Development of an Efficient Network Intrusion Detection System for Cloud-based Networks using Selected Data Mining Algorithms

Olatunde Yinka Olagunju
Department of Computer Science,
Faculty of Computing and
Digital Technologies,
Redeemer's University,
Ede, Osun State, Nigeria

Bosede Oyenike Oguntunde
Department of Computer Science,
Faculty of Computing and
Digital Technologies,
Redeemer's University,
Ede, Osun State, Nigeria

Samson Afolabi Arekete
Department of Computer Science,
Faculty of Computing and
Digital Technologies,
Redeemer's University,
Ede, Osun State, Nigeria

Adewale Opeoluwa Ogunde
Department of Computer Science,
Faculty of Computing and
Digital Technologies,
Redeemer's University,
Ede, Osun State, Nigeria

ABSTRACT
An efficient intrusion detection system is required since more and more networks are connecting to the internet, which has increased the amount of cyberattacks. For an additional layer of security in a cloud environment, intrusion detection techniques must be used in addition to preventive defense methods like firewalls. There are numerous intrusion detection methods and deciding one to use for implementation could be difficult because they all have different features yet share some capabilities in terms of efficiency and accuracy of detection. It is crucial to evaluate how these methods perform. The performance of five data mining algorithms for intrusion detection in a cloud environment was analyzed in this work, and the technique was implemented with excellent results. The Intrusion detection techniques examined in this work are Naive Bayesian (NB), Decision Tree, Support Vector Machine (SVM), K-Nearest Neighbor Classifier (KNN), and Random Forest. The Naïve Bayesian, Decision Tree, Support Vector Machine, K-Nearest Neighbor were trained on NSL-KDD dataset contained 148,517 records in total, of which 80% were used for training and 20% for testing. The analyses were carried out using python's scikit-learn, a powerful library for machine learning that offers a variety of effective tools for machine learning, Jupiter Notebook, a platform for sharing computational documents, Python V-3 Environment, and Anaconda Navigator, a graphical user interface (GUI) that makes it simple to launch programs and manage packages without having to use command-line commands. With an accuracy of 99.68 percent, Random Forest outperformed other algorithms, while Decision Tree, K-Nearest Neighbor, Naive Bayes, and Support Vector Machine had accuracy values of 99.47 percent, 99.17 percent, 90.67 percent, and 96.43 percent, respectively. The Python user interface (UI) module for the model was implemented as an Application Programming Interface (API) utilizing Sklearn modules and PyQt5. On a network server, the Intrusion Detection System under test distinguished between normal and abnormal network traffic. According to the type of attack, abnormal traffic is further categorized. The system will be monitored by this intrusion detection system, which can identify normal and abnormal activities. The best technique that performed better than the others were used to develop a predictive model using Python to implement Random Forest (i.e. a classifier) in a cloud environment, which helped to identify possible attacks on the network. This work presented an intrusion detection system utilizing five data mining techniques.

Keywords
Cloud, network, Random Forest, intrusion detection, classification.

1. INTRODUCTION
The massive volumes of data generated every day, as well as the rising interconnection of the world's internet infrastructures, has increased the number of security vulnerabilities found by security professionals each month. Cyber thieves can exploit these security flaws to get access to these infrastructures and carry out destructive operations. Peeping, snooping, and spying into locations are all examples of intrusion. Network infiltration refers to any unwanted behavior on a digital network, which frequently entails stealing valuable network resources and jeopardizing network and data security. Data mining is simply the practice of extracting useable information from a larger set of any raw data in order to identify knowledge in the data. Using one or more software programs, the data patterns are evaluated in huge batches [1]. Every company wants to employ data mining technologies to extract hidden yet useful facts from their data. Data mining has been used to extract implicit, previously unnoticed, and relevant information from enormous volumes of data for many years. It's frequently used to make predictions based on a knowledge pattern. Using algorithms and techniques, data mining is the process of obtaining information from large data sets [2].
Cloud computing refers to the on-demand availability of computer system resources, such as data storage and processing power, without the user having to manage them directly. The term is commonly used to characterize data centers that are accessible to many people via the internet and are primarily

used to supply computer services. Virtualization is the technology, while cloud is the environment. Data mining is a technique for cleaning, categorizing, and analyzing vast amounts of network data. Since there is a significant amount of network traffic that needs to be analyzed, the researcher uses data mining techniques. Numerous data-mining approaches, including clustering, classification, and association rules, have shown to be useful for analyzing network traffic. Cloud computing is becoming more widely accepted, and it is gaining traction in the scientific and industrial areas [3].

Cloud computing is the first among the top ten most important technologies, with a better outlook for companies and organizations in the coming years. Network access to a pool of configurable computer resources (such as networks, servers, storage, applications, and services) is provided via cloud computing. These resources can be quickly provided and released with little administrative effort or service provider interaction. By seeing all computer resources as services and supplying them via the internet, cloud computing, which is both a computational paradigm and a distribution architecture, aims to deliver secure, quick, and convenient service [4], [5]. Collaboration, agility, scalability, availability, the capacity to respond to demand variations, the ability to accelerate development work, and the possibility for cost savings through streamlined and efficient processing are all benefits of the cloud [6]. Cloud computing is a relatively new type of computing. There is a lot of doubt regarding how security can be achieved at all levels (network, host, application, and data) and how applications security can be migrated to Cloud Computing [7]. Because of this uncertainty, information executives have frequently stated that security is their top concern with cloud computing [8]. External data storage, reliance on the public internet, lack of control, multi-tenancy, and integration with internal security are all security risks. When compared to traditional technologies, the cloud has a few distinct characteristics, such as its large scale and the fact that cloud provider resources are completely distributed, heterogeneous, and virtualized. In their current state, traditional security mechanisms such as identity, authentication, and authorization are no longer enough for clouds [9].

1.2 System Overview and Problem Description

In addition to automatically creating the value for categorizing network activity and identifying cyberattacks, the concept proposed a method for achieving accurate and reasonable results in IDS, hence reducing false positives and false negatives in the network. To achieve the desired results, this study will make use of the NSL-KDD dataset and data mining techniques. The NSL-KDD dataset will be used for testing, 80% of the dataset is used to train the model while the remaining 20% of the dataset being used to test and verify the model. A pre-processing stage is necessary to convert the dataset into the format required for classifier and intrusion detection. An open-source Python utility that has many algorithms were utilized. Data preparation, data pre-processing, and intrusion detection using classifiers are the three procedures needed to assess the acquired data in order to detect intrusions. The NSL-KDD datasets provided for this project will be used in two categories, as proposed by [10], [11]: training and testing. The five classification techniques used for the classification and identification of attacks that can intrude in virtualized cloud settings are K-Nearest Neighbor Classifier, Random Forest, Naïve Bayesian, Decision Tree and Support Vector Machine (SVM). The behavior of the attacker will be classified as normal or abnormal.

As network attacks have become more frequent and severe in the cloud over the past few years, intrusion detection is becoming a more crucial aspect of network security. Security of networking systems have been an issue since computer networks became prevalent. Intrusions pose significant threats to the integrity, confidentiality and availability of information for the internet users [12]. In recent years, there has been an upsurge in both passive and active attacks in cloud computing. To maintain the integrity of network facilities, efforts aimed at detecting such intrusions are required. Eavesdropping, traffic analysis, and port scanning are examples of passive assaults [13].

Active assaults compromise the confidentiality, integrity, and accessibility of the virtualized cloud infrastructure, causing the targeted system to malfunction. In the cloud, a variety of strategies have been used to identify intrusions. Each has its own unique characteristics and operational capabilities. It becomes difficult to choose which strategies to use for implementation. As a result, assessing the performance of these algorithms is critical. The purpose of this study is to evaluate the effectiveness of a selected of these algorithms in order to create an intrusion detection system based on data mining for cloud environments [13].

2. LITERATURE REVIEW

A computer paradigm known as "cloud computing" involves connecting numerous devices via private or public networks to provide a dynamically scalable infrastructure for application, data, and file storage [14]. The cost of computing, application hosting, content storage, and dissemination has greatly reduced since the inception of this technology. Cloud computing is a practical approach to save money right away, and it can transform a data center from a capital-intensive to a variable-cost configuration. The premise of "reusability of IT skills" underpins the cloud computing paradigm. Cloud computing, unlike traditional concepts like "grid computing," "distributed computing," "utility computing," or "autonomic computing," broadens horizons across organizational boundaries.

Cloud Computing security measures are, for the most part, the same as security controls in any other IT system. Cloud computing, on the other hand, may provide different risks to an organization than traditional IT solutions due to the cloud service models used, the operational models used, and the technologies used to allow cloud services. Unfortunately, including security into these systems is frequently mistaken for making them more inflexible [15]. Moving key apps and sensitive data to public cloud settings is a major concern for companies that are expanding their network beyond their data center's management. To allay fears, a cloud solution provider must demonstrate that customers' apps and services will continue to have the same security and privacy controls, present evidence to customers that their company is secure and can meet service-level agreements and prove compliance audits. Identifying the primary vulnerabilities in these types of systems, as well as the most serious dangers reported in the Cloud computing audits literature [16]. These malicious behaviors can harm data, information, and the network to varying degrees, such as data and information loss, data integrity breach, denial of permitted network services, and so on. As a result, harmful activities must be dealt with in order to safeguard the integrity of data, information, and networks, making intrusion detection and prevention essential.

3. METHODOLOGY

3.1 Methodology

Data mining is a technique used to obtain valuable features from many datasets or unstructured data [17]. Using this data

mining technique, patterns can be grouped and the relation between the data can be classified [18]. Based on the patterns, the model or framework can be built where it helps for prediction. Researchers use data mining in most fields like education, medicine, business, weather prediction, cyclone, and building customer relationships [19]. Some essential concepts relating to network intrusion detection including dataset as well as methods of implementing are discussed in this section.

3.2 Data Collection

The University of New Brunswick's website (https://www.unb.ca/cic/datasets/nsl.html) is where all the NSL-KDD dataset can be downloaded. KDD CUP 99 has been improved with the NSL-KDD data set. For the classifiers to generate an unbiased output, redundant records are eliminated. The train and test data sets both include an adequate number of records, which allows experiments to be carried on the entire set. Further analysis of the KDD Train + data set has exposed one of the very important facts about the attack class network vectors. 80% to train, 20% to test. As a result, evaluation findings from various research projects will be comparable and consistent. Algorithms were used. A dataset is used to perform a data mining technique based on a classification method, and there are several steps involved.

3.3 The Classification Flowchart of the Intrusion Detection System

Figure 3.1 shows a flow diagram of the intrusion detection and classification process. The output is the result of the prediction as normal or abnormal attack.

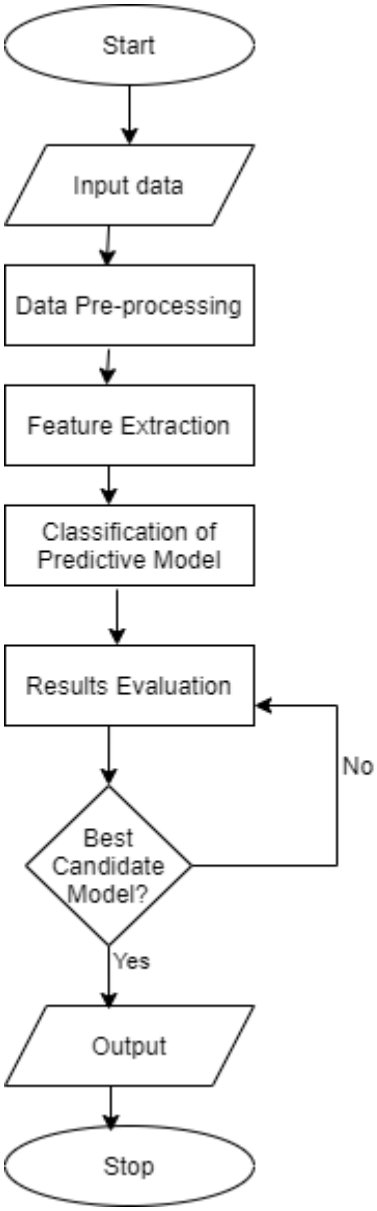

Figure 3.1: Flow diagram of detection and classification

The decision boundary rule determined which class an input belongs to which is based on the model's output. The model classify network as normal or attack. The decision box receives the model's output which is usually a probability or score, compares these probabilities, predicts and further makes the final classification of the intrusion as normal or abnormal.

3.4 Training and Testing

The test set was created to evaluate the algorithms' capacity to predict classifications while the training set was created to teach the algorithm how to make predictions. Decision Tree, K-Nearest Neighbor, Naive Bayes, Random Forest, and Support Vector Machine are some of the data mining techniques that will be utilized to model the classification and prediction of the intrusion detection in a virtual environment.

3.5 Dataset Evaluation

There are many various metrics for different algorithms, and these measures were created to evaluate various aspects. So, it ought to be a criterion for assessing different strategies that have been offered.

3.6 System Design of The Intrusion Detection System

The process flow diagram for intrusion detection and classification is shown in Figure 3.1. which makes the system design clearer and more convincing showed the architecture of the system, the flow of the data and the way each of the components work together to detect network intrusions in a cloud environment.

3.6.1 Classifiers used for the Intrusion Detection System

1. Decision Tree J48
2. Naïve Bayesian
3. K-Nearest Neighbor (K-Star)
4. Random forest
5. Support Vector machine

3.6.2 Evaluation parameters of the Intrusion Detection System

This is an essential aspect of the project that deals with parameters for evaluating the various classification techniques. The model may give satisfying results when evaluated using a metric like accuracy score but may give poor results when assessed against other metrics such as logarithmic loss or any other such metric. Furthermore, classification accuracy is utilized to measure how well the techniques perform. However, it is not enough to truly compare the techniques. The various parameters considered are classification accuracy, execution time (speed), error rate, confusion matrix and area under curve.

3.6.3 Confusion matrix

Confusion Matrix gives us a matrix as output and describes the complete performance of the technique. There are four important terms:

1. **True Positives:** The cases in which the algorithm predicted YES, and the actual output was also YES.
2. **True Negatives:** The cases in which the algorithm predicted NO and the actual output was NO.
3. **False Positives:** The cases in which the researcher predicted YES, and the actual output was NO.
4. **False Negatives:** The cases in which the researcher predicted NO and the actual output was YES.

The metrics given below were used to evaluate the model's performance.

i. **Accuracy** is defined as the proportion of samples that were correctly classified to all samples. When the dataset is balanced, accuracy is an appropriate metric. Accuracy may not be the best metric because in real network systems, normal samples are much more common than abnormal samples.

$$Accuracy = \frac{TP+FP}{TP+TN+FP+FN} \quad (3.1)$$

ii. **Precision (P)** is a measure of the accuracy of attack detection and is defined as the ratio of true positive samples to predicted positive samples.

$$\Pr ecision = \frac{TP}{TP+FP} \quad (3.2)$$

iii. **Recall (R)** is also known as the detection rate, and it is defined as the proportion of samples that are truly positive to all positive samples. The detection rate, a crucial IDS metric, shows how well the model can identify attacks.

$$Recall = \frac{TP}{TP+FN} \quad (3.3)$$

iv. **F-measure (F)** is referred to as the precision and recall's harmonic average.

$$F = \frac{2*P*R}{P+R} \quad (3.4)$$

3.6.4 Hardware Resources

The hardware configuration for the computer system that was used for the implementation of this study is shown in Table 3.1. The Jupiter Notebook Graphical User Interface (GUI) is the Cloud Resources.

Table 3.1: Computer Hardware Configuration

Configuration	Value
System manufacturer	DESKTOP-1KTCV15
System type	32-bit CPU, 64-bit operating system
Processor	2.00GHz Intel(R) Core (TM) i5-5005u CPU
Installed memory (RAM)	8.00GB
Operating system	Windows server 2016 (10 pro)
GUI	Jupiter Notebook

4. RESULTS

This section presents the description of data, implementation procedure, results of the study, metrics that define the outcome of the model and comparison of the model with related studies used as benchmarks.

4.2 Data Preprocessing

Data preprocessing is the first step to be carried out before initializing the process. Data preprocessing is basically used to transform and convert raw and unfiltered data into a much more suitable and understandable format. Typically, real world data might be incomplete, inconsistent, inaccurate, unstructured form and might also have some errors and missing values. Data preparation is done to get around all of this. It assists in preparing the raw data for use in creating machine learning models by helping to clean, format, and organize it. Data Preprocessing cannot be conducted into a single process hence it is distributed among several steps. The steps involved in data preprocessing [20].

4.2.1 Import libraries

The various libraries required to build a model were firstly imported before the programming. A library is primarily a collection of modules that can be called and used. Libraries is a collection of functions and methods which allows us to perform many actions without writing any code.

4.2.2. Import the dataset

Numerous datasets are available in CSV format. Data can be stored in tabular format using CSV files, which allow for comma-separated values based on the Network Intrusion Detection system.

4.2.3. Checking missing values

To fill the missing values, simply delete the entire row or replace the missing value with some sensible data.

4.2.4. Encoding categorical data

Text-based data cannot be processed by the computer since it is not understandable. It is required to transform categorical data into numerical data format since the models and systems rely on mathematical equations and calculations. The data was converted into numerical format using sklearn library and used its Label Encoder to conduct the process.

4.2.5. Splitting the dataset into a test set and a training set

After the data has been converted, the dataset must be divided into two sets: a training set and a testing set. Data train on machine learning model in training set. Then learning model will try to understand any correlations in training set and then test the model on testing set to check how accurately it can predict.

4.3 Model Evaluation

Model Evaluation is an integral part of model development process in machine learning. It helps to find the best model that represents the dataset and how well the chosen model will work in near future. For the dataset, selected five classification techniques such as: This section evaluates the selected data mining models for intrusion detection in cloud environment.

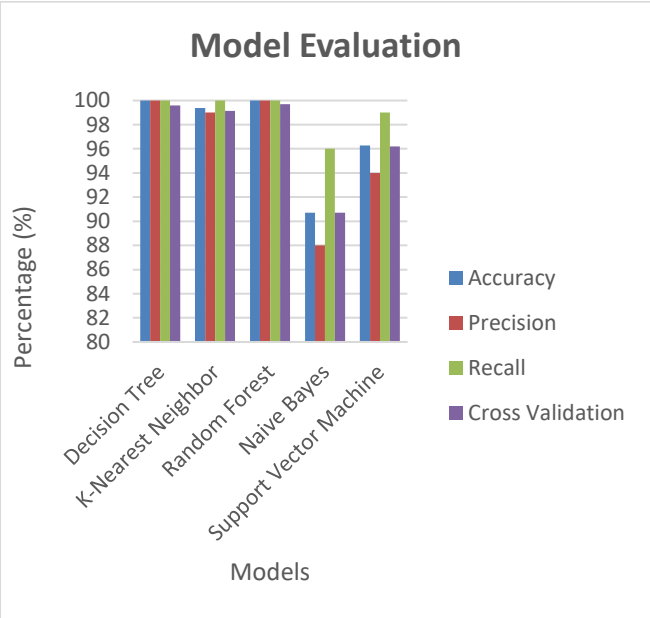

Figure 4-1: Performance summary of Model Evaluation

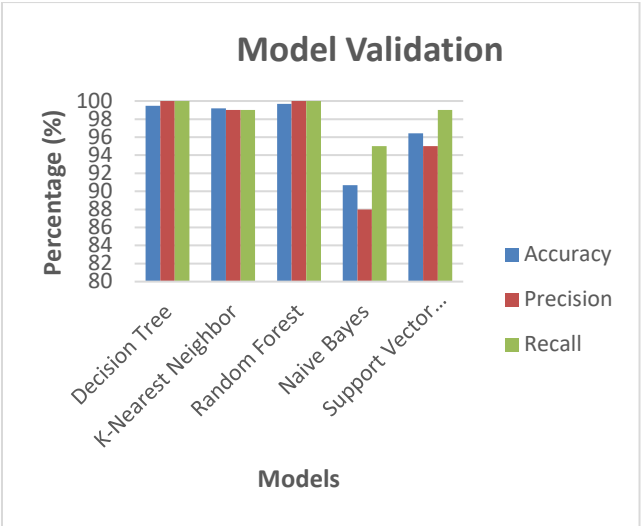

Figure 4-2: Performance summary of Model Validation

5. ILLUSTRATION OF THE IMPLEMENTATION AND APPLICATION INTERFACE

The model was deployed in the form of a cloud prediction service for real-time intrusion detection using Sklearn Machine Learning libraries and pyqt5 for its graphical UI module in python. Random forest from Model Validation input data with 99.68% accuracy. The model was trained using data from the UCI archive's NSL-KDD dataset. The Intrusion Detection Python Application that was running on a local server. This application app.py is running on a static host. When the internet is connected and a web browser is launched, the loopback internet protocol address (IP) at http://127.0.0.1 at port 5000 will display the intrusion detection cloud prediction interface where datasets entries will accurately predict, classify and detect different intrusions.

A function that maps an input to an output must be learned using examples of input-output pairs in this supervised learning (SL) problem. This implementation uses labeled training data, which consists of a collection of training samples, to infer a function. Creating a system that can learn the mapping between the input and the output is the aim of the type of learning being used. Based on the datasets, it can predict the system's output given new inputs. The labelled datasets are used to train the Random Forest algorithm to classify data and predict the outcomes accurately.

6. SUMMARY

Intrusion detection is a realistic and functional solution in offering a definition of defense in large and current networks (possible uncertainty) computer and networking programs. Intrusion monitoring systems are based on host audit-trail and network traffic analysis and are designed to detect threats, preferably in real time. Classification methods tend to be strong in modeling interactions. In this research work, supervised machine learning systems and rules were applied to intrusion detection data sets to forecast the probability of attack in the network context and the performance of the learning methods were evaluated based on their predictive precision and ease of learning. As classification techniques, Decision Tree, Random Forest, KNN, SVM, and Naive Bayes were utilized. The results of the evaluation show that the high accuracy rate is 99.68% with a recall rate of 0.10 at stage 1 of the evaluation and the

accuracy rate of the Random Forest is 99.68% with a recall rate of 100 at stage 2 of the validation. Results from experiments reveal that the Random Forest method outperforms decision tree SVM, KNN, and Naive Bayes machine learning classifiers in terms of accuracy.

7. CONCLUSION

Five data mining classification models were trained in this work, and their efficacy in detecting intrusions was evaluated. As data mining classification techniques, decision trees, random forests, K-Nearest Neighbor (KNN), support vector machines (SVM), and naive Bayes were employed to classify traffic into two categories (normal and abnormal). using the NSL-KDD dataset. Eighty percent of the 148,517 records were used for training, while twenty percent were used for testing. The outcome demonstrated that Random Forest performed much better than the other four models in terms of prediction accuracy, with a 99.68 percent accuracy rate. Furthermore, Random Forest was implemented to detect intrusion in a cloud environment. This approach takes less time and is less expensive, while also having a higher detection efficiency.

The future research proposes to extend this research by developing an Intrusion Detection (IDS) Model utilizing hybrid model deep learning approaches by investigating a hybrid deep neural network that combines Convolutional Neural Networks (CNNs) with Long Short-Term Memory (LSTM) networks. The proposed framework aims to leverage CNNs for automatic feature extraction and LSTMs for capturing temporal dependencies in network traffic, thereby improving intrusion detection accuracy, reducing false alarm rates, and enhancing the detection of sophisticated cyberattacks in Internet of Things (IoT) environments.

7.1 Contribution to Knowledge

Intrusion detection in a cloud environment has been grossly neglected in the literature. The study developed a framework and formulated a unique machine learning model that offered superior performance for intrusion detection in the cloud environment. The intrusion detection system developed in this work has helped to detect intrusion attacks in the cloud environment efficiently.

7.1.1 Declaration of Competing Interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

7.1.1.1 Funding Information

The research received no external funding. All costs associated with the study were funded by the first author.

7.1.1.2 Research Involving Human and/or Animals

This research did not involve human participants or animals. The study used publicly available datasets. Therefore, ethical approval and informed consent were not required.

8. ACKNOWLEDGMENTS

The author expresses gratitude to all the supervisors for their valuable guidance and continuous encouragement throughout this research. Appreciation also sincerely extended to the Department of Computer Science, Redeemer's University, Ede, Osun State, Nigeria, for providing an enabling academic environment that led to the successful completion of this study.

9. REFERENCES

[1] Muhammad Salman Taj, Syed Irfan Ullah, Abdus Salam & Wajid Ullah Khan. (2020). Enhancing Anomaly based intrusion detection techniques for virtualization in cloud computing using machine learning. (IJCSIS), Vol. 18. No 5.

[2] Ogunde A.O and Ajibade D.A. (2014). A data Mining System for predicting university students Graduation Grades Using ID3 Decision Tree Algorithm. American Research Institute for policy development, 01 - 26.

[3] Diptee Agrawal and Chetan Agrawal. (2020). A review of various method of intrusion detection system. Computer Engineering & Intelligent System, Vol.11 No 1, 2020.7.

[4] Zhao, L., Chaowei, Y., Qun ying, H., Fei, H. (2011) Big Data and cloud computing: innovation opportunities and challenges. International Journal of Digital Earth. DOI: 10.1080/17538947.2016.1239771. Vol 10, 2017 Issue 1, pages 13 -53. Informa UK Limited.

[5] Zhang, A. (2011). Survey of Data Mining Usage in Cloud Computing. EEE International Conference on Data Mining, Vol. III, no. 3/2011, pages 472 – 481.

[6] Briscoe, G and Marinos, A. (2009). Digital ecosystems in the clouds: Towards community cloud computing. Digital Ecosystems and Technologies, 2009. DEST '09. 3rd IEEE International Conference on. DOI: 10.1109/DEST.2009.5276725.Brown, L. D., Hua, H., and Gao, C. 2003. A widget framework for augmented interaction in SCAPE.

[7] Rosado, D. G., Rafael, G., Daniel, M. and Eduardo, F. (2011). security Analysis in the Migration to Cloud Environments. Future Internet, 4, pg.469-487; doi:10.3390/fi4020469.

[8] Mather, T., Kumaraswamy, S. and Latif, S. (2009). Cloud Security and Privacy: An Enterprise Perspective on Risks and Compliance. O'Reilly Media, Inc. Journal of Information Security, Vol.6 No.2. pages 777 -780.

[9] Li and Ping (2009). A Survey on Open-source Cloud Computing Solutions. VIII Workshop Clouds, Grids e Applicators. Caixa Postal 7851 – 50732-970 – Recife – PE

[10] Gupta, A., Suri, B., Kumar, V., & Jain, P. (2020). Extracting rules for vulnerabilities detection with static metrics using machine learning. International Journal of System Assurance Engineering and Management, 1-12. Vol. 9, DOI:10.1007/s13198-020-01036-0.

[11] Gupta D, Singhal S, Malik S & Singh A. (2016). Network intrusion detection system using various data mining techniques. In Research Advances in Integrated Navigation System (RAINS). IEEE Catalog Number: CFP16RAI-POD.page Nos 252 - 257, Vol.7, Issue 5.

[12] Adetunmibi A.O. et al., (2008). Network intrusion Detection Based on Rough Set and K-Nearest Neighbor. International Journal of Computing and ICT Research, Vol. 2, No 1 pp. 60 -66. http.www.ijcir.org/volume1-number 2/article7.pdf.

[13] Ahmadzadegan, M.H., Khorshidvand, A. A., & Valian M.G. (2015). Low-rate false alarm intrusion detection with generic Algorithm Approach. INSPEC Accession Number: 15870906.IEEE, 2ND International Conference on Knowledge - Based Engineering and Innovation

(KBEI). USA, pages 1045 -1048. IEEE. https://doi.org/10.1109/KBEI.2015.7436188

[14] Sour Leang .C (2017). Understanding about Cloud Computing.https://medium.com/@sourleangchhean/understanding-about-cloud-computing 76545af3b06a

[15] Cloud Security Alliance Innovation Conference (2012). https://cloudsecurityalliance.org/events/csa-innovation-conference-2012/

[16] Rittenhouse, J. (2010). Cloud Computing Implementation, Management, and Security. CRC Press Taylor & Francis Group. International Standard Book Number: 978-1-43980680-7 (Hardback). CRC Press. Vol 2, Issue 1.

[17] Saouabi, M., and Abdellah, E. (2020). A data mining process using classification techniques for employability prediction. IJEECS visitor statistics. DOI: http://doi.org/10.11591/ijeecs.v14.i2.pp1025-1029

[18] Neelamegam, S. and Ramaraj, E. (2013). Classification algorithm in Data mining: An Overview. International Journal of P2P Network Trends and Technology. Vol.3 Issue 5.

[19] Adebayo, A., Shi, Z., Shi, Z., Olumide S., A. (2006) in IFIP International Federation for Information Processing, Volume 228, Intelligent Information Processing III, eds. Z. Shi, Shimohara K., Feng D., (Boston; Springer), pp. 525-530.

[20] Ray, P (2018). A survey on Internet of Things architectures J. King Saud Univ. – Computer. Inf. Sci., 30 (3), pp. 291-31

Bigger and clearer version of the figures 4.1 and 4.2