Original Article
ISSN (Online): 2350-0530
ISSN (Print): 2394-3629

International Journal of Research - GRANTHAALAYAH
February 2023 11(2), 40–46

PREVENTION AND DETECTION OF INTRUSION IN CLOUD USING HIDDEN MARKOV MODEL

Bhavya Deep [1], Aman Jain [2]

[1] Associate Professor, Department of Computer Science, Bhaskaracharya College of Applied Sciences, University of Delhi, Delhi, India
[2] Student, Department of Computer Science, Bhaskaracharya College of Applied Sciences, University of Delhi, Delhi, India

Received 07 February 2023
Accepted 24 February 2023
Published 28 February 2023

CorrespondingAuthor

Bhavya Deep,
bhavya.deep@bcas.du.ac.in

DOI
10.29121/granthaalayah.v11.i2.2023.5022

Funding: This research received no specific grant from any funding agency in the public, commercial, or not-for-profit sectors.

ABSTRACT

Cloud computing is one of the fast-growing technologies in recent times. People are adopting cloud services often and they do not possess any other substitute for its services. At the same time, users have to be aware of privacy and security issues in the cloud environment. Due to the distributed nature of cloud computing, multi-domain support, and multi-user platform, the cloud-based system is more vulnerable to security threats. Security threats can be distributed denial of service attacks and intrusion prospects. Thus, organizations need to have techniques like intrusion detection as well as prevention, firewalls, encryption, authentication, etc. for securing the stored information on the cloud. Intruders attempt to identify loopholes to break security. For that, organizations are adopting the system for intrusion detection and prevention to provide privacy and security in the cloud environment. Attacks whether internal or external must be prevented and thus it is significant to adopt the technique of preventing and detection system for identifying intrusion. Therefore, this research intends to study the prevention and detection of intrusion in the cloud environment.

Keywords: Intrusion Detection System (IDS), Security, Threat, Cloud Computing, HMM

1. INTRODUCTION

Intrusion Detection System (IDS), also referred to as the 'functionality of firewall' Vinchurkar and Reshamwala (2012), acts as the key element of system security. It is used to identify the activities of the malicious in the computer network. A simple intrusion detection system contains the database, configuration, detector, counter measure, and information system. The intrusion detection system is classified based on the host-based and network-based IDS. The host-based intrusion

How to cite this article (APA): Deep, B., and Jain, A. (2023). Prevention and Detection of Intrusion in Cloud Using Hidden Markov Model. *International Journal of Research - GRANTHAALAYAH, 11*(2), 40–46. doi: 10.29121/granthaalayah.v11.i2.2023.5022

detection system is associated with the audit logs and the data source system calls. It also helps to analyze the binaries, password files and other activities related to the host. In network-based intrusion detection system buffer overflow attacks and denial of service attacks are analyzed. In addition to these, the attacks are detected by the host-based intrusion detection system and the network-based intrusion detection system Hassan (2013). An Intrusion Detection System is today one of the best technologies in network security. Support vector machine (SVM), kernelized support vector machine (KSVM), extreme learning machine (ELM), and kernelized extreme learning machine (KELM) are some of the essential techniques used in the intrusion detection system. The ultimate goal of intrusion detection is to predict security violations in information systems. Data mining is used to maintain and update the models in the intrusion detection system by detecting fraud and fault alarm management Jaiganesh et al. (2013). An IDS protects a system from compromise, attack, and misuse. It helps to monitor the network activity, vulnerabilities of system configurations, analyzing the data integrity, and audit the network. It also has the tendency to monitor, detect and generate the alert.

2. NEED FOR DETECTING INTRUSION IN CLOUD BASED SYSTEMS

IDS is used to detect threats and give more security in the cloud environment. It prevents the distributed denial of service (DDOS) attack in the cloud system. IDS acts as firewall security in which it protects the system from various malicious attacks on the internet. It is used to break in through the firewall security and it also tries to keep the system on the trusted side of security. Moreover, the IDS is used to automate the monitoring process and it also produces reports to the station of management. IDS focuses the network traffic and suspicious activity which activates an alert to the network administrator to prevent the causes. Signature-based intrusion detection systems monitor the packets on the network and detect the malware in an efficient manner. Intrusion detection systems are like software and hardware mechanisms that detect anomalous activities for further investigations Megha and Meniya (2013). IDS has played an important role in grid security management. It is used to detect unknown intrusions, known intrusions, and other kinds of dangerous events, apart from detecting threats and attacks but sometimes it gives false alerts. Grid systems support the security policies for the data grid and help to prevent future attacks inside the computing environment. The IDS systems for service grid integrate resources of node detection in the computing application Kodada (2011). An IDS can help the Cloud Management Platforms (CMPs) to provide secured services. Benefits of CMPs and a comparative study of features provided by major CMPs like OpenNebula, CloudStack, Eucalyptus and OpenStack was done by Bedi et al. (2018).

3. IMPACT OF INTRUSION ON THE PERFORMANCE OF CLOUD BASED SYSTEMS

The cloud computing intrusion detection system is used to integrate knowledge and behaviour analysis to detect intrusions. The computing environment is the target for intruders to exploit. The intruders can use malicious codes to attack the system. Intrusion detection system offers high and additional security measures for these kinds of environment by analyzing the configurations, network traffic, and attack behaviour of the user. IDS can be induced and distributed in the grid and cloud computing environment to provide firewall security. It also has the capability to detect the attack in each node in the cloud-based system. It also alerts every node in the computing environment and this communication creates an impact in the communication mechanisms Ram et al. (2012). Attacks are not visible to host-based intrusion detection systems. The intrusion detection service has used the two approaches such as the performance approach and the information approach. The performance approach is used to compare the user actions to the usual behaviour. The information approach is used to notice certain sequences of actions which also represent an attack. Finally, the intrusion detection system is used to improve energy efficiency and security in the cloud-based environment. Deep et al. (2020) estimated energy consumption of a virtualized server in a data centre.

4. REVIEW OF EXISTING TECHNIQUES FOR INTRUSION DETECTION IN CLOUD BASED SYSTEM

- According to Tayyebi and Bhilare (2015), signature detection, anomaly detection and soft computing-based detection are the techniques used to detect intrusion in the cloud based system. Signature based detection is used to attain high levels of accuracy and it decreases false positives. It acts as an efficient solution to detect known attacks in the cloud. This technique is easy to maintain and update the preconfigured rules. These signatures are associated with several elements which identify the traffic. The signature-based detection techniques are used at both the front end and back end of the cloud to detect external and internal intrusions. It cannot detect an unknown attack in the cloud. Data mining and statistical modeling are different ways to deal with anomaly detection problems. Anomaly detection techniques have the ability to decrease the false alarm for known and unknown attacks. The large numbers of network level and system level events in the cloud are difficult to monitor by using the anomaly detection technique. This is considered as the biggest disadvantage of this anomaly technique. Apart from these techniques, there are many soft computing techniques are artificial neural network (ANN), fuzzy logic, association rules mining, etc. These soft computing techniques are used to improve the efficiency of signature and anomaly detection-based intrusion detection system.
- According to Padmakumari et al. (2014), hot based intrusion detection system (HIDS) and network-based IDS (NIDS) are the major classifications of the intrusion detection system. HIDS are used to monitor the packets to and from individual devices on the network. Further, it determines the system resource accessibility. Apart from these, the NIDS is an intrusion detection system used to analyze the flow of the network and it also determines illegitimate access to a network of computers. It is also used to examine the information from the communication of the network. Authors have listed some of the existing techniques such as SNORT, OSSEC, OSSIM, Suricata, Bro, BASE and Sguil. The Suricata is the open source-based intrusion detection system (IDS) and the Bro technique is the Unix-based IDS.
- Modi et al. (2013) investigated some of the intrusion detection techniques in the cloud. Signature based detection or Misuse based detection, anomaly detection; and many soft computing techniques such as artificial neural network (ANN) based detection, Fuzzy logic-based IDS, Association rule based IDS, Support vector machine (SVM) based intrusion detection system (IDS), Genetic algorithm (GA) based IDS and hybrid technique.

These techniques are used to improve the detection accuracy and the signature-based intrusion detection system efficiency. Anomaly detection technique has the tendency to lower the false alarm rate for unknown attacks. Fuzzy logic-based intrusion detection system is used for quantitative features, and it also provides better flexibility to some problems. SVM based intrusion detection system can handle many massive features and it can correctly classify the intrusion. Genetic Algorithm based IDS has better efficiency which is used for cloud-based system, and it is used to select the correct features for detection.

- Kumar and Naik (2013) investigated the cloud-based intrusion detection system. The authors have focused on two techniques of intrusion detection techniques such as misuse detection systems (MDSs) and Anomaly detection systems. These two systems are used to identify the intrusions most accurately. The misuse detection system is used to recognize known bad behaviour. The expert system, key stroke monitoring, and pattern matching are some of the methods which are used in the misuse detection technique. An expert system is used to separate the rule matching phase from the action phase. This expert system component encodes the attack patterns and known scenarios. Key stroke monitoring act as a simple technique that is used to monitor the keystroke for attack patterns. The pattern matching encodes the known intrusion signatures which are then matched against the audit data. This implementation makes some of the transitions on certain events which are called as labels and the Boolean variables are called as guards which can be placed at each and every transition.
- Raghav et al. (2013) studied intrusion detection and prevention in the cloud environment. The authors have focused on the three techniques of the intrusion detection system in their study. They are misuse or signature-based detection, anomaly based detection and the hybrid detection. The misuse or signature-based detection is extremely accurate for the known attacks. It has the tendency to produce a false alarm. This technique covers the range of unknown attacks. This type of signature is easy to create and understand and it has the ability to detect intrusion and it cannot detect novel attacks. The efficiency of misuse-based detection decreases with the increase of new attacks because the signature based intrusion detection system creates a new signature for new attack. But the anomaly-based detection technique is used to identify the abnormal behavioural patterns on the network. The anomaly detection techniques have the ability to detect novel attacks and it can add new rules without altering the existing ones. The hybrid detection techniques are a combination of the anomaly detection technique and the signature-based detection which is used to detect intrusion in the cloud environment. It is less dependent on the operating environment.
- Shelke et al. (2012) studied the intrusion detection system for cloud computing. The intrusion detection system is used to improve security measures by examining the logs, configurations, and traffic of the network. Traditional intrusion detection systems (IDSs) are not suitable for cloud environments in which the network-based IDS (NIDS) and host based IDSs cannot have the tendency to detect the encrypted node communication. The storage holds behavioural and knowledge-based databases that are used in the cloud environment. The IDS prototype with simulation is used

for real implementation in the cloud environment. The audited data send to the IDS service core which is used to analyze the intrusion of data and alarm. The intrusion detection message exchange format (IDMEF) has been used for communication between the different sensors of the intrusion detection system.

5. PROPOSED TECHNIQUE FOR DETECTION AND PREVENTION OF INTRUSION IN CLOUD

This study examines the Hidden Markov Model which can be used to detect and prevent intrusion in the cloud. This model can reduce false alarm in the cloud environment. Accuracy, false alarm rate, and detection rate are also used to evaluate the performance of the intrusion detection system. Zhang et al. (2020) proposed an IDS using the feature selection method to improve detection accuracy and efficiency. Prasad et al. (2020) presented an IDS technique based on feature selection in their article. Using rough set theory, they reduced the number of features to half of the original set. They demonstrated in their work that feature selection can reduce system complexity while improving system performance. The HMM (Hidden Markov Model) can be deployed as a kind of topology and statistical parameters. It is probable for converting the action of a user into the appropriate dataset and train it. Then the trained data are adopted for further prediction.

The steps followed in the proposed system are:

1) Build a simulation environment for the cloud which involves an active quantity of data centers and users.
2) The transmitter can transmit packets to data center when establishing the cloud environment.
3) Choose the dataset on which testing and training of detecting intrusions is performed.
4) Train the dataset for input after finishing training it will create numerous rules.
5) After that, Hidden Markov Model is started with definite parameters at the broker cloud level or server.
6) Quantity of states involved in the model will rely on the clients in the cloud.
7) After that, the client initiates packet distribution to the data center, then the hidden markov model initiates computing the probability of every packet in the state of transition. At the same time, if any packet probability exceeds the already defined value for the threshold; then a system for rule is developed based on the feature values of the intrusion detection system dataset.
8) And then finally based on the value for the threshold, remove the packets.

A hidden markov model involves 5 tuples:

- S represents the number of states present in the model A {A1, A2, A3, A4, A5…..}
- represents the number of symbols in the observation B {B1, B2, B3, B4, B5….}
- T denotes state probabilities in the transition
- D represents each state's distribution
- Π denotes the initial distribution of the state.

Preliminary probability of transition from one state A1 to another state A2 at a specific occurrence of time e+1 relies on the state at time e based on hypothesis of markov that is.

$$q_{ij} = g\ (q_{e+1} = r_j\ a_e\ r_i)$$

Probabilities of states transition is independent of the original time application where transition occurs based on the fixed hypothesis that is.

$$g\ (a_{e+1} = r_j \mid a_1 = r_i) = g(a_{e+2} = r_j \mid a_1 = r_i)$$

Let n is the number of packets p transmit at a specific transition at specific time occurrence.

Calculate every state transition step which is most probable $a_{ii,}$ $1 \leq i \leq e$ for the observation h_{ii} , $1 \leq i \leq e$, state transition probability δe are computed with the help of viterbi algorithm of hidden markov model.

After every transition step, compute the common probability of every packet to the transferred to every step A.

Average state probability are computed with the help of

$$\delta_{avg} = \sum_{p=1}^{A} \delta z^{(i)}/T$$

Condition is checked that is if the average state of the probability is less that value for threshold then the intrusion is identified in the packet.

6. CONCLUSION

This study examines various techniques used in the intrusion detection of the cloud environment. The study found that the Hidden Markov Model can be used to detect and prevent intrusion in the cloud. It can be used as an alternative option to incorporate the detection and prevention technique into cloud-based environment. In this study, the HMM (Hidden Markov Model) can be deployed as a kind of topology and statistical parameters. It is probable for converting the action of the user into an appropriate dataset and train it. Then the trained data are adopted for further prediction.

CONFLICT OF INTERESTS

None.

ACKNOWLEDGMENTS

The authors are thankful to Bhaskaracharya College of Applied Sciences, University of Delhi for providing necessary infrastructural support as and when required.

REFERENCES

Bedi, P., Deep, B., Kumar, P., and Sarna, P. (2018). Comparative Study of Opennebula, Cloudstack, Eucalyptus and Openstack. International Journal of Distributed and Cloud Computing, 6(1), 37-42 ISSN : 2321-6840.

Deep, B., Mathur, I., and Joshi, N. (2020). Estimated Power Cost Comparison of Physical Server Vs Virtualized Server In A Data Center. International Journal of Advanced Science and Technology, 29(06), 5335-5342.

Hassan, M. M. M. (2013). Current Studies on Intrusion Detection System, Genetic Algorithm and Fuzzy Logic. International Journal of Distributed and Parallel Systems, 4(2). https://doi.org/10.48550/arXiv.1304.3535.

Jaiganesh, V., Mangayarkarasi, S., and Sumathi, P. (2013). Intrusion Detection Systems: A Survey and Analysis of Classification Techniques. International Journal of Advanced Research in Computer and Communication Engineering, 2(4).

Kodada, B. B. (2011). Intrusion Detection System Inside Grid Computing Environment (IDS-IGCE). International Journal of Grid Computing and Applications, 2(4), 27-36. https://doi.org/10.5121/ijgca.2011.2403.

Kumar, P. P., and Naik, B. K. (2013). A Survey on Cloud Based Intrusion Detection System, International Journal of Software And Web Sciences, 4(2), 98-102.

Megha, P., and Meniya, A. (2013). Prevent DDOS Attack Using Intrusion Detection System In Cloud. International Journal of Computers And Applications, 2(3).

Modi, C., Patel, D., Borisaniya, B., Patel, H., Patel, A., and Rajarajan, M. (2013). A Survey of Intrusion Detection Techniques In Cloud. Journal of Network and Computer Applications, 36(1), 42-57. https://doi.org/10.1016/j.jnca.2012.05.003.

Padmakumari, P., Surendra, K., Sowmya, M., and Sravya, M. (2014). Effective Intrusion Detection System for Cloud Architecture. ARPN Journal of Engineering and Applied Sciences, 9(11).

Prasad, M., Tripathi, S., and Dahal, K. (2020). An Efficient Feature Selection Based Bayesian and Rough Set Approach for Intrusion Detection. Applied Soft Computing, 87, 105980. https://doi.org/10.1016/j.asoc.2019.105980.

Raghav, I., Chhikara, S., and Hasteer, N. (2013). Intrusion Detection and Prevention In Cloud Environment: A Systematic Review. International Journal of Computer Applications, 68(24), 7-11. https://doi.org/10.5120/11725-7304.

Ram, S. M., Velmurugan, N., and Thirukumaran, S. (2012). Effective Analysis of Cloud Based Intrusion Detection System. International Journal of Computer Applications and Information Technology, 1(2).

Shelke, K. P., Sontakke, S., and Gawande, D. A. (2012). Intrusion Detection System for Cloud Computing. International Journal of Scientific and Technology Research, 1(4). https://doi.org/10.1504/IJCC.2012.046711.

Tayyebi, Y., and Bhilare, S. D. (2015). Cloud Security Through Intrusion Detection System (IDS) : Review of Existing Solutions. International Journal of Emerging Trends and Technology In Computer Science, 4(6).

Vinchurkar, P. D., and Reshamwala. (2012). A Review of Intrusion Detection System Using Neural Network and Machine Learning Technique. International Journal of Engineering Science And Innovative Technology, 1(2).

Zhang, Z., Wen, J., Zhang, J., Cai, X., and Xie, L. (2020). A Many Objective-Based Feature Selection Model For Anomaly Detection in Cloud Environment. In IEEE Access, 8, 60218-60231. https://doi.org/10.1109/ACCESS.2020.2981373.