Contents lists available at ScienceDirect

Measurement: Sensors

journal homepage: www.sciencedirect.com/journal/measurement-sensors

Accuracy determination using deep learning technique in cloud-based IoT sensor environment

B. Raviprasad [a,*], Chinnem Rama Mohan [b], G. Naga Rama Devi [c], R. Pugalenthi [d], L.C. Manikandan [e], Sivakumar Ponnusamy [f]

[a] *Marri Laxman Reddy Institute of Technology and Management, Hyderabad, 500043, India*
[b] *Department of Computer Science and Engineering, Visvesvaraya Technological University, Belgaum 590018, India*
[c] *Department of Computer Science and Engineering, CMR College of Engineering and Technology, Kandlakoya, Medchal, Hyderabad, 501401, India*
[d] *Department of Computer Science and Engineering, St.Joseph's College of Engineering, OMR, Chennai, 600119, India*
[e] *Department of Computer Science and Engineering, Valia Koonambaikulathamma College of Engineering and Technology, Thiruvananthapuram, Kerala, India*
[f] *Department of Computer Science and Engineering, SRM Institute of Science &Technology, Delhi NCR Campus, Modinagar Ghaziabad, Uttar Pradesh, 201204, India*

ARTICLE INFO

Keywords:
Network complexity
Intrusion detection systems
Image and signal processing
IoT environment
Deep learning

ABSTRACT

The Internet of Things (IoT) offers users a wide variety of facilities because it interconnects billions of smart devices. However, when connected to wireless connections, unlimited access to IoT gadgets poses potential risks. As it eases cost constraints on sensor nodes, the cloud service with IoT networks has received greater attention. In addition, the high complexity of the distribution and networking of IoT makes them vulnerable to attacks. Intrusion detection systems (IDSs) are selected to ensure the security of reliable information and operations. IDS successfully detects anomalies in complex network situations and guarantees network security. Deep Convolution Network (DCN) IDS have a slow learning curve and poor categorization precision. Deep Learning (DL) methods are often used in a wide range of safety data processing, imaging, and signal processing like Poor transfer learning ability, reusability of modules, and integration. To overcome the constraints of Machine Learning (ML) IDS is intended to provide a comprehensive mechanism to learn the detection mechanism for multicloud IoT environments. The proposed IDS approach increases training efficiencies while increasing detection accuracy. Experimental investigations of the proposed system using the considered database confirms that the performance of the proposed system is capable and in the range of acceptance with relative to existing methods. Further, achieving detection capability, reliability, and accuracy of 97.51, 96.28, and 94.41% respectively are achieved.

1. Introduction

The pace of innovation enables the creation of a variety of applications that use a network of connected telephones [1,2].According to recent research, the amount of data produced by IoT systems, each day was estimated to be 2.5 quintillion bytes, and it grows annually [3].The modern network will incorporate IoT, allowing anyone to connect it from anywhere and use smart objects to monitor, calculate, connect, and react to numerous physical and digital properties.The main benefits of the IoT seem to be self-configured paths, connections, and applications [4]. The IoT network and smart devices face limited availability. The customized storage could be used to activate and process the information to match the reduced capacity.Like public broadcasting, IoT mobile systems were sensitive to networking; security, and confidentiality of personal information [5].The onboard systems and network access architectures were faulty and open to intrusion.IoT connections have been integrated with a cloud environment to solve this problem.IoT customers were attracted to the Internet because of its affordable operating costs, and cloud technology could meet all the requirements of IoT networks [6].Through its geographically diverse sources of data, cloud technology can facilitate networks and also provide data processing, broadcasting, and management [7].

Cloud technology can efficiently address all of the needs of IoT systems. Fundamentally, the cloud serves as a transit barrier between IoT and programs, improving flexibility and agility while reducing complexity [8]. Although combining the cloud with IoT has many advantages, it also has several disadvantages, including concerns about service contracts, quality of service, portability, and security [9].

[*] Corresponding author.
E-mail address: rprasad.boddu@gmail.com (B. Raviprasad).

https://doi.org/10.1016/j.measen.2022.100459
Received 2 August 2022; Received in revised form 7 September 2022; Accepted 12 September 2022
Available online 28 September 2022

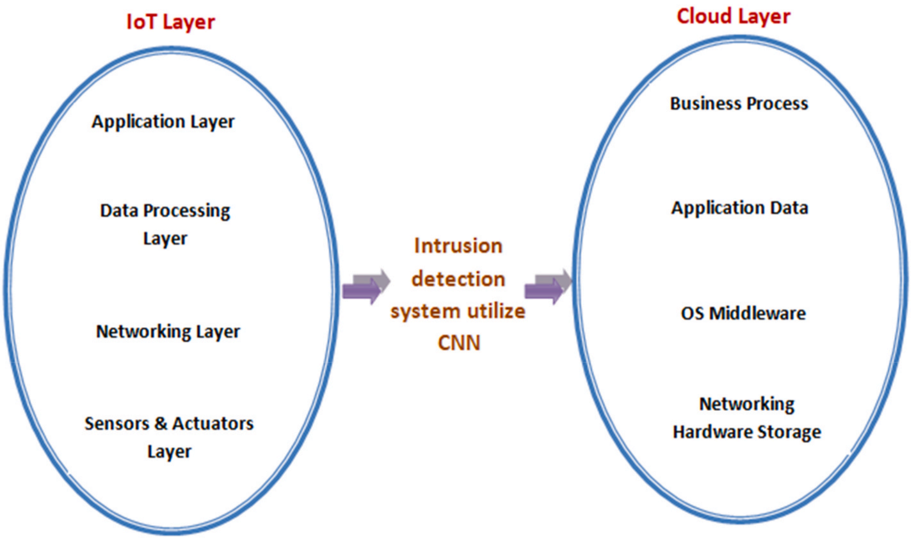


Fig. 1. Transformation of IoT layers to Cloud layers.

Depending on customer requirements, connecting an IoT module to cloud computing can involve a single cloud or multiple databases. The design of a cloud environment and perhaps a cross-system is different [10]. Clouds can be either public or private clouds that can connect. As opposed to a multi-cloud, that might include hybrid computing designs that combine cloud resources and several cloud environments. Various individual operators should offer a variety of services throughout cloud levels whenever it is a platform and must be linked depending on the IoT as a multi-cloud ecosystem [11].The detection method performs identification before the actual transmission in the multi-cloud context and has also been used for different network vulnerability analyses. Multiple different centers spread out over the Internet make up a multi-cloud system [12].

2. Related works

IoT systems that use different service providers can have a variety of problems if storage facilities were physically or topologically dispersed [13]. The communication cost of the networks would rise if all of them move to a single, centralized information center, and also the cloud infrastructure won't be able to accommodate the computational and storage needs of IoT systems. The likelihood of attacks that could degrade the QoS provided by multi-cloud IoT systems was dramatically increased when third parties were allowed to access the information. To detect potential attacks, intrusion detection and prevention for IoT modules that support multi-cloud environments seem to be a must [14]. Typically, intrusion prevention methods are divided into two types: anomaly-based intrusion detection techniques and signature-based detection techniques. In addition to these two varieties, hybrid cryptographic systems that function specifically have also been proposed.

Model matching approaches have used signature intrusion detection systems to characterize aggressions [15–17]. The current intrusion has been confirmed and the system has also learned of any fraudulent attack by comparing the characteristics of the previous intrusion. The introduction of an unusual occurrence, detection techniques, which use analytical or knowledge-based methods to identify hostile activity in the networks, contrasts with the former [18].

Unsupervised ML, Recurrent Neural Networks (RNN), and DL were the many types of unique intrusion prevention algorithms. Using a classification model, incursions were found in this controlled training process [19]. The learning stage identifies relevant characteristics and their categories, and through the learning experience, the foray or typical behavior has been categorized. Controlled adaptive learning, referred Decision Tree (DT) intrusion prevention system, first determines the test characteristics from the given criterion [20]. The examples consisted of branches and also the possible choices were recovered as branches from the test attributes. Normal and aberrant network connections have been divided into categories by a tree-shaped structure.

The intrusion prevention system of the Naïve Bayes methodology offers superior calculation performance since it takes into account the probability of attack and the typical behavior [21]. In addition, the designer's recognition performance may be affected if the autonomous assumption used was incorrect. Moreover, the total speed of the reconnaissance module is hampered by complex characteristic relationships. The reliability of responses in scalable automated process detection methods has been enhanced by the choice & replication operations. The progressive individual's chromosome coding classifications were based on clustering and clustering [22]. Moreover, a major disadvantage of genetically determined detection techniques seems to be the high cost of processing.

Convolutional Neural Networks (CNN) were commonly used in regression security mechanisms for detecting multiple ransomware [23]. Guided adaptive learning called the backpropagation neural method assesses connection error based on parameters for finding malware. In addition, ANN-based intrusion prevention systems have lower detection performance and need to be improved. Less common attacks have a smaller classification pattern than more attacks, which helps networks better understand attacks [24].The long learning process, local characteristics, and poor high detection seem to be the main disadvantages of controller detection techniques. In safeguards, unsupervised classification would be used to extract critical data from input data that lacks classifiers. The information was organized into different categories using the learning experience, & incursions were found by training a model. In the unsupervised technique, teams are established and grouped into clusters, and exceptions are treated as anomalies. K-means has the advantage of looking at different behaviors in several well-known intrusion detection methods, including PCA and clustering algorithms [25]. While PCA decreases the computational complexity of malware detection by extracting smaller space features from a huge dataset. Described blockchain-based trust paradigm reduces communication protocol and computational cost and prevents single data point failures.

The flaw of the model provided, moreover, would be that the algorithm can only detect certain attacks of black and grey holes [26].From the foregoing, it has been shown that the reliability and computational

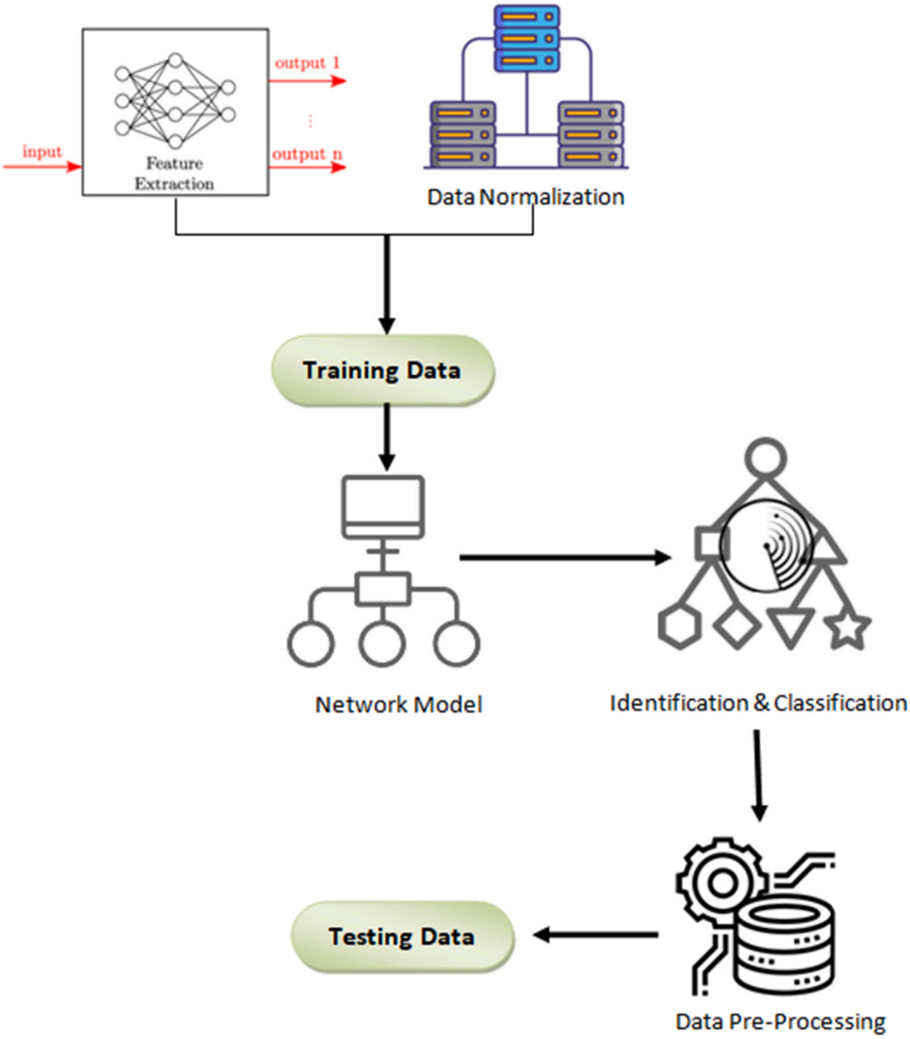


Fig. 2. Proposed IDS model.

efficiency of Conventional DL intrusion prevention systems could be increased [27].Compared to a CNN, an intrusion prevention model based on DL provides opportunities to prevent class intrusions. This study fills a gap in research by developing a detection mechanism based on DL for a multi-cloud IoT environment that enhances detection performance while consuming less processing power.

3. Proposed work

The proposed remote monitoring methodology employs a DNN. To identify attacks on the IoT network and safeguard the cloud infrastructure, the detection method was established between the Internet and the IoT gateway. The integrated process proposed by the researcher is depicted in Fig. 1. The IoT level consists of the many IoT systems which have been linked to the proposed approach and perhaps even a variety of cloud environments. The routing method is not exactly discussed in the research, so Fig. 1 provides a short description. Fig. 2 shows the procedure for malware detection. Data pretreatment, trait extraction, learning, validation, and classification are all included.The characteristics were first collected during the pre-treatment phases and then standardized to equalize the characteristic dimensions. It must be crucial to assess both low-level and high-level aspects; hence, the

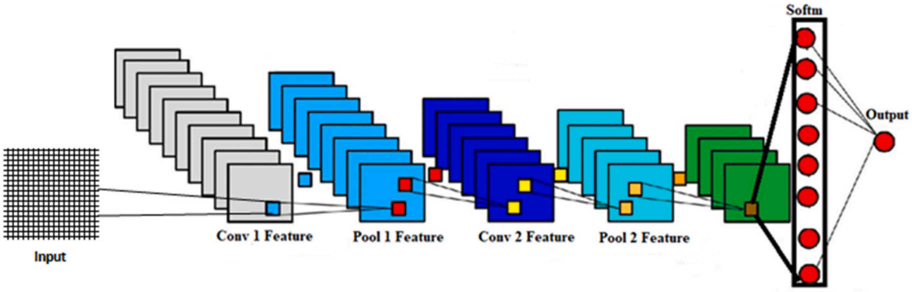


Fig. 3. Proposed model.

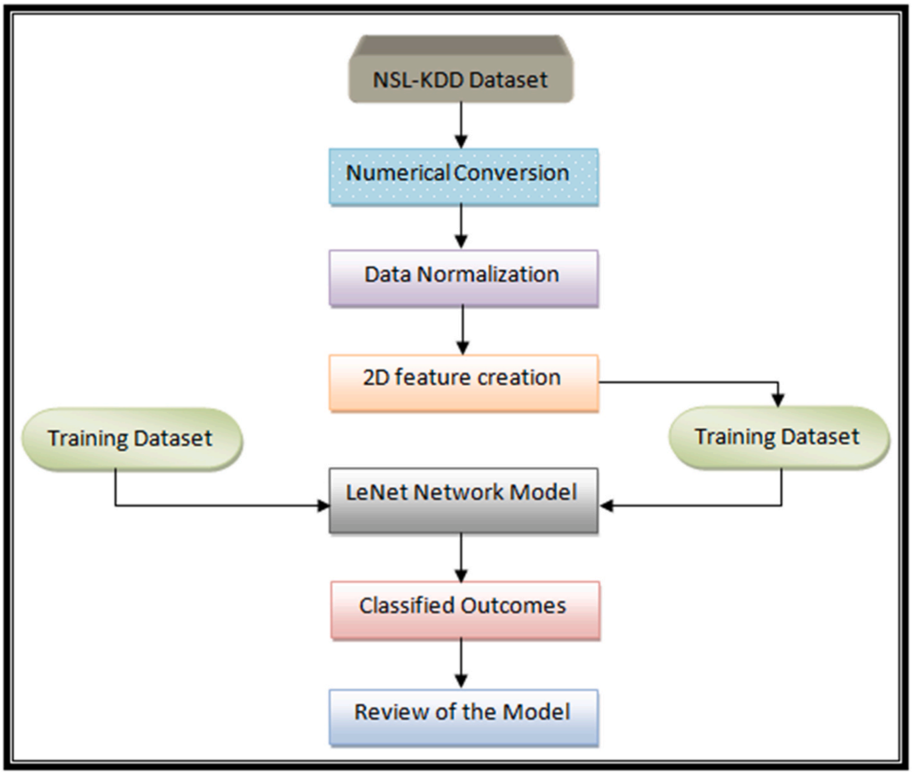


Fig. 4. LeNet model for proposed IDS.

proposedtechnique needs to be standardized.

The characteristics were first collected during the preprocessing phases and then standardized to equalize the characteristic dimensions. However, multiplies the number of characteristics for each conversion, potentially extending development/certification periods. Accordingly, the nominal numbers in this future framework have been translated by assigning specific parameters alphabetically. For instance, ICMP received a rating of 1, TCP received a value of 2, and UDP received a value of 3.The time to develop/certify the classification algorithm is shortened thanks to this technique, which does not increase the number of variables. The network structure used by the intrusion prevention system is depicted in detail in Fig. 3. Many CNN has been developed for IDS.The main factors in choosing the CNN model for this proposed strategy are competence in feature extraction and analysis, good precision, and computer efficiency. ALeNet-based monitoring system for the multicloud IoT architecture has been proposed in this discussion paper. The proposed LeNet-based model provides superior efficiency and is therefore computationally more effective with inputs than previous approaches such as Google Net and Alex Net. Especially in comparison to other Convolutional networks, the learning time & number of iterations were excellent.

The proposed LeNet model provides superior efficiencies with inputs than existing approaches such as Google Net and Alex Net.The proposedmethod reduces functionality by using two layers of convoluted and pooling and then classifies the provided features using a fully connected layer. The detailed formulations of SoftMax classification for n number of neurons in several categories is showsn as Equation (1):

$$f_k(l) = \frac{e^{l_k}}{\sum_k e^{l_k}} \tag{1}$$

Fig. 4 presents the flowchart indicating the operation of the proposed IDS. The procedure begins with the conversion of digital data and then proceeds to normalization. The system is then formed using the data provided after the characteristic vectors are translated into bidimensional characteristics. Most DL-IDS use the conventional CNN model, which requires an extra amount of training. But the study's uniqueness has been said to lie in its choice of the minimum features and use of the LeNet model to determine various attacks.

Table 1
Training and testing records.

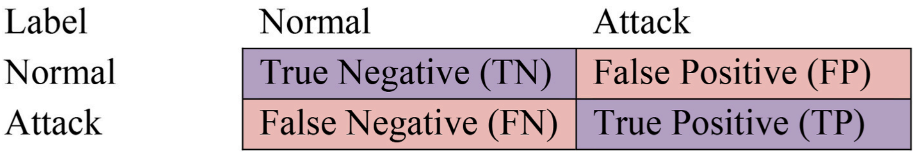
Attack	Training	Testing
Normal	14,657	9791
Dos	9354	7536
Probe	2368	2522
R2L	211	2768
U2R	12	200
Total	26,101	22,600

Table 2
Comparison of data over performance.

S.no	Performance (%)	SVM	RNN	Proposed
1	Accuracy	89.80	92.32	97.29
2	Precision	77.6	89.6	94.65
3	Detection rate	90.2	94.2	98.55
4	False Positive rate	10.5	9.6	6.5

4. Result and discussion

The results of the simulations used to test the hypothetical intrusion detection system were described in detail in this section. The experience uses the NSL-KDD dataset. The dataset consists of 41 characteristics representing various qualities and has been assigned one of two tags—attack or normal. Depending on the type of attack, it must be broken down into DoS, Probe, R2L, & U2R.The following table provides a list of training and validation information from the NSL-KDD databases.



Label	Normal	Attack
Normal	True Negative (TN)	False Positive (FP)
Attack	False Negative (FN)	True Positive (TP)

Fig. 5. Detection rate comparison.

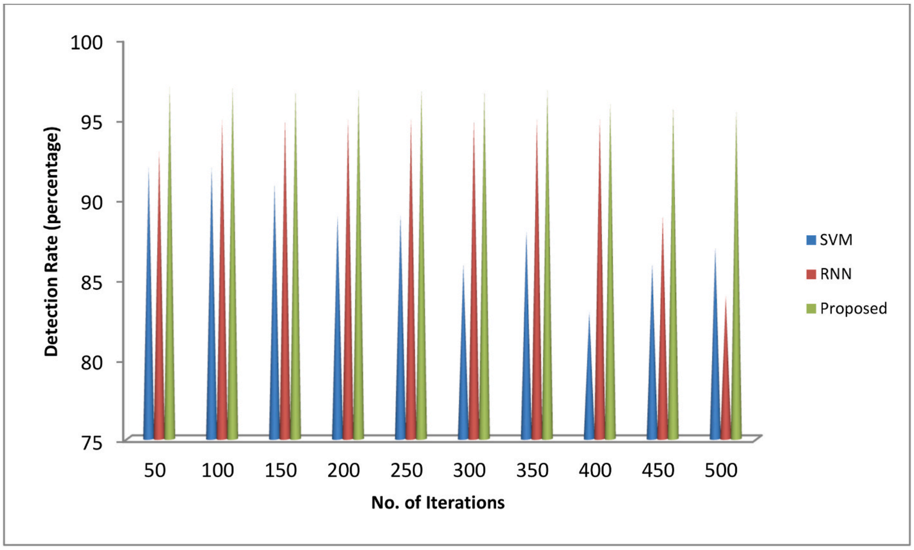


Fig. 6. Quantification of sensing performance.

The following table presents information on training and validation from the NSL-KDD databases. Table 1 provides the hyperparameters for the LeNet network. The proposed approach achieves reliable results 60 times when the experiment was carried out with various historical parameters. The accuracy rises and also the logistic regression falls as time grows. The learning and skills of the proposed model participants were 99% for both with a low false alarm. The confusion matrix indicates the link between the measurements (see Table 2).

For the proposed network model, see Fig. 3. Values are classified as True Positive (TP), True Negative (TN), False Positive (FP), and False Negative (FN) by label (FN). The grouping algorithm was produced using the expected and observed numbers. Reliability, detection accuracy, poor detection rates, precision, & learning duration seem to be the methods used to measure the effectiveness of the proposed system.

The clustering algorithm was produced using the expected and observed counts. Fig. 5 compares and illustrates proposed malware detection rates with existing Support Vector Machine (SVM), RNN-IDS. It was proposed that the existing approach has great detection accuracy compared to other approaches. The RNN performance of the model was 4% lower than the proposed model, while the SVM performance of the model was 8% lower than the proposed strategy. The proposed model's performance maintains an average of 97.5% throughout the iteration,

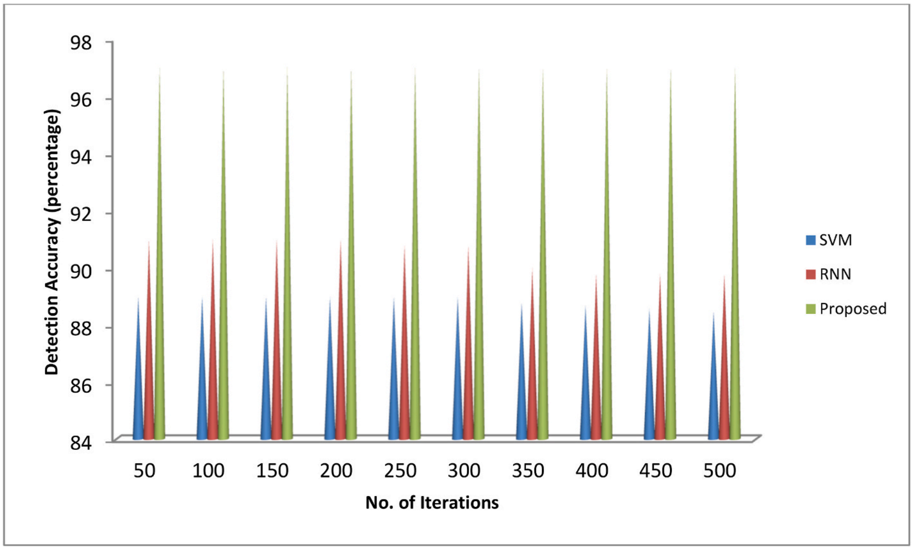


Fig. 7. Precision comparison.

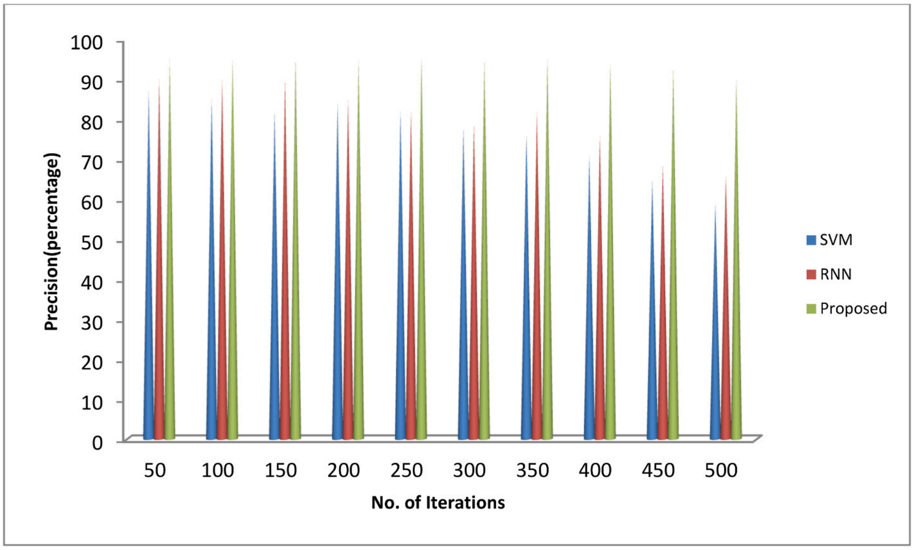


Fig. 8. Detection rate comparison vs number of requests.

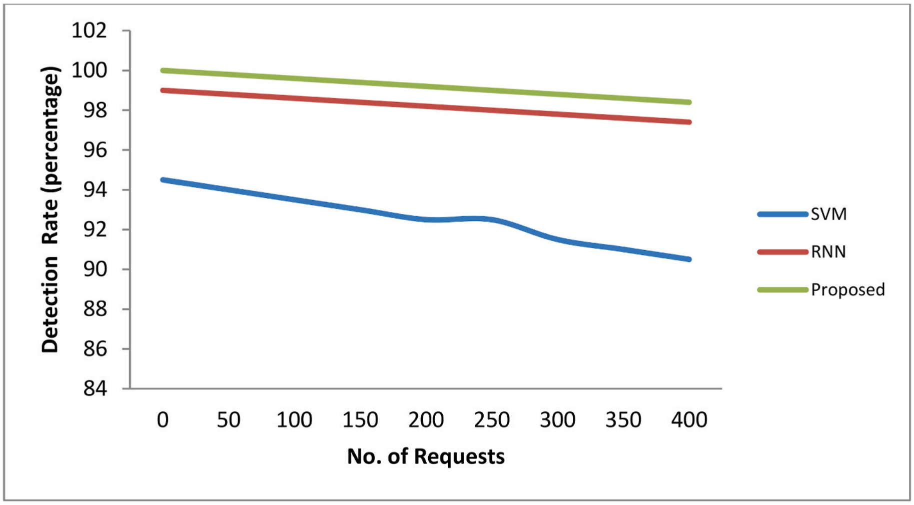


Fig. 9. Training time comparison.

with a slight change in the detection accuracy when it reaches 1000. While SVM's feature processing features in the intrusion prevention environment result in significant changes in SVM's detection accuracy.

The algorithm to classify the assessment for each of the three models can be found in Fig. 6. The proposed approach provides an average accurate result of 96.28%, compared to SVM and RNN 88.84 and 91.17%, accordingly. The detection performance presented in the figure indicates the extent to which the proposed approach efficiently identifies attacks. As opposed to classification results, which use the consistency score to identify the type of assault. The proposed model's detection accuracy is increased by the feature conversion and training phase. While identification and risk increase, the performance of the classifier's proposed intrusion prevention model can be seen in a slightly reduced detection accuracy. It classifies assaults better than other systems.

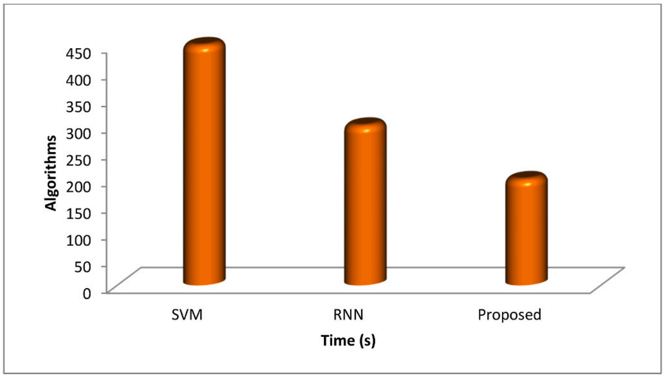


Fig. 10. Compares detection rates for various attacks.

In Fig. 7, the proposed model's classification performance has been compared with other algorithms. According to the study, the proposed framework has the highest level of certainty, but they operate as efficiently for the classification algorithm & Revenue model was only ever half as high after 1000 iterations. The proposed model achieves maximum precision through the immense contribution of extraction and production via deep neural network functionalities. The SVM works badly and achieves only the minimum precision needed in comparison with the recommended technique. While RNNs operate as effectively as they do for a given iteration, as the number of observations increases, the accuracy decreases.

Table 3
Numeric Summary of Performance Measure.

Label	Normal	Attack
Normal	True Negative (TN)	False Positive (FP)
Attack	False Negative (FN)	True Positive (TP)

According to the number of requests, Fig. 8 It is noted that the proposed model outperforms SVM in terms of performance even when the number of queries is at its highest. The performance of the NRN is superior, but it remains inferior to that of the proposed model. Fig. 9 compares the training times for the proposed model with the current methods used. One of the objectives of the study is to reduce training time, which was perceived as the main drawback of machine learning algorithms. Compared to existing methods, the formation time of the proposed model is reduced by the small number of characteristics. The proposed deep learning-based intrusion detection model uses the least amount of computational time when compared to conventional techniques, as can be seen from the figure.

Fig. 10 presents a comparison of proposed and existing detection algorithms for various threats. The results show that the proposed strategy achieves maximum detection performance across a range of threats. While the proposed network works satisfactorily for DoS & probe, it works badly for R2L and U2R attacks. Table 3 provides a numeric summary of the performance measures that were used to select the appropriate model for the current products. From the making a comparison, it can be shown that the proposed DL model performs better across the board, including in terms of detection performance, higher accuracy, accuracy, & false positive rate. The proposed model was suitable to identify invasions in the multi-cloud IoT scenario, as evidenced by its increasing efficiency on RNN.

5. Conclusion

To improve information security, this revolutionary research introduces a multi-cloud IoT intrusion detection system based on DL. The proposed IDS overcomes the longer practice times and low recognition accuracy of modern machine learning algorithms. The features of the data set are widely exploited by the proposed DL method increases classification performance. In terms of classification accuracy, predictive accuracy, sensitivity, and false alarm rates features can be extracted through CNN at different levels. The NSL-KDD dataset was used for the experimental assessment, and the results also compared with contemporary vector-based SVM and recursive scanning of NN vulnerabilities. The proposed model performs better on the whole. The implementation of architectures to recognize meticulous attacks in the cloud infrastructure will also support the work.

CRediT authorship contribution statement

B. Raviprasad: Writing – original draft. **C Rama Mohan:** Methodology. **G. Naga Rama Devi:** Supervision, Writing – review & editing. **R. Pugalenthi:** Data curation. **L.C. Manikandan:** Conceptualization. **Sivakumar Ponnusamy:** Validation.

Declaration of competing interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Data availability

No data was used for the research described in the article.

References

[1] D. Tiwari, B.S. Bhati, B. Nagpal, S. Sankhwar, F. Al-Turjman, An enhanced intelligent model: to protect marine IoT sensor environment using ensemble machine learning approach, Ocean Eng. 242 (2021), 110180.

[2] R. Akhter, S.A. Sofi, Precision Agriculture Using IoT Data Analytics and Machine Learning, Journal of King Saud University-Computer and Information Sciences, 2021.

[3] G. Uganya, D. Rajalakshmi, Y. Teekaraman, R. Kuppusamy, A. Radhakrishnan, A Novel Strategy for Waste Prediction Using Machine Learning Algorithm with IoT Based Intelligent Waste Management System, Wireless Communications and Mobile Computing, 2022, 2022.

[4] N.G. Rezk, E.E.D. Hemdan, A.F. Attia, A. El-Sayed, M.A. El-Rashidy, An efficient IoT-based smart farming system using machine learning algorithms, Multimed. Tool. Appl. 80 (1) (2021) 773–797.

[5] A.S. Rajawat, P. Bedi, S.B. Goyal, A.R. Alharbi, A. Aljaedi, S.S. Jamal, P.K. Shukla, Fog big data analysis for IoT sensor application using fusion deep learning, Math. Probl Eng. (2021), 2021.

[6] H. Nankani, S. Gupta, S. Singh, S.S. Subashka Ramesh, Detection analysis of various types of cancer by logistic regression using machine learning, Int. J. Eng. Adv. Technol. 9 (1) (2019) 99–104.

[7] P. Mittal, Machine learning (ml) based human activity recognition model using smart sensors in IoT environment, in: 2022 12th International Confer*ence on Cloud Computing, Data Science & Engineering*, IEEE, Confluence), 2022, January, pp. 330–334.

[8] H. Mezni, M. Driss, W. Boulila, S.B. Atitallah, M. Sellami, N. Alharbi, Smartwater: a service-oriented and sensor cloud-based framework for smart monitoring of water environments, Rem. Sens. 14 (4) (2022) 922.

[9] L.S. Kondaka, M. Thenmozhi, K. Vijayakumar, R. Kohli, An intensive healthcare monitoring paradigm by using IoT-based machine learning strategies, Multimed. Tool. Appl. (2021) 1–15.

[10] M.A. Alsoufi, S. Razak, M.M. Siraj, I. Nafea, F.A. Ghaleb, F. Saeed, M. Nasser, Anomaly-based intrusion detection systems in IOT using deep learning: a systematic literature review, Appl. Sci. 11 (18) (2021) 8383.

[11] M.S. Minu, R. AroulCanessane, S.S. Subashka Ramesh, Optimal Squeeze Net with Deep Neural Network-Based Arial Image Classification Model in Unmanned Aerial Vehicles, Traitement du Signal 39 (1) (2022) 275–281.

[12] M. Monica, P. Sivakumar, S.J. Isac, K. Ranjitha, PMSG Based WECS: Control Techniques, MPPT Methods and Control Strategies for Standalone Battery Integrated System, in: AIP Conference Proceedings, vol. 2405, AIP Publishing LLC, 2022, April, 040013.

[13] V.K.S. Maddala, K. Jayarajan, M. Braveen, R. Walia, P. Krishna, S. Ponnusamy, K. Kaliyaperumal, Multisensor data and cross-validation technique for merging temporal images for the agricultural performance monitoring system, J. Food Qual. (2022), 2022.

[14] G. Naga Rama Devi, Sivakumar Ponnusamy, Jyotsna Pandit, B. Buvaneswari, A. SuhanaNafais, Sushma Jaiswal, Development of medicinal industries in building A replica to the damaged human tissue for artificial organs with the application of micro-and nano technology (mnt), J. Optoelectron. - Laser 41 (3) (2022) 79–83.

[15] C. Wang, J. Qin, C. Qu, X. Ran, C. Liu, B. Chen, A smart municipal waste management system based on deep learning and the Internet of Things, Waste Manag. 135 (2021) 20–29.

[16] H. Kim, E. Song, Behavior detection mechanism for trust sensor data using deep learning in the internet of things, Webology 19 (1) (2022) 4546–4554.

[17] P.R. Garikapati, K. Balamurugan, T.P. Latchoumi, G. Shankar, A quantitative study of small dataset machining by agglomerative hierarchical cluster and K-medoid, in: Emergent Converging Technologies and Biomedical Systems, Springer, Singapore, 2022, pp. 717–727, https://doi.org/10.1007/978-981-16-8774-7_59.

[18] D. Jagadish, P. Vinoth Kumar, P. Ashok, V. Hariharan, R. Maniraj, LMSDS: learning management system for deaf students in collaborative learning environment, Indian Journal of Science and Technology 9 (16) (2016), 92203.

[19] T.P. Latchoumi, R. Swathi, P. Vidyasri, K. Balamurugan, Develop new algorithm to improve safety on WMSN in health disease monitoring, in: 2022 International Mobile and *Embedded Technology Conference (MECON)*, 2022, March, pp. 357–362, https://doi.org/10.1109/MECON53876.2022.9752178. IEEE.

[20] O. Cheikhrouhou, R. Mahmud, R. Zouari, M. Ibrahim, A. Zaguia, T.N. Gia, One-dimensional CNN approach for ECG arrhythmia analysis in fog-cloud environments, IEEE Access 9 (2021) 103513–103523.

[21] A.P. Venkatesh, T.P. Latchoumi, S. Chezhian Babu, K. Balamurugan, S. Ganesan, M. Ruban, L. Mulugeta, Multiparametric optimization on influence of ethanol and biodiesel blends on nano coated engine by full factorial design, J. Nanomater. (2022), https://doi.org/10.1155/2022/5350122, 2022.

[22] S.K. Chandrasekaran, P. Savarimuthu, P. Andi Elumalai, K. Ayyaswamy, Primary Path Reservation Using Enhanced Slot Assignment in Tdma for Session Admission, vol. 2015, Scientific World Journalthis link is disabled, 2015, 405974.

[23] T. Raguntha, P. Ashok, N. Gopinath, M. Subashini, A strong reinforcement parallel implementation of k-means algorithm using message passing interface, Mater. Today Proc. 46 (2021) 3799–3802, https://doi.org/10.1016/j.matpr.2021.02.032.

[24] P. Deeraj, G. Rohit, K.S. Abhishek, S.S. Subashka, A trash barrel suitable for both indoor and outdoor uses (A better way to clean your garbage), International Journal of Advanced Science and Technology 29 (5) (2020) 3103–3110.

[25] S. Mishra, A.K. Tyagi, The role of machine learning techniques in the internet of things-based cloud applications, in: Artificial Intelligence-Based Internet of Things Systems, Springer, Cham, 2022, pp. 105–135.

[26] V. Ponnusamy, S. Natarajan, Precision agriculture uses the advanced technology of IoT, unmanned aerial vehicles, augmented reality, and machine learning, in: Smart Sensors for Industrial Internet of Things, Springer, Cham, 2021, pp. 207–229.

[27] A. Thakkar, R. Lohiya, A review on machine learning and deep learning perspectives of IDS for IoT: recent updates, security issues, and challenges, Arch. Comput. Methods Eng. 28 (4) (2021) 3211–3243.