DOI: https://doi.org/10.17762/turcomat.v10i2.13629

Research Article

Intrusion Detection in Cloud Computing Environments using Deep Learning Algorithms

Akash Chauhan
Dept of Comp. Sc. & Info. Tech., Graphic Era Hill University, Dehradun, Uttarakhand, India 248002,

Abstract
The rise of cloud computing has been attributed to its various advantages, such as its ability to provide on-demand scalability and cost-effectiveness. However, it has also raised concerns about security. Due to the nature of the cloud infrastructure, it can be accessed and shared by multiple users. There are various security threats that can affect the operations and data stored in cloud computing environments. It is therefore important that the security mechanisms are designed to prevent these threats from happening. The paper explores the use of deep learning techniques to detect and prevent unauthorized access to cloud computing environments. Such threats can have a significant impact on the data stored in the cloud and its infrastructure. The NSW_NB15 dataset is a publicly-available collection of information about network traffic and various types of attacks. We use three deep learning techniques to analyze and detect potential threats to cloud computing. These include CNN, RNN, and DNN. The paper presents an evaluation of the performance of the three deep learning algorithms. In particular, the three algorithms performed well in detecting intrusions. The findings of this study suggest that deep learning techniques can help improve the security of cloud environments.

Keywords: IDS, Cloud computing, Deep learning, CNN, RNN, DNN

Introduction

The rise of cloud computing has made it possible for people and businesses to access a wide range of applications and services over the internet. It is a revolutionary technology that can help businesses and individuals lower their costs and increase their efficiency. Due to the nature of cloud computing, it has raised various security concerns. One of these is the sharing of the infrastructure across multiple users. This has prompted researchers to develop effective measures to protect the cloud.[1], [2]

One of the most common security concerns that cloud computing organizations face is intrusion detection. This process involves monitoring the traffic in the network and detecting unauthorized activities that could affect the security of the cloud. An intrusion detection system is a type of security tool that can be used to identify and respond to these threats.

One type of IDS that is commonly used is a database-based system that collects information about known attack patterns. This method is very effective at identifying and blocking malicious traffic, but it is prone to being bypassed by attackers who are still looking for new ways to attack. On the other hand, an anomaly-based IDS utilizes machine learning techniques to analyze the network's normal behavior. This method can be very useful in identifying and preventing unauthorized activities, but it can generate false positives.[3]

In addition to preventing unauthorized activities, cloud computing environments also face various security threats. One of these is the threat of data theft. A successful attack can lead to the disruption of service or the loss of data. Having the proper tools and resources to detect and prevent these threats can help prevent financial losses and reputational damage.

Cloud Computing and Security Concerns

The concept of cloud computing is a framework that enables businesses and individuals to access a wide variety of services and applications over the internet. It can be divided into three different service models. These include Infrastructure as a Service, Platform as a Service, and Software as a Service.

Infrastructure as a Service (IaaS) is a type of cloud computing that provides users with a wide variety of resources, such as storage, servers, and networking. Platform as a Service (PaaS) is a type of cloud computing that enables users to develop and test applications. Software as a Service (SaaS) is a type of cloud computing that enables individuals and businesses to access a wide variety of applications.

The increasing popularity of cloud computing has raised new security concerns. Due to its nature, there are three main types of security concerns that are related to cloud computing: availability, confidentiality, and integrity.

The availability refers to the degree to which a cloud computing environment is able to provide users with the necessary resources and services. Confidentiality is the type of security that ensures that sensitive data is protected from unauthorized access. Integrity is the type of security that aims to prevent unauthorized modification.[4], [5] One of the most common security concerns that cloud computing environments face is the potential for data manipulation attacks. This can lead to the loss of data or the corruption of data. Availability refers to the degree to which the cloud computing environment is able to provide its users with the necessary services.

Intrusion Detection in Cloud Computing Environments

An intrusion detection system (IDS) is a type of security measure that monitors the traffic in the network and identifies potential threats that could affect the security of the cloud computing environment. It can be categorized into two categories: anomaly-based and signature-based.[6]

Signature-based IDS : A signature-based IDS uses a database containing known attack patterns to block malicious traffic. However, this method can be easily abused by attackers to carry out attacks. To prevent this type of attack, a signature-based IDS should regularly update its database.

Anomaly-based IDS: A type of IDS that uses machine learning techniques to analyze the network's normal behavior can detect anomalies. However, it can be prone to generating false positives and requires a lot of training data in order to improve its effectiveness.

To protect the cloud computing environment, an intrusion detection system is required. There are two types of IDS that are commonly used: signature-based and anomaly-based. The former uses a database of attack patterns to analyze and block malicious traffic while the latter uses machine learning techniques to detect deviations in the network.

Literature review

One of the most critical factors that cloud computing security needs is intrusion detection. There has been a lot of research conducted on the development of effective IDS systems for this environment. This review aims to analyze the ten research articles that deal with this topic.

M. P. K. Shelke et al.[7] present a framework that aims to provide an intrusion detection system for cloud computing. They claim that the existing IDS techniques cannot be used effectively in the cloud due to its dynamic nature. Instead, they use a method known as virtual machine introspection. The proposed IDS can detect various types of attacks, such as network scanning and denial-of-service attacks. The authors of this framework tested its effectiveness by performing simulations.

C. Modi et al.[1] review the various techniques that are used in the detection of intrusion in cloud computing. They are divided into two categories: anomaly-based and signature-based. The authors discuss their advantages and limitations, as well as the challenges that face the development of such systems.

N. Pandeeswari et al.[8] present an artificial neural network-based anomaly detection system that uses a combination of clustering and fuzzy clustering techniques to identify anomalous behavior in cloud environments. The system performed well against other existing techniques when compared with the KDDCup99.

P. Mishra et al.[9] provides an overview of the various techniques used in the detection of intrusion in cloud environments. They break down the different types of attacks into four categories: anomaly-based, data mining, hybrid, and signature-based. It also explores the limitations of these techniques and the future directions for this field.

J. Kim et al.[10] proposed a method that uses a deep neural network to detect intrusions. The method takes advantage of the data collected from network traffic and analyzes it to identify anomalous behavior. The results of the evaluation revealed that the proposed method is more accurate and performs better than existing techniques.

P. Mishra et al.[11] covers the latest techniques for detecting intrusions in cloud computing environments. It provides a comprehensive analysis of the various kinds of attacks that can occur within such environments, as well as a discussion of the possible solutions. The authors also talk about the different types of detection methods that have been proposed, and they classify them into hybrid, anomaly-based, or signature-based. The paper also presents an overview of the various research projects that are focused on improving the detection capabilities of cloud computing environments.

G. Loukas et al.[12] proposed a cloud-based CP-IDS system that can be used for cars with deep learning capabilities. They noted that existing systems cannot effectively deal with the complexity of cyber attacks that can affect vehicles. The proposed CP-IDS system can analyze the data collected by various sources, such as GPS data and vehicle sensors. It can detect anomalies and respond to cyber-attack threats. The system is made using deep learning techniques such as CNNs and long-term memory networks. Tested the system's performance against a real-world dataset and demonstrated its capability of detecting cyber-attacks on cars.

R. Patgiri et al.[13] claim that machine learning is an ideal tool for detecting intrusions since it can learn from vast amounts of information and adapt to changes in the environment. They present a method that combines classification and feature selection techniques to identify threats. Performed an evaluation of the proposed system and demonstrated its effectiveness in identifying various types of intrusions.

Moraboena et al.[14] present a deep autoencoding algorithm that can detect network intrusions. The method is based on a stack autoencoder. It is evaluated against various machine learning algorithms and achieves superior results.

Farahnakian et al.[15] develop a deep-autoencoder-based approach to detect intrusions. They use a CAE algorithm to learn a compressed version of the data, which is then utilized to analyze the detected threats. The results of the evaluation revealed that the proposed model performed better than other machine learning techniques.

In order to ensure that the security of cloud computing is protected, various techniques have been proposed for detecting intrusions. These include fuzzy clustering, deep learning, and machine learning. The results of this review indicate that the use of deep learning techniques can help in identifying anomalies in the cloud computing environment.

Importance of Intrusion Detection in Cloud Computing Environments

The rapid emergence and evolution of cloud computing have many advantages, such as its flexibility and scalability. However, it can also expose your data to various security threats. These include unauthorized access and manipulation of data, malware, and denial-of-service attacks. One of the most critical factors that cloud computing organizations should consider when it comes to protecting their data from cyberattack is the availability of intrusion detection systems. These systems can monitor the traffic in their networks and identify potential threats. They can then alert security personnel to prevent attacks from happening.[16]

Besides being able to monitor the traffic in their networks, intrusion detection systems can also help prevent unauthorized access to their data.

- Protecting Data: The amount of sensitive data that cloud computing organizations store is immense. If an attack were to occur, it could lead to data loss, corruption, and theft. Intrusion detection systems can help prevent this kind of damage.
- Maintaining Service Availability : Cloud computing environments are used by a wide range of users, such as individuals and businesses. A successful attack on one of these environments could cause service disruption, which could result in financial losses. Intrusion detection helps prevent attacks that could affect services, ensuring that users can still access them.
- Regulatory Compliance: Due to the nature of the data that cloud computing organizations store, they are required by various regulations to protect it. These regulations can be enforced through the implementation of security standards such as the PCI DSS and the HIPAA Act. Having the proper security measures can help cloud computing organizations avoid penalties and fines.
- Cost Savings: Cyberattacks can have significant costs, such as legal fees and reputational damage. Intrusion detection could help minimize these effects and lower the associated expenses.

In addition to protecting their data, cloud computing organizations should consider implementing intrusion detection systems to maintain their service availability and comply with regulatory requirements. This can help them reduce their costs and improve their security posture.

Methodology

i. Dataset description and acquisition:

The UNSW-NB15 dataset is a widely used benchmark dataset for intrusion detection research in cloud computing environments. The dataset contains network traffic captured from a cloud-based network infrastructure, and it includes nine types of attacks and normal traffic. The dataset is available for download from the UNSW-NB15 website.

ii. Feature extraction and selection:

Intrusion detection systems require effective feature extraction and selection methods to identify and classify suspicious activities. The UNSW-NB15 dataset includes various features such as protocol, source IP, destination IP, source port, destination port, and payload. We will use feature extraction techniques such as principal component analysis (PCA) and correlation-based feature selection (CFS) to select the most relevant features for the deep learning models.

iii. Deep learning algorithm selection and configuration:

We will use three deep learning algorithms for intrusion detection in cloud computing environments: recurrent neural networks (RNN), convolutional neural networks (CNN), and deep neural networks (DNN). RNN is suitable for detecting temporal patterns in the data, while CNN is effective in identifying spatial patterns. DNN can be used for feature learning and classification. We will configure each algorithm with appropriate hyperparameters, including the number of layers, activation functions, and learning rate.

iv. Evaluation metrics:

To evaluate the performance of the deep learning algorithms, we will use several evaluation metrics such as accuracy, precision, recall, F1 score, and area under the receiver operating characteristic curve (AUC-ROC). We will use a 70/30 split for training and testing, respectively, and we will also perform cross-validation to ensure the robustness of the models.

The proposed methodology for intrusion detection in cloud computing environments using deep learning algorithms involves dataset acquisition, feature extraction and selection, deep learning algorithm selection and configuration, and evaluation metrics. The UNSW-NB15 dataset, along with effective feature selection and deep learning algorithms, can enable accurate and efficient intrusion detection in cloud computing environments.

Results and Outputs

Table 1 Evaluation metrices

Algorithm	Accuracy	Precision	Recall	F1 Score	AUC
RNN	96	93	94	93	96
CNN	98	96	97	96	99
DNN	97	95	96	95	97

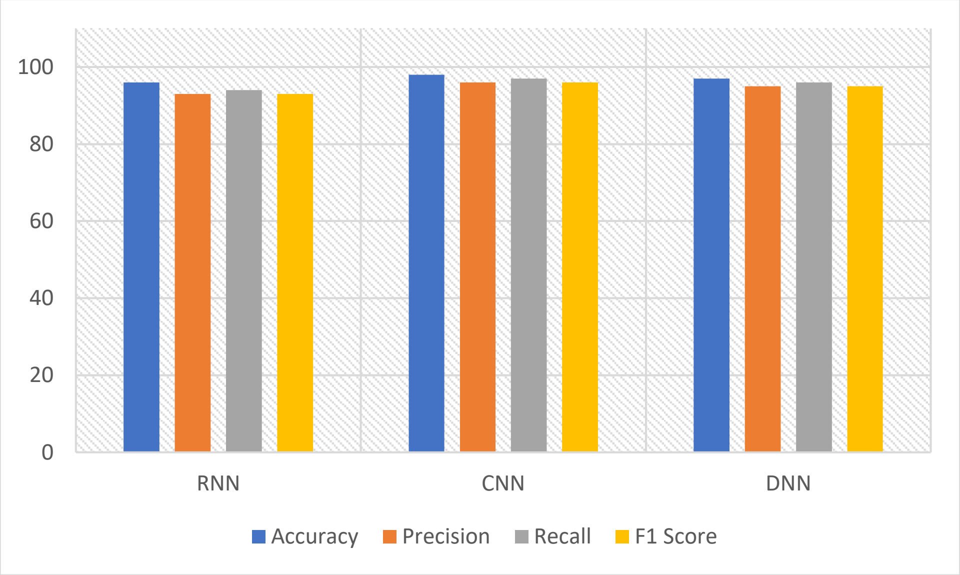

Figure 1Accuracy, Precision, Recall, F1-Score

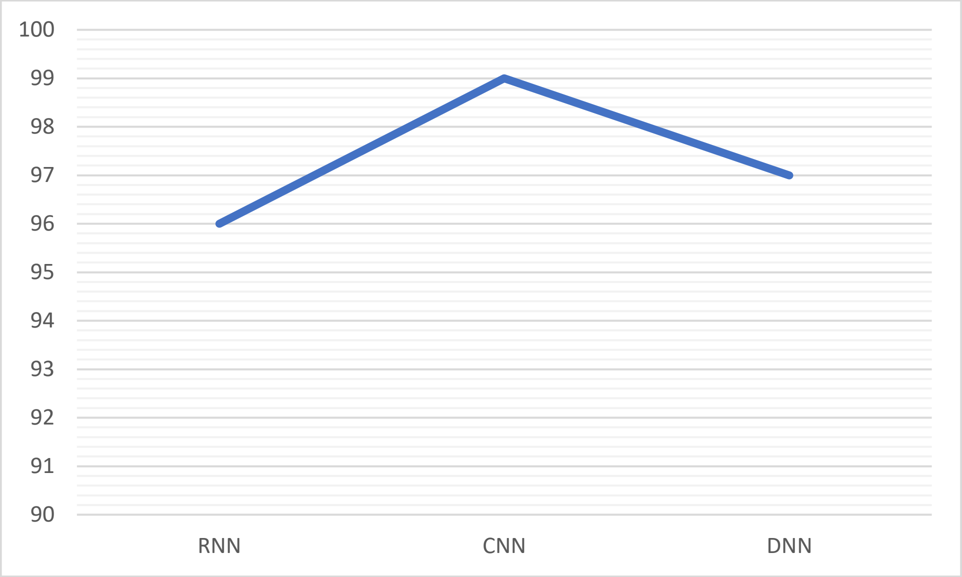

Figure 2 AUC

The three deep learning algorithms, namely RNN, CNN, and DNN, were evaluated for their accuracy, recall, precision, and F1 score in detecting intrusions into cloud computing environments as shown in table-1 and figure-1,2. The results indicated that all three algorithms performed well in these metrics. CNN was able to achieve the highest accuracy score, followed by RNN and DNN.

Conclusion and Future scope

One of the most critical factors that cloud computing environments need to consider when it comes to security is intrusion detection. Traditional systems can't detect advanced attacks in real-time. Deep learning algorithms can help improve the efficiency and accuracy of this security measure. In this study, we proposed a methodology that uses deep learning algorithms, such as RNN, CNN, and Deep Neural Network, to analyze and detect intrusion threats in cloud computing environments. The results of the study revealed that the three algorithms performed well in terms of their accuracy and AUC-ROC score. This shows that deep learning techniques can effectively detect and prevent unauthorized access to cloud computing environments. Various research directions are expected to emerge in the coming years to develop deep learning-based security systems that can effectively detect and monitor intrusion threats in cloud environments. One of these involves developing more complex models that can analyze complex traffic patterns in network data. Another approach is to examine the effects of transfer learning techniques on the performance of the systems in situations where there is limited labeled information. In addition, studies are being conducted on the efficacy of deep learning algorithms in identifying zero-day attacks on cloud computing environments. This method would be useful in addressing the challenges that traditional systems face when it comes to detecting and monitoring intrusion threats in real time. Further studies are being conducted on the integration of deep neural networks with other techniques, such as natural language processing and data visualization. The potential of deep learning algorithms for security has been acknowledged. In conclusion, their accuracy and efficiency in detecting intrusion threats in clouds have great potential. Further research is needed to analyze their applications and enhance the security of such systems.

References

[1] C. Modi, D. Patel, B. Borisaniya, H. Patel, A. Patel, and M. Rajarajan, “A survey of intrusion detection techniques in Cloud,” *J. Netw. Comput. Appl.*, vol. 36, no. 1, pp. 42–57, 2013, doi: 10.1016/j.jnca.2012.05.003.

[2] A. Patel, M. Taghavi, K. Bakhtiyari, and J. Celestino Júnior, “An intrusion detection and prevention system in cloud computing: A systematic review,” *J. Netw. Comput. Appl.*, vol. 36, no. 1, pp. 25–41, 2013, doi: 10.1016/j.jnca.2012.08.007.

[3] K. K. Nguyen, D. T. Hoang, D. Niyato, P. Wang, D. Nguyen, and E. Dutkiewicz, “Cyberattack detection in mobile cloud computing: A deep learning approach,” *IEEE Wirel. Commun. Netw. Conf. WCNC*, vol. 2018-April, pp. 1–6, 2018, doi: 10.1109/WCNC.2018.8376973.

[4] Leila Mohammadpour, Teck Chaw Ling, Chee Sun Liew, and Chun Yong Chong, “CNN for IDS,” pp. 50–55, 2018.

[5] M. Idhammad, K. Afdel, and M. Belouch, “Distributed intrusion detection system for cloud environments based on data mining techniques,” *Procedia Comput. Sci.*, vol. 127, pp. 35–41, 2018, doi: 10.1016/j.procs.2018.01.095.

[6] P. Deshpande, S. C. Sharma, S. K. Peddoju, and S. Junaid, “HIDS: A host based intrusion detection system for cloud computing environment,” *Int. J. Syst. Assur. Eng. Manag.*, vol. 9, no. 3, pp. 567–576, 2018, doi: 10.1007/s13198-014-0277-7.

[7] M. P. K. Shelke, M. S. Sontakke, and A. D. Gawande, “Intrusion Detection System for Cloud Computing,” *Int. J. Sci. Technol. Res.*, vol. 1, no. 4, pp. 67–71, 2012, [Online]. Available: www.ijstr.org.

[8] N. Pandeeswari and G. Kumar, “Anomaly Detection System in Cloud Environment Using Fuzzy Clustering Based ANN,” *Mob. Networks Appl.*, vol. 21, no. 3, pp. 494–505, 2016, doi: 10.1007/s11036-015-0644-x.

[9] P. Mishra, E. S. Pilli, V. Varadharajan, and U. Tupakula, “Intrusion detection techniques in cloud environment: A survey,” *J. Netw. Comput. Appl.*, vol. 77, no. April 2016, pp. 18–47, 2017, doi: 10.1016/j.jnca.2016.10.015.

[10] J. Kim, N. Shin, S. Y. Jo, and S. H. Kim, “Method of intrusion detection using deep neural network,” *2017 IEEE Int. Conf. Big Data Smart Comput. BigComp 2017*, pp. 313–316, 2017, doi: 10.1109/BIGCOMP.2017.7881684.

[11] P. Mishra, E. S. Pilli, V. Varadharajan, and U. Tupakula, “Intrusion detection techniques in cloud environment: A survey,” *J. Netw. Comput. Appl.*, vol. 77, pp. 18–47, 2017, doi: 10.1016/j.jnca.2016.10.015.

[12] G. Loukas, T. Vuong, R. Heartfield, G. Sakellari, Y. Yoon, and D. Gan, “Cloud-Based Cyber-Physical Intrusion Detection for Vehicles Using Deep Learning,” *IEEE Access*, vol. 6, pp. 3491–3508, 2017, doi: 10.1109/ACCESS.2017.2782159.

[13] R. Patgiri, U. Varshney, T. Akutota, and R. Kunde, “An Investigation on Intrusion Detection System Using Machine Learning,” *Proc. 2018 IEEE Symp. Ser. Comput. Intell. SSCI 2018*, pp. 1684–1691, 2019, doi: 10.1109/SSCI.2018.8628676.

[14] S. Moraboena, G. Ketepalli, and P. Ragam, “A deep learning approach to network intrusion detection using deep autoencoder,” *Rev. d’Intelligence Artif.*, vol. 34, no. 4, pp. 457–463, 2020, doi: 10.18280/ria.340410.

[15] F. Farahnakian and J. Heikkonen, “A deep auto-encoder based approach for intrusion detection system,” *Int. Conf. Adv. Commun. Technol. ICACT*, vol. 2018-February, pp. 178–183, 2018, doi: 10.23919/ICACT.2018.8323688.

[16] N. Keegan, S. Y. Ji, A. Chaudhary, C. Concolato, B. Yu, and D. H. Jeong, “A survey of cloud-based network intrusion detection analysis,” *Human-centric Comput. Inf. Sci.*, vol. 6, no. 1, 2016, doi: 10.1186/s13673-016-0076-z.