**State-of-the-art Intrusion Detection Systems (IDS) for Cloud Computing**

Name

Instructor

Course

Institution

Due Date

**Abstract**

Intrusion Detection System (IDS) is a very crucial part of SOC, i.e., Security Operations Center, which plays a huge part in preserving system security for any organization. An IDS monitors a network for any malicious activity or security policy violations. Any such violation is reported and stored within a Security Information and Event Management (SIEM) system. The selected topic focuses on implementing this IDS onto cloud computing. The resulting research paper will initially explain the working of cloud system and then present the implementation of IDS to improve the level of security. Unlike the traditional computing system, cloud computing works on a different platform and uses different kinds of resources resulting in different types of security threats/vulnerabilities. In this state-of-the-art IDS, network traffic is mirrored, which then is inspected by a SOC team which will scan the network for threats. The system uses multiple VMs to inspect the network traffic on a cloud system and detects any lateral movement. Since cloud computing stands for scalability, elasticity, reliability and performance, the state-of-the-art IDS which is mentioned in this topic will satisfy all the mentioned requirements and provide ultimate security.

**State-of-the-art Intrusion Detection Systems (IDS) for Cloud Computing**

**Introduction**

Cloud computing is a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services). This technology allows enterprises to scale their IT resources up or down as business needs change, without incurring the upfront capital expenditure of buying and managing those resources themselves. An intrusion detection system (IDS) is a network security tool that monitors network traffic for suspicious activity and raises an alarm when such activity is detected. IDSs can be deployed as hardware, software, or a combination of both. They can be deployed as a network appliance, a server plugin, or a standalone application.

There are many ways to implement an IDS on cloud computing. One way is to use a network mirroring technique. In this technique, all network traffic is mirrored and then sent to a central location for inspection. Another way is to use multiple virtual machines (VMs) to inspect the network traffic. This can be done by installing the IDS software on each VM. There are many benefits of implementing an IDS on cloud computing. One benefit is that it can help to detect lateral movement of attackers. Another benefit is that it can help to identify unusual or suspicious activity on the network. Additionally, IDS can help to reduce the false positive rate of alerts. There are some challenges of implementing an IDS on cloud computing. One challenge is that the network traffic on a cloud system can be quite dynamic, which can make it difficult to detect suspicious activity. Another challenge is that the IDS system itself can be a target for attack. Additionally, IDS can generate a large number of alerts, which can be difficult to manage.

**Review of Literature**

An article by Wang et al. (2020), titled "Cloud intrusion detection method based on stacked contractive auto-encoder and support vector machine," discusses the use of intrusion detection systems (IDS) in cloud computing. It explains how cloud computing works and how IDS can be used to improve security. IDS monitors network traffic and can detect malicious activity or security policy violations. The article describes how IDS can be used in a cloud computing environment and how it can be used to detect and prevent attacks.

In order to protect cloud computing from malicious attacks, Wang et al. (2020) propose the use of software-defined networking (SDN) to redirect network traffic to an intrusion detection system (IDS). However, traditional IDS systems are not well-suited for detecting unknown attacks in a cloud environment. Anomaly detection systems have been developed to address this issue, but they suffer from a high false alarm rate.

Machine learning techniques have been applied to IDS in order to improve performance, but these approaches still have limitations. Deep learning technology has shown promise for IDS, particularly in the area of feature extraction. The proposed stacked contractive autoencoder (SCAE)–SVM model is designed to extract essential features from raw network data and input them into a shallow classifier for effective identification of attacks. The proposed CIDS framework is designed to redirect network traffic to the SCAE–SVM model for analysis. Experimental results show that the proposed framework is effective in detecting unknown attacks with a low false alarm rate.

The article discusses the use of deep learning technology for intrusion detection in a cloud computing environment. Traditional IDS systems are not well-suited for detecting unknown attacks in a cloud environment. Anomaly detection systems have been developed to address this issue, but they suffer from a high false alarm rate.

The research made use of software-defined networking (SDN) to direct network traffic to an intrusion detection system (Wang et al., 2020). The IDS was then used to detect unknown attacks in a cloud environment. Deep learning technology was used to improve the performance of the IDS by extracting essential features from raw network data. The proposed stacked contractive autoencoder (SCAE)–SVM model is designed to extract essential features from raw network data and input them into a shallow classifier for effective identification of attacks. The proposed CIDS framework is designed to redirect network traffic to the SCAE–SVM model for analysis. Experimental results show that the proposed framework is effective in detecting unknown attacks with a low false alarm rate.

The study found that the proposed stacked contractive autoencoder (SCAE)–SVM model is effective in detecting unknown attacks with a low false alarm rate (Wang et al., 2020). The SCAE–SVM model is designed to extract essential features from raw network data and input them into a shallow classifier for effective identification of attacks. The proposed CIDS framework is designed to redirect network traffic to the SCAE–SVM model for analysis. Experimental results show that the proposed framework is effective in detecting unknown attacks with a low false alarm rate.

The study demonstrates that the proposed SCAE+SVM-IDS model achieves promising classification performance in terms of six metrics compared with three state-of-the-art methods. The proposed SCAE+SVM-IDS approach has shown encouraging performance, but it can be improved by further optimizing the classifier. The SVM classifier cannot effectively recognize some new attacks existing in the testing dataset. Therefore, designing an optimal classifier requires careful consideration in future studies.

In their article “Intrusion detection for cloud computing using neural networks and artificial bee colony optimization algorithm,” Hajimirzaei & Navimipour (2019) propose a new intrusion detection system (IDS) that is based on a combination of a multilayer perceptron (MLP) network, and artificial bee colony (ABC) and fuzzy clustering algorithms. The system is designed to improve upon existing IDS systems by reducing the number of incorrectly classified instances, as well as the MAE and RMSE. The kappa statistic is also improved in the proposed system. The system is verified through the use of the CloudSim simulator and NSL-KDD dataset.

The proposed IDS system seeks to improve upon existing systems by reducing the number of incorrectly classified instances, as well as the MAE and RMSE. The kappa statistic is also improved in the proposed system. The system is verified through the use of the CloudSim simulator and NSL-KDD dataset. The system is designed to function in a cloud computing environment and makes use of ANN, ABC, and fuzzy clustering algorithms. The system is designed to improve the training speed rate by separating the dataset into uniform subsets. The ABC helps the ANN to determine ideal values for linkage weights and biases more quickly. However, the addition of two algorithms to the ANN is costly.

The proposed method uses fuzzy clustering, an ABC algorithm, and a multilayer perceptron (MLP) network. The fuzzy clustering technique is utilized to create various training subsets. The identification of normal and abnormal packets in network traffic is done by the MLP. The features of the NSL-KDD 99 dataset play the main role in creating the structure of the MLP. Moreover, the training of the MLP is done by the ABC algorithm by optimizing the values of linkage weights and biases.

The artificial neural network (ANN) is a computational system inspired by the structure and function of biological neural systems. The ANNs are mostly used in machine learning, classification, and pattern recognition as well as prediction. Input, hidden, and output layers are the three layers of ANN structure. A number of nodes that are defined by the problem type are included in each layer. The linkage weights help each node to connect to nodes in the next layer. Furthermore, the bias weights help a bias node to connect all nodes on that particular layer. The values of the linkage and bias weights between the layers of an ANN structure are updated using one of the optimization algorithms. The weighted inputs at the node and the activation function used affect the output of each node in each layer.

The study found that the proposed IDS outperformed other IDSs with respect to the evaluation criteria. The proposed IDS showed a 2.23% improvement in correctly-classified instances (true positive and false positive), and a decrease in incorrectly classified instances (true negative and false negative). The proposed IDS is a combination of ANN, ABC, and fuzzy clustering. This combination generates a new IDS which is more accurate than other IDSs. The proposed IDS is able to correctly classify instances with a 2.23% improvement, and decrease the amount of incorrectly classified instances. The IDS is also able to produce different training subsets by using the fuzzy clustering method. The IDS is able to discriminate between normal and abnormal packets in network traffic by using the MLP. The ABC algorithm is used to update the values for linkage weights and biases in order to train the MLP. The CloudSim software and the NSL-KDD dataset were used for the simulation. Various evaluation criteria, such as MAE, RMSE, and the kappa statistic, were used to compare similar IDSs with the proposed IDS. The proposed IDS was found to be more accurate than other IDSs with respect to all evaluation criteria.

Currently, most businesses and IT organizations are moving towards cloud computing because of its distributed and scalable nature. However, its open architecture also makes it vulnerable to potential cyber-attacks by intruders. Intrusion Detection Systems (IDS) play a significant role in detecting and preventing such malicious activities in cloud-based systems. In his paper "A review of intrusion detection system in cloud computing," Rani (2019) systematically reviews different IDS detection techniques based on various approaches such as soft computing methods, data mining, and many others. It also provides a combined survey of IDS methods on the basis of signature and anomaly detection approaches, in order to get a clear understanding of the attacks that can be detected, the advantages and challenges of existing methods.

IDS systems can be classified into three types: network-based IDS, host-based IDS, and distributed IDS. Each type has its own advantages and disadvantages, and is suitable for different purposes. For example, network-based IDS is suitable for detecting attacks that target a network as a whole, while host-based IDS is more suitable for detecting attacks that target a specific host. The main advantage of using IDS systems is that they can detect attacks that would otherwise go unnoticed. However, IDS systems also have some disadvantages, such as the high rate of false positives (i.e. when an IDS system incorrectly identifies a legitimate activity as an attack). Another challenge is that IDS systems must be constantly updated to keep up with the ever-changing landscape of attacks. Despite the challenges, IDS systems are an essential part of security measures for cloud-based systems. By constantly improving and updating IDS systems, we can make it more difficult for intruders to successfully launch attacks.

Rani (2019) uses a systematic approach to review different IDS detection techniques. The paper first classifies IDS systems into three types: network-based IDS, host-based IDS, and distributed IDS. The paper then surveys the literature on each type of IDS system, and compiles a list of the advantages and disadvantages of each approach. One limitation of the research is that it does not provide a detailed analysis of each IDS detection technique. Another limitation is that the survey of IDS methods is limited to signature and anomaly detection approaches.

One limitation of the research is that it does not provide a detailed analysis of each IDS detection technique. The authors only provide a general overview of each type of IDS system, and do not go into detail about the specific advantages and disadvantages of each approach. Another limitation is that the survey of IDS methods is limited to signature and anomaly detection approaches. This means that other IDS detection techniques, such as rule-based or heuristic-based approaches, are not discussed in the paper.

The study found that there are many different types of IDS systems, each with its own advantages and disadvantages. The most common types of IDS systems are network-based IDS, host-based IDS, and distributed IDS. Each type of IDS system is suitable for different purposes. For example, network-based IDS is suitable for detecting attacks that target a network as a whole, while host-based IDS is more suitable for detecting attacks that target a specific host.

The advantages and disadvantages of each type of IDS system vary depending on the specific system. For example, network-based IDS systems are typically more effective at detecting attacks than host-based IDS systems, but they can also generate more false positives. The study also found that IDS systems must be constantly updated to keep up with the ever-changing landscape of attacks. This can be a challenge, as it requires ongoing effort and resources. However, the benefits of using IDS systems outweigh the challenges, as they can play a vital role in detecting and preventing attacks. IDS systems are an essential part of security measures for cloud-based systems. However, IDS systems must be constantly updated to keep up with the ever-changing landscape of attacks. This can be a challenge, as it requires ongoing effort and resources.

**Methods**

A qualitative approach was chosen for this research in order to gain a better understanding of the topic at hand and to provide a more comprehensive overview of the state-of-the-art IDSs for cloud computing. A literature review was conducted in order to find relevant articles on the topic. The articles were then critically analyzed in order to extract the main ideas and findings. This qualitative approach allowed for a more in-depth understanding of the topic and the different IDSs that are available for cloud computing.

**Results**

The results of the research showed that there are many different types of IDS systems available for cloud computing. Each type of IDS system has its own advantages and disadvantages. The most common types of IDS systems are network-based IDS, host-based IDS, and distributed IDS. The research also showed that IDS systems must be constantly updated to keep up with the ever-changing landscape of attacks. This can be a challenge, as it requires ongoing effort and resources. However, the benefits of using IDS systems outweigh the challenges, as they can play a vital role in detecting and preventing attacks.

**Conclusion**

In conclusion, the use of intrusion detection systems (IDS) is beneficial for cloud computing environments. However, there are some challenges that need to be considered when implementing an IDS system as discussed in the essay. One crucial challenge is that the network traffic on a cloud system can be quite dynamic, which can make it difficult to detect suspicious activity. Additionally, the IDS system itself can be a target for attack. It is still a challenge that IDS can generate a large number of alerts, which can be difficult to manage. Despite these challenges, IDS systems can play a vital role in detecting and preventing attacks.

**References**

Hajimirzaei, B., & Navimipour, N. J. (2019). Intrusion detection for cloud computing using neural networks and artificial bee colony optimization algorithm. Ict Express, 5(1), 56-59.

Rani, M. (2019, February). A review of intrusion detection system in cloud computing. In Proceedings of International Conference on Sustainable Computing in Science, Technology and Management (SUSCOM), Amity University Rajasthan, Jaipur-India.

Wang, W., Du, X., Shan, D., Qin, R., & Wang, N. (2020). Cloud intrusion detection method based on stacked contractive auto-encoder and support vector machine. IEEE transactions on cloud computing.