Analysis of Wazuh SIEM's Effectiveness in Cloud Security Monitoring

Wasan Saad Ahmed[1,*], Ziyad Tariq Mustafa AL-Ta'I[1]

[1]Computer Science Department, College of Science, University of Diyala, Diyala, Iraq

Emails: wasan@uodiyala.edu.iq; ziyad1964tariq@uodiyala.edu.iq

Abstract

In today's rapidly evolving digital landscape and interconnected, organizations are increasingly dependent on cloud -based infrastructure, which introduces significant cybersecurity challenges due to escalating cyber threats and attacks. To effectively manage these threats, a central monitoring system is essential. Security Information and Event Management (SIEM) solution address these issues by providing real-time monitoring and analysis of security events. This research investigates the efficiency of the Wazuh SIEM system in monitoring AWS cloud services, EC2 instance, and File integrity. Wazuh automates the collection, centralization, and analysis of security events. This approach enables the detection of unauthorized activities, monitoring of file integrity, and collection of user activity logs in real-time. This study evaluates Wazuh SIEM's capabilities by executing different types of attacks in an AWS cloud environment. The result was that it generated 1774 security alert within one week. The findings demonstrate that Wazuh SIEM provides comprehensive security monitoring and threat detection, offering significant advantages for organizations security that utilize cloud services.

Keywords: Cloud Computing; Cloud Monitoring; Wazuh; Network security; Security Information

1. Introduction

Nowadays, cloud computing has become more commonly used over the years within organizations due to the numerous advantages it offers. The features and resources offered by cloud computing are constantly expanding such as elasticity, speed, pooling, and on-demand self-service, which is one of the main reasons why organizations are transferring to the cloud. It proposes many services and resources that can be effortlessly extended or reduced according to the organization's requests. This allows companies and businesses to professionally manage their IT infrastructure and optimize resource utilization. As the cloud continues to evolve at an alarming rate, the number of cloud service users is also increasing, as the establishments identify the benefits it brings in terms of cost-effectiveness, scalability, and agility. As a result, there is an enormous number of users heading towards cloud computing marketing space. Today's cloud environment has improved dramatically over time since its inception [1].

Now cloud platforms can provide various aspects and a service portfolio tailored to customer needs. Consequently, cloud platforms show a remarkable level of diversity. In 2023, 94% of company's worldwide use cloud computing services. The rate of increase 14% from 2020 [2].

As the utilization of cloud resources continues to grow, it also draws the attention of more advanced adversaries to exploit its potential. Cybercriminals have recognized the extensive value proposition that cloud platforms offer, allowing them to scale up their operations and carry out sophisticated attacks. According to a survey conducted between March 2022 and March 2023 among cybersecurity leaders of worldwide organizations shows on average, 66% of organizations worldwide were victim a ransomware attack [3]. Estimated cost of cybercrime to increase from 2023 to 2028 reaching 5.7 trillion USD (+69.94%) [4].

Cybercrime costs include damage and destruction of data, stolen money, lost productivity, theft of intellectual property, theft of personal and financial data, embezzlement, fraud, and post-attack disruption to the normal course

DOI: https://doi.org/10.54216/JCIM.150119
Received: April 13, 2024 Revised: June 11, 2024 Accepted: August 03, 2024

of business, forensic investigation, restoration and deletion of hacked data and systems, and reputational harm [5]. Therefore, an organization must continuously monitor its security status to limit the risk of a security breach because the security objectives is to protect the confidentiality, integrity and availability of resources for information and information systems which is also known as the IT infrastructure [6].

The attack also can be from within the organization itself as happened at Amazon by the case of Paige Thompson, a former Amazon employee find guilty in June 2022 for her involvement in the 2019 Capital One data breach. Thompson exploited vulnerabilities in cloud servers while working at Amazon Web Services, infiltrating Capital One and over 30 other companies, resulting in unauthorized access to sensitive personal data belonging to over 100 million individuals, including their names, dates of birth, and social security numbers [7]. Organizations frequently encounter difficulties managing problems in the cloud-computing environment because of a lack of visibility, accessibility to cloud resources and events, and lack of knowledge of the cloud architecture and security requirements [8]. Although cloud providers offer security tools but still has limited capability in monitoring and the attacker can attack these services. Therefore, there is a need for a platform with real-time monitoring to identify and respond to both insider activity and external threats. Security Information and Event Management (SIEM) systems play a vital role in cloud security by providing real-time monitoring, detection, and response capabilities. Wazuh is open-source platform offering comprehensive security monitoring and threat detection functionalities. This research paper aims to analyze the efficiency of Wazuh SIEM in monitoring cloud environments, focusing on its detection capabilities, integration with cloud services, and incident response effectiveness. The contributions of this study are:

- The research assesses Wazuh's capabilities in real-time monitoring, threat detection, and incident response within AWS cloud services, EC2 instances and file integrity monitoring.
- The research highlights how this framework can be effectively integrated into organizational security practices to enhance visibility and control over cloud resources.
- It provides a foundation for future studies aiming to enhance security monitoring tools and techniques for cloud infrastructures.
- The research outcomes can serve as a benchmark for evaluating other SIEM systems and their effectiveness in cloud security, fostering further innovation and development in the field.
- This research provides practical insights and guidance for organizations seeking to implement Wazuh SIEM for cloud security monitoring.

2. The Materials and Methods

Wazuh system are consist of three main components: the Wazuh server, Wazuh indexer, Wazuh dashboards, and Wazuh agent [9]. Wazuh platform with its components Wazuh server, indexer, and dashboard installed on local server. There are many cloud platforms available such as Microsoft Azure, Google Cloud, AWS Cloud, IBM, Alibaba Cloud, etc. Therefore, it is important to select the cloud platform to be monitored and then enable the model with Wazuh and begin the integration process. For this project, the Amazon AWS cloud platform was chosen to monitor. For full monitoring of the Amazon AWS cloud, two monitoring ways have been used:

2.1 Monitoring Amazon Elastic Compute Cloud (AWS EC2 instances):

Monitoring the integrity of files and all actions inside AWS EC2 instances is essential to gather various types of application, system, security, file logs within EC2 and send these logs to the Wazuh manager. For this study, two servers were creating one windows server and Linux server. The Wazuh agent installed on the EC2 instant wants to monitor as shown in Figure 1. AWS EC2 instance is a cloud-based virtual server provided by Amazon Web Services that offers highly customizable computational resources [10]. To monitor the file integrity the osses.conf file with agent server configure and add the path to the file want to be monitored.

2.2 Monitoring AWS services

To enhance security visibility, organizations can enable necessary services based on their system requirements and integrate them with a SIEM solution then ingest security events from these services into the Wazuh manager. All events from different sources collected and centralized in the one server, including details about instance configurations, unauthorized behavior, data stored in Amazon simple storage service S3, and more. This integration enables Wazuh to trigger alerts based on events obtained from AWS services, providing rich and comprehensive information about the infrastructure, thereby extending the security monitoring capabilities of the infrastructure. Through this enhanced monitoring and analysis, organizations can achieve a higher level of security and better protect their AWS environment. To integrate Cloud Trail services with Wazuh to ingest the logs create a bucket in S3 storage to store the CloudTrail events as shown in Figure 1. Cloud trail enabled and created trail

DOI: https://doi.org/10.54216/JCIM.150119
Received: April 13, 2024 Revised: June 11, 2024 Accepted: August 03, 2024

events and the bucket that created chosen to save CloudTrail logs. Additionally, created an Identity and Access Management (IAM) user and got credentials (access and secret key) to configure the AWS module in the Wazuh server.

The IAM user gave permission to access the logs from these services therefore a policy created with low privilege and read-only access to S3 and attacked to user Then create IAM roles with name siem-wahzu to a allows S3 to call cloud trail services and attached to user. Then configure the AWS model in osses.conf XML file in wazuh manager to ingest the logs to Wazuh and analysis them and generate alerts when the logs match the rules in Wazuh.

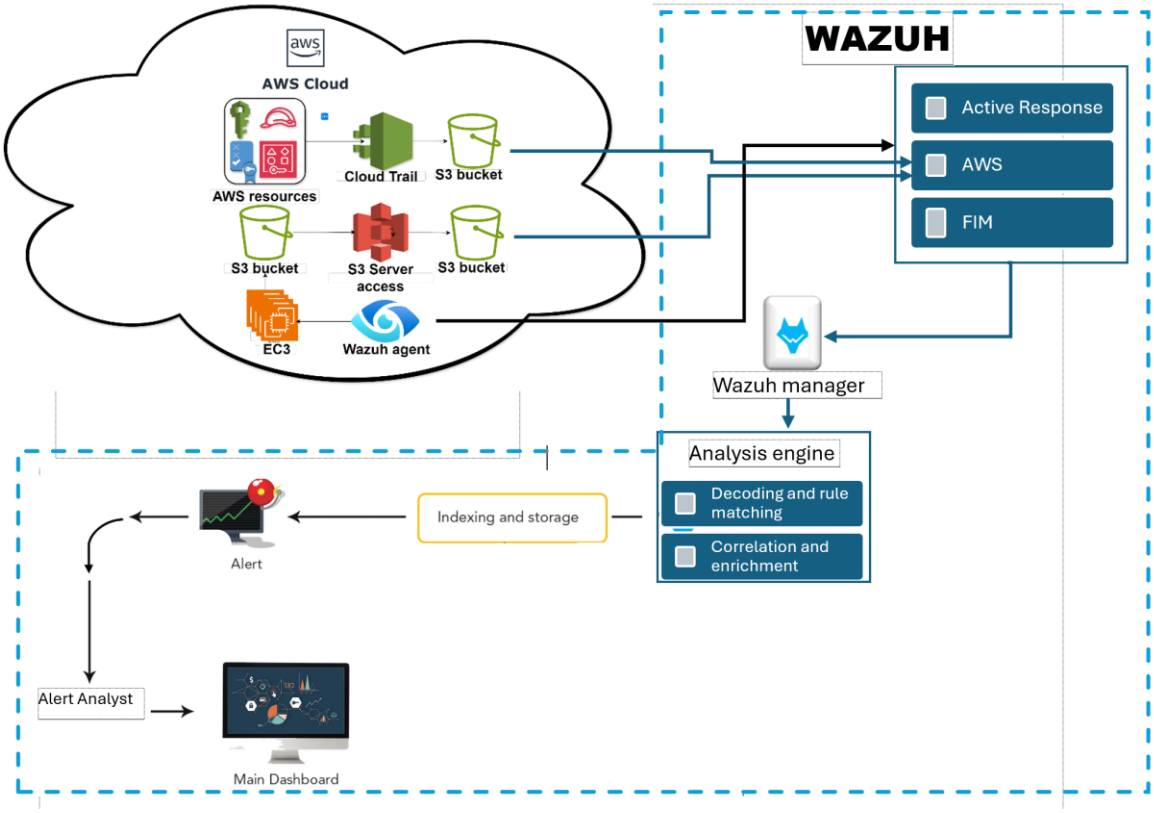

Figure 1. Integrated Wazuh to Monitor AWS

3. Experimental and Results

To evaluate the Wazuh to monitor the AWS cloud, detect the attack, and generate alert different scenario of attack executed. First scenario was performing the windows command shell attack T1059.003 that is sub-techniques from the technique Command and Scripting Interpreter. The attacker often uses command-line interface (CLI) to execute scripts in operating systems [11]. This attack applied by using Caldera[12].

The wazuh manager generat Security events alert with detailed data shown in Table1. In the rule description, describe the attack that Windows command prompt started by an abnormal process and classify based on MITRE ATT&CK framework with filed rule.mitre.technique that has the value Windows Command Shell.

Table1: Logs information on Windows Command Shell attack

Field Name	Values
agent.id	001
agent.ip	172.31.21.216
agent.name	windows
data.win.eventdata.commandLine	C:\Windows\system32\cmd.exe /c C:\"Program Files"\Amazon\EC2Launch\EC2Launch.exe run
data.win.eventdata.currentDirectory	C:\Windows\system32\
data.win.eventdata.description	Windows Command Processor
data.win.eventdata.image	C:\Windows\System32\cmd.exe

DOI: https://doi.org/10.54216/JCIM.150119
Received: April 13, 2024 Revised: June 11, 2024 Accepted: August 03, 2024

data.win.eventdata.integrityLevel	System
data.win.eventdata.product	Microsoft® Windows® Operating System
rule.description	Windows command prompt started by an abnormal process
rule.groups	sysmon, sysmon_eid1_detections, windows
rule.id	92052
rule.level	4
rule.mitre.id	T1059.003
rule.mitre.tactic	Execution
rule.mitre.technique	Windows Command Shell
timestamp	Jun 7, 2024 @ 09:57:30.743

The second scenario was executed BrutForec attack on Linux Server by through hydra library using the sub-technique, which is Password Guessing of Brute Force technique of credential access tactic [13]. There was Security events generated with detailed log shown in Table 2. In the full log field, found failed password for root and register the number of attempted with the field rule. Frequency, which is 8.

Table 2: logs from the security event about Brute Force attack

Fields	Rule. id 5760
GeoLocation.country_name	United States
GeoLocation.country_name	New Jersey
data.dstuser	root
data.srcip	68.183.48.199
data.srcport	34744
decoder.name	sshd
full_log	Jun 6 13:58:50 vmi1856092 sshd[164291]: Failed password for root from 68.183.48.199 port 34744 ssh2
rule.frequency	8
rule.groups	syslog, sshd, authentication_failed
rule.mitre.tactic	Credential Access, Lateral Movement
rule.mitre.technique	Password Guessing, SSH

The Third scenario was executed privilege escalation attack, which is the attacker try to get higher privilege [14]. To apply this attack, the vulnerability created with the user policy. Then by using the Pacu tool, the attacker found vulnerability after the enumeration and exploited it to give admin privilege policy to himself. This action detected with rule id 80202 and description "**PutUserPolicy**" as shown in Table 3 and the source for the logs information was Cloud trail.

Table 3: Summary of Detected AWS PutUserPolicy Event

Field Name	**Value**
Timestamp	June 15, 2024 @ 13:14:08.651
rule.description **rule.id**	AWS Cloudtrail: iam.amazonaws.com - PutUserPolicy.
rule.id	80202
rule.level	3
data.aws.eventName	PutUserPolicy
data.aws.eventSource	iam.amazonaws.com
data.aws.userAgent	Boto3/1.28.54 md/Botocore#1.31.54 md/awscrt#1.0.0.dev0 ua/2.0 os/linux#6.6.15-cloud-amd64 md/arch#x86_64 lang/python#3.11.8

DOI: https://doi.org/10.54216/JCIM.150119
Received: April 13, 2024 Revised: June 11, 2024 Accepted: August 03, 2024

	md/pyimpl#CPython cfg/retry-mode#adaptive Botocore/1.31.54
data.aws.eventID	896d21a0-65c9-4826-8f30-90a367bb3091
data.aws.userIdentity.userName	Mr-attacker (arn:aws:iam::724049165955 /Mr-attacker)
data.aws.source_ip_address	54.196.42.249
data.aws.requestParameters.policyDocument	{ "Version": "2012-10-17", "Statement": [{ "Effect": "Allow", "Action": "*", "Resource": "*" }] }
data.aws.requestParameters.policyName	8ldemhiwoe
MITRE ATT&CK Tactic	Privilege Escalation, Persistence
MITRE ATT&CK Technique	T1078 - Valid Accounts

The fourth scenario to test To test the File integrity monitoring (FIM) model to detect file changing after specifying the path to file that we want to monitor. A File called hacker test.txt created then modified for first time then to verify detection, another modification was made, and finally the file was deleted. Summary of security events that was manager generated in Table 4.

Table 4: Summery of alerts related to hacker-test file

Field	Add file	Modify1	Modify 2	delete
agent.id	003	003	003	003
agent.ip	172.31.93.137	172.31.93.137	172.31.93.137	172.31.93.137
decoder.name	syscheck_new_entry	syscheck_integrity_changed	syscheck_integrity_changed	syscheck_deleted
full_log	File 'c:\users\administrator\desktop\hacker-test (2).txt' added Mode: realtime	File 'c:\users\administrator\desktop\hacker-test (2).txt' modified Mode: realtime Changed attributes: size,mtime,md5,sha1,sha256 Size changed from '0' to '13' Old modification time was: '1719753181', now it is '1719753238' Old md5sum was: 'd41d8cd98f00b204e9800998ecf8427e' New md5sum is : 'd340ecf981583dbfbe7ff8efd78971ba' Old sha1sum was: 'da39a3ee5e6b4b0d3255bfef95601890afd80709' New sha1sum is : '1258e920fb7eefe3c1648212514246e631350a9a' Old sha256sum was: 'e3b0c44298fc1c149afbf4c8996fb92427ae41e4649b934ca495991b7852b855' New sha256sum is : 'd0f09869093dcae852c4b937	File 'c:\users\administrator\desktop\hacker-test (2).txt' modified Mode: realtime Changed attributes: size,mtime,md5,sha1,sha256 Size changed from '13' to '28' Old modification time was: '1719753238', now it is '1719753311' Old md5sum was: 'd340ecf981583dbfbe7ff8efd78971ba' New md5sum is : '82279a26699be1fb341747fecbdf34a4' Old sha1sum was: '1258e920fb7eefe3c1648212514246e631350a9a' New sha1sum is : 'a5c740132e74a87e0c76329c208b76f3aa9dee0f' Old sha256sum was: 'd0f09869093dcae852c4b93742564a79d3be6207fdf73576dcce623e2aaa43eb' New sha256sum is : 'ec188e4c44f8e842ac31fd26d	File 'c:\users\administrator\desktop\hacker-test (2).txt' deleted Mode: realtime

DOI: https://doi.org/10.54216/JCIM.150119
Received: April 13, 2024 Revised: June 11, 2024 Accepted: August 03, 2024

		42564a79d3be6207fdf73576dcce623e2aaa43eb	2a52a944002a1c2ef21aa9ec55fab1ce4e95ecb'	
rule.description	File added to the system.	Integrity checksum changed	Integrity checksum changed	
rule.id	554	550	550	553
rule.mitre.id		T1565.001	T1565.001	T1070.004, T1485
rule.mitre.tactic		Impact	Impact	Defense Evasion, Impact
rule.mitre.technique		Stored Data Manipulation	Stored Data Manipulation	File Deletion, Data Destruction
syscheck.diff		Hello world	Hello world2	ARCHIVE
syscheck.event		modified	modified	deleted
syscheck.path	c:\users\administrator\desktop\hacker-test (2).txt	c:\users\administrator\desktop\hacker-test (2).txt	c:\users\administrator\desktop\hacker-test (2).txt	c:\users\administrator\desktop\hacker-test (2).txt

The result of the entire security event that generated to monitor AWS with the alert level shown in Figuer2.

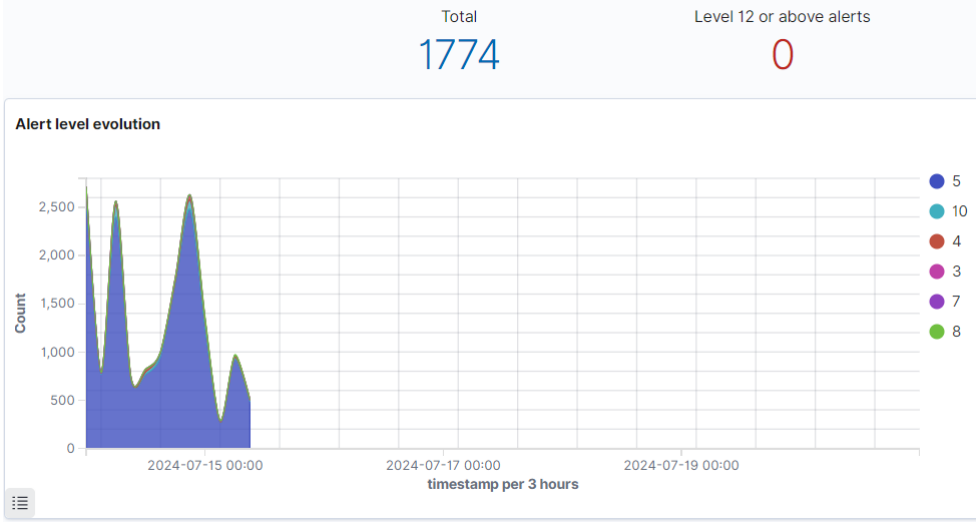

Figure 2. Number of Security event with alert level evolution

The limitation of this work, Wazuh used to monitor Amazon Web Services (AWS) only and not used across other cloud providers or in different cloud environments.

4. Conclusion

This study demonstrates the robust capabilities of the Wazuh Security Information and Event Management (SIEM) system in monitoring and securing cloud environments. By focusing on AWS cloud services, particularly EC2 instances and file integrity, Wazuh has proven effective in providing real-time monitoring, detecting unauthorized activities, and centralizing security events for comprehensive analysis. The research involved executing various types of attacks within an AWS cloud environment, during which Wazuh generated 1,774 security alerts over one week. This high alert generation indicates Wazuh's sensitivity and responsiveness to potential threats. The system's ability to automate the collection and analysis of logs, track user activities, monitor file integrity, and detect malware demonstrates its comprehensive threat detection and incident response capabilities. Wazuh's proficiency in providing detailed information on log events, user activity, file changes, the integration of Wazuh

DOI: https://doi.org/10.54216/JCIM.150119
Received: April 13, 2024 Revised: June 11, 2024 Accepted: August 03, 2024

with AWS cloud services enhances its capability to offer real-time insights and actionable intelligence, making it a valuable tool for organizations aiming to strengthen their cloud security posture. In conclusion, the findings of this study confirm that Wazuh SIEM is a highly effective tool for monitoring and securing cloud environments. Its comprehensive security monitoring and threat detection functionalities offer significant advantages for organizations utilizing cloud services, ensuring a proactive defense against cyber threats and enhancing overall cloud security. For future work, suggest to using wazuh monitoring different cloud environments.

Funding: "This research received no external funding"

Conflicts of Interest: "The authors declare no conflict of interest."

References

[1] Ahmed, O. (2024). Enhancing Intrusion Detection in Wireless Sensor Networks through Machine Learning Techniques and Context Awareness Integration. International Journal of Mathematics, Statistics, and Computer Science, 2, 244–258. https://doi.org/10.59543/ijmscs.v2i.10377

[2] "Cloud Computing Statistics (How Many Companies Use Cloud Computing?) - Colorlib." Accessed: Feb. 27, 2024. [Online]. Available: https://colorlib.com/wp/cloud-computing-statistics/

[3] "Ransomware attacks worldwide by country 2022 | Statista." Accessed: Feb. 27, 2024. [Online]. Available: https://www.statista.com/statistics/1246438/ransomware-attacks-by-country/

[4] "Global cybercrime estimated cost 2028 | Statista." Accessed: Feb. 27, 2024. [Online]. Available: https://www.statista.com/forecasts/1280009/cost-cybercrime-worldwide

[5] "Cybercrime To Cost The World $10.5 Trillion Annually By 2025." Accessed: Feb. 27, 2024. [Online]. Available: https://cybersecurityventures.com/cybercrime-damage-costs-10-trillion-by-2025/

[6] C. M. Gutierrez and W. Jeffrey, "FIPS PUB 200 Minimum Security Requirements for Federal Information and Information Systems," 2006.

[7] "Amazon Data Breaches: Full Timeline Through 2023." Accessed: Feb. 28, 2024. [Online]. Available: https://firewalltimes.com/amazon-data-breach-timeline/

[8] "Access control list (ACL) overview - Amazon Simple Storage Service." Accessed: Mar. 20, 2024. [Online]. Available: https://docs.aws.amazon.com/AmazonS3/latest/userguide/acl-overview.html

[9] "Components - Getting started with Wazuh · Wazuh documentation." Accessed: May 03, 2024. [Online]. Available: https://documentation.wazuh.com/current/getting-started/components/index.html

[10] P. Kumar Verma Ram Manohar, A. Choudhary, P. Kumar Verma, and P. Rai, "A walkthrough of Amazon Elastic Compute Cloud (Amazon EC2): A Review," vol. 9, 2021, doi: 10.22214/ijraset.2021.38764.

[11] "Command and Scripting Interpreter: Windows Command Shell, Sub-technique T1059.003 - Enterprise | MITRE ATT&CK®." Accessed: Jul. 11, 2024. [Online]. Available: https://attack.mitre.org/techniques/T1059/003/

[12] "Welcome to MITRE Caldera's documentation! — caldera documentation." Accessed: Jul. 11, 2024. [Online]. Available: https://caldera.readthedocs.io/en/latest/

[13] "hydra | Kali Linux Tools." Accessed: Jul. 11, 2024. [Online]. Available: https://www.kali.org/tools/hydra/

[14] "Privilege Escalation, Tactic TA0004 - Enterprise | MITRE ATT&CK®." Accessed: Jul. 11, 2024. [Online]. Available: https://attack.mitre.org/tactics/TA0004/

DOI: https://doi.org/10.54216/JCIM.150119
Received: April 13, 2024 Revised: June 11, 2024 Accepted: August 03, 2024