System to Detect Cloud Security by Using Logging and Intrusion Detection

[1]Sumit Jadhav, [2]Prof. Dr. Santosh Gaikwad
[1,2] Department of Computer Applications JSPM University
doi.org/ 10.64643/JATIRV2I6-140369-001

***Abstract*— With technology becoming an essential part of modern businesses, these companies face many dangers associated with it. Among them are different types of cybersecurity attacks including unauthorized access. Other examples of such cybersecurity attacks include phishing, malware attacks, and intrusion attacks. This research proposes a Cloud Security Detection System that employs the methods of log analysis, intrusion detection and Artificial Intelligence to detect and prevent cyber threats. The proposed system uses various types of logs, which may include data about system activity, network flow, and user activity, to detect suspicious activities.**

With the help of machine learning and Natural Language Processing methods, the Cloud Security Detection Systems can detect problems or any malicious acts performed by hackers and intruders on the web. The Cloud Security Detection Systems can perform this task fast. Moreover, the Cloud Security Detection Systems use Intrusion Detection Systems to detect any signs of intrusion attempts. The Cloud Security Detection Systems will also analyze previous incidents to make sure that there was no intrusion before.

Apart from the ability to identify cyberattacks, the Cloud Security Detection Systems can send out notifications and respond to any dangerous situations without human assistance. The Cloud Security Detection Systems use the technique of analysis to detect any cyberattacks. In this way, they are able to identify such attacks more accurately and decrease the rate of false positives. The Cloud Security Detection Systems were implemented. They functioned effectively and detected many cyber threats.

The Cloud Security Detection Systems use machine learning and Natural Language Processing to detect problems or phishing attempts and other malicious acts committed by hackers. The Cloud Security Detection Systems can perform this task fast. Moreover, the Cloud Security Detection Systems employ Intrusion Detection Systems to find out whether anyone tries to gain access to the cloud infrastructure without authorization. The Cloud Security Detection Systems will also analyze previous instances of intrusion to determine whether there was any in the past.

In addition, the Cloud Security Detection Systems will issue notifications and respond when something suspicious occurs. The Cloud Security Detection Systems can do all this fast as

there will be no need for human interference. Finally, the Cloud Security Detection Systems use analysis to detect any cyber threats. As a result, it becomes easier to detect such threats more accurately and decrease the rate of false positives. The Cloud Security Detection Systems were implemented and performed successfully.

I. INTRODUCTION

The evolution of cloud computing has changed the way companies utilize resources in terms of storing, processing, and managing their information. Due to the advent of cloud computing, large cloud service providers such as AWS, Microsoft Azure, and Google Cloud Platform have enabled organizations to shift their information architecture to the cloud for a better, more flexible, and efficient working environment. However, the fast-paced technological development in this realm has also increased the number of vulnerabilities for cyberattacks.

Indeed, cybersecurity remains one of the most critical challenges of modern cloud computing. Due to constant emergence of new types of cyberattacks, which cannot necessarily be predicted and detected by conventional methods, many potential breaches can happen to jeopardize the security of valuable information. Below are some of the most prominent threats in the cloud computing ecosystem:

* Unauthorized access
* Loss or theft of data
* Phishing
* Malware
* Insider threats

Traditional rule-based security methods which operate on predefined rules and patterns often lack the capacity to effectively detect new cyber threats. Furthermore, the nature of modern cloud services involves large amounts of dynamic distributed data, which makes monitoring these log files for security breaches a very challenging task..

II. MOTIVATION

Organizations have started moving towards cloud computing, and as a result, they are changing the manner of storing, managing and processing data. Thanks to Amazon Web Services (AWS), Microsoft Azure and Google Cloud, organizations have scalable, flexible and inexpensive ways of taking advantage of cloud services. However, moving to cloud has created several security problems including access to confidential data, data leaks, misconfigurations and cyberattacks.

Traditional security measures are ineffective when it comes to protecting against threats in the cloud environment owing to its dynamic and distributed nature. The attackers are able to exploit any vulnerabilities in the cloud through various methods such as credential theft, privilege escalation and lateral movement; leaving undetectable traces in numerous logs produced by systems and networks.

What is needed here is an intelligent automation system capable of:Continuous monitoring of all cloud operations Analyzing the huge amount of data in logs Real-time detection of anomalies or intrusions Taking proactive actions

The difficulty of implementing cybersecurity is based on the fact that companies use cybersecurity solutions which rely on intelligence. Intelligence-based cybersecurity solutions perform better compared to conventional approaches to cybersecurity since the artificial intelligence can process a significant amount of data, be adaptive to different cybersecurity threats and improve the quality of threat detection over time. In such a manner, artificial intelligence is very effective in the protection from spamming, phishing and other kinds of e-mail threats in cybersecurity.

III. CONTRIBUTIONS OF THIS RESEARCH

Some critical problems have been tackled regarding cybersecurity and e-mail threats. What the paper contributes:

1) The paper offers an approach that aims at integrating the concepts of intelligent log analysis and intrusion detection for improving the security of cloud-based computing. Main contributions include:

(a) The Integrated Cloud Security Detection Approach The authors offer a conceptually unified framework that includes intelligent log analysis and intrusion detection systems. Typically, traditional approaches analyze logs and detect intrusions independently of one another. However, the integration of cloud security enables connecting multiple sources of information, including application logs, system logs, and even network traffic logs, in order to make a holistic evaluation of security events.

(b) The Real-time Log Analysis Approach

The authors offer a real-time mechanism to analyze logs in huge volumes and, thus, provide the possibility for detecting any potential security violations in a real-time manner. Such approach allows identifying potentially dangerous actions (failed login attempts, suspicious behavior of users, or anomalies of system configuration), preventing security threats.

(c) The Anomaly-based Intrusion Detection Model

Third contribution of the paper includes the development of an anomaly-based intrusion detection model. Such approach is especially valuable for enterprises as a large number of signature-based solutions do not identify any new kinds of attacks (so-called zero-day attacks).

IV. LITERATURE REVIEW

The increased use of cloud computing and digital commu-nication has caused a considerable amount of research to be conducted in the area of cybersecurity, focusing primarily on log analysis, intrusion detection, and AI-based threat detection systems.

The original methods utilized for intrusion detection were primarily signature-based. Signature-

based intrusion detection systems detect and compare system events to pre-set rules (or signatures) to identify known attacks. While this method of detection was successful for detecting attacks that had been previously seen, it could not detect attacks that were new or changed. To overcome the limitations of signature-based approach to intrusion detection, researchers created an anomaly-based intrusion detection system (IDS) that defines the normal behaviour of users and systems and marks events that deviate from normal behaviour as potential intrusions. Anomaly-based IDS' have had better success with detecting
zero-day intrusions, but a major disadvantage of anomaly-based IDS is that they tend to produce a high number of false positives.

Machine learning (ML) technologies created an opportunity for researchers to develop ML models for use in intrusion detection systems. Numerous different ML algorithms, such as decision trees, support vector machines (SVMs), k-nearest neighbour (KNN) and neural networks, have been applied to the modelling of normal and malicious behaviours for the purpose of intrusion detection. The models are able to improve their detection accuracy as they develop knowledge from historical data and/or adapting to new patterns over time. However, the performance of these models is strongly impacted by the quality and quantity of training data used in their creation.

A. Predictive Threat Intelligence and Automation

Cyber threats are becoming more complex. CSO Magazine (July 2017) states that organizations need proactive systems, such as Predictive Threat Intelligence with automation, for early detection and quicker response to cyber attacks with less human interaction than traditional security measures have been able to provide thus far.

V. RESEARCH GAPS AND PROBLEM STATEMENT

Research Gaps:

Poor integration between log analysis and email intrusion detection in AI-based email intrusion detection systems Poor performance of anomaly detection system in terms of high false-positive rates Scalability issues when implementing real-time detection Large number of cloud-based emails that cannot be processed in real time Lack of consideration of adaptive learning algorithms to deal with changing threats

Problem Statement: Existing solutions do not offer an integratedapproach to detect email-based attacks in cloud computing technology These tools have advanced technologies that make it difficult to detect any anomalies. Moreover, their response time is very low, and they struggle to manage massive volumes of data. These tools exhibit poor detection accuracy due to their complex technologies. These detection tools are equipped with advanced technologies that create problems. This study will design an AI-based email intrusion detection system that integrates log analysis and intrusion detection in real-time to enhance detection accuracy, scalability, and immediate response to potential threats

VI. PROBLEM STATEMENT

In terms of cloud security, it is important to pay attention to the fact that the Cloud Security Detection System is crucial as it provides log analysis and intrusion detection. As for the latter, it should be noted that a variety of services such as Amazon Web Services generates large volumes of logs which cannot be analyzed manually.

Thus, the solution to this problem consists in the automatic collection and intelligent analysis of logs. The Cloud Security Detection System provides both anomaly-based detection and signature-based detection, thus making it possible to detect both known and unknown threats to cloud infrastructure. Various intrusion detection systems like Snort and Suricata monitor the current state of affairs on our network and hosts.

However, there is still a list of improvements to be made. Namely, there is too much false positives detected by the system, as well as too much data in the process. We need to ensure that the system will scale according to our needs.

If we integrate visualization tools like Kibana into the Cloud Security Detection System, we will get an insight into what happens in our network. These visualizations are represented on various dashboards. Thus, we can claim that Cloud Security Detection System can become an excellent way to ensure that our cloud infrastructure is protected.

VII. ARCHITECTURE MODEL

The Cloud Security Detection System, consisting of log analysis and intrusion detection system, is to be installed using an architecture that has several layers. Data acquisition constitutes the first layer and involves the acquisition of data from diverse sources including cloud infrastructures such as Amazon Web Services, application, system, and network log information. Ingestion software collects logs that are stored in databases and data lakes. Cleaning, structuring, and log analysis occur in the process layer using techniques based on signatures and anomalies to identify potential malicious actions. IDS software, including Snort and Suricata, continuously monitor all network and host activities. Generation of alerts would occur when there is any malicious activity identified, while blocking of malicious IP addresses will be done automatically.

VIII. DISCUSSION

Indeed, this system demonstrates the significance of incorporating log analysis and proactive approaches into intrusion detection techniques used in modern clouds. As the number of log files that may be produced by applications and services like Amazon Web Services grows, analyzing logs manually becomes an impossible task. That is why the use of the proposed Cloud Security Detection System makes the process of collecting information and analyzing the collected log files more efficient and fast.

Thanks to using both approaches, signature-based detection and anomaly-based detection, the system in question detects attacks of both types. By deploying tools like Snort and Suricata, one can ensure that network traffic and host activities are constantly analyzed, which enhances the monitoring process. Still, some challenges are present, such as the high frequency of false alarms, large volume of data, and scalability.

To further facilitate monitoring and enhance situation awareness, it is recommended to use visualization tools. By employing Kibana, the user will gain access to valuable insights and visual representations of various metrics and data available within the Cloud Security Detection System. Indeed, the system itself provides a proactive approach to cloud security; however, its proper functioning presupposes certain factors – the right configuration and constant improvement.

IX. LIMITATIONS

At the same time, the Cloud Security Detection System poses a number of challenges to its users. Nevertheless, the Cloud Security Detection System features a lot of advantages. The problem that arises while working with cloud platforms, for example, Amazon Web Services is handling huge amounts of logs. They can occupy all available storage space and hinder the ability to analyze the logs.

As well as that, the Cloud Security Detection System generates numerous notifications especially when working with anomalous behavior detection techniques. It is one of the main issues arising when working with the Cloud Security Detection System. In fact, Cloud Security Detection System was introduced to improve our safety. And the Cloud Security Detection System has a lot of issues which require further investigation and solving.

Signature-based detection tools such as Snort only detect previously identified attack patterns. That means that there is a risk that the signature-based system won't detect the so-called zero-day attacks because they haven't been seen before. Scalability of the suggested solution is another issue. An increased number of cloud solution operations will lead to increased requirements for computing resources and new techniques will have to be developed. Process-ing latency may influence real-time response time as well. Also, a significant amount of time and efforts will have to be spent on the integration of the Cloud Security Detection System into the existing infrastructure and maintaining its current state. Moreover, the perfor-mance of the cloud security detection system highly depends on configuration settings and experience of the person operat-ing the cloud security detection system.

X. FUTURE RESEARCH DIRECTIONS

Future research should concentrate on improvements and innovations, including increasing the accuracy, scalability and automation of Cloud Security Detection Systems, as well as enhancing the ability to effectively detect anomalies, including advanced machine learning and deep

learning algorithms. Such innovations would be crucial in detecting complex attack patterns within the cloud (in case of AWS) and enhance the accuracy of existing solutions by decreasing false positive results. Another way to develop future research in Cloud Security Detection Systems is to introduce real-time stream processing frameworks as a way to significantly increase efficiency while working with high-velocity log data. In this regard, it is important to detect emerging and zero-day attacks that may be based on the threats provided by other companies and not rely solely on solutions such as Snort. Application of Zero Trust Architecture would contribute to more robust access control policy and decrease the number of insider threats. The introduction of automated response system (SOAR) would result in more efficient handling of incidents and mitigate their impact at the earliest possible point. Finally, future research could benefit from considering privacy preserving techniques, for example, federated learning, thus ensuring safe usage of data and obtaining data for its analysis. As a summary, future research should concentrate on developing intelligent, adaptable, self-learning cloud security solutions.

XI. CONCLUSION

In general, a Cloud Security Detection System that analyzes logs and performs intrusion detection can be used as an efficient way of protecting cloud Computing systems. A Cloud Security Detection System uses logs generated by platforms like AWS, allowing continuous monitoring of user and system event activity. A Cloud Security Detection System provides various means of analyzing and detecting attacks, including use of tools like Snort. Many challenges of Cloud Security Detection System solutions are overcome in the proposed architecture due to its solid ground for proactive security measures in the cloud.

XII. CONCLUSION

A Cloud Security Detection System that uses log analysis and intrusion monitoring is a proven method for helping to protect today's cloud Computing environments. The Cloud Security Detection System leverages the logs created by plat- forms like AWS, providing the capabilities to continuously monitor and assess the activity of users and system events.This Cloud Security Detection System includes a variety of detection techniques with tools such as Snort, to improve real-time detection and response to potential threats.Many of the challenges associated with Cloud Security Detection Systems, including scalability, false positives, and complexity within the cloud infrastructure, are addressed with the proposed architecture as a strong foundation for proactive security within the cloud. Analysts utilize visualisation tools to assist in understanding threat patterns and system performance within the cloud.As a whole, the Cloud Security Detection System utilises proactive and real-time threat detection, shortened response times, and enhanced data protection. Additionally, continu- ous improvements in machine learning and automation will allow Cloud Security Detection Systems to continue evolving into more intelligent, adaptable systems that can effectively respond to new cyber threats.

REFERENCES

[1] K. Raskin, , S. Kumaraswamy, and S. Latif, Cloud Security and Privacy: An Enterprise Perspective on Risks and Compliance, O'Reilly Media, 2009. National Institute of Standards and Technology (NIST), Guidelines on Security and Privacy in Public Cloud Computing, Special Publication 800-144, 2011. European Union Agency for Cybersecurity (ENISA), Cloud Computing Security Risk Assessment, 2009. Snort, Cisco Systems, "Snort User Manual," Online. Suricata, Open Information Security Founda- tion, "Suricata Documentation," Online. Kibana, Elastic NV, "Kibana Guide," Online. Elasticsearch, Elastic NV, "Elasticsearch Reference," Online