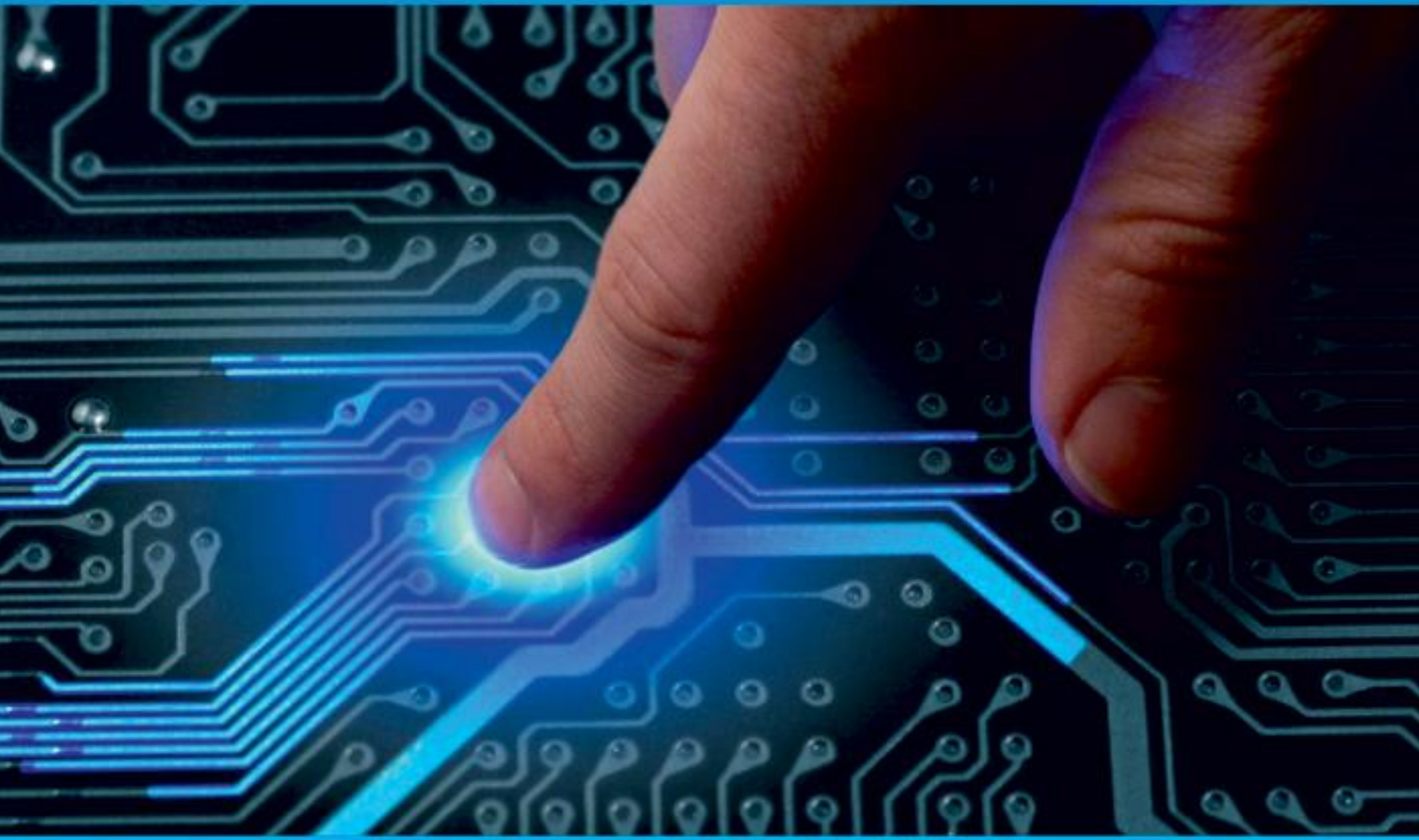
IJIRCCE

e-ISSN: 2320-9801 | p-ISSN: 2320-9798



INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

Volume 12, Issue 4, April 2024

INTERNATIONAL
STANDARD
SERIAL
NUMBER
INDIA

Impact Factor: 8.379

| DOI: 10.15680/IJIRCCE.2024.1204152 |

SecFedIDM-V1: A Secure Federated Intrusion Detection Model

Dr. V. Rama Krishna, Akalankam Godha Devi, Gangishetty Akhilesh, Bareddy Karthikeya Reddy

Assistant Professor, Department of CSE, Anurag University, Hyderabad, India

Department of CSE, Anurag University, Hyderabad, India

Department of CSE, Anurag University, Hyderabad, India

Department of CSE, Anurag University, Hyderabad, India

ABSTRACT: Cloud computing, a innovation encouraging proficient utilize of computing foundations and a trade show for offering computing assets and administrations, faces noteworthy security challenges due to its complex and conveyed nature, making it an alluring target for cyber-attacks. These assaults posture extreme dangers to benefit quality and information keenness, privacy, and accessibility. The expanding complexity of cyber-attacks presents challenges in viably identifying interruptions. Conventional Interruption Location Frameworks (IDS) can be overpowered by tall activity and pernicious exercises. In spite of different Profound Learning (DL) approaches proposed as elective arrangements, relevant security issues endure, especially in unified cloud computing spaces. This work proposes a Secure Unified Interruption Discovery Demonstrate Form 1 (SecFedIDM-V1), coordination blockchain innovation and Bidirectional Long Short-Term Memory (BiLSTM) Repetitive Neural Arrange (RNN). CIDDS has been handled and separated into preparing, testing, and approval sets. SecFedIDM-Vl, a Python web app, captures arrange parcels to classify potential assaults as typical or malevolent. Assault parcels are recorded in a Hyperledger Texture blockchain, serving as a signature database for arrange hubs. Assessment comes about appear the prevalence of the 80:10:10 BiLSTM organize over GRU, accomplishing tall accuracy, review, and Fl Score. SecFedIDM-V1 can be sent nearby Firewalls in combined cloud computing situations to upgrade framework security.

KEYWORDS: Blockchain, intrusion detection, deep learning, recurrent neural network.

I. INTRODUCTION

Cloud computing offers IT services over the Internet, allowing users to access computational power provided by Cloud Service Providers (CSPs) and pay only for what they consume. This shift from upfront payments to pay-as-you-go models transforms capital expenses into operational expenses. Cloud computing encompasses various shared resources such as computation, storage, software applications, and network infrastructures, accessible to businesses and individuals via social media, email, and web application hosting.Key cloud storage solutions like AWS, Microsoft Azure Blobs, and Google Cloud Storage are widely used, with significant investments exceeding $1 trillion. The advantages of cloud computing include scalability, resource allocation based on demand, reduced management overhead, adjustable pricing models, and simplified application development and delivery. While large data centers entail significant upfront costs, smaller businesses can leverage federations of computing and storage utilities to achieve similar scale impacts.

Cloud federation supports interoperability through resource migration, redundancy, and the aggregation of complementary services from multiple providers. The primary service models in cloud computing are Infrastructure-as-a-Service (IaaS), Platform-as-a-Service (PaaS), and Software-as-a-Service (SaaS), each catering to different user needs. However, security concerns remain paramount, with cloud providers and users frequently reporting attacks. Active Intrusion Detection Systems or Models (IDS/IDM) are essential for securing IT cloud infrastructure, with Machine Learning (ML) algorithms increasingly employed to enhance security by accurately identifying and mitigating cyber threats.Traditional ML algorithms, such as Support Vector Machines (SVM) and Decision Trees (DT), have been used for developing IDMs, but they face challenges in handling large datasets efficiently. Deep Learning (DL) algorithms have emerged as a solution to overcome these challenges, especially in multi-class scenarios, by improving IDM performance. Blockchain technology has also gained prominence in ICT, offering a decentralized ledger for recording transactions without the need for trusted third parties. The paper proposes a Secure Federated Intrusion Detection Model (SecFedIDM-V1), leveraging Bidirectional Long Short-Term Memory (BiLSTM) deep learning algorithm to detect and classify malicious activities on the network. The classified packet details are stored in a blockchain ledger on a private network, serving as a signature database for enhanced security.

II. RELATED WORK

The excerpt presents a comprehensive overview of studies and proposed models in the realm of cyberattack detection, with a focus on intrusion detection systems (IDS) and their integration of machine learning (ML) and blockchain technologies. One notable approach discussed is a novel outlier-based method devised by Talaei Khoei and Kaabouch to detect zero-day cyberattacks with high precision. Their evaluation, utilizing datasets such as CICIDS2017 and NSL-KDD, showcased impressive detection accuracies across various attack types. Additionally, the excerpt highlights the development of the Hierarchical Deep Learning System based on Big Data (BDHDLS) by Sharafaldin et al., which leverages behavioral and content features to understand network traffic characteristics, achieving high accuracy rates on the ISCXIDS2012 dataset. Another noteworthy advancement is the adaptive ensemble learning paradigm introduced by Lee et al., which utilizes multiple basic classifiers and achieved improved detection effects on the NSL-KDD dataset. Moreover, various studies explored CNN-based models for network intrusion detection, hybrid IDS approaches combining classifier algorithms, and blockchain-based decentralized ML architectures for enhancing UAV performance. These efforts underscore the importance of integrating cutting-edge technologies to bolster cybersecurity measures and address evolving threats in an increasingly interconnected digital landscape.

Limitations and Challenges:
For your project, it's essential to address various aspects based on the limitations and insights gleaned from the literature. Firstly, ensure the datasets utilized align closely with your project's context, focusing on cyberattacks relevant to your application. Evaluate methods to enhance the robustness and generalization capabilities of intrusion detection models, considering techniques like data augmentation and hyperparameter tuning. Additionally, optimize model training and inference processes, exploring strategies such as model quantization and hardware acceleration for efficient deployment.

Integrating blockchain technology can bolster data integrity and decentralization within your system, but attention must be paid to privacy and security concerns. Implement encryption and access control mechanisms to safeguard sensitive data and ensure compliance with regulatory requirements. Rigorous validation experiments should be designed to assess system performance across various attack scenarios, with real-world testing recommended for validation.

User interface design is crucial for facilitating effective monitoring and analysis of network traffic. Develop intuitive interfaces with visualization tools and interactive features to empower users in identifying and responding to security threats. Continuous evaluation and iteration based on real-world feedback will be vital for refining and improving the system's effectiveness and practicality over time.

III. PROPOSED SYSTEM

The proposed architecture and its various components are presented and discussed in this section. The architecture in Fig. 1 depicts the proposed model deployed within a single cloud platform, while Fig. 2 illustrates SecFedIDM-V1 deployed in a Cloud Federation. In this federation, each cloud region hosts the model as a Network Intrusion Detection System (NIDS), as indicated in the diagram technology facilitates the secure replication of logs across all regions automatically.. Blockchain System Overview

A. Dataset Curation and Pre-processing:

We began by curating the dataset from the Coburg Intrusion Detection Data Sets (CIDDS), specifically tailored for OpenStack-based cloud systems like the FEDGEN Testbed. This dataset's attributes were outlined, emphasizing its relevance to modeling similar cloud platforms. The subsequent steps detailed the process of data curation and pre-processing for this study.

Step 1: Importing the dataset involved handling four Comma Separated Values (CSV) files. We stored the file locations in variables and initialized an empty list to hold the imported data. An iterative procedure was then employed to import and append each file into the list.

Step 2: We conducted a thorough check for missing values, NaN cells, and inconsistent data, removing any problematic rows from the dataset.

Step 3: Encoding categorical data was necessary to convert categories into numerical representations suitable for machine learning models. We applied one-hot encoding to the Attack Type and Proto columns.

Step 4: Feature selection was performed using the Pearson Correlation Coefficient (PCC) to identify and remove highly correlated columns, resulting in the selection of seven features.

Step 5: Numerical data underwent scaling or normalization using the minMaxScaler to ensure smooth gradient descent flow and expedite algorithm convergence.

Step 6: The dataset, containing 22,116,202 records after preprocessing, was divided into three subsets for training, testing, and validation purposes.

B. Design of the Deep Learning Models:

The CIDDS dataset, with 22,116,202 samples and 5 classes, was deemed suitable for supervised learning. We split the dataset into training, testing, and validation subsets and compared BiLSTM and GRU networks to determine the most suitable architecture for classifying traffic sequences in the proposed SecFedIDM-V1.

Both models shared a similar configuration, incorporating a dropout layer with a 0.1 dropout rate and a dense layer in the hidden layer. The models were multi-class, with classification outputs including 'normal,' 'portScan,' 'dos,' 'pingScan,' or 'bruteForce,' making the SoftMax activation function appropriate.

C. Network Monitoring and Packet Capture:

The cloud-native web application deployed on the federated cloud testbed utilized the SecFedIDM-V1 module for monitoring network traffic and identifying potential security threats in real-time. Network traffic was captured by a Packet Sniffer connected to the OpenStack network service Neutron, allowing for effective traffic classification.

D. Blockchain Component of the SecFedIDM-V1 Architecture:

Hyperledger Fabric served as a security layer to ensure the safety and security of records/logs. The process involved generating cryptographic keys and certificates, defining the business network, creating transaction configurations, launching network nodes using Docker images, creating channels, and joining peers to the channel. Finally, the chaincode was installed and instantiated to facilitate transaction processing within the network.

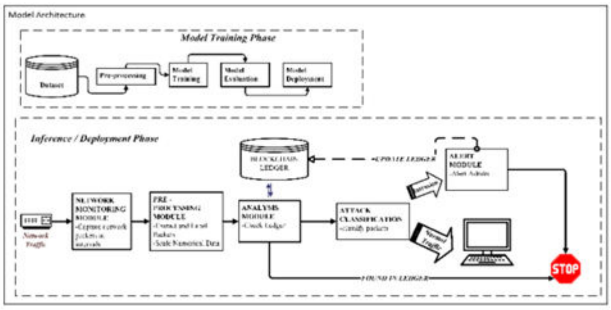


Figure 1.Architecture of the proposed SecFedIDM-V1.

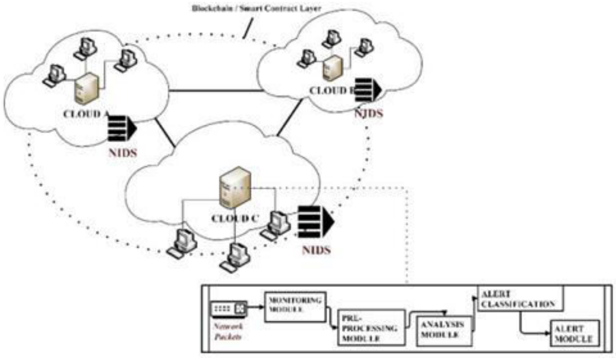
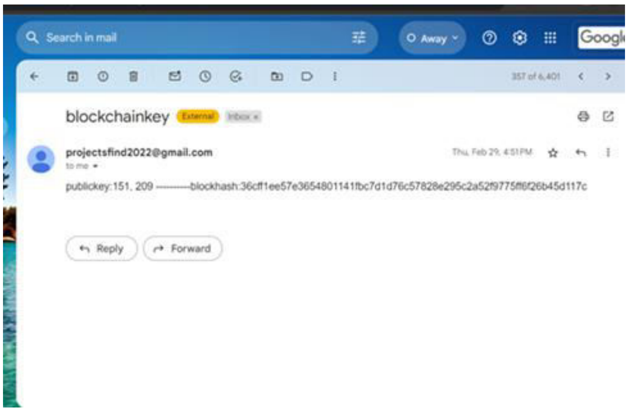


Figure 2. Architecture of the proposed

SecFedIDM-V1 within a federated cloud infrastructure

| DOI: 10.15680/IJIRCCE.2024.1204152 |

III. RESULTS



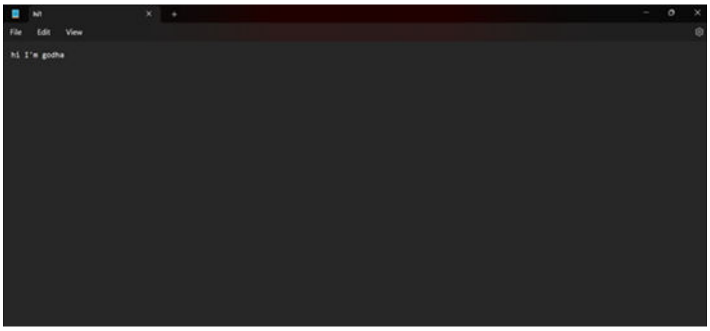
blockchainkey

projectsfind2022@gmail.com

Thu, Feb 29, 4:51 PM

publickey:151, 209 ----------blockhash:36cff1ee57e3654801141fbc7d1d76c57828e295c2a52f9775ff6f26b45d117c

Figure 3 Sending key to open the text file



hi I'm godha

Figure 4 Output Text File

COMPARISON WITH PREVIOUS METHODS:

The results obtained from the implementation of RecoverEase demonstrate notable improvements over previous methods of lost item management in several key areas:

Accuracy:

Traditional Methods: Traditional methods, such as rule-based systems and manual monitoring, rely on predefined signatures or human analysis to detect intrusions. While these methods may be effective in identifying known threats, they can be prone to false positives and may struggle to detect novel or previously unseen attacks.

Modern Methods: Modern intrusion detection methods, such as machine learning and deep learning algorithms, offer higher accuracy by leveraging advanced analytics and anomaly detection techniques. These methods can analyze large volumes of data to identify patterns and anomalies indicative of suspicious behavior, leading to more accurate threat detection.

Efficiency:

Traditional Methods: Traditional methods often require manual intervention and human analysis, leading to slower response times and inefficiencies in detecting and responding to security threats. Rule-based systems may also generate a high number of false alarms, requiring additional time and resources for investigation.

Modern Methods: Modern intrusion detection methods, particularly those based on machine learning and artificial intelligence, offer greater efficiency by automating the detection and response process. These methods can analyze vast amounts of data in real-time, enabling faster threat identification and response, thereby reducing the workload on security teams.

Scalability:

Traditional Methods: Traditional intrusion detection methods may struggle to scale effectively to meet the demands of large or complex networks. Manual monitoring and rule-based systems may become overwhelmed by the volume of network traffic or the complexity of attack patterns.

Modern Methods: Modern methods, such as machine learning and deep learning algorithms, are highly scalable and can adapt to changing network conditions and attack patterns. These methods can analyze large datasets efficiently and are well-suited for deployment in cloud-based or distributed environments.

Adaptability:

Traditional Methods: Traditional methods rely on static rules or signatures to detect intrusions, which may become outdated or ineffective against new and evolving threats. Manual updates to detection rules may be time-consuming and may lag behind emerging attack techniques.

Modern Methods: Modern intrusion detection methods are more adaptable and can continuously learn and evolve based on new data and emerging threats. Machine learning and deep learning algorithms can adapt their detection models in real-time, enabling proactive threat detection and response**.**

IV. CONCLUSION

The study addresses the growing need for secure transactions and communication within federated cloud platforms amidst
rising malicious activities and cyber-attacks. Introducing SecFedIDM-V1, a federated cloud platform equipped with a BiLSTM-based Intrusion Detection System (IDS), the research provides a multi-faceted approach to bolstering security. Firstly, a cloud federation testbed was developed utilizing OpenStack, establishing a foundation for experimentation. Secondly, leveraging the CIDDS dataset, experiments demonstrated the efficacy of BiLSTM RNN in detecting intrusion traffic, with superior performance metrics observed on the OpenStack-based testbed. Thirdly, to fortify the architecture's security, a blockchain was integrated to function as a secure datastore for intrusion signatures. Additionally, to facilitate usability for cloud system administrators, a cloud-native web application incorporating the BiLSTM IDS model was developed. As demonstrated in proof-of-concept scenarios, the application successfully detected various classes of malicious traffic with high precision. The flexibility of deployment on experimental or production-federated cloud platforms highlights the applicability and scalability of the solution. Looking ahead, future efforts aim to expand the architecture and web application to cover a broader spectrum of network attack classes, further enhancing the platform's defensive capabilities and adaptability to evolving threats.

REFERENCES

[1] M. R. M. Assis and L. F. Bittencourt, ‘‘A survey on cloud federation architectures: Identifying functional and non-functional properties,’’ J. Netw. Comput. Appl., vol. 72, pp. 51–71, Sep. 2016, doi: 10.1016/j.jnca.2016.06.014.

[2] O. Alkadi, N. Moustafa, and B. Turnbull, ‘‘A review of intrusion detection and blockchain applications in the cloud: Approaches, challenges and solutions,’’ IEEE Access, vol. 8, pp. 104893–104917, 2020, doi: 10.1109/ACCESS.2020.2999715.

[3] D. Villegas, N. Bobroff, I. Rodero, J. Delgado, Y. Liu, A. Devarakonda, L. Fong, S. M. Sadjadi, and M. Parashar, ‘‘Cloud federation in a layered service model,’’ J. Comput. Syst. Sci., vol. 78, no. 5, pp. 1330–1344, Sep. 2012, doi: 10.1016/j.jcss.2011.12.017.

[4] M. J. Molo, J. A. Badejo, E. Adetiba, V. P. Nzanzu, E. Noma-Osaghae, V. Oguntosin, M. O. Baraka, C. Takenga, S. Suraju, and E. F. Adebiyi, ‘‘A review of evolutionary trends in cloud computing and applications to the healthcare ecosystem,’’ Appl. Comput. Intell. Soft Comput., vol. 2021, pp. 1–16, Sep. 2021, doi: 10.1155/2021/1843671.

[5] B. Rochwerger, C. Vázquez, D. Breitgand, D. Hadas, M. Villari, P. Massonet, E. Levy, A. Galis, I. M. Llorente, R. S. Montero, and Y. Wolfsthal, ‘‘An architecture for federated cloud computing,’’ in Cloud Computing—Principles and Paradigms. Hoboken, NJ, USA: Wiley, 2011.

[6] T. Kurze, M. Klems, D. Bermbach, A. Lenk, S. Tai, and M. Kunze, ‘‘Cloud federation,’’ in Proc. 2nd Int. Conf. Cloud Comput., GRIDs, Virtualization, 2011, pp. 32–38.

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING