IJIRSET
International Journal of Innovative Research in
SCIENCE | ENGINEERING | TECHNOLOGY

e-ISSN: 2319-8753 | p-ISSN: 2347-6710

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

Volume 13, Special Issue 1, April 2024

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 8.423

9940 572 462 | 6381 907 438 | ijirset@gmail.com | www.ijirset.com

ISSN (Online) : 2319 - 8753
ISSN (Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology
An ISO 3297: 2007 Certified Organization Volume 13, Special Issue 1, April 2024
11th National Conference on Frontiers in Communication & Signal Processing Systems (NCFCSPS '24)
25th - 26th April 2024
Organized by
Department of ECE, Adhiyamaan College of Engineering, Hosur, Tamilnadu, India

A Novel & Effective Deep Learning Methodologies for Intrusion Detection in Cloud Computing

Muppa Varshitha[1], Dr.E. Saikiran[2]

Research Scholar, Department of Computer Science Engineering, Chaitanya Deemed to be University, Hyderabad, India[1]

Associate Professor, Department of Computer Science Engineering, Chaitanya Deemed to be University, Hyderabad, India[2]

ABSTRACT: This article seeks to inform that recent technologies and advancements have urged users to adopt a cloud-based environment. Due to the dispersed nature of cloud solutions, security is a major issue. Because it is highly exposed to intruders for any type of assault, security and privacy are major obstacles to the success of the on-demand service. A massive increase in network traffic has paved the way for increasingly difficult and widespread security vulnerabilities. Several intrusion detection systems have recently been suggested for cloud computing environments. The current IDS can exhibit overfitting, low classification accuracy, and a high false positive rate when provided with a large volume of variety of network data. In this study, we provide an effective optimal security solution for intrusion detection in a cloud computing environment using a hybrid deep learning algorithm. Preprocessing is performed using the improved heap optimization technique, which ensures data quality by removing unnecessary data from the data set. Then, for optimal feature selection, we offer a chaotic red deer optimization technique, which is responsible for dimensionality reduction due to big data. Then, for cloud attacks and intrusion detection and classification, a Kronecker deep neural network is shown. To illustrate its effectiveness, the proposed EOS-IDS strategy is evaluated on two benchmark datasets, DARPA IDS and CSE-CIC-IDS2018, and the results are compared with different existing IDS strategies.

I. INTRODUCTION

In recent years, cloud computing has become the most popular Internet-based technology in the information technology industry. A system layer, a platform layer, and an application layer are the three levels that make up cloud computing. The first two tiers deal with virtual machines and operating systems, while the third layer deals with cloud-based applications such as web applications. Along with the advantages and popularity of cloud computing, it faces significant challenges that act as obstacles to its growth. One of them is cloud security, which most companies consider a key barrier to cloud adoption. This is due to the open and completely dispersed nature of the cloud environment, making it more vulnerable to security threats and vulnerabilities. As a result, intruders are more likely to launch attacks against the cloud or cloud-connected devices. Another weakness of cloud security is that users access their data on distant servers in the cloud, with the cloud being fully responsible for storing and maintaining the data. On the other hand, cyberattacks and cloud services could have a detrimental influence on cloud computing infrastructure performance and QoS needs. Additionally, cloud computing customers are concerned about security issues that could jeopardize data availability or result in data loss. As cyberattacks become increasingly sophisticated, it is critical to develop attacks to prevent them and ensure the security of data stored and processed in cloud computing. Cloud computing now encompasses all components, including end users, networks, access control, and infrastructures. Security communities face issues ranging from data duplication to failure to discover security risks in a timely manner without a clear view of cloud architecture, as well as loss of control over data protection. and access to meet regulatory compliance.

ISSN (Online) : 2319 - 8753
ISSN (Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology
An ISO 3297: 2007 Certified Organization Volume 13, Special Issue 1, April 2024
11th National Conference on Frontiers in Communication & Signal Processing Systems (NCFCSPS '24)
25th - 26th April 2024
Organized by
Department of ECE, Adhiyamaan College of Engineering, Hosur, Tamilnadu, India

We anticipate fast new growth in the computational demands offered by cloud computing paradigms as cloud computing becomes more integrated into our daily lives and digital environments. Cloud computing presents several security problems due to data transfer and apps outside of customers' administrative domains. Investigation of security risks, vulnerabilities, and threats across multiple network levels is vital due to the crucial necessity of security in cloud computing.

Using Deep-Q network logic, a deep reinforcement learning-based IDS discovers and classifies complex network attacks in various dispersed agents and attention techniques. Density peak (DPeak) is a clustering algorithm that converts data of any dimension into two dimensions and automatically detects density centres and noise. A MapReduce-based intelligent model is presented to intelligently automate intrusion detection. MR-IMID is a network intrusion detection system that uses commodity hardware to consistently perform a range of data categorization tasks. An intelligent and effective network intrusion detection system (NIDS) based on deep learning uses a non-symmetric deep auto-encoder to give complete functionality and performance for network intrusion detection concerns. The long short-term memory is a system designed to identify and mitigate DDoS attacks in a public cloud network. An effective cloud IDS that improves the overall security of a cloud-based computing environment by using sandpiper-based feature selection and extended equilibrium deep transfer learning classification. To detect attacks at the fog node, a lightweight support vector machine IDS model based on cloud-fog cooperation is deployed. Distributed Denial of Service (DDoS) attacks are one of the most dangerous types of hostile invasions. DDoS attacks are difficult to counteract because they are high-level, difficult-to-absorb threats with a wide range of forms, attacks, and complexity. Machine learning techniques are used in cloud computing to provide an accurate and comprehensive strategy for detecting and preventing attacks.

For further enhancement in cloud computing, an efficient optimal security system is proposed for intrusion detection using hybrid deep learning technique (EOS-IDS). The main contributions of our proposed work are summarized as follows:

- An improved heap optimization (IHO) algorithm is used for data pre-processing which ensures the data quality through removal of unwanted data from dataset.
- A chaotic red deer optimization (CRDO) algorithm used for optimal feature selection process which selects best optimal features among multiple features.
- The hybrid deep Kronecker neural network (DKNN) is illustrated for cloud attacks and intrusion detection and classification.
- Finally, the efficacy of our proposed EOS-IDS approach is assessed using two benchmark datasets: DARPA IDS and CSE-CIC-IDS2018, and the findings are compared to several current IDS strategies.

II. PROBLEM METHODOLOGY

Integrating powerful machine learning algorithms into IDSs is becoming more important in safeguarding mobile edge computing systems. However, our current society's mobility necessitates increasingly complex IDSs to strike a fair balance between dealing with the enormous rise of traffic data and reacting to attacks. For intrusion detection, the Ant Lion optimization technique is combined with a novel optimized custom recurrent convolutional neural network. CNN is combined with LSTM.

III. PROPOSED METHODOLOGY

The working method of our suggested IDS model for cloud computing environment employing hybrid deep learning approach is described in this part (EOS-IDS). The working process is divided as three steps as follows:

- Pre-processing using improved heap optimization algorithm
- Feature selection using chaotic red deer optimization algorithm

ISSN (Online) : 2319 - 8753
ISSN (Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology
An ISO 3297: 2007 Certified Organization Volume 13, Special Issue 1, April 2024
11th National Conference on Frontiers in Communication & Signal Processing Systems (NCFCSPS '24)
25th - 26th April 2024
Organized by
Department of ECE, Adhiyamaan College of Engineering, Hosur, Tamilnadu, India

- Intrusion detection and classification using a deep Kronecker neural network

Simulation Results
We use the benchmark DARPA-IDS and CSE-CIC-IDS2018 datasets to verify our proposed EOS-IDS model in this part. The suggested EOS-IDS model includes the processes of data pre-processing with the IHO method, optimum feature selection with the CRDO algorithm, and intrusion detection with the DKNN classifier. To develop this EOS-IDS model in Jupyter Notebook, we used Anaconda 3.0, Scikit version 0.19.1, and Pandas version 0.23.1. In terms of accuracy, true positive rate (TPR), true negative rate

IV. CONCLUSION

In this paper, using a hybrid deep learning method, we suggest an optimal and efficient security solution for IDS in cloud computing. The following are the main contributions of our suggested EOS-IDS model: An enhanced heap optimization algorithm is used for preprocessing that ensures data quality by removing unwanted data from the dataset. A CRDO algorithm is used for optimal selection of features that are responsible for dimensionality reduction due

REFERENCES

1. E. Balamurugan et al, Network optimization using defender system in cloud computing security based intrusion detection system withgame theory deep neural network (IDSGT-DNN), Pattern Recognit Lett, (2022)
2. M. Mayuranathan et.al, An efficient optimal security system for intrusion detection in cloud computing environment using hybrid deep learning technique, Advances in Engineering Software, Volume 173, November 2022
3. J.K. Samriya et al. Network intrusion detection using ACO-DNN model with DVFS based energy optimization in cloud framework Sustain Computer Inf Syst, 2022
4. W. Qiu et al., Hybrid intrusion detection system based on Dempster-Shafer evidence theory Computer Security, 2022
5. K. Sethi et al., Attention based multi-agent intrusion detection systems using reinforcement learning, J Inf Security Application, 2021
6. M. Yan et al., Intrusion detection based on improved density peak clustering for imbalanced data on sensor-cloud systems, J Syst Arch, 2021
7. H. Aydın et al., A long short-term memory (LSTM)-based distributed denial of service (DDoS) detection and defense system design in public cloud network environment, Computer Secur,2022
8. M. Chen et al., FCM technique for efficient intrusion detection system for wireless networks in cloud environment, Computer Electrical Eng, 2018
9. S. Dey et al.
10. A machine learning based intrusion detection scheme for data fusion in mobile clouds involving heterogeneous client networks, Inf Fusion, (2019)
11. Abusitta et al.,A deep learning approach for proactive multi-cloud cooperative intrusion detection system, Future Gener Comput Syst,(2019)
12. Y. Aldwyan et al., Latency-aware failover strategies for containerized web applications in distributed clouds, Future Gener Comput Syst,(2019)

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

INNO SPACE SJIF Scientific Journal Impact Factor

doi cross ref

निस्केयर NISCAIR

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

9940 572 462 6381 907 438 ijirset@gmail.com

www.ijirset.com

Scan to save the contact details