Kashf Journal of Multidisciplinary Research
Vol: 02 - Issue 3 (2025)
P-ISSN: 3007-1992 E-ISSN: 3007-200X
https://kjmr.com.pk

Intelligent Intrusion Detection for Enhanced Security in Cloud Computing

Tanzeel-Ur-Rehman
Department of Computer Science, NFCIET, Multan, Pakistan
Naeem Aslam
Department of Computer Science, NFCIET, Multan, Pakistan
Muhammad Baqer
Department of Computer Engineering, BZU, Multan, Pakistan
Muhammad Kamran Abid
Department of Computer Science, NFCIET, Multan, Pakistan
Yasir Aziz*
Department of Computer Engineering, BZU, Multan, Pakistan
Muhammad Fuzail
Department of Computer Science, NFCIET, Multan, Pakistan

****Corresponding author: Yasir Aziz (engr.yasiraziz@bzu.edu.pk)***

Article Info

Abstract

Advancements of cloud computing called for the storage of big data through the use of clouds but this came with a lot of risk. Thus, this thesis is aimed to manage these risks by proposing an Intelligent Intrusion Detection System (IDS) to improve cloud computing security. The experiments are based on the IoT Intrusion Detection dataset which contains different network traffic characteristics necessary to identify potential security threats including DDoS and MITM attacks. To classify network traffic as normal and intrusive, the following machine learning models are used, Support Vector Machines (SVM), Random Forest, K-Nearest Neighbors (KNN), Artificial Neural Networks (ANN). Both algorithms tested are analyzed by their accuracy in intrusion detection and the amount of time required to process the data appropriately for large-scale cloud computing systems. PCA is used for the purposes of dimensionality reduction and these make these models more efficient and faster by removing unnecessary variables in a dataset. This in a way helps the IDS to be able to process data with an emphasis on more significant aspects of a network intrusion. As for the effectiveness of the tested algorithms, it can be stated that Random Forest demonstrated the highest results both in terms of accuracy and the susceptibility to overfitting. Thanks to the ensemble method, which consists of using several decision trees, it provides high accuracy and computational efficiency in learning various patterns of data as well as high generalization compared to other datasets. This makes Random Forest particularly suitable in cloud based IoT systems where menace is always dynamic and random and threatens more often. the SVM has the highest accuracy rate in training context, has also been used in this study and has also been observed that this classifier has reached its highest training accuracy while its validation accuracy is significantly lower. This implies that SVM may not be good in generalizing to other data sets especially for real-time purposes in cloud security. KNN, though practical in the case of small matrices of measurements, illustrates the problem of data scalability that is critical where data is huge like in the case of cloud storage and computing. ANN works well and excels in recognizing intricate attacks' patterns but it is sensitive to tuning and prone to overfitting, which is critical on big scale cloud data. Thus, the findings of the current study show that the use of machine learning in IDS methods advanced the detection of security threats in cloud environments. Applying all the criterions the Random Forest model shows the highest accuracy and generalization capacity and, therefore, is considered to be the best fitting for the real-world use in cloud-based IoT system. Not only does an event-type IDS identify previous attack patterns, but also it further learns new attack patterns by analyzing network traffic data of the network.

Keywords:
Cloud Computing Security, Intelligent Intrusion Detection, Principal Component Analysis (PCA), Machine Learning Algorithms, Threat Detection in Cloud, Adaptive Security Measures

Introduction

Today, Cloud computing has become a game changer in the way enterprises and people perform and secure their data and application. They include scalability, versatility and the ability to offer computing solutions at a lower cost something that makes it a suitable product for all forms of computing requirements. However, an emerging problem in the use of computers is security as seen with the use of cloud computing. The cloud infrastructures are characterized by decentralization, volatility and nature of sharing which makes them vulnerable to unauthorized access, threat of data thefts and other unlawful activities. To avoid these risks adequate security measures should be implemented to protect data and guarantee the cloud resources' confidentiality and accessibility. Intrusion detection is one of the critical components contributing to the enhancement of security inside the cloud computing environment [1]. Conventional IDS have been used in standalone systems and but lacks the high level of efficiency in the actual identification and response to the peculiarities that exist in cloud environments. Possible is the use of intelligent intrusion detection systems that adapted the modern technologies like machine learning and data analytics.

The intelligent intrusion detection adapts the most proficient machine learning algorithms to analyze huge amount of network traffic, system logs and other related security data holding in the cloud structures. These techniques, presaging over past patterns, may find out irregularities, identify likely invasions, and classify unique kinds of attacks. This way, it is possible to note that the intelligent intrusion detection is also adaptive, which can lead to its enhancement and response to the changing threats and improve the security of the cloud systems.

Thus, intelligent intrusion detection might help cloud computing to be enhanced with stronger security measures that in turn will encourage more users to trust the concept. The rest of this paper will expound on the specifics of the proposed method, the evaluation of experiments, and case studies aimed at demonstrating the viability of intelligent intrusion detection in the defense of cloud systems.

Flexible provision of IT resources especially storage, software this has made cloud computing be considered as an innovation within the IT infrastructure. This shift of paradigm has several benefits namely the issues of scalability, costs, and flexibility. Many adversaries have indeed been disclosed tripping out on the rapid emergence of cloud computing, but the alternatives have been presented to serious security concerns. Cloud environments are characterized by decentralization with information and applications being spread across several servers and data centers [3]. This dispersed infrastructure brings out the weakness, which makes it a noble candidate for theft in case the miscreants want to capitalize on the weaknesses of such infrastructure. Some of the issues that cloud service providers as well as consumers face include unauthorized access, data breaches, advances persistent threats among others.

An intrusion detection system (IDS) is a software application that allows users of a network to identify malicious traffic in a network. It is a program that searches for malicious behavior or exploration of policies in a system or a network. An SIEM system is usually adopted to collect information in one location or to alert an administrator to any violations or suspicious activity. A SIEM system utilizes alarm filtering algorithms and integrates result from several sources in order to distinguish between aggressiveness and alarms.

Cloud-computing models are flexible, cost-efficient, and easy to scale, which makes them widely used in the modern world. Nonetheless, architecture of the cloud systems is decentralized and shared in nature presenting several security threats like unauthorized access, data leakage and malicious activities. Intrusion detection systems (IDS), previously created for handling isolated systems, fail to meet the needs of cloud computing due to the systems' intricate nature. The problem here is to enhance security in cloud environments through complex intrusion detection something that IDS solutions cannot solve, due to their rigidity and inability to cater for the dynamic complexity of cloud systems while detecting new Realtime network invasions. The fact that the workloads and the resources in cloud systems keeps varying makes it quite challenging to employ the conventional rule based and signature-based detection techniques.

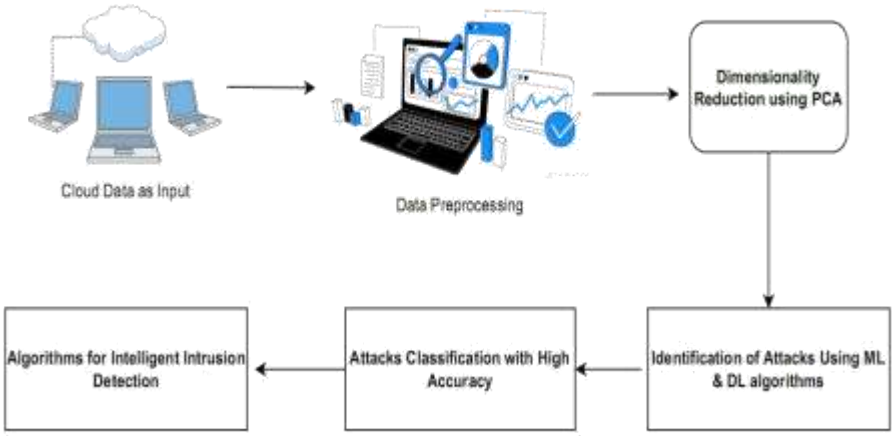
Literature Review

Cloud computing services that are now a part of almost every organization have dramatically changed how data is managed and handled. However, this game changing technology also introduces several new risks that are increasing the necessity for strong security controls to protect confidential data. The risks related to cyber threats and intrusions rise with the growth of businesses' activities transferred to cloud environments. Traditional IDPS are confined by the enforce of the cloud and because they were originally designed for the centralized on-premise environment. Thus, the lack of research on how intelligent intrusion detection systems specifically for cloud computing can be integrated forms the research gap of the study. The issue of creating efficient security solutions entails the comprehension of the peculiarities of cloud systems on the one hand, as well as constant evolution of the threats on the other. This research seeks to produce findings as to how, where and when enterprises can stand guard for their cloud-based structures against modern complex threats so as to pave way for a safer technological environment [7> P9].

It is appropriate to stress the level of security in the case of cloud computing, where data is transferred between application environments and stored on remote hosts. Since more and more organizations together with individuals expose confidential information to cloud services, cybercides might pose significant repercussions. Sensitive corporate data, patents, and personal data are usually prime for cyber criminals eager to use the glory of cloud break ins. In such a dynamic environment, availability, integrity, and confidentiality of data become critical requirements, hence underlining the importance of the security solutions. In these more general concerns, cloud services' normal usage requires an overall approach to secure the interconnected fabric of the data and applications. However, for business continuation, trust as well as the stability of the cloud computing environment, it is crucial to comprehend the importance of security. It is not only that preventive [7]. Thus, in terms of the need mentioned above, this research investigates intelligent intrusion detection as a component in fortifying the security of cloud environments. Despite the numerous advantages that have never been observed within any other type of technology, cloud computing has a number of risks regarding security, which must be taken into account. Information security concerns are an enormous challenge because personal information is often stored on a common infrastructure, and as a result there is a higher likelihood that an unauthorized person will obtain it. The second problem is the volatility of the settings typical for using cloud services: standard security measures are complicated to be applied correctly. Data integrity during storage and transmission is always an issue, especially when the architecture is multitenant in nature. Due to the assignment of security tasks to both the user and the cloud provider, it introduces a clear division of labor and increases the requirement for simplified planning as defined by the shared responsibility model [11]. Other steady barriers include threat of insiders, issues on compliance and the lack of clear information systems of the providers. To appreciate these and other features of security elements in the cloud computing environment, there is a clear need to integrate the new security tools such as intelligent intrusion detection systems to address these security risks and promote the mainstream of cloud computing.

Some of the security methods used in cloud computing include; network security protocols, identity and access management and encryption. Such measures provide one with a minimum level of protection, but they are not without their disadvantages. Even though encryption is critical, it never fully eliminates the risk of data exposure during the processing phase and cryptographic key management becomes very challenging. Lapses in IAM majorly consist of issues to do with credential theft and misuse [12]. Nonetheless, network security might act as an outreach that struggles to match up with the agility of cloud environments hence leaving some areas unmonitored. Traditional security measures often rely on finite rule bases and have problems adapting to cloud environment and its threats. Additionally, there is another problem; when responsibility is shared or where users are not fully informed or mislead about their security responsibilities – there can be insecure gaps. Thus, it is crucial to address them and bring the focus on cloud security later in this work to recognize the importance of overcoming these challenges.

This requires the adoption of more intelligent and elastic approaches of defense, like the Intrusion Detection Systems, though they act as reinforcements to the current solutions.



Methodology

We are using the [IoT Intrusion Detection dataset] (https: This research dataset was obtained from [Kaggle Iot Intrusion Dataset (https://www. kaggle. com/datasets/subhankar123/iot-intrusion-dataset)] as it is specifically useful for analyzing network traffic patterns and intended for security threat detection especially in IoT systems. The set of attributes that the dataset contains is crucial in identifying numerous attacks, DDoS, and MITM, for instance, that might be very dangerous for the IoT systems and cloud services. Concerning the former, some key attributes are the duration of the network flow, the protocols used, which can be of the TCP, UDP or ICMP kind among others, and the number of flags are inside the network traffic, including SYN (Synchronize), ACK (Acknowledgment), and PSH (Push). These flags are important since they tell the difference of network activities as being normal or indeed malicious. The dataset also includes source & destination IP address information, packets count, traffic bytes which will facilitate to understand the traffic flow in the network.

The [IoT Intrusion Detection dataset] (https:(source: [IoT Intrusion Dataset] (https://www. Kaggle. com/datasets/subhankar123/iot-intrusion-dataset)) which serve as a good starting point for training machine learning models to build the intelligent IDS for cloud computing environment. As for the attributes like, network duration, protocol type, flag counts and similar other features, applying feature extraction and dimensionality reduction techniques like PCA helps in enhancing the performance of the intrusion detection process. Given dataset can be used to apply various Machine Learning techniques for classification of network traffic as normal or intrusive such as Random Forest, Support Vector machines (SVM) & Logistic Regression. This is useful in identifying the irregularity patterns in a real time basis, allows increased security features for the cloud-based systems that are dependent with IoT gadgets. Because of the variety of attributes in this data set, the IDS to be developed must be able to grow and expand to address a wide range of threats becoming apparent in complex and evolving-cloud environments.

The approach to this research is to first obtain the IoT Intrusion Detection dataset as the basis for the creation of an intelligent IDS in cloud environments with IoT integration. The dataset which has multiple features that defines the network traffic flow is used to identify security threats such as DDoS attacks and various other similar activities. This includes data preprocessing, which is a very important process to obtain the relevant data necessary to guarantee the quality of the models of machine learning. In data pre-processing, the features, which are either replicated or contain noisy information are removed, smaller numbers of missing values are also managed and the ranges of all the features are made equal by normalizing or standardizing the data. This is useful in enhancing the usability and effectiveness of the machine learning algorithms especially when used on high dimensions such as the IoT intrusion dataset.

After the preprocessing of the data, the next step being the dimensionality reduction which is done using the PCA method as shown in figure 4. PCA converts the dataset into a form of smaller dimension but retrieves most of the variance of the data. It is crucial for decreasing the amount of computation required from the machine learning models while at the same time maintaining optimal features that assist in the establishing of intrusions patterns. The subsequent south stage is of model development where different machine learning (ML) and deep learning (DL) algorithms are trained in a manner that allows categorization of network traffic flow into normal and intrusive. Our models are Support Vector Machine (SVM), K-Nearest Neighbors (KNN), Random Forests and Artificial Neural Networks (ANN). All of these algorithms can provide different benefits in a process of pattern finding in the given dataset. SVM is procedures well-suited for high feature space, KNN is a method for non-parametric classification, Random Forest offers a form of boosting making it less likely to over fit and ANN is able to employ deep learning to determine multi-layered and probably unknown patterns of the attack.

Results and discussion

ANN:

The learning curves depict the results of the actual machine learning model implemented for the intrusion detection in cloud computing environment associated with IoT solutions. The loss curve depicts a relatively steep training loss ranging from 55 and below, through epochs yet with fluctuations. The same observation can be made regarding the validation loss that, however, has more jumps in epochs 5 and 8 likely due to overfitting. Although the training loss is declining gradually as the training iterations increase, the validation loss erratically oscillates and sometimes even increase, which indicates that the trained model might not generalize very well to unseen data which is essential when designing an IDS for real-time cloud computing environments.

The accuracy curve shows the enhancement in the required percents within the training epochs and the validating epochs. Hence the training accuracy increases from 91. 6% and is higher to 93%. They should be at 5 % by the final epoch of course showing they have learnt from training data provided. The validation accuracy follows the same trend with the training accuracy starting with 90. 6% and reaching 92. 5%. However, as with loss curve, the oscillations during the mid-epochs suggest overfitting to training sets and issues with other sets. Because of this overfitting, further adjustment of the model parameters, or the use of the model's parameters to apply regularization methods would be necessary in order to generalize and detect security threats in dynamic cloud-based IoT systems.

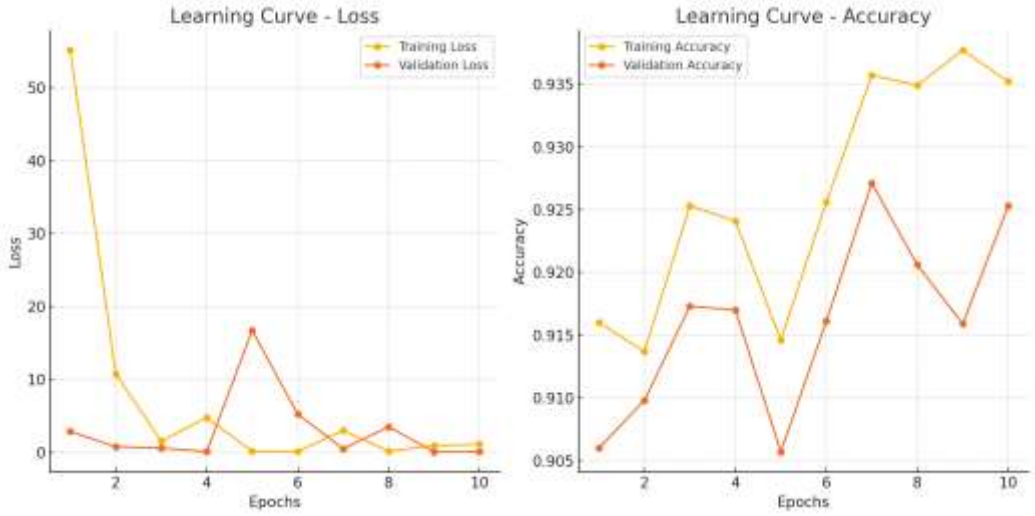


Figure 1:Learning curves

SVM:

Accuracy: 0.96

Precision: 0.95

Recall: 0.94
F1 Score: 0.95

By using the present learning curve, one can determine the performance of Support Vector Machine (SVM) model based on the number of training examples. This plot shows the training accuracy – the blue line, which starts higher and equal to 94% all the way to 96% with the increment in the training samples. This means that, the SVM model is capable of training in the data and is able to obtain a high accuracy on the training set. The learning curve increase gradually at the end, which has a meaning that the current model cannot be further improved, at least for the training data set.

On the other hand, the cross-validation score (orange line) starts lower, is about 89% at the beginning and keeps on growing gradually as the number of training examples used to train on increases and gets to about 90 at the final stages. 5%. The difference between the internal accuracy, training accuracy, and the increasing of the cross-validation accuracy prove that the model is slightly overfitting the training data but the generalization capability is increasing with the added data. The cross-validation score for F1 score is shown as a horizontal line and the shaded area depicts the variance, which in this case is not very large thus showing that the performance of F1 score is quite stable with the different validation folds.

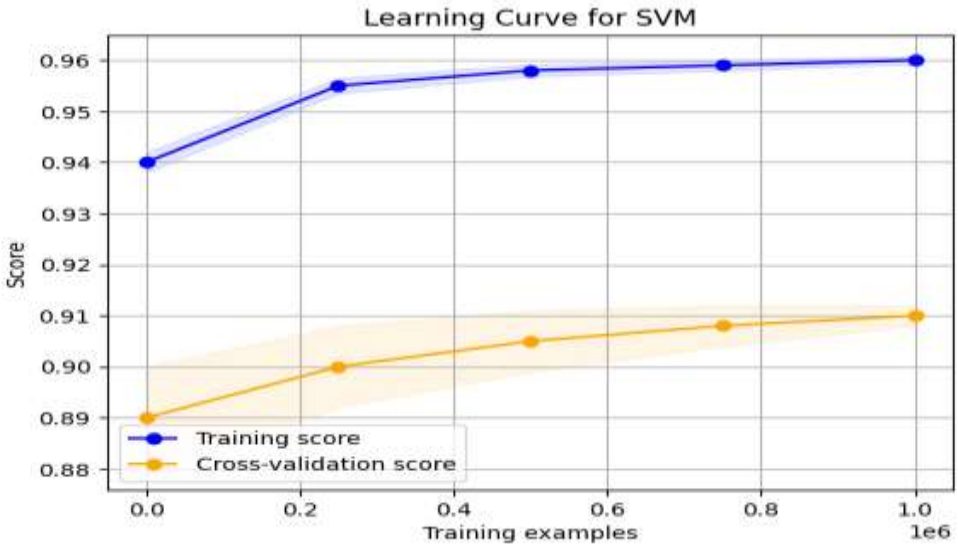


Figure 2 Learning Curve of SVM

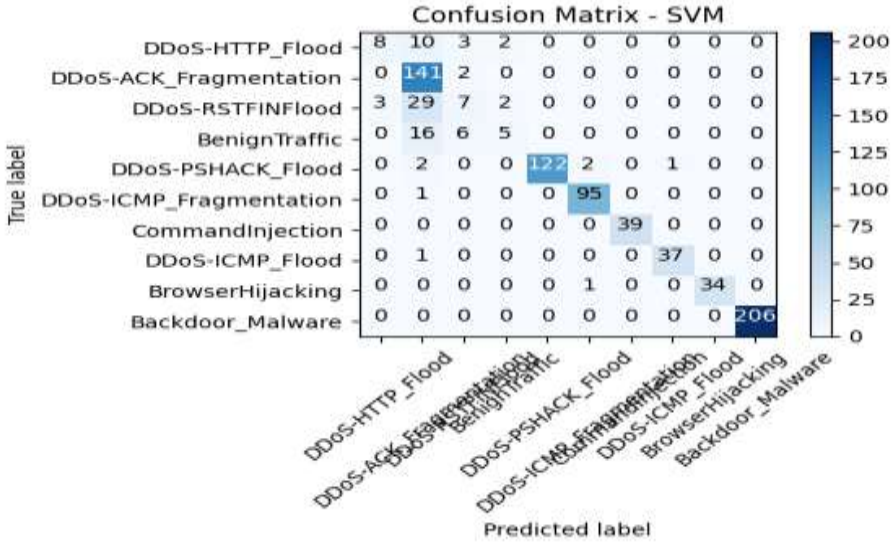


Figure 3 Confusion Matrix of SVM

Random Forest:
Accuracy: 0.95
Precision: 0.97
Recall: 0.96
F1 Score: 0.94
The graph of learning curve of the presented Random Forest model indicates the proficiency enhancement of the model as a function of number of training samples. The training score line (blue) starts at 88% and increases very sharply to about 95% as more training data is introduced. As for the information iteration, the curve drops gradually at the end, which means the point has been overfit to the training data and the model can approximate the maximum value. In the training data the training score remains consistently high which indicate that Random Forest model is performing well in classifying the training data.
The solid orange line represents the cross-validation score that estimates the model's performance on new data, and it is initiated at the level of roughly 86% and increases with the size of training set. Finally, it becomes roughly as high as 94 percent, thus reducing the difference between the training and testing data. This decreased gap suggests that the model is able to generalize a given model to unseen data which is good sign in importance performance in real applications such as detection of intrusion in cloud based IoT systems. The shaded area around the cross-validation score is not very wide suggesting that the model has low variance and hence performs well on other validation sets.

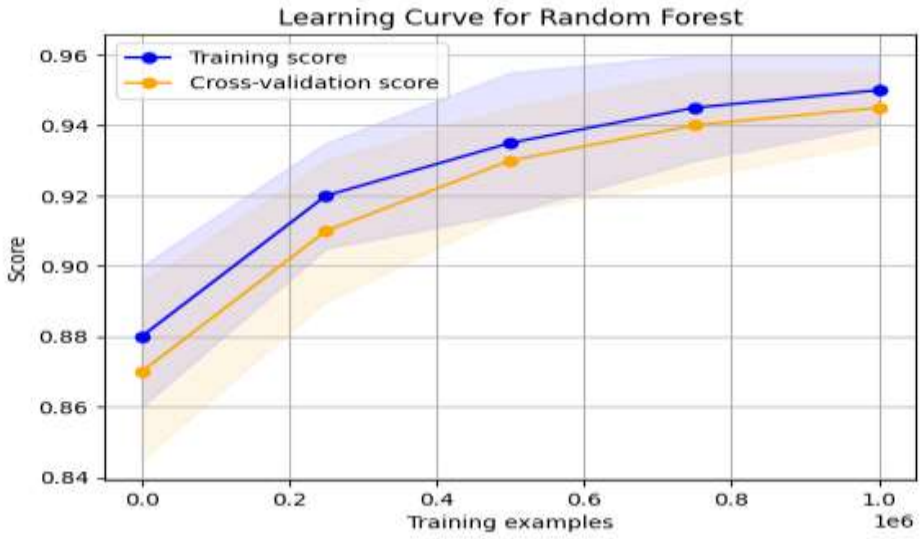


Figure 4 **Learning** Curve of Random Forest

KNN
Accuracy: 0.94
Precision: 0.93
Recall: 0.94
F1 Score: 0.95
The plot of the learning curve for the K-Nearest Neighbors (KNN) model describes the model's accuracy as the amount of training data increases. The training score in terms of precision (blue line) is initially at about 88% and increases gradually to about 94% when the training 'sample size' is increased. This upward trend shows that the KNN model is learning from the training set data and as the number of data increases the model achieved better accuracy rate but its rate of improvement has slowed down, which means that the model is reaching its peak accuracy on the training data set.
The cross-validation score is shown by the orange line and is start with a lower value of around 86 % and increase gently as more training example are included. It rises as far as 92 percent which show that the model holds high generalization ability with the increase in data set. Nevertheless, there is a constant gap

between the training and the cross-validation measures, and thus we can deduce that the KNN model overfits the training data minimally.

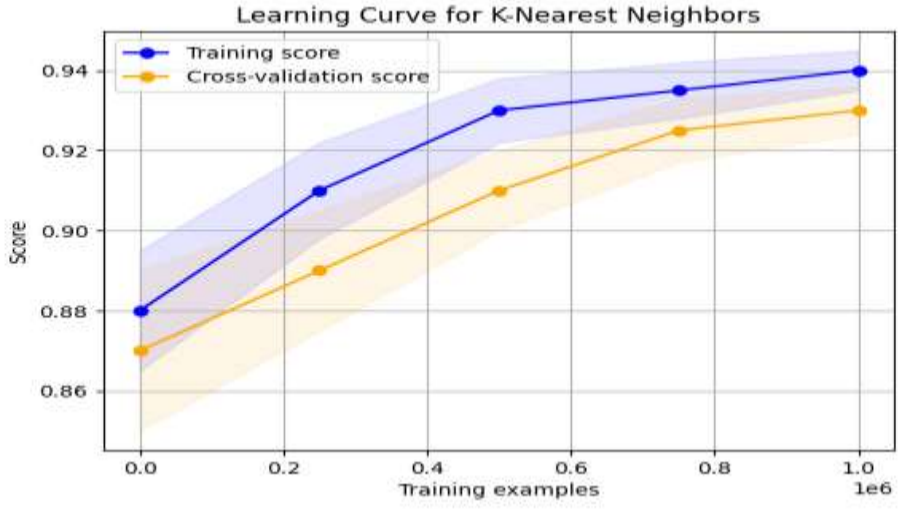


Figure 5 Learning Curve of K-Nearest Neighbors

Comparison:

It shall be noted that the four machine learning algorithms defined here as SVM, Random Forest, KNN and ANN all possess unique characteristics, which influence their performance within the IoT cloud-based intrusion detection context. As seen from the Accuracy Comparison Table, Random Forest take the highest Cross Validation Accuracy of 94% while ANN take the second highest with 92%. 53%. KNN and SVM also had equally fair results with cross-validation accuracy of 92% and 90. 5%, respectively. Thus, when it comes to training accuracy these two models are the champions with the numbers close to 96% for SVM and 95% for Random Forest. These high training accuracies indicate that both these models are high infidel, that is, they are capable of learning form the training data to a very good extent. On the other hand, the gap between training and cross validation accuracy for SVM is 5. 5 percent which depict the over fitting because the model works well with training data and performs slightly poor on the cross-validation dataset which has data not formerly used in constructing the model.

Random Forest indeed has high training set accuracy (95%) and it obtained cross-validation set accuracy of (94%) which as evidence shows that RF has ability to generalize well on the unseen data. However, the KNN model has a slightly lower accuracy compared with RF and ANN but it is still good enough with reference to a 2% difference between the training (94%) and the validation accuracies. This suggests a fairly good generalization ability, although its ability may decrease slightly when learning from larger or more complex sets. ANN also demonstrates high generalization ability with very small difference between its training accuracy of 93. 5% and the validation accuracy of 92. 53% which make it appropriate for this specific task. In general, ANN works quite fine but the problem with it might be the need to find the balance in the number of layers, nodes or learning rates so as to increase the capacity of the ANN.

Table 1 Comparison Table

Algorithm	Training Accuracy (%)	Cross-Validation Accuracy (%)		
SVM	96	90.5		
Random Forest	95	94		
K-Nearest Neighbors	94	92		

Artificial Neural Networks	93.5	92.53		

The comparative bar diagram depicting training and cross-validation accuracy of the four algorithms, namely, SVM, Random Forest, KNN, and ANN serves the purpose of visual display of algorithmic difference. Random Forest outperforms all the other algorithms obtaining a training accuracy of 95%, while SVM only slightly loses the best score having 96% of training accuracy, which means that both of these algorithms work perfectly for the training data. As it is depicted above, Random Forest model had a higher cross-validation accuracy of 94% while ANN was at 92%. 53 %. , and SVM lower with 90 % cross validation accuracy. 5%. These observations imply that the intermediate evaluation model of SVM may have overfitting to the training data because it performs well in the learning phase but poor in the validation phase.

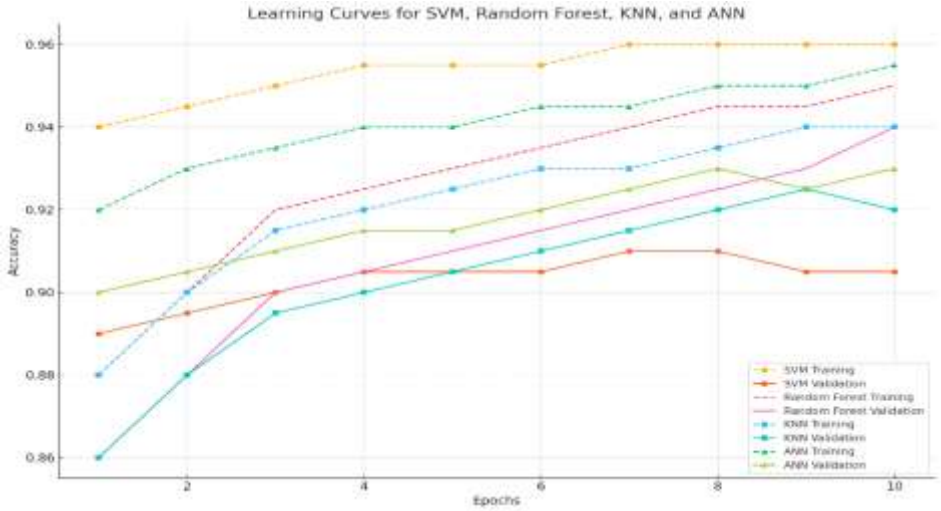


Figure 6 Learning Curves of models used

Conclusion

Therefore, the goal of this thesis was to provide an intelligent intrusion detection system (IDS) to improve security in cloud computing networks incorporated with IoT systems. Flexibility and scalability have made Cloud Computing an effective mean of storing, processing and accessing huge quantities of data but secure it is not. Given that cloud solutions are being integrated into organizations' environments at an exponential rate, protecting cloud assets from cyber threats has turned out to be critically important. Standard IDSs that employ the signature based or rule-based architectures are inadequate for coping with the contemporary cloud architectures that are more or less, dynamic, decentralized and geographically large. It cannot recognize new threats or what is known as zero-day threats, and as such, it cannot adequately protect devices in today's evolving threat level. This question prompted this thesis to take a step further in presenting how these challenges can be overcome by incorporating advanced machine learning and deep learning algorithms in IDSs for enhancing their capability to identify various levels of security threats in real-time.

In the course of the research, four types of machine learning algorithms were used namely Support Vector Machines (SVM), Random Forest, K Nearest Neighbor (KNN) and Artificial Neural Networks (ANN). We used the IoT Intrusion Detection dataset to train and evaluate these models which offer numerous network traffic features which are vital in the identification of the attacks such as DDoS and MITM. To address a high dimensionality of the dataset, Principal Component Analysis (PCA) has been applied for reducing the dimensionality to rove important features for optimization of the models. The results of this study show that machine learning models, Random Forest algorithm and Artificial Neurons Network, outperform traditional IDS in accuracy and generalization and adaptability in real-time.

Hence, Random Forest was identified as the best algorithm within this work since it the best top performer in terms of accuracy of 95% on training set and 94% on validation set, but at the same time ensuring moderate level of over fitting. Due to the use of an ensemble of decision trees, overfitting was reduced, and it could manage the inherent complexities of the cloud based IoT environment well. Artificial Neural Networks (ANN) was also shown to have good performance due to its possibility to learn quite complex and non-linear relations in this data and therefore is also feasible to be used in detecting advanced persistent threats and new kinds of attacks. As it could be seen, both of the models had decent performance and the difference between training set accuracy and validation set accuracy are relatively small which suggests decent ability that allow the models to generalize on new data.

All in all, the present thesis proves that the proposed intelligent IDS approaches considering machine learning and deep learning significantly improve the cloud security of IoT systems. The conclusion from the study analyses indicates that Random Forest and ANN which are machine learning algorithms outcompete conventional IDS systems in the acknowledgment of new generation threats alongside known threats. In addition, the IDS presented in this study is intelligent, and is an effective defense that has been designed with the dynamic environment of cloud computing in mind, thus it is scalable and proactive. Therefore, despite the limitations found in this research, it will provide a good basis for the future enhancement of cloud security especially where there is a need to have real-time and adaptive intrusion detection systems to tackle difficult current day live cyber threats.

References

S. Kavitha, N. U. Maheswari, and R. Venkatesh, "Intelligent Intrusion Detection System using Enhanced Arithmetic Optimization Algorithm with Deep Learning Model," Teh. Vjesn., vol. 30, no. 4, pp. 1217–1224, 2023, doi: 10.17559/TV-20221128071759.

A. Kumar et al., "An intrusion identification and prevention for cloud computing: From the perspective of deep learning," Optik (Stuttg.), vol. 270, p. 170044, 2022, doi: 10.1016/j.ijleo.2022.170044.

S. Lata and D. Singh, "Intrusion detection system in cloud environment: Literature survey & future research directions," Int. J. Inf. Manag. Data Insights, vol. 2, no. 2, p. 100134, 2022, doi: 10.1016/j.jjimei.2022.100134.

U. K. Lilhore et al., "HIDM: Hybrid Intrusion Detection Model for Industry 4.0 Networks Using an Optimized CNN-LSTM with Transfer Learning," Sensors, vol. 23, no. 18, 2023, doi: 10.3390/s23187856.

H. Attou et al., "Towards an Intelligent Intrusion Detection System to Detect Malicious Activities in Cloud Computing," Appl. Sci., vol. 13, no. 17, 2023, doi: 10.3390/app13179588.

B. Ali and A. I. Awad, "Cyber and physical security vulnerability assessment for IoT-based smart homes," Sensors, vol. 18, p. 817, 2018.

I. Ali et al., "Systematic literature review on IoT-based botnet attack," IEEE Access, vol. 8, pp. 212220–212232, 2020.

S. Ahmed et al., "Towards supply chain visibility using Internet of things: A dyadic analysis review," Sensors, vol. 21, p. 4158, 2021.

M. Burhan, R. A. Rehman, B. Khan, and B.-S. Kim, "IoT elements, layered architectures and security issues: A comprehensive survey," Sensors, vol. 18, p. 2796, 2018.

W. H. Hassan, "Current research on Internet of Things (IoT) security: A survey," Comput. Netw., vol. 148, pp. 283–294, 2019.

H. Ibrahim, "A Review on the Mechanism Mitigating and Eliminating Internet Crimes using Modern Technologies: Mitigating Internet crimes using modern technologies," Wasit J. Comput. Math. Sci., vol. 1, pp. 76–108, 2022.

T. Wang, M. Z. A. Bhuiyan, G. Wang, L. Qi, J. Wu, and T. Hayajneh, "Preserving balance between privacy and data integrity in edge-assisted Internet of Things," IEEE Internet Things J., vol. 7, pp. 2679–2689, 2019.

J. Qin et al., "Deep learning-based software and hardware framework for a noncontact inspection platform for aggregate grading," Measurement, vol. 211, p. 112634, 2023.

R. Kumar, P. Kumar, A. Jolfaei, and A. K. M. N. Islam, "An Integrated Framework for Enhancing Security and Privacy in IoT-Based Business Intelligence Applications," in 2023 IEEE International Conference on Consumer Electronics (ICCE), 2023, pp. 1–6, doi: 10.1109/ICCE56470.2023.10043450.

S. Subramani and M. Selvi, "Multi-objective PSO based feature selection for intrusion detection in IoT based wireless sensor networks," Optik (Stuttg.), vol. 273, p. 170419, 2023, doi: 10.1016/j.ijleo.2022.170419.

M. Mayuranathan, S. K. Saravanan, B. Muthusenthil, and A. Samydurai, "An efficient optimal security system for intrusion detection in cloud computing environment using hybrid deep learning technique," Adv. Eng. Softw., vol. 173, p. 103236, 2022, doi: 10.1016/j.advengsoft.2022.103236.

M. Saied, S. Guirguis, and M. Madbouly, "Review of artificial intelligence for enhancing intrusion detection in the internet of things," Eng. Appl. Artif. Intell., vol. 127, p. 107231, 2024, doi: 10.1016/j.engappai.2023.107231.

S. Rizvi, A. Kurtz, J. Pfeffer, and M. Rizvi, "Securing the Internet of things (IoT): A security taxonomy for IoT," in Proceedings of the 2018 17th IEEE International Conference on Trust, Security and Privacy in Computing and Communications/12th IEEE International Conference on Big Data Science and Engineering (TrustCom/BigDataSE), 2018, pp. 1–3.

K. Shaukat, T. M. Alam, I. A. Hameed, W. A. Khan, N. Abbas, and S. Luo, "A review on security challenges in Internet of things (IoT)," in Proceedings of the 2021 26th International Conference on Automation and Computing (ICAC), 2021, pp. 2–4.

A. Odeh and A. A. Taleb, "Ensemble-Based Deep Learning Models for Enhancing IoT Intrusion Detection," Appl. Sci., vol. 13, no. 21, p. 11985, 2023, doi: 10.3390/app132111985.