International Journal of Engineering Research-Online
A Peer Reviewed International Journal
ISSN: 2321-7758 http://www.ijoer.in editorijoer@gmail.com
Vol.14., S1, 2026
January

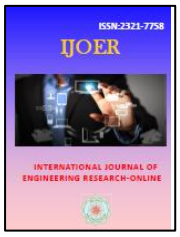
Special issue

ISSN: 2321-7758

Using Machine Learning to Automatically Find Attacks in Distributed Architectures as a Way to Make Cloud Security Better

Chatla Vijaya Kumar[1] and Saladi Devi Prasanna[2]
[1] Department of Computer Science, VKV GDC Kothapeta-533223, A.P., India.
[2] Department of Computer Applications, Pithapur Rajah's Government College (A), Kakinada-533001, A.P., India.
Corresponding Author: Email: vijaych.1789@gmail.com

DOI: 10.33329/ijoer.14.S1.135



Abstract
In decentralized systems, secure cloud security is important for keeping things running and keeping private information safe. Cloud-based distributed systems are more vulnerable and face more complicated threats that can get past regular security measures. The research examines the utilization of machine learning for autonomous threat detection in remote cloud systems. There are many places where data comes from, such as server logs, recordings of user activity, and network traffic. The DBSCAN algorithm finds strange behaviors by grouping data and looking for outliers. The Inter-Cloud Federation Framework (ICFF) lets cloud providers work together. This makes it easier to share information about threats and find attacks that happen in more than one cloud. The Sandpiper Optimization Algorithm (SOA) changes the settings for machine learning on the fly to make it easier and faster to find things. Future research should focus on making things more scalable and using new technologies like federated learning to make it easier to find and fix problems in different cloud environments in real time.

Keywords: DBSCAN, Sandpiper Optimization Algorithm, Machine Learning, Threat Detection in the Cloud, Distributed Systems, and the Inter-Cloud Federation Framework (ICFF)..

Introduction

Cloud computing makes it easier to set up, keep up, and expand distributed systems. These systems are cheap, easy to expand, and reliable, but they also make security harder in new ways. The distributed design makes it easier for insider threats, advanced persistent threats, and coordinated hacks to happen. Older security technologies that use signatures and static rules often miss new and complicated attacks. This means that we need security solutions that can change to deal with new threats.

Machine learning is a good way to automate risk detection because it can look at a lot of different kinds of data and find patterns that are out of the ordinary. Cloud-based distributed systems use machine learning models to look at data from apps, virtual machines, network traffic, and user actions to help keep hackers out. This study uses machine

learning to make cloud systems that are spread out more secure. DBSCAN finds weird things on its own, and the Inter-Cloud Federation Framework (ICFF) helps cloud providers share threat information with each other. This makes it easier to find attacks in different clouds. The Sandpiper Optimization Algorithm (SOA) changes the settings of machine learning on the fly to get the best results. The purpose of this technology is to improve automated threat detection in cloud systems by making it faster, more accurate, and able to handle more threats.

2. Methodology

The suggested method includes tools for finding problems, working together in the cloud, and making things better to make dispersed cloud systems safer. Collecting and cleaning data, finding problems, sharing information between clouds about possible threats, and making the whole system better are all parts of it.

2.1.Getting Information

One way to find out about cloud security is by looking at logs of network activity, such as packet flow, bandwidth usage, and connection attempts. Logs of events from servers and virtual machines. How things are used and how people get to them. Keeps track of what happens at the application level. All of these data points give a full picture of how the system works, which makes it possible to find strange behavior with great accuracy.

2.2 Getting the Data Ready

We process the data to make it work better before we give it to the model. This process includes reducing the number of dimensions, finding patterns, making the data more uniform, and getting rid of data that isn't needed. By getting rid of noise and extra features, it is easier to find groups and outliers.

2.3 How to Use DBSCAN to Find Weird Things

DBSCAN helps us find odd things in data that is kept in the cloud. It's better than other clustering algorithms because it can find noise and outliers without needing to know how many groups there are. When everything is working properly, DBSCAN puts data points that are close together into groups. When something bad or strange happens, the points look like they're by themselves. This method is good for finding new threats in systems that aren't very closely connected.

2.4 The ICFF, or Inter-Cloud Federation Framework

The ICFF lets cloud service providers share information about threats and strange behavior, which helps them work together. If one cloud in the group notices something wrong, it tells the others. When these groups work together, they make the whole system stronger because they can find attacks that happen between two or more clouds.

2.5 Using the Sandpiper Optimization Algorithm (SOA) to Make Things Better.

The Sandpiper Optimization Algorithm (SOA) changes important machine learning settings on its own, such as DBSCAN's epsilon and minimum points, to make detection more accurate and lower the number of false positives. It's easier to handle cloud workloads that change all the time when you can change settings in real time.

3. Discussion

DBSCAN, ICFF, and SOA together make a cloud security solution that is both smart and strong. DBSCAN can find strange behavior without needing data that has been labeled. This is good because it can be hard to find attack data that has been labeled in real cloud systems. ICFF makes things safer by letting people work together in the cloud. This is important for finding big, planned cyberattacks. SOA improves the system even more by letting you change model settings on the fly. This speeds up calculations and makes them more accurate. This system is more adaptable than fixed security methods because it can deal with new threats and changes in workloads. There are still

problems, like having to do more work to keep an eye on big systems and work together in the cloud.

Method	**Detection Technique**	**Adaptability to New Threats**	**False Positive Rate**	**Scalability**	**Key Observations**
Signature-Based IDS	Rule/Signature Matching	Low	High	Moderate	Ineffective against zero-day attacks
Statistical Models	Threshold-Based Analysis	Moderate	Moderate	Moderate	Sensitive to dynamic workload changes
ML without Optimization	Supervised/Unsupervised ML	High	Moderate	High	Performance degrades with static parameters
DBSCAN-Based Detection	Density-Based Clustering	High	Low	High	Effectively identifies anomalies without labeled data
DBSCAN + ICFF	Anomaly Detection + Threat Sharing	Very High	Low	Very High	Detects cross-cloud and coordinated attacks
Proposed Model (DBSCAN + ICFF + SOA)	Optimized ML with Inter-Cloud Collaboration	Very High	Very Low	Very High	Improved accuracy and real-time adaptability

4. Conclusion

This article talks about how to use machine learning to make decentralized cloud infrastructures safer. You can optimize models in real time with the Sandpiper Optimization Algorithm (SOA). The Inter-Cloud Federation Framework (ICFF) lets clouds talk to each other about threats. DBSCAN is good at finding things that are not normal. These parts work together to fix problems with the old ways of keeping the cloud safe. The suggested method is flexible, makes it easier to find threats, and works well in cloud environments that are always changing. The goal of future development is to make the system more flexible, make it cheaper for clouds to talk to each other, and add advanced features like deep learning models and federated learning. These changes should make it even easier to find and stop attacks on a lot of big cloud infrastructures in real time.

References

[1]. Buyya, R., Vecchiola, C., & Selvi, S. T. (2013). Mastering Cloud Computing. Morgan Kaufmann.

[2]. Alpaydin, E. (2020). Introduction to Machine Learning. MIT Press.

[3]. Bhuyan, M. H., Bhattacharyya, D. K., & Kalita, J. K. (2014). Network anomaly detection: Methods, systems and tools. IEEE Communications Surveys & Tutorials, 16(1), 303–336.

[4]. Ester, M., Kriegel, H. P., Sander, J., & Xu, X. (1996). A density-based algorithm for discovering clusters in large spatial databases with noise. Proceedings of KDD, 226–231.

[5]. Zhang, Q., Chen, M., Li, L., & Wang, Y. (2021). Inter-cloud security and trust management: A survey. Journal of Cloud Computing, 10(1), 1–18.

[6]. Abualigah, L., et al. (2020). Sandpiper optimization algorithm: A novel nature-inspired metaheuristic. Neural Computing and Applications, 32, 16829–16847.

[7]. Zissis, D., & Lekkas, D. (2012). Addressing cloud computing security issues. Future Generation Computer Systems, 28(3), 583–592.