Humaira *et al. (IJECI)* 2023

(IJECI)
ISSN: 2522-3429 (Print)
ISSN: 2616-6003 (Online)

International Journal for
Electronic Crime Investigation

DOI: https://doi.org/10.54692/ijeci.2023.0702153

Research Article

Vol. 7 issue 2 Year 2023

Analysis of Network Security in IoT-based Cloud Computing Using Machine Learning

Humaira Naeem

Department of computer science, Virtual university of Pakistan

Corresponding author: humairanaeem@vu.edu.pk

Received: March 07, 2023; **Accepted**: March 22, 2023; **Published**: June 15, 2023

Abstract:

Network security in IoT-based cloud computing can benefit greatly from the application of machine learning techniques. IoT devices introduce unique security challenges with their large-scale deployments and diverse nature. Machine learning can help address these challenges by analyzing IoT network traffic, detecting anomalies, identifying potential threats, and enhancing overall network security. The security of cloud networks is validated using binary classification to detect attacks. Random forest classifiers achieved an accuracy of 96%, while K nearest classifier had an accuracy of 93% and a precision value of 0.96. The proposed model ensures security of big data against intrusion attacks on the network. Although machine learning techniques can be powerful for protecting cloud computing networks, challenges still need to be addressed before widespread adoption. Understanding the potential and limitations of machine learning approaches to network security can help researchers and practitioners develop more effective strategies for safeguarding their systems in an increasingly interconnected world. Network security of big data in cloud computing can be enhanced by applying machine learning techniques. Machine learning algorithms can analyze large amounts of data to detect patterns, anomalies, and potential security threats. Here are several ways machine learning can be utilized to improve network security in the context of big data and cloud computing:

Keywords: Cloud computing ; NID; KNN; RF ; Machine learning

1. Introduction

The convergence of IoT (Internet of Things) and cloud computing has revolutionized the way we interact with and manage vast networks of interconnected devices. IoT-based cloud computing systems enable seamless communication, data storage, and analysis, facilitating a wide range of applications across industries. However, this rapid proliferation of IoT devices and the utilization of cloud services also bring forth significant network security challenges. The need to protect sensitive data, ensure device integrity, and

safeguard against emerging threats has become paramount [1].

To address these challenges, machine learning techniques have emerged as a powerful approach to enhance network security in IoT-based cloud computing environments. Machine learning algorithms have the capacity to analyze massive volumes of data generated by IoT devices and cloud services, enabling the identification of patterns, anomalies, and potential security threats. By leveraging machine learning capabilities, organizations can significantly strengthen their network security posture and mitigate the risks associated with IoT deployments[2].

This paper aims to explore the analysis of network security in IoT-based cloud computing using machine learning. We will delve into how machine learning techniques can be applied to bolster network security, such as intrusion detection, anomaly detection, device authentication, security analytics, threat intelligence, and privacy protection. Furthermore, we will examine the implications of machine learning in enabling predictive maintenance and proactive security measures within IoT-based cloud computing environments [3].

By harnessing the power of machine learning, organizations can better safeguard their IoT networks, protect sensitive data, and respond effectively to emerging threats. This paper will provide insights into the potential benefits, challenges, and considerations in implementing machine learning-based network security strategies in IoT-based cloud computing[4][5].

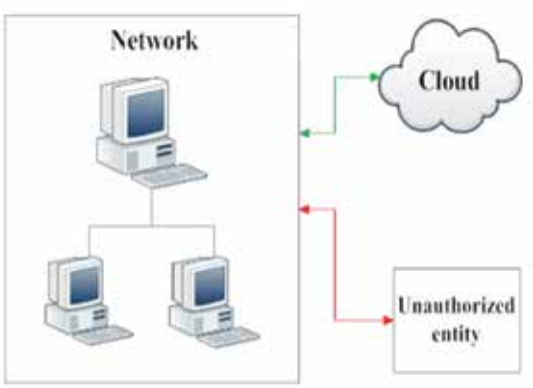

Figure 1: Unauthorized access of data

Machine learning algorithms can analyze network traffic data from IoT devices to identify patterns associated with known attacks or intrusions. By monitoring network packets, data payloads, and device behavior, machine learning models can detect and raise alerts for suspicious activities, helping prevent unauthorized access and data breaches [6].

IoT devices generate massive amounts of data, and machine learning can be utilized to identify abnormal patterns or behaviors. By training models on historical data, machine learning algorithms can learn the normal behavior of IoT devices and detect any deviations that may indicate potential security threats. For example, abnormal traffic patterns, unusual data transfers, or unexpected device behavior can be flagged for further investigation [7].

Machine learning can enhance device authentication mechanisms in IoT-based cloud computing. Machine learning models can differentiate between legitimate and unauthorised devices by analyzing device characteristics, communication patterns, and contextual

information. This helps enforce access control policies and prevent unauthorized access to cloud resources.]

Machine learning algorithms can be applied to analyze security-related data from IoT devices and cloud environments. Machine learning models can identify potential security events or trends by aggregating and correlating data from multiple sources, such as device logs, network traffic, and system logs. This enables proactive threat mitigation and aids in making informed security decisions [8].

Threat Intelligence and Response: Machine learning can assist in the analysis of threat intelligence feeds and security-related data to identify emerging threats and vulnerabilities in By integrating external threat intelligence sources with internal network data, machine learning models can provide real-time threat detection, enabling quick response and mitigation measures [9].

IoT devices often handle sensitive data, and machine learning can protect privacy. By applying machine learning techniques such as differential privacy, data anonymization, and encryption, IoT data can be secured while maintaining its utility for analysis and insights. Machine learning can help predict and prevent security incidents in IoT-based cloud computing environments. By analyzing historical data on device performance, maintenance logs, and security events, machine learning models can identify patterns that lead to security vulnerabilities or device failures. This enables proactive maintenance and security measures to prevent future incidents [10].

It's crucial to continuously train and update machine learning models in IoT-based cloud computing environments to adapt to evolving threats. Regular evaluation, monitoring, and collaboration with domain experts are necessary to ensure the effectiveness and accuracy of these models. Additionally, implementing security best practices such as secure device provisioning, network segmentation, and encryption protocols in conjunction with machine learning can create a comprehensive security framework for IoT-based cloud computing networks.

Figure 2: Cloud deployment Models

2. Related Work

In [11] proposed an intrusion detection system for IoT-based cloud computing using a deep learning approach. The study employed deep neural networks to analyze network traffic data and detect malicious activities. The model achieved high accuracy in identifying various types of attacks, highlighting the effectiveness of deep learning in IoT network security.

[12] presented a machine learning-based anomaly detection framework for IoT networks in cloud computing. The research focused on analyzing network traffic patterns to identify deviations from normal behavior. The proposed framework utilized machine learning algorithms, including clustering and classification, to detect anomalous activities in real-time.

In this paper [13] explored the use of machine learning techniques for threat intelligence in IoT-based cloud computing environments. The study integrated external threat intelligence feeds with network data to identify and classify emerging threats. Machine learning models were employed to analyze the data and provide timely threat detection and response.

Privacy preservation in IoT-based cloud computing has also received attention. Author proposed a privacy-preserving framework based on machine learning for IoT networks. The approach employed techniques such as differential privacy and data anonymization to protect sensitive data while still allowing effective analysis and insights. Predictive maintenance and security have been addressed through the application of machine learning in IoT-based cloud computing. The research focused on analyzing historical device performance data and maintenance logs to predict security vulnerabilities and device failures. Proactive maintenance measures and security enhancements were then implemented to prevent future incidents.

These studies highlight the diverse applications of machine learning in improving network security within IoT-based cloud computing. By leveraging machine learning algorithms, organizations can detect intrusions, identify anomalies, analyze threat intelligence, protect privacy, and implement predictive security measures. However, challenges such as data quality, model robustness, and scalability must be addressed to ensure the effectiveness and practicality of machine learning-based network security solutions in real-world deployments. The concepts of big data, the Internet of Things, and cloud computing are closely related and have the potential to bring significant benefits to industries such as healthcare and engineering. However, concerns related to their interconnectivity are also addressed in the proposed methodology outlined in [14].

Smart homes rely on the Internet of Things (IoT), which generates significant amounts of data from sensors and actuators for various activities. The utilization of IoT applications benefits homeowners and industrialists alike. A study proposed in paper [15] focuses on the use of cloud computing and fog nodes to store, network, and process IoT data. The methodology was validated using a Canadian smart home dataset and demonstrated promising results.

Cloud-based architectures provide computational models for performing big data operations, offering cost efficiency, elasticity, and virtualization benefits. Security concerns arise as data stored in the cloud is operated over the internet. The paper [16] proposes a big data-based security model for the cloud called

Big Cloud. The main goal is to address security concerns through automatic security evaluation. The system is validated using a case study of the Apache Hadoop stack, evaluating the strengths and weaknesses of the proposed methodology.

Big data faces several challenges due to data storage, data misuse, and illegal access. This research [17] addresses these issues and proposes an encryption technique for large-scale data storage in multiple cloud storages. The study's main objective is to provide a secure architecture that restricts unauthorized access to the system. The proposed framework involves processes such as uploading, slicing, indexing, distributing, decrypting, retrieving, and combining data. The study introduces a hybrid cryptographic method to secure vast amounts of data before storing them in multiple clouds.

The proposed methodology in this study [18] starts by examining the already in-use tiered cloud architectures before presenting a solution for storing massive data. The study then focuses on the usage of a P2P Cloud System (P2PCS) for processing and analyzing large data. Additionally, a case study is presented, which is related to the healthcare system, and offers a hybrid mobile cloud computing approach consisting of cloudlets. The Mobile Cloud Computing Simulator (MCCSIM) is used to simulate the model, and the hybrid cloud model outperforms classic cloud models by up to 75%. To validate the security and privacy safeguards, the system is evaluated against potential threats.

Data in big data may be organized, unstructured, or semi-structured, providing critical insights for businesses to make informed decisions. Many businesses rely on big data to manage and analyse their data stores. Storage management is crucial to big data management to ensure that data is stored properly, securely, and readily available. Despite the numerous benefits of big data technology, it still faces storage management challenges, especially when combined with cloud computing, such as the significant issue of data security. This paper [19] addresses the aforementioned security challenge.

Jaleel [20] proposed a fragmentation scheme based on columns, where the server side stores encrypted pieces of data. Each fragment is assigned a unique ID to support queries through two processing stages. First, the client sends the ID to fetch data from the server, and then the client decrypts the fragment before using it for the query. The result is returned after executing the query on the fetched fragment. However, this method may not be suitable for large datasets as it requires significant overhead for the entire database. Additionally, the need to fetch the entire database to the client side eliminates the benefits of cloud computing's storage capabilities, and the need to perform the query twice slows down the overall performance. Thus, this strategy is not an ideal solution for this problem as it hinders the primary benefit of cloud computing's storage.

Tabassum [21] proposed a solution to the challenge of data confidentiality when outsourcing a database. They argued that no

software-based solution could be entirely secure due to inconsistent internet security standards, so they suggested using a smart card as a mediator on the cloud side. The smart card would encrypt the data before loading it into the database and decrypt it before sending it to the user. This approach assumes that the client and the cloud communication occurs securely. The system has processing power and memory capacity limitations due to the smart card's limitations and the challenges of inserting it into the cloud provider's server. Therefore, it is not a practical solution for outsourcing sensitive data, and the situation worsens if the database system needs to be distributed.

Imran et al. [22] proposed a technique to secure data stored on untrusted cloud providers. The authors differentiated between private and public data by encrypting sensitive information and storing it on a smart USB key. Non-sensitive data was stored in plain text on a public cloud server. However, this approach is not practical for general usage as it necessitates the use of a USB key to access or query the data. To connect the two segments, a distributed protocol was suggested.

Tabassum et al. [23] proposed an approach to improve the security of data stored with untrusted cloud providers by utilizing encryption techniques, a proxy, and the user's application. The method consists of six encryption techniques to handle different types of queries that cannot be solved with a single encryption algorithm. Other research studies in this area are also available.

Peter et al. [24] propose a new approach to enhance security by combining encryption techniques and a fragmentation methodology. The scheme's architecture is illustrated in Figure 1. The public clouds are composed of a master cloud and several slave clouds. The master cloud stores an encrypted clone of the entire database while individual public clouds store extended columns. Column-based fragmentation technique consists of two parts: master cloud and slave clouds. The whole database is encrypted with a highly secure encryption method and stored in the master cloud without providing the encryption key to the master cloud provider during initial setup. None of the keys are shared with the cloud service providers.

Abadi's study [25] developed a technique for secure query processing on cloud-based data storage using an order-preserving homomorphism encryption approach. The algorithm uses a secret-splitting strategy to enable the CSP to handle complex SQL queries. The proposed PHE approach provides a balance between security and efficiency in real-world settings, and is both effective and cost-efficient. To evaluate the algorithm's effectiveness in terms of overhead, query processing capability, storage, and computational costs, CSPs and AUs will conduct further assessments [26]

3. Security Concerns In Cloud

Integrity: Ensuring the integrity of information stored in a system is crucial to guarantee that the requested information accurately represents the original data and hasn't been tampered with by unauthorized parties. To

protect against potential data loss, each network service typically has multiple backup systems in place. Regular backups of data are usually stored on removable media, which are kept off-site for additional security [27].

Availability: In the context of computer security, availability refers to the assurance that authorized users can access computational resources and services whenever they need to. This is crucial for ensuring the uninterrupted operation of mission-critical systems, as any unauthorized activity that hinders access to these resources can have serious consequences. Therefore, maintaining high availability is a fundamental aspect of a robust security strategy [28].

Confidentiality: Maintaining data confidentiality is critical to prevent unauthorized access to sensitive information by third parties. Unauthorized access can occur through various means such as social manipulation, technical vulnerabilities, or failure to encrypt communications between clients and servers. Social manipulation can lead to actual loss of confidentiality while technical vulnerabilities can result in compromised security. Therefore, it is important to adopt appropriate measures to ensure data confidentiality [29].

Figure 3: Security Concerns in Cloud

4. METHODOLOGY

The methodology of the proposed research is shown in figure 4 and is divided into the following:

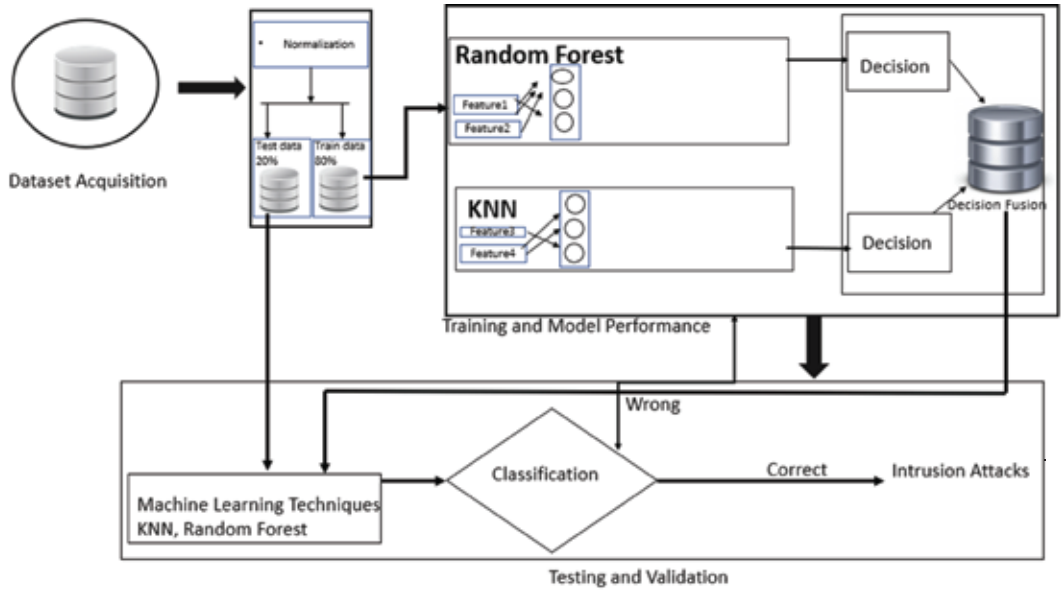

Figure 4: Proposed Methodology

4.1. Dataset Collection

The initial stage of the research involves gathering pertinent data. The UNR-IDD dataset is the focus of our investigation, which includes port statistics and TCP port data indicating changes in port statistics over a designated period. By examining network traffic at the port level where decisions are made, the port statistics offer a comprehensive analysis that enables the prompt detection of potential security breaches [30].

4.2. Preprocessing

This phase involves preprocessing operations on the dataset to remove artifacts such as null values and fabricated data. Proper preprocessing is fundamental as it greatly influences classification performance. If the data is not preprocessed correctly, the model will not produce the desired output [31].

4.3. Feature Extraction

The following data features have been captured in the targeted dataset:

Metrics and magnitudes are gathered from each port within the SDN during a simulated flow between two hosts in order to provide port statistics.

Delta Port Statistics: Change in collected metrics from each port within the SDN during a simulated flow between two hosts, observed over a 5-second interval for increased intrusion detection detail[32].

Flow Entry and Flow Table Statistics: Metrics that offer information on the network's switch conditions, gathered in any network environment, together with port statistics.

4.4. Training

In this phase, the model is trained for the task of evaluating network breaches. To address the challenge of tail classes, a targeted dataset is created with sufficient samples to enable machine learning classifiers to perform well. Furthermore, the dataset ensures completeness by having no missing data. In the proposed research, Random Forest and K-nearest neighbor are utilized to train the model [33].

4.5. Classification

The aim of this binary classification is to differentiate between normal operations and intrusions, with the ability to predict whether a network is under attack. However, the model does not provide information about the type or nature of the attack. Figure 5 shows data flow diagram of proposed systemc[34].

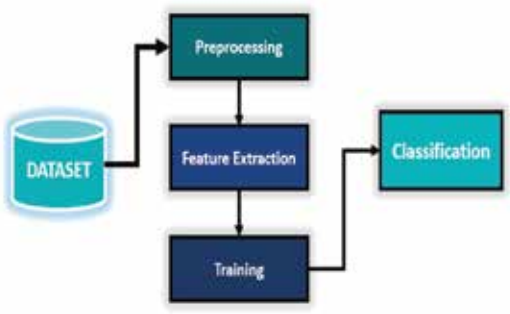

Figure 5: Data flow diagram

5. RESULTS

For the simulation of our proposed model we use Google Colaboratory where we implement our system using python. They diagram below shows the feature selection plot from our dataset [35].

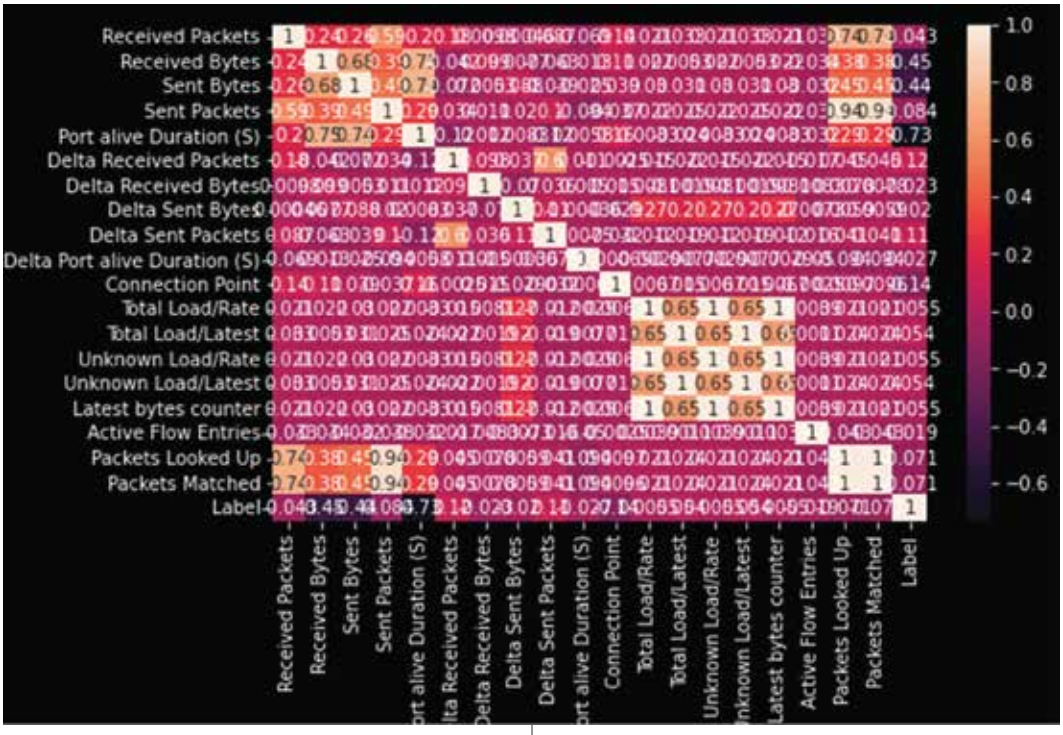

Figure 5: Feature Selection

A visual representation of the binary classifier labels is presented in Figure 6.

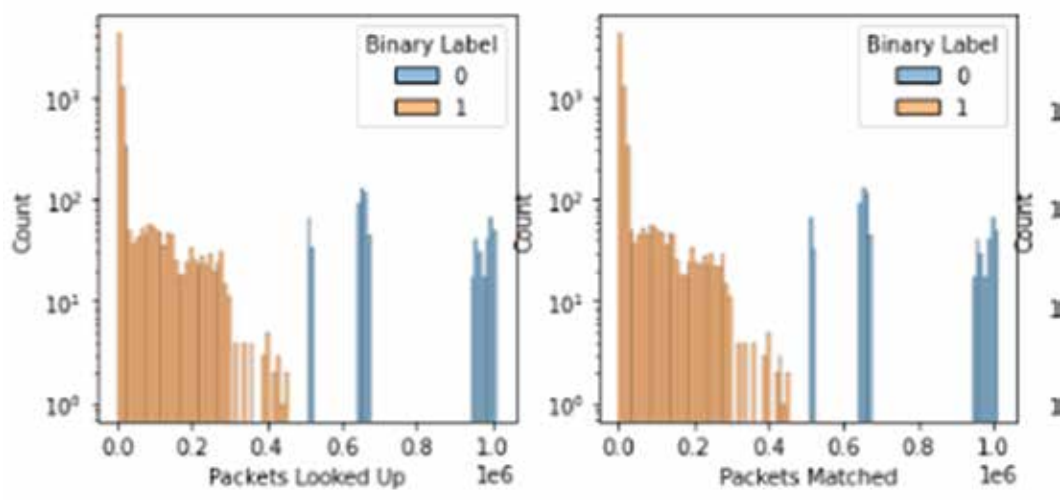

Figure 6: Packet Matching

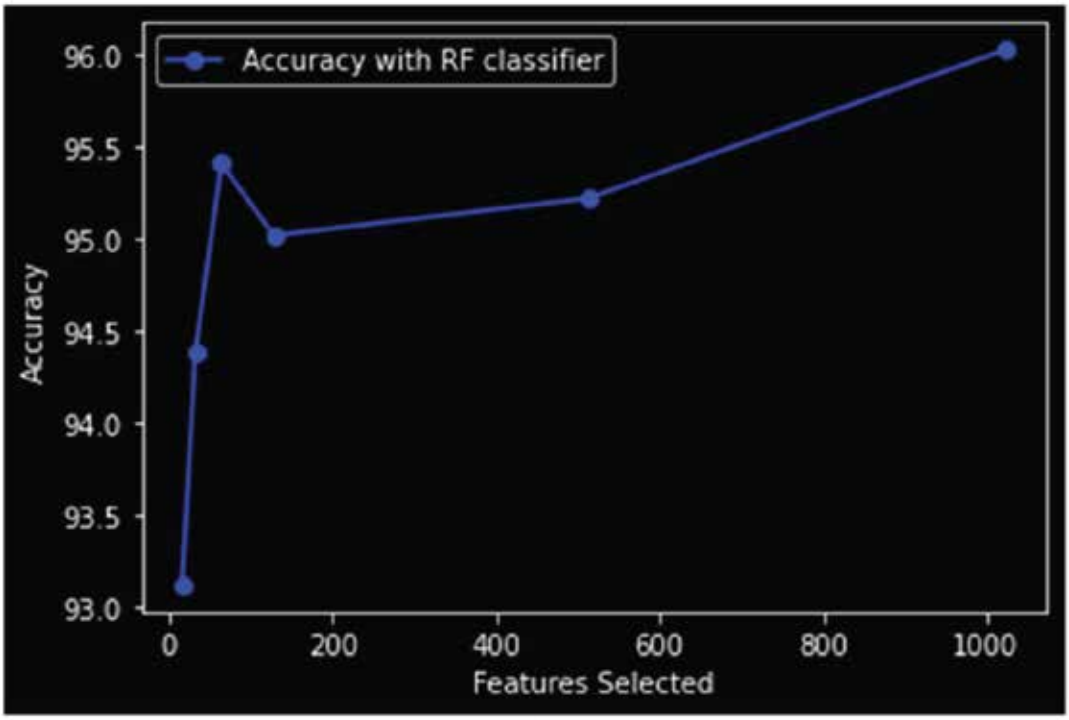

Figure 7: Accuracy Curve

In IoT-based cloud computing, network security is critical due to the large-scale deployment of IoT devices and the diverse nature of their communication. Machine learning techniques can play a crucial role in enhancing network security by leveraging the power of algorithms to analyze data and identify patterns or anomalies that indicate potential security threats [36].

One key application of machine learning is intrusion detection, where algorithms analyze network traffic data from IoT devices to identify known attack patterns. By examining network packets, data payloads, and device behavior, machine learning models can learn to recognize signatures of previous attacks and raise alerts when similar patterns are detected. This helps prevent unauthorized access and data breaches [37].

Another important aspect is anomaly detection. IoT devices generate massive amounts of data, and machine learning algorithms can be trained to understand the normal behavior of these devices. By analyzing historical data, machine learning models can identify deviations from the norm that may indicate security risks. For example, abnormal traffic patterns, unexpected data transfers, or unusual device behavior can be flagged for further investigation [38].

Machine learning can also contribute to device authentication and access control in IoT-based cloud computing. Machine learning models can differentiate between legitimate and unau-

thorised devices by analyzing device characteristics, communication patterns, and contextual information. This enables the enforcement of access control policies and prevents unauthorized access to cloud resources [39].

Security analytics is another area where machine learning can be applied effectively. Machine learning models can identify potential security events or trends by aggregating and correlating data from various sources, such as device logs, network traffic, and system logs. This enables proactive threat mitigation and facilitates informed security decisions [40].

Machine learning can also help in the analysis of threat intelligence feeds and security-related data to identify emerging threats and vulnerabilities in IoT-based cloud computing. By integrating external threat intelligence sources with internal network data, machine learning models can provide real-time threat detection, allowing quick response and mitigation measures [41].

Privacy and data protection are important considerations in IoT environments. Machine learning techniques, such as differential privacy, data anonymization, and encryption, can be employed to secure IoT data while preserving its utility for analysis and insights [42].

Furthermore, machine learning can facilitate predictive maintenance and security. By analyzing historical data on device performance, maintenance logs, and security events, machine learning models can identify patterns that lead to security vulnerabilities or device failures. This enables proactive maintenance and security measures to prevent future incidents [43].

The analysis demonstrates how machine learning techniques can be applied in IoT-based cloud computing to enhance network security. By leveraging the capabilities of machine learning algorithms, organizations can detect and prevent security threats, improve access control mechanisms, analyze security-related data, protect privacy, and implement proactive security measures. Continuous training, evaluation, and collaboration with experts are essential to ensure the effectiveness and accuracy of the machine learning models in evolving threat landscapes [44].

6. Conclusion

To validate the security of the system, binary classification is utilized for detecting attacks on cloud networks. Random forest classifiers achieved an accuracy of around 96.0%, while K nearest classifier had an accuracy of 93% and a precision value of 0.96. The proposed model ensures big data security against intrusion attacks on the network. While machine learning techniques can be powerful for protecting cloud computing networks, challenges still need to be addressed before these techniques can be widely adopted. Understanding the limitations and potential of machine learning approaches to network security can help researchers and practitioners develop more effective strategies for protecting their systems in a highly interconnected world.

7. References

[1]. N. Tabassum, A. Namoun, T. Alyas, A. Tufail, M. Taqi, and K. Kim, "applied sciences Classification of Bugs in Cloud Computing Applications Using Machine Learning Techniques," 2023.

[2]. M. I. Sarwar, Q. Abbas, T. Alyas, A. Alzahrani, T. Alghamdi, and Y. Alsaawy, "Digital Transformation of Public Sector Governance With IT Service Management–A Pilot Study," IEEE Access, vol. 11, no. January, pp. 6490–6512, 2023, doi: 10.1109/ACCESS.2023.3237550.

[3]. T. Alyas, K. Ateeq, M. Alqahtani, S. Kukunuru, N. Tabassum, and R. Kamran, "Security Analysis for Virtual Machine Allocation in Cloud Computing," Int. Conf. Cyber Resilience, ICCR 2022, no. Vm, 2022.

[4]. T. Alyas, "Performance Framework for Virtual Machine Migration in Cloud Computing," Comput. Mater. Contin., vol. 74, no. 3, pp. 6289–6305, 2023.

[5]. T. Alyas, S. Ali, H. U. Khan, A. Samad, K. Alissa, and M. A. Saleem, "Container Performance and Vulnerability Management for Container Security Using Docker Engine," Secur. Commun. Networks, vol. 2022, 2022.

[6]. M. Niazi, S. Abbas, A. Soliman, T. Alyas, S. Asif, and T. Faiz, "Vertical Pod Autoscaling in Kubernetes for Elastic Container Collaborative Framework," 2023.

[7]. T. Alyas, A. Alzahrani, Y. Alsaawy, K. Alissa, Q. Abbas, and N. Tabassum, "Query Optimization Framework for Graph Database in Cloud Dew Environment," 2023.

[8]. T. Alyas, "Multi-Cloud Integration Security Framework Using Honeypots," Mob. Inf. Syst., vol. 2022, pp. 1–13, 2022.

[9]. Alyas, N. Tabassum, M. Waseem Iqbal, A. S. Alshahrani, A. Alghamdi, and S. Khuram Shahzad, "Resource Based Automatic Calibration System (RBACS) Using Kubernetes Framework," Intell. Autom. Soft Comput., vol. 35, no. 1, pp. 1165–1179, 2023.

[10]. G. Ahmed et al., "Recognition of Urdu Handwritten Alphabet Using Convolutional Neural Network (CNN)," Comput. Mater. Contin., vol. 73, no. 2, pp. 2967–2984, 2022.

[11]. M. I. Sarwar, K. Nisar, and I. ud Din, "LTE-Advanced – Interference Management in OFDMA Based Cellular Network: An Overview", USJICT, vol. 4, no. 3, pp. 96-103, Oct. 2020.

[12]. A. A. Nagra, T. Alyas, M. Hamid, N. Tabassum, and A. Ahmad, "Training a Feedforward Neural Network Using Hybrid Gravitational Search Algorithm with Dynamic Multiswarm Particle Swarm Optimization," Biomed Res. Int., vol. 2022, pp. 1–10, 2022.

[13]. T. Alyas, M. Hamid, K. Alissa, T. Faiz, N. Tabassum, and A. Ahmad, "Empirical Method for Thyroid Disease Classification Using a Machine Learning Approach," Biomed Res. Int., vol. 2022, pp. 1–10, 2022.

[14]. T. Alyas, K. Alissa, A. S. Mohammad, S.

Asif, T. Faiz, and G. Ahmed, "Innovative Fungal Disease Diagnosis System Using Convolutional Neural Network," 2022.

[15]. H. H. Naqvi, T. Alyas, N. Tabassum, U. Farooq, A. Namoun, and S. A. M. Naqvi, "Comparative Analysis: Intrusion Detection in Multi-Cloud Environment to Identify Way Forward," Int. J. Adv. Trends Comput. Sci. Eng., vol. 10, no. 3, pp. 2533–2539, 2021.

[16]. S. A. M. Naqvi, T. Alyas, N. Tabassum, A. Namoun, and H. H. Naqvi, "Post Pandemic World and Challenges for E-Governance Framework," Int. J. Adv. Trends Comput. Sci. Eng., vol. 10, no. 3, pp. 2630–2636, 2021.

[17]. W. Khalid, M. W. Iqbal, T. Alyas, N. Tabassum, N. Anwar, and M. A. Saleem, "Performance Optimization of network using load balancer Techniques," Int. J. Adv. Trends Comput. Sci. Eng., vol. 10, no. 3, pp. 2645–2650, 2021.

[18]. T. Alyas, I. Javed, A. Namoun, A. Tufail, S. Alshmrany, and N. Tabassum, "Live migration of virtual machines using a mamdani fuzzy inference system," Comput. Mater. Contin., vol. 71, no. 2, pp. 3019–3033, 2022.

[19]. M. A. Saleem, M. Aamir, R. Ibrahim, N. Senan, and T. Alyas, "An Optimized Convolution Neural Network Architecture for Paddy Disease Classification," Comput. Mater. Contin., vol. 71, no. 2, pp. 6053–6067, 2022.

[20]. J. Nazir et al., "Load Balancing Framework for Cross-Region Tasks in Cloud Computing," Comput. Mater. Contin., vol. 70, no. 1, pp. 1479–1490, 2022.

[21]. N. Tabassum, T. Alyas, M. Hamid, M. Saleem, S. Malik, and S. Binish Zahra, "QoS Based Cloud Security Evaluation Using Neuro Fuzzy Model," Comput. Mater. Contin., vol. 70, no. 1, pp. 1127–1140, 2022.

[22]. M. I. Sarwar, K. Nisar, and A. Khan, "Blockchain – From Cryptocurrency to Vertical Industries - A Deep Shift," in IEEE International Conference on Signal Processing, Communications and Computing (ICSPCC), September 20-23, 2019, Dalian, China, 2019, pp. 537–540. doi: 10.1109/ICSPCC46631.2019.8960795.

[23]. S. Malik, N. Tabassum, M. Saleem, T. Alyas, M. Hamid, and U. Farooq, "Cloud-IoT Integration: Cloud Service Framework for M2M Communication," Intell. Autom. Soft Comput., vol. 31, no. 1, pp. 471–480, 2022.

[24]. W. U. H. Abidi et al., "Real-Time Shill Bidding Fraud Detection Empowered with Fussed Machine Learning," IEEE Access, vol. 9, pp. 113612–113621, 2021.

[25]. M. I. Sarwar et al., "Data Vaults for Blockchain-Empowered Accounting Information Systems," IEEE Access, vol. 9, pp. 117306–117324, 2021, doi: 10.1109/ACCESS.2021.3107484.

[26]. N. Tabassum, T. Alyas, M. Hamid, M. Saleem, and S. Malik, "Hyper-Convergence Storage Framework for EcoCloud Correlates," Comput. Mater. Contin., vol. 70, no. 1, pp. 1573–1584, 2022.

[27]. N. Tabassum et al., "Semantic Analysis of Urdu English Tweets Empowered by Machine Learning," 2021.

[28]. N. Tabassum, A. Rehman, M. Hamid, M. Saleem, and S. Malik, "Intelligent Nutrition Diet Recommender System for Diabetic ' s Patients," 2021.

[29]. D. Baig et al., "Bit Rate Reduction in Cloud Gaming Using Object Detection Technique," 2021.

[30]. G. Ahmad et al., "Intelligent ammunition detection and classification system using convolutional neural network," Comput. Mater. Contin., vol. 67, no. 2, pp. 2585–2600, 2021.

[31]. N. Tabassum et al., "Prediction of Cloud Ranking in a Hyperconverged Cloud Ecosystem Using Machine Learning," Comput. Mater. Contin., vol. 67, no. 3, pp. 3129–3141, 2021.

[32]. M. I. Tariq, N. A. Mian, A. Sohail, T. Alyas, and R. Ahmad, "Evaluation of the challenges in the internet of medical things with multicriteria decision making (AHP and TOPSIS) to overcome its obstruction under fuzzy environment," Mob. Inf. Syst., vol. 2020, 2020.

[33]. N. Tabassum, M. Khan, S. Abbas, T. Alyas, A. Athar, and M. Khan, "Intelligent reliability management in hyper-convergence cloud infrastructure using fuzzy inference system," ICST Trans. Scalable Inf. Syst., vol. 0, no. 0, p. 159408, 2018.

[34]. M. I. Sarwar, K. Nisar, S. Andleeb, and M. Noman, "Blockchain – A Crypto-Intensive Technology - A Review," in 35th International Business Information Management Association (IBIMA) Conference, November 4-5,2020, Seville, Spain, pp. 14803–14809.

[35]. M. A. Khan et al., "Effective Demand Forecasting Model Using Business Intelligence Empowered with Machine Learning," IEEE Access, vol. 8, pp. 116013–116023, 2020.

[36]. A. Amin et al., "TOP-Rank: A Novel Unsupervised Approach for Topic Prediction Using Keyphrase Extraction for Urdu Documents," IEEE Access, vol. 8, pp. 212675–212686, 2020.

[37]. S. Abbas, M. A. Khan, A. Athar, S. A. Shan, A. Saeed, and T. Alyas, "Enabling Smart City With Intelligent Congestion Control Using Hops With a Hybrid Computational Approach," Comput. J., vol. 00, no. 00, 2020.

[38]. M. Muhammad, T. Alyas, F. Ahmad, F. Butt, W. Qazi, and S. Saqib, "An analysis of security challenges and their perspective solutions for cloud computing and IoT," ICST Trans. Scalable Inf. Syst., pp. 166718, 2018.

[39]. M. Mehmood et al., "Machine learning enabled early detection of breast cancer by structural analysis of mammograms," Comput. Mater. Contin., vol. 67, no. 1, pp. 641–657, 2021.

[40]. N. Iqbal, S. Abbas, M. A. Khan, T. Alyas, A. Fatima, and A. Ahmad, "An RGB Image Cipher Using Chaotic Systems, 15-Puzzle Problem and DNA Computing," IEEE Access, vol. 7, pp. 174051–174071, 2019.

[41]. A. Alzahrani, T. Alyas, K. Alissa, Q. Abbas, Y. Alsaawy, and N. Tabassum, "Hybrid Approach for Improving the Performance of Data Reliability in Cloud Storage Management," Sensors (Basel)., vol. 22, no. 16, 2022.