IARJSET

ISSN (Online) 2393-8021
ISSN (Print) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

Vol. 8, Issue 6, June 2021

DOI: 10.17148/IARJSET.2021.8626

A Survey on Cloud Security Based on Intrusion Detection System

Geetha T V[1], Deepa A.J[2]

[1]Assistant Professor, Computer Science and Engineering, Ponjesly College of Engineering, Nagercoil, Tamil Nadu

[2]Professor, Computer Science and Engineering, Ponjesly College of Engineering, Nagercoil, Tamil Nadu.

Abstract: Cloud computing is surrounded by many security issues like securing data, and examining the utilization of cloud by the cloud computing vendors. The wide acceptance www has raised security risks along with the uncountable benefits, so is the case with cloud computing. The boom in cloud computing has brought lots of security challenges for the consumers and service providers. This study aims to identify the most vulnerable security threats in cloud computing by multi-layered security using IDS (Intrusion Detection Methods) that provides an average better performance than the single-layered approach. This method will improve the overall performance in execution time of data security.

Keywords: Cloud computing, Cloud Security, Intrusion Detection Method, Artificial Neural Network, Deep Learning, KDD Dataset.

I. INTRODUCTION

1.1 Cloud Security

Cloud computing has become popular in almost all business sectors, like education, healthcare, government, finance. Even though so many advantages are provided by the cloud service providers, security is the major challenging issue in it. NIST defined four different types of cloud, private cloud, public cloud, hybrid cloud and community cloud considering deployment models of cloud. Each of those cloud system requires a strong mechanism for maintain security.

Although several distributed Intrusion Detection Systems (IDSs) have been proposed to monitor and protect large scale networks, their utilization and deployment in Cloud Computing faces many difficulties and is still a challenging task. The security of applications and services provided in Cloud, against cyber attacks, is tough to realize for the complexity, heterogeneity, and dynamic of such systems.

In particular, some challenges that have to be faced by developers, during development and deployment of IDS for Cloud Computing, are presented:

- In traditional distributed system, due to static essence of the monitored infrastructure, the security policies tend to be static, or at least rarely change over time. In a Cloud infrastructure, the monitored virtual networks and nodes are dynamically changed, added, and removed, and their security requirements tend to be different.
- Today the main limit to Cloud adoption is related to the perception of a security loss the customers have Customers have security requirements, which have to be granted by Cloud providers. Therefore, the Cloud provider should offer service and tools to assess and monitor the implemented security requirements.
- The recent researches have provided evidence that most of the intruders come from insiders. Therefore, Cloud providers got to know if their systems and infrastructure is employed by 'legitimate' users to penetrate other Cloud victims.
- In traditional systems, the security policies are usually established and managed by a security administrator responsible for the whole system. The Cloud federation has several system security administrators, which adopt different policies and mechanisms to guard their Cloud infrastructure.
- The shared infrastructure and virtualization technology put more vulnerability on Cloud Computing.
- Finally, lack of collaboration among different Cloud providers for detection of attacks is another drawback to current proposed approaches. Creating comprehensive distributed database to be used for detection issues is another major requirement in order for IDSs act as a comprehensive defence mechanism in the federated Clouds.

Both Cloud providers and customers will benefit significantly if there is a comprehensive IDS that evolves on the base of their requirements. The IDS components have to be easily integrated in different layers of the Cloud environment and

IARJSET

ISSN (Online) 2393-8021
ISSN (Print) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

Vol. 8, Issue 6, June 2021

DOI: 10.17148/IARJSET.2021.8626

cale without losing any functionality. Therefore, proposing a collaborative and distributed framework that considers the different Cloud security requirements is the motivation in this work.

1.2 Intrusion Detection System

An Intrusion Detection System (IDS) is designed to identify any doubtful pattern when a system or a network is attacked by someone who tries to interrupt in. It performs a spread of functions, which include monitoring the user and system activities, auditing system configurations for vulnerabilities and misconfigurations, accessing the integrity of critical system and data files, recognizing known attack patterns within the system activity, and identifying abnormal activities through statistical analysis. IDS are commonly classified as Network Intrusion Detection Systems (NIDS) and Host-based Intrusion Detection Systems (HIDS). It is also probable to classify IDS using detection approach. They are signature-based detection and anomaly-based detection.

Signature-based

Signature-based IDS indicates the detection of attacks by searching specific patterns, like byte sequences in network traffic, or known malevolent instruction sequences worn by malware. It start off from anti-virus software, which demotes to the detected patterns as signatures. Even though signature-based IDS can effortlessly detect known attacks, it is tricky to detect fresh attacks, for which there is no available pattern.

Anomaly-based

Anomaly-based intrusion detection systems were chiefly introduced to detect unknown attacks, in some measure due to the swift development of malware. The vital approach is to apply machine learning to form a model of trustworthy doings, and then match up to new behaviour against this model. Since these models can be qualified according to the applications and hardware configurations, machine learning based scheme has a better comprehensive property in evaluation to traditional signature-based IDS. This approach facilitates the detection of prior unknown attacks. It may endure from false positives, previously unknown legitimate activity may also be classified as malicious. Most of the available IDSs suffer from the time-consuming during detection process that demeans the performance of IDSs. Efficient feature selection algorithm crafts the classification process used in detection more trustworthy.

II. FEATURE SELECTION

Gnanaprasanambikai et al., [1] use Principle Component Analysis method is used for feature extraction. PCA is a linear method in dimensionality reduction for data analysis and compression. It is based on transforming a relatively large number of uncorrelated features by finding a orthogonal linear combinations of the original features with the largest variance. Wei Wang et al., [6] propose HAST-IDS, which uses deep neural networks that can automatically learn hierarchical spatial-temporal features directly from raw network traffic data. Also it uses CNNs to learn the spatial features of network packets and then uses an LSTM to learn the temporal features among multiple network packets. As a result, it obtains more accurate spatial-temporal traffic features.

Pankaj Kumar et al., [12] use a hybrid Meta heuristic algorithm for feature selection. Girish Chandrashekar et al., [14] mention two methods for feature selection. First is a Filter method that use Correlation criteria and Mutual Information (MI) use variable ranking techniques as the principle criteria for variable selection by ordering. Ranking methods are applied before classification to filter out the less relevant variables. The feature relevance property provides a measurement of the feature's usefulness in discriminating the different classes. Second is Wrapper method that use Sequential selection algorithms and Heuristic search algorithms use the predictor as a black box and the predictor performance as the objective function to evaluate the variable subset. Verónica et al., [15] suggest the use of filters since they are independent of the induction algorithm and are faster than embedded and wrapper methods, as well as having good generalization ability. Gang Koua et al., [16] use multiple criteria decision-making (MCDM) based methods for evaluating feature selection methods with 10 feature selection methods. They are document frequency (DF), information gain(IG), Gini index(GI), distinguishing feature selector (DFS), expected cross-entropy (ECE), class discriminating measure (CDM), Chi-squared (CHI), odds ratio (OR), mutual information (MI), and weighted log likelihood ratio (WLLR). Among all these methods DF method results good effectiveness of the used MCDM-based methods.

III. PREPROCESSING

Revathi et al., [7] use hybrid Simplified Swarm Optimization (SSO) algorithm to pre-process the information. SSO may be a simplified Particle Swarm Optimization (PSO) that features a self-organizing ability to emerge in highly distributed control problem area, and is flexible, strong and price effective to resolve complex computing environments. It recognize not only known attacks but also filters noisy and irrelevant data which will result on knowledge Discovery and data processing (KDDCup 1999) dataset and compared to a new hybrid Partial Swarm Optimization with Random Forest (PSO-RF) and with other benchmark classifiers. The testing result shows that the projected method affords competitively elevated detection rates and bring into being a close to finest solution.

IARJSET

ISSN (Online) 2393-8021
ISSN (Print) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

Vol. 8, Issue 6, June 2021

DOI: 10.17148/IARJSET.2021.8626

Srikanth Yadav et al., [8] presents a knowledge preparation and data pre-processing framework to support deep learning and network security experts in producing qualitative data for empirical experimental analysis of intrusion detection data. The One hot encoder and min-max normalization approaches are used in this proposed pre-processing module. This research paper focuses totally on analyzing two datasets, specifically KDD Cup' 99, and NSL-KDD datasets, which are commonly wont to investigate network intrusion detection. Jonathan et al., [9] presents Pre-processing techniques from data mining, including data transformation, cleaning, reduction, and discretization. A data reduction technique often used with the KDD Cup 99 dataset was principal component analysis (PCA). PCA was found to greatly reduce the data dimensionality, thereby reducing the computational requirements of the NIDS.

Jayshree Jha et al., [10] give a completely unique approach to pick best feature for detecting intrusion. The proposed approach is predicated on hybrid approach which mixes filter and wrapper models for choosing relevant features. Shon et al., [2] use a preliminary feature selection process using GA is provided to select more appropriate packet field.

Olamantanmi et al., [11] propose an ANN based IDS developed and evaluated on UNSW-NB15 intrusion detection dataset. Binarization and discretization technique was used on continuous attributes and Gain ratio in ranking attributes. This model gives an accuracy of 76.96% and MCC of 0.57 which shows a direct correlation.

Pankaj Kumar et al., [12] use grey wolf optimisation (GWO) is hybrid with a crow search algorithm (CSA), for feature selection which extracts relevant features from the cloud network connection to be processed more effectively.

IV. CLASSIFICATION

Gnanaprasanambikai et al., [1] generate decision rules from other classification models algorithms such as Ripper Algorithm, PART Algorithm and C4.5 decision rule generating algorithm are analyzed and c4.5 Algorithm is selected as suitable for problem solving.

Shon et al., [2] proposes a Machine Learning Model using a modified Support Vector Machine (SVM) that combines the benefits of supervised and unsupervised learning.

Ozgur et al., [3] proposed detection model uses J.48 decision tree algorithm to classify various types of attacks and a rule-based Decision Support System (DSS) is also developed for interpreting the results of both anomaly and misuse detection modules. The new hybrid approach gives better performance over individual approaches.

Chen et al., [4] uses RST (Rough Set Theory) and SVM (Support Vector Machine) to detect intrusions. First, RST is used to pre-process the data and reduce the dimensions. The features selected by RST are sent to SVM model to learn and test respectively. This method effectively decreases the space density of data.ng. It use a preliminary feature selection process using GA is provided to select more appropriate packet field.

Ganapathy et al., [5] provides an intelligent multi level classification technique for effective intrusion detection in Mobile Ad-hoc Networks. The algorithm uses a mixture of a tree classifier which uses a labeled training data and an Enhanced Multiclass SVM algorithm. Moreover, an efficient preprocessing technique has been proposed and implemented during this add order to enhance the detection accuracy and to scale back the time interval.

Pankaj Kumar et al., [12] use a Deep Sparse Auto-Encoder (DSAE) for classification purpose.

Gurbani et al., [13] describes GWO is used to optimize ANN. KDD-99 data-set is used to classify various types of attacks i.e. denial of service (DOS), normal and other attacks. It provides detailed analysis about the performance of Artificial Neural Network and optimized Artificial Neural Network with GA, PSO and GWO.

V. CONCLUSION

This paper compares various algorithms based on Feature Selection, Pre-processing and Classification. It shows in order to achieve efficient security on cloud environment intrusions must be identified based on anomaly based attacks using the hybrid methods in Feature selection and Classification of Intrusion detection methods.

REFERENCES

[1]. L. Gnanaprasanambikai and Nagarajan Munnusamy , “Data Preprocessing and Classification for Traffic Anomaly Intrusion Detection using NSLKDD Dataset”, International Journal of Pure and Applied Mathematics Volume 119 No. 10 2018, 847-858.
[2]. T.Shon, Y.Kim, C.Lee & J.Moon, “A Machine Learning Framework for Network Anomaly Detection svm & ga”, Proceedings of ieee, 2005
[3]. Ozgur Depren, Murat Topallar, Emin Anarim, M. Kemal Ciliz, “An intelligent intrusion detection system (IDS) for anomaly and misuse detection in computer networks”, Expert Systems with Applications, November 2005, Pages 713-722.
[4]. R.C. Chen, K.F Cheng and C. F Hsieh, “Using support vector machine and rough set for network intrusion system”, 2009.
[5]. S. Ganapathy, P. Yogesh, and A. Kannan , “An Intelligent Intrusion Detection System for Mobile Ad-Hoc Networks Using Classification Techniques”, PEIE 2011, CCIS 148, pp. 117–122, Springer-Verlag Berlin Heidelberg 2011.
[6]. Wei Wang , Yiqiang Sheng , Jinlin Wang , Xuewen Zeng , Xiaozhou Ye , Yongzhong Huang and Ming Zhu, “HAST-IDS: Learning Hierarchical Spatial-Temporal Features Using Deep Neural Networks to Improve Intrusion Detection”.
[7]. S. Revathi, Malathi, “Data Preprocessing for Intrusion Detection System using Swarm Intelligence Techniques”, International Journal of Computer Applications (0975 – 8887) Volume 75– No.6, August 2013.

IARJSET

ISSN (Online) 2393-8021
ISSN (Print) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

Vol. 8, Issue 6, June 2021

DOI: 10.17148/IARJSET.2021.8626

[8]. M Srikanth Yadav, R Kalpana, "Data Pre-processing for Intrusion Detection System Using Encoding and Normalization Approaches", IEEE 11th International Conference on Advanced Computing (ICoAC), 2019.
[9]. Jonathan J. Davis, Andrew J. Clark, "Data pre-processing for anomaly based network intrusion detection: A review", Computers & Security Elsevier, 2011.
[10]. Jayshree Jha, Leena Ragha, "Intrusion Detection System using Support Vector Machine", International Journal of Applied Information Systems (IJAIS) International Conference & workshop on Advanced Computing, 2013.
[11]. Olamantanmi Mebawondua, Olufunso D.Alowolodub, Jacob O.Mebawondua, Adebayo O.Adetunmbi, "Network intrusion detection system using supervised learning paradigm", Science Africian, Elsevier, 2020.
[12]. Pankaj Kumar Keserwani ,Mahesh Chandra Govil &Emmanuel S. Pilli, "An Optimal Intrusion Detection System using GWO-CSA-DSAE Model", Journal Cyber-Physical Systems.
[13]. Gurbani Kaur, Dharmender Kumar , "Classification of Intrusion using Artificial Neural Network with GWO", International Journal of Engineering and Advanced Technology (IJEAT) ISSN: 2249 – 8958, Volume-9 Issue-4, April 2020.
[14]. Girish Chandrashekar, Ferat Sahin, "A survey on feature selection methods", Computers and Electrical Engineering, 2013.
[15]. Verónica Bolón-Canedo, Noelia Sánchez-Maroño & Amparo Alonso Betanzos, "A review of feature selection methods on synthetic data", Knowledge and Information Systems An International Journal, Springer, 2015.
[16]. Gang Koua, Pei Yanga, Yi Pengb, Feng Xiaoa, Yang Chena, Fawaz E Alasdair, "Evaluation of feature selection methods for text classification with small datasets using multiple criteria decision-making methods", Applied Soft Computing Journal, 2020.