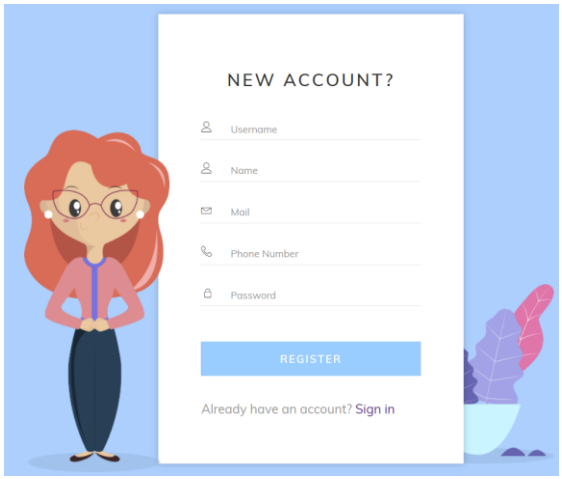
"Graph.2 Comparison Graph – NSLKDD"



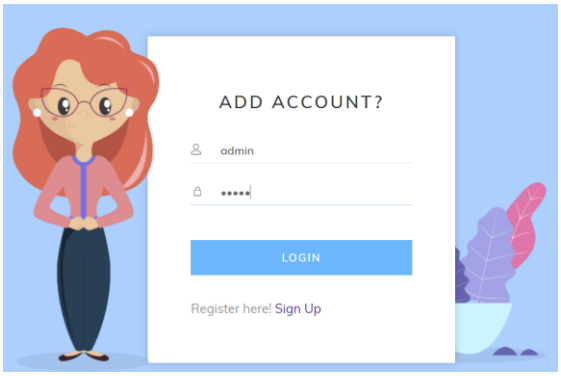
"Accuracy is shown in blue, precision in red, recall in green, and F1-Score in purple in Graphs 1 and 2". Relative to the other models, the Extension CNN demonstrates enhanced performance across all measures, attaining the highest values. The graphs above graphically represent these results.



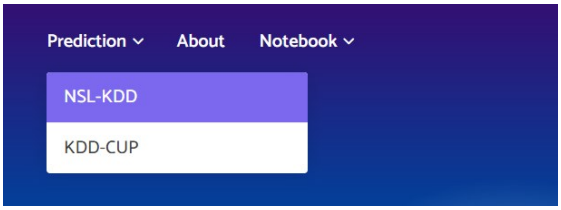
"Fig 4 Web page"



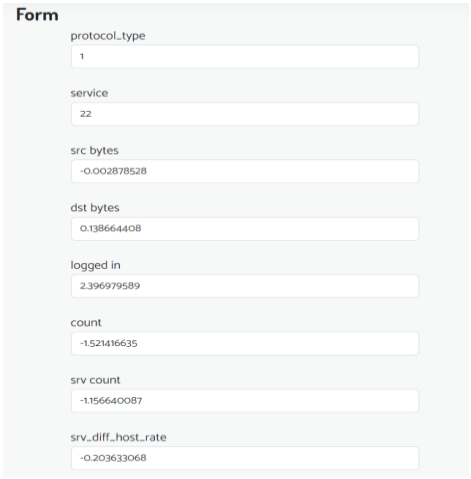
"Fig 5 sign in page"



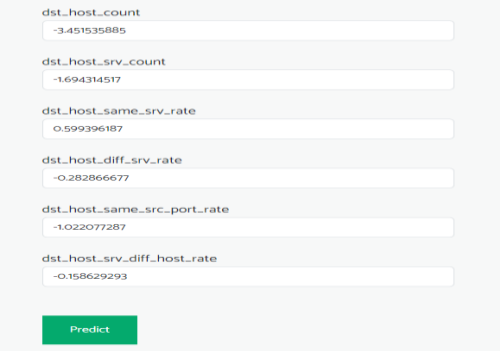
"Fig 6 sign up page"



"Fig 7 NSL-KDD dataset"

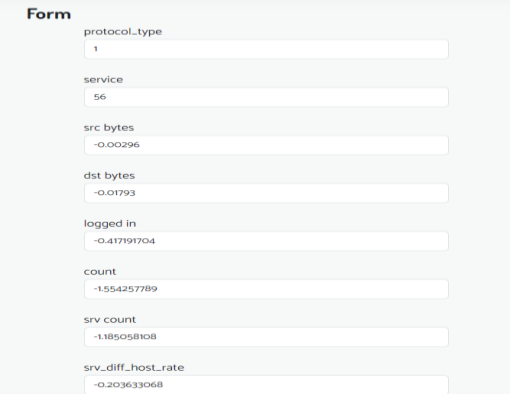


"Fig 8 upload input data"

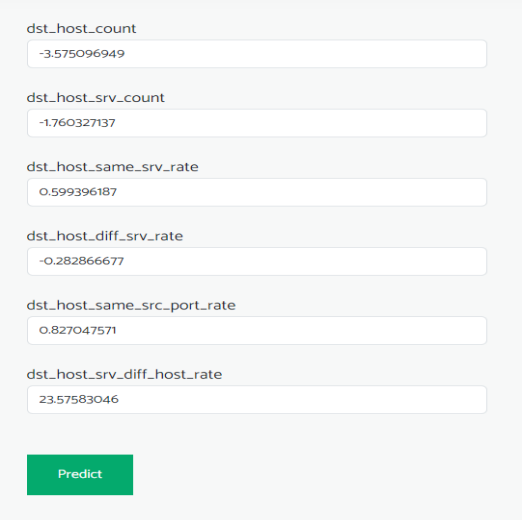


"Fig 9 upload input data"

"Fig 10 Predict result"



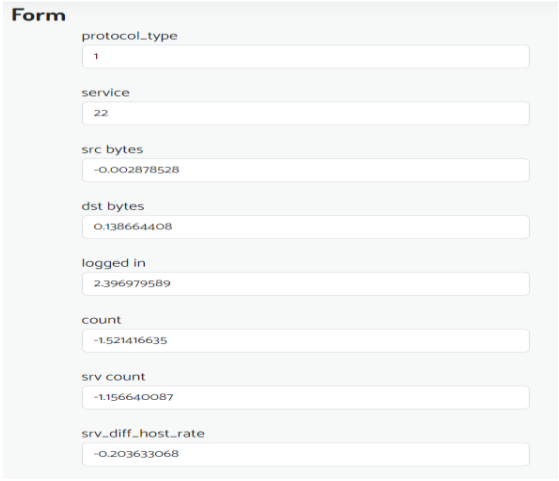
"Fig 11 upload input data"



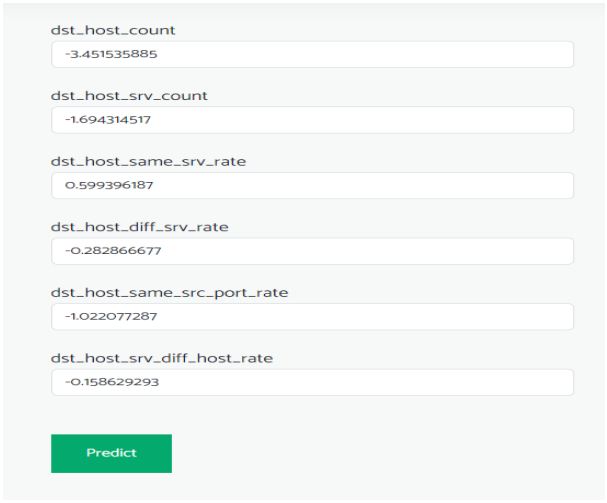
"Fig 12 upload input data"

"Fig 13 Final outcome"

"Fig 14 KDD CUP dataset"

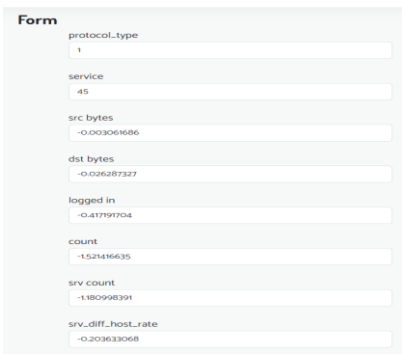


"Fig 15 upload input data"

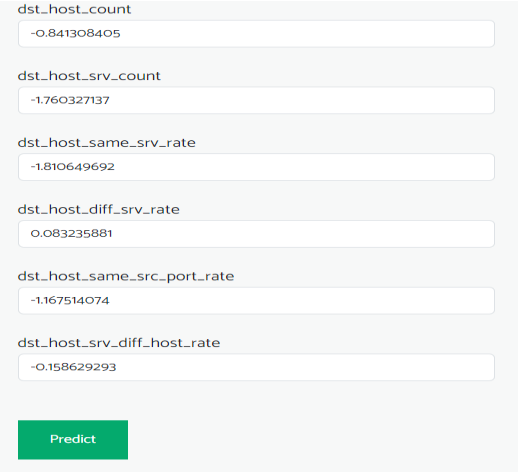


"Fig 16 upload input data"

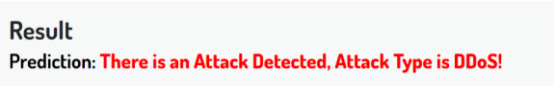
"Fig 17 Final outcome"



"Fig 18 upload input data"



"Fig 19 upload input data"



"Fig 20 Predict result"

5. CONCLUSION

Research shows exceptional expertise in robust detection of disruption by modern technologies, such as DNNs and autoencoders, and therefore guarantee proactive defense against potential network attacks. A variety of characteristics, such as the types of protocol, information about services and the numbers of bytes, are adept combined to recognize complex patterns in network traffic. This extensive set of functions improves the model's ability to accurately identify abnormalities. Improved algorithm, file integration and intuitive interface, showed exceptional effectiveness in fraud detection. The flask -based interface has been tested with different element values, which demonstrates its durability and flexibility, which underlines its efficiency for reliable detection of disturbance in practical financial contexts. This initiative significantly helps the fight against financial crime protection of digital financial transactions in intelligent environments. The capability of the version to pick out abnormalities and capacity threats in actual time is vital to preserve the integrity and protection of monetary transactions that defend people and groups from feasible economic losses. Effectively integration of SQLITE for consumer control, in conjunction with the intuitive interface, shows the usefulness of the undertaking. This person -targeted layout prepares a version for implementation in lots of real contexts and ensures availability and value for users.

6. FUTURE SCOPE

The future task trajectory includes the extension of the proposed system to healthy a much wider range of threats, specifically the ones focused on cell and IOT structures. This extension seeks to reinforce guarantees before fraudulent sports in clever digital environments and consequently supports sustainable urbanization. Other deep learning algorithms and hierarchical processes can be protected to improve the overall performance of the gadget. This method seeks to decide the handiest answer for positive statistics units and therefore increases the overall performance of the disruption detection system. Exploring enhancements in BIG Data generation provides a possible possibility to derive one of a kind styles from network statistics and device events. This exam can also significantly improve the efficiency of the detection machine through distinguishing between benign and harmful activities in extensive data sets. The use of state-of-the-art fashions of DL, mainly fashions based totally on car -gauge, suggests the ability for spotting offensive organizations and spotting assaults on compulsion. This improvement can toughen the gadget's capability to pick out complex formulation indicating protection worries. Future research efforts can awareness on mitigating limits in the proposed device, inclusive of concerns about floods and injection. In addition, the exploration of alternative DL of

fashions has the opportunity to growth the performance of the gadget and the adaptability of diverse cyber threats.

REFERENCES

[1] C. Badii, P. Bellini, A. Difino, and P. Nesi, "Smart city IoT platform respecting GDPR privacy and security aspects," IEEE Access, vol. 8, pp. 23601–23623, 2020.

[2] D. Larson, "Distributed denial of service attacks—Holding back the flood," Netw. Security, vol. 2016, no. 3, pp. 5–7, 2016.

[3] Cheng, D., Zou, Y., Xiang, S., & Jiang, C. (2025). Graph neural networks for financial fraud detection: a review. *Frontiers of Computer Science*, *19*(9), 199609.

[4] Y. Xin et al., "Machine learning and deep learning methods for cybersecurity," IEEE Access, vol. 6, pp. 35365–35381, 2018.

[5] Sudharson, K., Varsha, S., Rajalakshmi, S., Rajalakshmi, D., & Santhiya, R. (2025). Financial Transactional Fraud Detection using a Hybrid BiLSTM with Attention-Based Autoencoder. *International Research Journal of Multidisciplinary Technovation*, *7*(2), 135-147.

[6] A. Azab, M. Alazab, and M. Aiash, "Machine learning based bot net identification traffic," in Proc. 15th IEEE Int. Conf. Trust Security Privacy Comput. Commun., Tianjin, China, Aug. 2016, pp. 1788–1794.

[7] G. Muhammad, M. S. Hossain, and A. Yassine, "Tree-based deep networks for edge devices," IEEE Trans. Ind. Informat., vol. 16, no. 3, pp. 2022–2028, Mar. 2020.

[8] X. Yang, T. Zhang, C. Xu, S. Yan, M. S. Hossain, and A. Ghoneim, "Deep relative attributes," IEEE Trans. Multimedia, vol. 18, no. 9, pp. 1832–1842, Sep. 2016.

[9] G. Muhammad, M. F. Alhamid, and X. Long, "Computing and process ing on the edge: Smart pathology detection for connected healthcare," IEEE Netw., vol. 33, no. 6, pp. 44–49, Nov./Dec. 2019.

[10] S. Qian, T. Zhang, C. Xu, and M. S. Hossain, "Social event classifica tion via boosted multimodal supervised latent dirichlet allocation," ACM Trans. Multimedia Comput. Commun. Appl., vol. 11, no. 2, pp. 1–22, Jan. 2015.

[11] Adejumo, A., & Ogburie, C. (2025). Forensic accounting in financial fraud detection: Trends and challenges. *International Journal of Science and Research Archive*, *14*, 1219-1232.

[12] A. Ozgur and H. Erdem, "A review of KDD99 dataset usage in intru sion detection and machine learning between 2010 and 2015," PeerJ PrePrints, vol. 4, Apr. 2016, Art. no. e1954.

[13] Chen, Y., Zhao, C., Xu, Y., & Nie, C. (2025). Year-over-year developments in financial fraud detection via deep learning: A systematic literature review. *arXiv preprint arXiv:2502.00201*.

[14] Lee, C. W., Fu, M. W., Wang, C. C., & Azis, M. I. (2025). Evaluating machine learning algorithms for financial fraud detection: insights from Indonesia. *Mathematics*, *13*(4), 600.

[15] Aljunaid, S. K., Almheiri, S. J., Dawood, H., & Khan, M. A. (2025). Secure and transparent banking: explainable AI-driven federated learning model for financial fraud detection. *Journal of Risk and Financial Management*, *18*(4), 179.

[16] L. Ertöz, M. Steinbach, and V. Kumar, "Finding clusters of different sizes, shapes, and densities in noisy, high dimensional data," in Proc. SIAM Int. Conf. Data Min., 2013, pp. 47–58.

[17] Liu, W., Wang, Z., & Zhang, X. (2025). Research on financial fraud detection by integrating latent semantic features of annual report text with accounting indicators. *Journal of Accounting & Organizational Change*.

[18] D.-Y. Yeung and C. Chow, "Parzen-window network intrusion detectors," in Proc. 16th Int. Conf. Pattern Recognit., vol. 4. Quebec City, QC, Canada, Aug. 2002, pp. 385–388.

[19] Al-dahasi, E. M., Alsheikh, R. K., Khan, F. A., & Jeon, G. (2025). Optimizing fraud detection in financial transactions with machine learning and imbalance mitigation. *Expert Systems*, *42*(2), e13682.

[20] K. Lin, J. Song, J. Luo, W. Ji, M. S. Hossain, and A. Ghoneim, "Green video transmission in the mobile cloud networks," IEEE Trans. Circuits Syst. Video Technol., vol. 27, no. 1, pp. 159–169, Jan. 2017.

[21] A. J. Deepa and V. Kavitha, "A comprehensive survey on approaches to intrusion detection system," Procedia Eng., vol. 38, pp. 2063–2069, Jan. 2012.

[22] M. A. Salama, H. F. Eid, R. A. Ramadan, A. Darwish, and A. Hassanien, "Hybrid intelligent intrusion detection scheme," in Soft Computing in Industrial Applications, A. Gaspar-Cunha, R. Takahashi, G. Schaefer, and L. Costa, Eds. Heidelberg, Germany: Springer, 2011, pp. 293–303.

[23] H. Liu, B. Lang, M. Liu, and H. Yan, "CNN and RNN based payload classification methods for attack detection," Knowl. Based Syst., vol. 163, pp. 332–341, Jan. 2019.

[24] N. Gao, L. Gao, Q. Gao, and H. Wang, "An intrusion detection model based on deep belief networks," in Proc. 2nd Int. Conf. Adv. Cloud Big Data, Huangshan, China, Nov. 2014, pp. 247–252.

[25] C. Kolias, G. Kambourakis, A. Stavrou, and S. Gritzalis, "Intrusion detection in 802.11 networks: Empirical evaluation of threats and a pub lic dataset," IEEE Commun. Surveys Tuts., vol. 18, no. 1, pp. 184–208, 1st Quart., 2016.

[26] M. E. Aminanto, R. Choi, H. C. Tanuwidjaja, P. D. Yoo, and K. Kim, "Deep abstraction and weighted feature selection for Wi-Fi imper sonation detection," IEEE Trans. Inf. Forensics Security, vol. 13, pp. 621–636, 2018.

[27] M. Tang, M. Alazab, and Y. Luo, "Big data for cybersecurity: Vulnerability disclosure trends and dependencies," IEEE Trans. Big Data, vol. 5, no. 3, pp. 317–329, Sep. 2019.

[28] M. Alhussein and G. Muhammad, "Voice pathology detection using deep learning on mobile healthcare framework," IEEE Access, vol. 6, pp. 41034–41041, 2018.

[29] M. S. Hossain, S. U. Amin, G. Muhammad, and M. Al Sulaiman, "Applying deep learning for epilepsy seizure detection and brain map ping visualization," ACM Trans. Multimedia Comput. Commun. Appl., vol. 15, no. 1s, p. 17, Feb. 2019.

[30] P. Wu and H. Guo, "LuNet: A deep neural network for network intrusion detection," Sep. 2019. [Online]. Available: arXiv:1909.10031.

DATASET LINKS:

NSL-KDD:

https://www.kaggle.com/datasets/kaggleprollc/nsl-kdd99-dataset

KDD-CUP99:

https://www.kaggle.com/datasets/galaxyh/kdd-cup-1999-data