DS Journal of Cyber Security
Volume 1 Issue 1, 46-52, Jul - Sep 2023
ISSN: 2584-0665 / https://doi.org/10.59232/CYS-V1I1P105

Original Article

Cyberattack Detection via Artificial Intelligence in Cloud Computing Environment

N. Suresh

Sri Venkateswara College of Engineering and Technology, Andrapradesh, India.

sureshncse70@gmail.com

Received: 05 June 2023; Revised: 17 June 2023; Accepted: 3 July 2023; Published: 6 July 2023;

Abstract - Cyberattack detection is the ability of IT firms to quickly and efficiently identify threats to the network, apps, or other network assets. The first step in creating a successful cyber detection and response strategy is understanding the risks that exist in the online environment. In cyberspace, every method utilised to defend a business's assets, personnel, and operations from online threats is referred to as cyber security. Due to more complex networks and more frequent and sophisticated attacks, organisations need various cyber security solutions to reduce their cyber risk. A deep learning-based cyberattack detection system is proposed in this paper for detecting cyberattacks in cloud environments. Prior to reducing the dimensions, independent component analysis is used to extract the relevant characteristics. As a result, LSTM with multi-head attention is used to categorise different sorts of cyberattacks. The deep learning model's energy usage and detection time will be assessed and contrasted with alternative approaches. We demonstrate through experimental findings that our suggested framework not only distinguishes various cyberattacks but also achieves a high level of detection accuracy (up to 99.1%).

Keywords - Cyber security, Cyberattack, Intrusion detection, Dimension reduction, Multi-Head LSTM, Deep Learning.

1. Introduction

The basic goal of homeland security is to protect the country from all dangers. Safety and security at home encompass a wide range of issues, including video surveillance, image recognition, cyberattack detection, and modern homeland security. The area of cyberattack detection is examined in this research. Additional security measures are also necessary to protect personal information in the virtual world.

Cyberattacks are attempts to get through a computer system's security safeguards. The actual description of cyberattack detection is “the difficulty of detecting individuals accessing a computer system without authorisation and those who have legitimate access to the system but are abusing their privileges.”

The development of a cyberattack detection strategy by the cloud user is beneficial, and cloud service providers have launched a “Cloud Intrusion Detection System Service” to protect their customers from cyberattacks. The “Cloud Intrusion Detection System Service” consists of three parts. The user network is connected to the intrusion detection service agent to get the necessary information. It is possible to generate attack specifications automatically using a variety of automated techniques. The vast majority of misuse detection systems lack this capability. The majority of systems focus on data produced by a single source.

Deep learning Convolutional Neural Network (CNN) is used to recognise cyberattacks. In contrast to existing knowledge of deep neural network approaches, Deep Learning can disclose higher-level features and more

abstract ideas that expose more complex and complex linkages. Deep learning is defined by a significantly higher number of sequentially connected neural layers. Artificial Intelligence, or AI, is the ability of a computer or robot to carry out tasks that are traditionally done by humans because they involve human intelligence and judgement. Big data analytics, such as data analysis, diagnostic analytics, predictive analytics, and predictive analysis, can give a range of information when attached to the IoT.

The cloud infrastructure will then employ the neural network to detect online cyberattacks. We show how well our proposed framework can distinguish between various sorts of attacks through experimental results. We have also compared our proposed framework's performance with conventional intrusion detection methods to emphasise our approach's efficacy.

- The IoT platform can highlight the cyberattack mostly on the main dashboard owing to the newly introduced deep learning method.
- The developed scheme may evaluate the processing state accurately because it is more precise than deep learning techniques. The proposed model may evaluate the machining state accurately since it is more precise than deep learning techniques.

The remaining section of this paper is organised as follows, Section 2 contains the literature review of previous research, Section 3 describes an in-depth explanation of the proposed methodology, Section 4 presents the results, and Section 5 holds the conclusion.

2. Literature Survey

In 2015, J. Cao et al. suggested a method that uses the state of virtual machines, such as CPU and network consumption, to detect attacks. Information entropy is used in monitoring the condition of virtual computers to discover attack behaviors based on this observation. Even though the fact that the entropy average rises as ns increases, our tests show that setting 0>7 6 6 13 maintains a nearly identical level of system identification accuracy. Several types of VMs coexisting in the same zone may lessen competition for the same crucial resources, increasing the data center's overall efficiency.

In 2013, M. N. Ismail et al., suggested three phases of a novel model to identify flooding-based DoS assaults in cloud systems. The initial stage of baseline profiling involves modelling the typical traffic pattern, which is then followed by the intrusion detection stage and, ultimately, the preventive stage. The detecting method makes use of the covariance matrix mathematical model. The first and second phases have been tested in real-world settings. The outcome demonstrates the ability to identify flooding attacks efficiently.

In 2017, A. Sahi et al., suggested a novel classifier system for public cloud DDoS TCP flood assaults identification and mitigation. By classifying the arriving packets and basing decisions on the classification outcomes, the suggested CS DDoS system provides a method for protecting stored information. It has a Kappa coefficient of 0.89 and can identify DDoS TCP flood attacks from a single source with roughly 97% accuracy; from several sources, it can do so with 94% accuracy and a Kappa coefficient of 0.9. Additionally, a K-fold cross-validation model is used to validate the results, and accuracy is addressed—and time complexity.

In 2016 M. Chouhan and H. Hasbullah suggested a brand-new detection method for CSCA be created using the Bloom Filter (BF). This method generates CSCA signatures using a difference mean calculator and treats cache miss sequence as one. Due to the adaptive nature of this method, it is possible to identify previously unnoticed CSCA patterns. This, to some extent, lessens this security issue. An adaptive detection method for CSCA is created in this research study.

In 2016, K. Wang and Y. Hou suggested a type of SQL detection technique that combines input filtering and dynamic taint analysis. Additionally, it is integrated into the cloud environment to achieve web application protection during cloud deployment. The detection module's addition boosts accuracy as well. The experiment's findings demonstrate that the technique can identify typical attacks. As a result, in the cloud environment, SQL injection detection is more accurate.

In 2016, G. Nenvani and H. Gupta suggested that to ensure no changes may be made to messages transmitted by the hypervisor, A safe virtualisation method is suggested, using message digests, public and private keys for all VMs, and digital signatures. A study is conducted on cloud computing security concerns and cloud attack methods. Further research can be done to create a supervised learning-based profile system that can send out alerts when any of these behaviors are suspected.

In 2017, A. Nezarat, suggested a set of mobile agents serve as sensors for improper actions in a cloud environment. They begin a non-cooperative game with the alleged attacker, calculate the Nash equilibrium value and utility, and use this information to distinguish between an attack and valid requests and gauge the attack's severity and point of origin. According to the simulation results, this approach can accurately detect attacks 86% of the time. Reduced system overhead and an expedited detection procedure have resulted from using mobile agents and their trainability features.

3. Proposed Methodology

This paper proposes a deep learning-based cyberattack detection system to recognise cyberattacks in cloud environments. To extract the pertinent characteristics, independent component analysis is first used for dimension reduction. As a result, LSTM with multi-head attention is used to categorise different kinds of cyberattacks. The deep learning model's energy use and detection time will be assessed and compared to alternative methods. Figure 1 illustrates the suggested method's overall procedure.

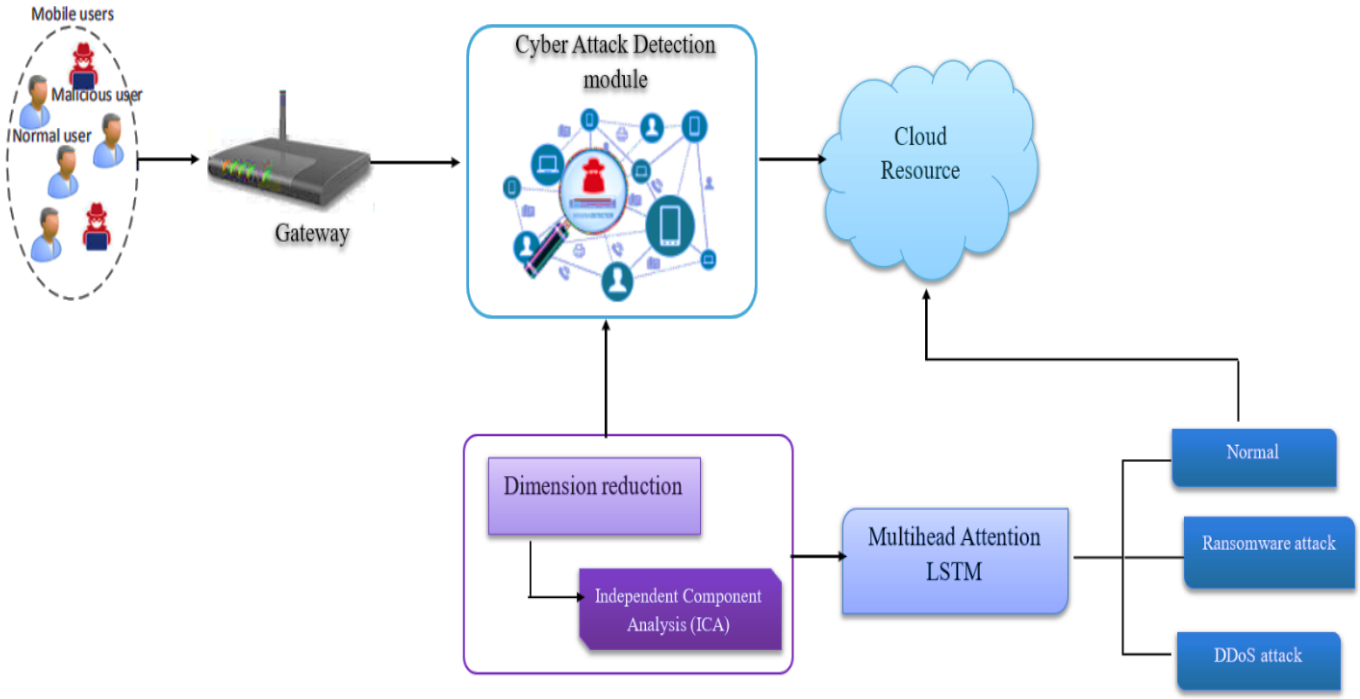

Fig. 1 Proposed methodology block diagram

3.1. Attack Detection Module

Using the previously learned deep learning model, incoming requests are classified. The deep learning model will carry out this task after being trained offline.

This section explains the system's operation after describing the suggested system model for cyberattack detection and its key functionalities. According to Figure 1, whenever a request or packet is made to the system by a mobile user, the attack detection module receives it. Data gathering and preparation, attack detection, and request processing are the three main duties of this module.

3.1.1. Data Collection and Pre-Processing Function

It is in charge of gathering information and preparing the request for fitting into the deep learning method. This function accelerates the convergence of the gradient descent approach employed during training, which is crucial for improving the functionality of our model.

3.1.2. Request Processing

The attack detection function assesses a request as either normal or suspicious when received. If the request is normal, the cloud resources will accommodate it. Otherwise, the security control module will be notified about the request.

3.2. Dimension Reduction

Independent Component Analysis (ICA) is utilised in dimension reduction. Data packets include numerous properties with a variety of qualities. Certain features are redundant and useless, which slows down the detecting process and lowers performance. In order to reduce computing costs and boost learning accuracy, it is crucial to choose features that maintain a dataset's most crucial information. Independent Component Analysis (ICA) is a computational method for breaking down a multivariate signal into additive segments in signal processing. The segments are assumed to be statistically independent of one another and that only one subcomponent, at most, is Gaussian to achieve this.

The "cocktail party problem" is a straightforward ICA application where the underlying speech signals are distinguished from a sample of simultaneous conversations taking place in a room. Generally, assuming there are no time delays or echoes simplifies the issue.

Three consequences of combining source signals and two premises underlie the very good results that the ICA separation of mixed signals produces. Two suppositions:

- The source signals are separate from one another.
- Each source signal's values have a non-Gaussian distribution.

3.3. Attack Classification

The LSTM method is used to categorise cyberattacks. LSTM networks are useful for classifying, processing, and making predictions based on time series data since there may be lags of varying lengths between important occurrences in a time series. The development of LSTMs addressed the potential problem of vanishing gradients that could occur during the training of regular RNNs. Feedback is connected to the LSTM. Such a recurrent neural network is capable of analysing entire data sequences as well as single data points (like images), as well as speech or video. Because of this feature, LSTM networks are excellent at organising and making predictions about data. For example, LSTM can be applied to various activities, including speech translation, robot control, vocal activity detection, video games, and healthcare. Applications like linked, unsegmented handwriting identification are also possible with it.

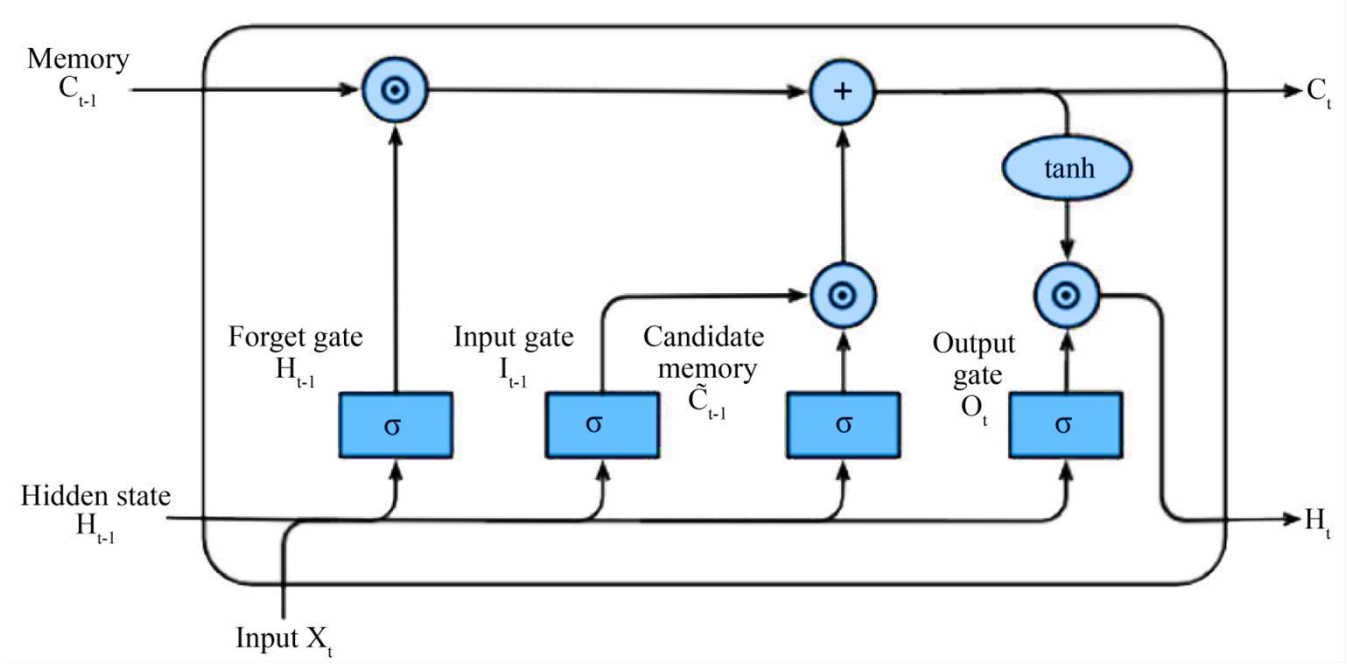

Fig. 2 LSTM architecture

Multi-head attention enables the neural network to control information mixing between portions of an input sequence, resulting in richer representations and better performance on machine learning tasks. "Multi-Head Attention" is a module for attention mechanisms that is cycled repeatedly and concurrently through an attention mechanism. The individual attention outputs are then linearly combined to obtain the expected dimension. There are numerous ways to pay attention to a word; thus, we need several heads of attention to convey the comment's entire semantics. Each word is given the proper importance from a range of perspectives in each head.

$$Y = \tanh(w_{k1} H^T) \quad (1)$$

$$Z = \text{softmax}(w_{k2}\, Y) \quad (2)$$

The attention layer inputs all of the hidden states as H, multiply them with W_{k1} R ^{g2p,} and then passes the result to the tanh function to obtain Y. Softmax is used to determine the Using multiple heads (q) of standardised significance weight, each component's attention from various variables is separated, and multiplying Y by W_{k2} R ^{q*g} results in a vector of weights Z.

Combining equations (1) and (2) yields a two-layer Multi-Layer Perceptron (MLP), with parameters W_{k1} and W_{k2} and a hidden unit number g. The sentence embedding is represented by the matrix M, created by finding the q-weighted sum after multiplying the hidden states of the word H by the weight vector Z.

$$M = ZH \quad (3)$$

4. Result & Discussion

A cyberattack that uses deep learning to identify cyberattacks in a cloud setting. The deep learning model's energy usage and detection time will be assessed and contrasted with alternative approaches. This study analyses the deep-learning cyberattack detection model using performance measures like accuracy, recall, precision, and specificity, which are common machine learning characteristics. Additionally, we contrast with existing deep learning methods. Our suggested model for detecting cyberattacks on actual devices and assessing the model's

accuracy in real time. Also, the deep learning model's energy usage and detection time will be assessed and contrasted with alternative approaches.

4.1. Evaluation Metrics

The proposed model has been evaluated using the conventional numerical parameters listed below. Accuracy, recall, specificity, and sensitivity were each determined using Equations (4), (5), (6), and (7), respectively. The accuracy was determined using equation (4):

$$\text{Accuracy} = \frac{\text{TP+TN}}{\text{TP+TN+FP+FN}} \tag{4}$$

$$\text{Specificity} = \frac{\text{TP}}{\text{TP+FP}} \tag{5}$$

$$\text{Recall} = \frac{\text{TP}}{\text{TP+FN}} \tag{6}$$

$$\text{Percision} = \frac{\text{TP}}{\text{TP+FP}} \tag{7}$$

Four alternative results for the given data exist False Negative (FN), True Negative (TN), False Positive (FP), and True Positive (TP). False negative data is labeled positively, whereas genuine positive data is labeled positively and categorised as such. False positive data is referred to as positive, while TN data is labeled negative and labeled as negative. The comparison graph is plotted below.

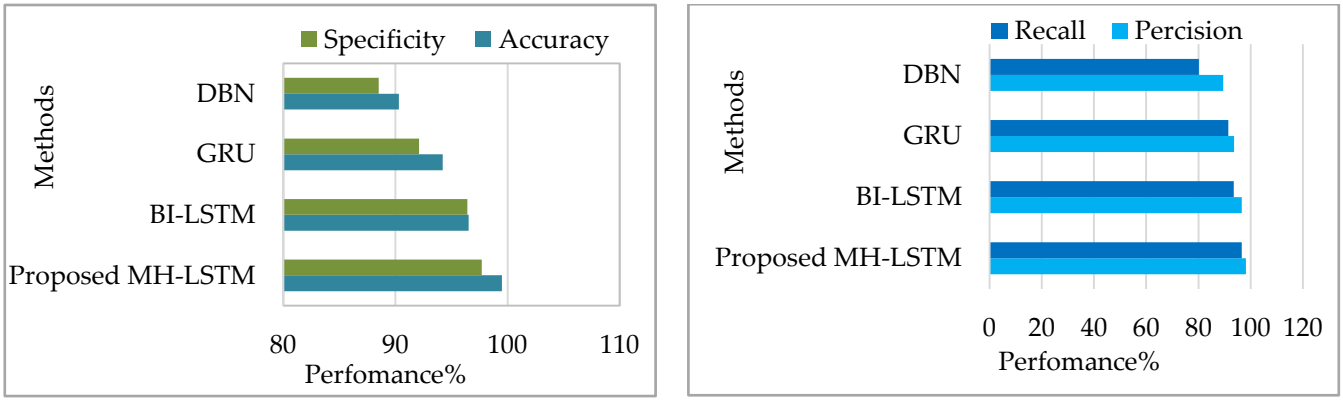

Fig. 3 Comparative analysis of the proposed method

In Figure 3, several metrics, such as recall, accuracy, specificity, and precision rate, are represented graphically as an overview of proposed and existing approaches. The results of the graphs make it abundantly evident that the suggested methodology is better than all currently employed methods and appropriate for identifying attacks. The specificity and sensitivity of the suggested approaches are 98.07% and 98.02%, respectively. The proposed framework outperformed the current BI-LSTM, GRU, and DBN in terms of sensitivity and specificity when compared to earlier models.

5. Conclusion

The idea of cyberattack detection makes use of a deep learning technique to find cyberattacks in a cloud environment. In order to recognise cyberattacks in cloud environments, a deep learning-based cyberattack detection system has been proposed in this paper. Independent component analysis is used to conduct the dimension reduction before extracting the relevant attributes. As a result, LSTM with multi-head attention is used to categorise different kinds of cyberattacks. The deep learning model's energy usage and detection time will be assessed and contrasted with alternative approaches. Using experimental findings, we demonstrate that our

suggested framework can detect cyberattacks with a high degree of accuracy (up to 99.1%) while differentiating between various types of attacks. We contrast our strategy with current deep-learning methodologies. We demonstrate using experimental findings that our suggested framework not only distinguishes between various cyberattacks but also accurately (up to 99.1%) identifies attacks. Sensitivity, accuracy, specificity, and recall are the measures used to gauge the effectiveness of the proposed model. The proposed methodology effectively improves accuracy by about 99.01% when compared to BI-LSTM, GRU, and DBN**.**

References

[1] Avinash Kumar et al., "Sarcasm Detection Using Multi-Head Attention Based Bidirectional LSTM," *IEEE Access*, vol. 8, pp. 6388-6397, 2020. [CrossRef] [Google Scholar] [Publisher Link]

[2] Jamal Raiyn, "A Survey of Cyber-Attack Detection Strategies, " *International Journal of Security and Its Applications*, vol. 8, no. 1, pp. 247-256, 2014. [CrossRef] [Google Scholar] [Publisher Link]

[3] Alfonso Valdes, and Keith Skinner, "Adaptive, Model-Based Monitoring for Cyber-Attack Detection," *Recent Advances in Intrusion Detection, RAID 2000*, vol. 1907, pp. 80-93, 2000. [CrossRef] [Publisher Link]

[4] Shailendra Singh, and Sanjay Silakari, "A Survey of Cyber-Attack Detection Systems," *International Journal of Computer Science and Network Security*, vol. 9, no. 5, pp. 1-10, 2009. [Google Scholar] [Publisher Link]

[5] Nong Ye, Yebin Zhang, and C. M. Borror, "Robustness of the Markov-Chain Model for Cyber-Attack Detection," *IEEE Transactions on Reliability*, vol. 53, no. 1, pp. 116-123, 2004. [CrossRef] [Google Scholar] [Publisher Link]

[6] Eman Mousavinejad et al., "A Novel Cyber-Attack Detection Method in Networked Control Systems," *IEEE Transactions on Cybernetics*, vol. 48, no. 11, pp. 3254-3264, 2018. [CrossRef] [Google Scholar] [Publisher Link]

[7] Noam Ben-Asher, and Cleotilde Gonzalez, "Effects of Cyber Security Knowledge on Attack Detection," *Computers in Human Behavior*, vol. 48, pp. 51-61, 2015. [CrossRef] [Google Scholar] [Publisher Link]

[8] Usman Inayat et al., "Learning-Based Methods for Cyber-Attacks Detection in IoT Systems: A Survey on Methods, Analysis, and Future Prospects," *Electronics*, vol. 11, no. 9, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[9] Hadis Karimipour et al., "A Deep and Scalable Unsupervised Machine Learning System for Cyber-Attack Detection in Large-Scale Smart Grids," *IEEE Access*, vol. 7, pp. 80778-80788, 2019. [CrossRef] [Google Scholar] [Publisher Link]

[10] Abdulrahman Al-Abassi et al., "An Ensemble Deep Learning-Based Cyber-Attack Detection in Industrial Control System," *IEEE Access*, vol. 8, pp. 83965-83973, 2020. [CrossRef] [Google Scholar] [Publisher Link]

[11] Rupinder Paul Khandpur et al., "Crowdsourcing Cybersecurity: Cyber-Attack Detection Using Social Media," *CIKM '17: Proceedings of the 2017 ACM on Conference on Information and Knowledge Management*, pp. 1049-1057, 2017. [CrossRef] [Google Scholar] [Publisher Link]