International Journal of Advanced Engineering Research and Science (IJAERS)
Peer-Reviewed Journal
ISSN: 2349-6495(P) | 2456-1908(O)
Vol-12, Issue-2; Feb, 2025
Journal Home Page Available: ***https://ijaers.com/***
Article DOI: *https://dx.doi.org/10.22161/ijaers.122.5*

XKFHnet: Xception Kronecker Forward Fractional Net for Intrusion Detection in Cloud

D. R. Lodha[1], Dr Rokade P.P.[2]

[1]SND College of Engineering and Research Center Yeola, Savitribai Phule Pune University
darshanasethiya2012@gmail.com
[2]SND College of Engineering and Research Center Yeola, Savitribai Phule Pune University,
prakashrokade2005@gmail.com

Received: 11 Jan 2025,

Received in revised form: 12 Feb 2025,

Accepted: 19 Feb 2025

Available online: 25 Feb 2025

Keywords— ***Deep Learning, Hypervisor, Kronecker Neural Network, Virtual Machine, Xception***

Abstract— *In this new era of on-demand cloud computing, security is crucial. To find breaches in the cloud computing environment, researchers have surveyed a number of intrusion detection methods. The majority of them discuss conventional abuse and anomaly detection methods. By positioning the analysing component outside the virtual machine, usually at the hypervisor, Virtual Machine Introspection techniques are highly useful in identifying various stealth attacks that target user-level and kernel-level processes operating in VMs. Techniques such as Hypervisor Introspection protect the hypervisor and stop a compromised hypervisor from attacking virtual machines that run on it. Through the use of hardware-assisted used in virtualization-enabled technologies, introspection approaches examine the hypervisor. Our paper's primary goal is to present a thorough literature review of the many intrusion detection methods that have been suggested for cloud environments, along with an evaluation of their capacity to detect attacks. To clarify the vulnerabilities in the cloud, we offer a threat model and attack taxonomy. Our taxonomy of IDS techniques offers a thorough analysis of approaches together with their distinguishing characteristics, and it represents the state of the art in classification. In the survey, we have given a thorough understanding of methods based on Virtual Machine Introspection and Hypervisor Introspection. With the help of our study, researchers should be able to start investigating intrusion detection techniques in cloud environments.*

I. INTRODUCTION

With its various characteristics for increasing corporate efficiencies, cost-benefit analysis, and advantages over traditional computing processes, cloud computing has been in the spotlight for around 20 years [1]. The capacity to implement cloud-based threats and attacks has made it possible for hackers, attackers, and cyber invaders to have a high-quality plan globally, which means they can significantly impact the quality of the cloud environment. Numerous kinds of assaults can target cloud computing. These consist of identity theft, malicious insiders, unsecured interfaces and APIs, data loss, data breaches, and unknown risk profiles [2]. DoS/DDoS attacks and other cloud-based threats have the ability to quickly deactivate a target and cause significant financial losses. Threats and attacks continue to expand significantly and continuously, with an extended volume and criticality, even with the abundance of traditional threat detection systems. An entity that aims to take advantage of system weaknesses is referred to as an intruder in cybersecurity. Techniques based on anomalies or signatures can be used to identify intrusions.

While the anomaly-based approach, which compares user patterns to known patterns, has a high false positive rate of detection, outdated signature-based intrusion detection systems (IDS) are unable to adapt to new attacks. However, an efficient classification technique can be used to resolve issue. Users' data security and privacy are seriously jeopardized by cybersecurity problems.

Because cloud systems are open, new security dangers and assaults require more clever and efficient responses [3]. Network intrusions are one of the biggest security threats that many organizations deal with nowadays. The importance of network security has grown as a result of the quick development of big data, cloud computing, related technologies, and information, as well as the growing dependence of our everyday communications on networked services [4]. Persistently complicated adversaries can assault traditional security mechanisms like encryption systems and fire barriers. Detective, deterrent, corrective, and preventative controls are the four types of security controls that are used in the cloud. These controls employ deterrence control, which lowers the attack level by warning the system. To make preventive measures and techniques more resilient to intruder attacks, preventive control is employed. The procedure of corrective control aids in identifying the threat and employs techniques to retrain the system to fend against future assaults [5]. In the cloud context, the IDS is a component of the detective control utilized for security control mechanisms . In the cloud context, the IDS is a component of the detective control utilized for security control mechanisms. IDS can be either a software system that uses identification and alerting to automatically monitor threats or a hardware system that uses physical devices to identify threats. IDS have been categorized according to their location, mode of operation, and action . In the literature, several Machine Learning (ML)-based models for network intrusion detection have been put out; some of these models are currently in use in the commercial sector. IDSs come in three varieties: hybrid, anomaly-based, and signature-based. According to machine learning approaches in anomaly-based intrusion detection systems can be used to mitigate the known threat. This method uses unidentified patterns or signatures to identify the packet that the hackers have targeted. Because it models host, user, and network behavior, it is also known as a behavior-based detection system. As a result, an alarm is triggered if the system's behavior deviates from its typical pattern. The signature of the last known threat or attack is stored in the database of a signature-based intrusion detection system. It is possible to identify packets from intruders using the signature and packet patterns. This method has a very high detection accuracy. . When the system does not have the arriving packet signature, this approach does not work. Although hybrid intrusion detection systems (IDS) combine the two previously mentioned techniques, they are rarely employed since they do not yield the required detection accuracy.

II. LITERATURE REVIEW

The growing reliance on cloud computing has brought significant advantages, such as scalability, flexibility, and cost-effectiveness. However, these benefits also come with an increased risk of cyberattacks. Intrusion detection in cloud environments has therefore become a critical research area. Traditional intrusion detection systems (IDS) are often not sufficient to handle the scale, complexity, and dynamic nature of cloud systems. As a result, there has been a surge in research on using machine learning (ML), deep learning (DL), and advanced mathematical techniques for building more effective and scalable intrusion detection solutions. Below is a review of the relevant literature on the subject. Kavitha, C., Gadekallu, T.R., K, et "Filter-based ensemble feature selection and deep learning model for intrusion detection in cloud computing", Electronics, vol.12, no.3, pp.556, 2023. Deep Learning Model (DLM) used. This method offered more robust feature selections, reduced the chances of including noisy or less informative features. The dependency on statistical tests failed to capture non-linear relationships that were crucial for intrusion detection.[1]

Aldallal, A., "Toward efficient intrusion detection system using hybrid deep learning approach", Symmetry, vol.14, no.9, pp.1916, 2022. Gated recurrent units (GRUs) and improved long short-term memory (LSTM) through a computing unit (Cu-LSTMGRU). It provided a high level of symmetry between cloud computing security and the detection of intrusions and malicious attacks. This technique did not consider both memory utilization and time complexity.[2]

Chakravarthi, S.S., Kannan, R.J.et "Deep Learning Based Intrusion Detection in Cloud Services for Resilience Management", Computers, Materials & Continua, vol.71, no.3, 2022.It used Auto-Encoder (AE). This model resolved the security concerns in cloud services for its application in manufacturing sector. Failed to detect more number of attacks by enhancing the features set with more optimal features.[3]

Sajid, M., Malik, K.R., Almogren, A. "Enhancing intrusion detection: a hybrid machine and deep learning approach", Journal of Cloud Computing, vol.13, no.1, pp.123, 2024. This system used XGBoost-LSTM Group-Artificial Bee Colony (G-ABC). It executed more effectively and operated at peak efficiency. Also, it had quick detection speed. This technique prevented overfitting and improved training efficiency. It required more training time due to its complexity. More attacks were not evaluated to further extend the effectiveness of IDS[4].

Gulia, N., Solanki, K., Dalal, S. "Intrusion Detection System Using the G-ABC with Deep Neural Network in Cloud Environment", Scientific Programming, vol.2023, no.1, pp.7210034, 2023. In this paper Group-Artificial Bee Colony (G-ABC) is used. This technique prevented overfitting and improved training efficiency. More attacks were not evaluated to further extend the effectiveness of IDS[5].

Basahel, A.M., Yamin, M."Enhanced coyote optimization with deep learning based cloud-intrusion detection system", Computers, Materials & Continua, vol.74, no.2, pp.4319-4336, 2023. In this paper Enhanced Coyote Optimization with Deep Learning based Intrusion Detection System for Cloud Security (ECODL-IDSCS) was used. It can be utilized as an effectual tool to achieve maximum security in the cloud platform. The performance of the model was not improvised by the use of advanced DL classifiers[6].

Nazoksara, A.G. AutoIDS: A semantic autonomous intrusion detection system based on cellular deep learning and ontology for malware detection in cloud computing", 2024. Semantic autonomous intrusion detection system (SAutoIDS) was used in this paper. The autonomous nature and advanced detection capabilities allowed for quicker responses to attacks, thereby minimizing potential damage. It was capable to produce false positives or negatives, which led to unnecessary investigations or missed threats.[7]

Ogwara, N.O., Petrova, K. et "Towards the development of a cloud computing intrusion detection framework using an ensemble hybrid feature selection approach", Journal of Computer Networks and Communications, vol.2022, no.1, pp.5988567, 2022[8]. In this paper Cloud computing attack and intrusion detection (CCAID) system used. It was able to analyses heavy cloud computing network traffic in real time and detected attack packets with high detection accuracy and a low false alarm rate. It did not include validation of model with other network intrusion datasets.[9].

Challenges in Existing System

The challenges experienced by classical schemes that are collected regarding intrusion detection in cloud computing are described as follows.

DLM designed in [1] for intrusion detection in a cloud computing environment obtained effective results. How ever,this technique was failed to enhance performance and reduce over fitting.In[2], Cu-LSTMGRU model was introduced to improve IDS efficiency with low false alarm rate, though this approach did not address the data imbalance issues to achieve better results. To detect intrusion detection in cloud, XGBoost-LSTMwas presented in[4] with low test accuracy scores, but still it failed to detect a wide range of attack patterns as it did not use fusion methods. G-ABC [5] with the DNN model was used to select best features from the dataset. Nevertheless, this approach did not address the integration of a hybrid deep learning model, which was crucial for ensuring the model's scalability to handle large volumes of network traffic[10]. The increased adoption of cloud computing resources produces major loopholes in cloud computing for cybersecurity attacks. An IDS is one of the vital defenses against threats and attacks to cloud computing. Current IDSs encounter two challenges, namely, low accuracy and a high false alarm rate. Due to these challenges, additional efforts are required by network experts to respond to abnormal traffic alerts.[11]

Motivation

Primary motivation behind XKFHnet for cloud-based intrusion detection is to overcome the limitations of traditional IDS by leveraging the power of deep learning, advanced feature fusion techniques, and fractional networks. This approach aims to improve the detection of sophisticated and evolving cyberattacks, provide scalability for large cloud environments, and reduce false positives to ensure timely and accurate identification of threats in real-time. By incorporating models like Xception and Kronecker Forward Fractional Networks, XKFHnet promises to enhance the performance and reliability of intrusion detection systems in the ever-growing and complex cloud ecosystem.

III. PROPOSED SYSTEM

The **XKFHnet** project aims to develop a cutting-edge intrusion detection system tailored for the unique needs of cloud computing environments. The challenges associated with cloud-based IDS—such as handling large datasets, detecting evolving attacks, minimizing false positives, ensuring real-time performance, and addressing privacy concerns—define the scope of the project. By integrating Xception, Kronecker product fusion, and Forward Fractional Networks, the XKFHnet system offers a novel approach to overcoming these challenges and providing robust security solutions for cloud infrastructures.

The **XKFHnet** (Xception Kronecker Forward Fractional Net) is a deep learning-based model proposed for intrusion detection in cloud computing environments[12]. It combines state-of-the-art techniques from deep learning (Xception architecture), advanced mathematical feature fusion (Kronecker products), and fractional calculus to address the challenges of detecting sophisticated and evolving cyber threats in the cloud.

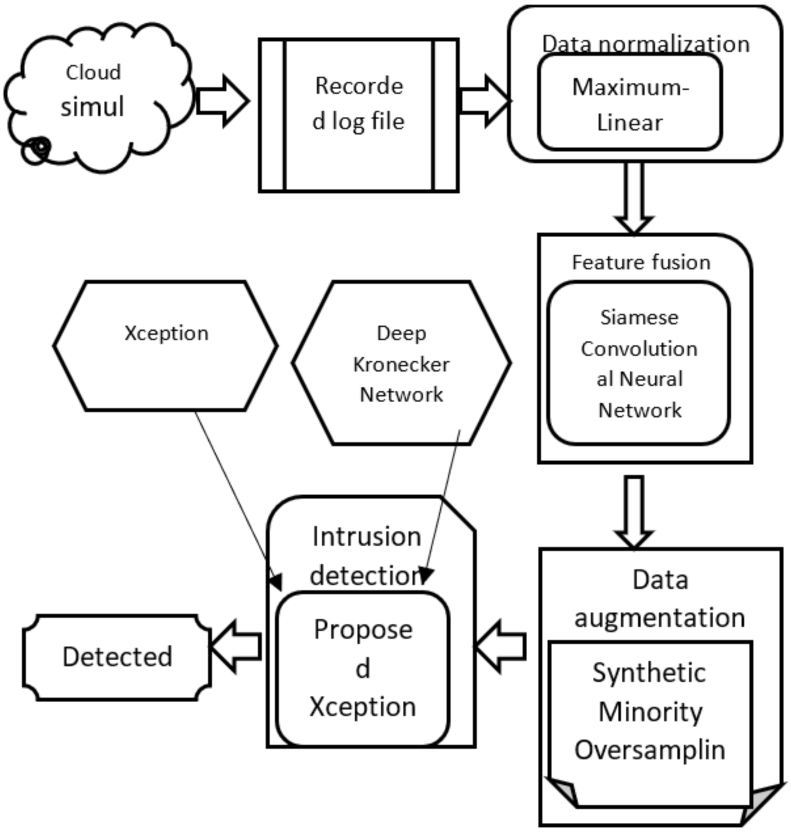

Fig.1.Block diagram of XKFHNet for intrusion detection in cloud

IV. WORKING

In Cloud Computing is the preferred choice of every IT organization since it provides flexible and pay-peruse based services to its users. Cloud Computing represents both a technology for using computing infrastructures in a more efficient way, and a business model for selling computing resources and services. On the other hand, such complex and distributed architectures become an attractive target for intruders. Moreover, the security and privacy are a major hurdle in its success because of its open and distributed architecture that is vulnerable to intruders. IDS is the most commonly used mechanism to detect attacks on cloud. The main aim of this research is to proposeXKFHNet for intrusion detection in cloud. Initially, cloud will be simulated and recorded log file will be taken from specific dataset [13],[14]. Then, data normalization will be carried out utilizing Maximum-Linear Normalization. After that, feature fusion will be conducted employing Siamese Convolutional Neural Network (SCNN) [15] with harmonic mean. Thereafter, data augmentation will be executed using SMOTE based oversampling [16] to enhance dimensionality of data. Next, intrusion detection will be performed employing XKFHNet. However, XKFHNet will be designed by combining Xception and Deep Kronecker Network (DKN) [17], where layers are modified based on Fractional calculus (FC) . Finally, attack mitigation will be conducted to reduce the impact or likelihood of attacks. The proposed XKFHNet will be implemented in PYTHON tool using data set mentioned in it. The performance of XKFHNet will be evaluated regarding metrics namely precision, recall and F1-score[18][19]. Additionally, designed XKFHNet will be compared with existing methods to prove its efficacy. Figure 1 demonstrates the block diagram of XKFHNet for intrusion detection in cloud.

V. APPLICATION

1.Network traffic analysis: IDS can analyze network traffic in real-time to detect threats and generate alerts.

2.Identifying known vulnerabilities: IDS can compare incoming packets against a database of known vulnerabilities to identify active instructions.

3.Threat detection: IDS can enhance threat detection and meet compliance mandates.

4. Threat prevention: IDS can help organizations stay ahead of the curve in threat prevention.

5. Network assurance and security: IDS can provide network assurance and security solutions.

VI. CONCLUSION

In this system we are using Xception Kronecker Forward Fractional Net (XKFHNet) for intrusion detection in cloud to improve detection rates of intrusions while managing the complexities of cloud-based network data. It will perform feature fusion, Siamese Convolutional Neural Network (SCNN)with harmonic mean is used for leveraging the strengths of different features while minimizing their weaknesses, leading to improved accuracy and robustness in predictive models .Also it will conduct data augmentation using Synthetic Minority Oversampling Technique (SMOTE) based over sampling to improve the dimensionality of data.

REFERENCES

[1] Kavitha, C., Gadekallu, T.R., K, N., Kavin, B.P. and Lai, W.C., "Filter-based ensemble feature selection and deep learning model for intrusion detection in cloud computing", Electronics, vol.12, no.3, pp.556, 2023.

[2] Aldallal, A., "Toward efficient intrusion detection system using hybrid deep learning approach", Symmetry, vol.14, no.9, pp.1916, 2022.

[3] Chakravarthi, S.S., Kannan, R.J., Natarajan, V.A. and Gao, X.Z., "Deep Learning Based Intrusion Detection in Cloud Services for Resilience Management", Computers, Materials & Continua, vol.71, no.3, 2022.

[4] Sajid, M., Malik, K.R., Almogren, A., Malik, T.S., Khan, A.H., Tanveer, J. and Rehman, A.U., "Enhancing intrusion detection: a hybrid machine and deep learning approach", Journal of Cloud Computing, vol.13, no.1, pp.123, 2024.

[5] Gulia, N., Solanki, K., Dalal, S., Dhankhar, A., Dahiya, O. and Salmaan, N.U., "Intrusion Detection System Using the G-ABC with Deep Neural Network in Cloud Environment", Scientific Programming, vol.2023, no.1, pp.7210034, 2023.

[6] Basahel, A.M., Yamin, M., Basahel, S.M. and Lydia, E.L., "Enhanced coyote optimization with deep learning based cloud-intrusion detection system", Computers, Materials & Continua, vol.74, no.2, pp.4319-4336, 2023.

[7] Nazoksara, A.G., Etminan, N. and Hosseinzadeh, R., "SAutoIDS: A semantic autonomous intrusion detection system based on cellular deep learning and ontology for malware detection in cloud computing", 2024.

[8] Ogwara, N.O., Petrova, K. and Yang, M.L., "Towards the development of a cloud computing intrusion detection framework using an ensemble hybrid feature selection approach", Journal of Computer Networks and Communications, vol.2022, no.1, pp.5988567, 2022.

[9] Koch, G., Zemel, R. and Salakhutdinov, R., "Siamese neural networks for one-shot image recognition", In proceedings of ICML deep learning workshop, vol.2, no.1, pp.1-30, July 2015.

[10] Zhou, S., Chen, B., Zhang, Y., Liu, H., Xiao, Y. and Pan, X., "A feature extraction method based on feature fusion and its application in the text-driven failure diagnosis field", 2020.

[11] Chollet, F., "Xception: Deep learning with depthwise separable convolutions", In Proceedings of the IEEE conference on computer vision and pattern recognition, pp.1251-1258, 2017.

[12] Feng, L. and Yang, G., "Deep kronecker network", arXiv preprint arXiv:2210.13327, 2022.

[13] Bhaladhare, P.R. and Jinwala, D.C., "A clustering approach for the l-diversity model in privacy preserving data mining using fractional calculus-bacterial foraging optimization algorithm", Advances in Computer Engineering, vol.2014, no.1, pp.396529, 2014.

[14] Lansky, J., Ali, S., Mohammadi, M., Majeed, M.K., Karim, S.H.T., Rashidi, S., Hosseinzadeh, M. and Rahmani, A.M., "Deep learning-based intrusion detection systems: a systematic review", IEEE Access, vol.9, pp.101574-101599, 2021.

[15] Abusitta, A., Bellaiche, M., Dagenais, M. and Halabi, T., "A deep learning approach for proactive multi-cloud cooperative intrusion detection system", Future Generation Computer Systems, vol.98, pp.308-318, 2019.

[16] Chkirbene, Z., Erbad, A., Hamila, R., Mohamed, A., Guizani, M. and Hamdi, M., "TIDCS: A dynamic intrusion detection and classification system based feature selection", IEEE access, vol.8, pp.95864-95877, 2020.

[17] Velliangiri, S. and Premalatha, J., "Intrusion detection of distributed denial of service attack in cloud", Cluster Computing, vol.22, no.5, pp.1