International Journal of Safety and Security Engineering
Vol. 15, No. 11, November, 2025, pp. 2323-2331
Journal homepage: http://iieta.org/journals/ijsse

Enhancing Private Cloud Security Using Knowledge Understanding Assessment Defense Method for Distributed Denial of Service Attack Mitigation

Hero Wintolo[1,2*], Imam Riadi[3], Anton Yudhana[4]

[1] Department of Informatics, Universitas Ahmad Dahlan, Yogyakarta 55198, Indonesia
[2] Department of Informatics, Institut Teknologi Dirgantara Adisutjipto, Yogyakarta 55198, Indonesia
[3] Department of Information System, Universitas Ahmad Dahlan, Yogyakarta 55198, Indonesia
[4] Department of Electrical Engineering, Universitas Ahmad Dahlan, Yogyakarta 55198, Indonesia

Corresponding Author Email: 2437083004@webmail.uad.ac.id

https://doi.org/10.18280/ijsse.151112

Received: 23 October 2025
Revised: 24 November 2025
Accepted: 27 November 2025
Available online: 30 November 2025

Keywords:
Goldeneye, OwnCloud, Knowledge Understanding Assessment Defense, Distributed Denial of Service mitigation, network forensics

ABSTRACT

Cloud computing provides significant flexibility and scalability; however, it is still susceptible to Distributed Denial of Service (DDoS) attacks, which pose a risk to service availability. This research presents an improved mitigation framework that incorporates the Knowledge Understanding Assessment Defense (KUAD) method within a private cloud environment utilizing OwnCloud. Simulations of Goldeneye-based DDoS attacks were conducted, with network performance being monitored through the use of Snort, Wireshark, nload, and iPerf. The attack resulted in a significant rise in network load, elevating jitter from an average of 0.1561 ms to 0.1519 ms and amplifying packet loss from 0.24% to 0.89%. The mitigation phase, which involved blocking attacker IP addresses, effectively restored service stability, minimized jitter, and greatly decreased packet loss. The results indicate that the KUAD framework facilitates the acquisition of forensic evidence while also allowing for prompt recovery through its built-in mitigation mechanism. The research presents a practical and adaptive defense model aimed at strengthening private cloud resilience in the face of DDoS attacks.

1. INTRODUCTION

The development of cloud computing has transformed the landscape of data storage and processing, providing remarkable scalability and cost-effectiveness. This technology allows for flexible data storage and access over the internet, providing users with the ability to retrieve information anytime and from any location. Nonetheless, connectivity through networks poses significant obstacles regarding the safeguarding of data. While conventional methods for encryption and decryption can successfully safeguard data, the decryption phase frequently demands significant computational power and may present possible security weaknesses [1]. At this stage, data is exposed to risks including cyberattacks and unauthorized access. To address these issues, innovative techniques such as homomorphic encryption and secret sharing have been developed as promising approaches. These techniques allow for computations to occur directly on encrypted data, eliminating the necessity for prior decryption and ensuring data confidentiality is preserved during processing in the cloud computing environment. These innovations signify an essential advancement in establishing a secure, efficient, and privacy-preserving cloud infrastructure that can effectively support contemporary digital ecosystems [2]. Furthermore, additional studies have suggested a clear geometric embedding inspired by the Coulomb approach to improve analytical resilience to local noise while maintaining computational efficiency. This method enhances cryptographic techniques by stabilizing data representation, which in turn facilitates more secure and efficient analysis in intricate cloud-based systems [3].

The advancement of data security approaches has resulted in notable progress due to innovations in encryption, decryption, and authentication mechanisms. The ongoing enhancements have strengthened the core of cloud security architecture, facilitated superior safeguarding of sensitive data, and created a more robust environment against emerging cyber threats [4]. Nonetheless, a primary difficulty in data security remains in the utilization of lengthy encryption keys. While extended keys can augment security, they simultaneously prolong encryption duration and diminish overall system performance [5]. Conversely, conventional authentication mechanisms, such as password-based systems, continue to be susceptible to numerous attack vectors, including credential theft and account hijacking. Biometric identification methods provide enhanced security through the use of physical or behavioral traits, although they possess intrinsic limitations. Vulnerabilities to spoofing, diminished accuracy due to alterations in users' physical conditions, and apprehensions regarding the privacy of biometric data pose persistent challenges that must be resolved in the deployment of authentication mechanisms within cloud computing environments [6]. Practical implementations have shown that

the coupling of biometric authentication with ECC encryption yields promising results in private cloud computing environments. This hybrid paradigm enhances the secrecy and integrity of stored data while facilitating more rapid encryption and decryption procedures than conventional RSA-based systems [7]. However, the integration of this method into cloud infrastructures requires additional research, especially on scalability and data privacy considerations [8].

Technical issues and cloud computing security also face challenges in detecting and preventing attacks [9]. Conventional Intrusion Detection and Prevention Systems (IDS/IPS) are only effective against known attack patterns, making them less capable of identifying zero-day attacks [10, 11]. Similarly, single-password or unimodal biometric authentication methods remain vulnerable to spoofing and phishing, highlighting the need for multifactor authentication [12]. Furthermore, traditional encryption algorithms are often inefficient on resource-constrained devices, making lightweight encryption approaches increasingly relevant [13]. Emerging technologies such as blockchain and machine learning (ML) are being integrated to enhance cloud security, although challenges remain in terms of scalability and computational complexity [14]. In the context of the Internet of Things (IoT), increasingly complex cyber threats have been addressed through the integration of ML and Deep Learning (DL) within IDS [15]. Therefore, there is an urgent need for adaptive and comprehensive cloud security solutions that combine multiple approaches [16].

Cloud computing serves as a fundamental component of contemporary information technology (IT) infrastructure; however, notable security challenges remain to be resolved [17]. The primary vulnerability of cloud computing is its susceptibility to Distributed Denial of Service (DDoS) attacks, which can disrupt service availability by overwhelming the server with excessive traffic [18]. A significant issue in data security involves the use of insufficient encryption and ineffective key management, which may result in the exposure of sensitive information [19]. Risks are generally mitigated through encryption methods and access control mechanisms as primary strategies [20]. Additionally, the application of attack mitigation strategies in Software-Defined Networking (SDN), applicable to both cloud and IoT infrastructures, can enhance detection and prevention mechanisms [21-23]. Nonetheless, a significant gap persists in the integration of AI-based methods with adaptive cloud security strategies [24]. A combination of behavioral analysis and ML has been proposed as an effective solution for detecting insider threats [25, 26].

The implementation of complex techniques to enhance cloud security presents ongoing challenges, especially regarding personal data protection and cybersecurity issues [27]. Additionally, energy consumption in the implementation of cloud security necessitates careful consideration due to its substantial power usage, which is comparable to that of supercomputing systems. Research on performance and energy efficiency has been carried out utilizing the Exa Mon framework, which employs a compositional methodology [28, 29]. The Improved Bald Eagle Search (IBES) algorithm has been proposed for the optimization of cloud resource allocation, presenting a more efficient alternative to traditional optimization methods [30]. Recent studies point out that cybersecurity is essential for protecting cloud systems against threats, including data ownership inconsistencies and security exploitations [31]. The zero-trust strategy has gained significance in risk management, as it effectively mitigates unauthorized access and privilege escalation [32]. Furthermore, it contributes to shaping positive users. Additionally, it plays a role in influencing favorable user perceptions of the security level associated with cloud services [33]. A promising approach is the application of deep reinforcement learning to enhance access control mechanisms [34]. User trust in cloud service providers is fundamentally influenced by the provider's capacity to manage and safeguard sensitive data [35]. The adoption of more secure cloud solutions is constrained by several factors, including uncertainty, a limited number of competent providers, and inadequate risk management capabilities in both public and private organizations [36]. Recent studies have emphasized the significance of optimization techniques, such as the pre-copy approach, in cloud container migration, as they can decrease service downtime and mitigate security risks during migration processes [37]. This study presents a unique contribution by applying the Knowledge Understanding Assessment Defense (KUAD) framework to a private cloud service utilizing OwnCloud to address Goldeneye DDoS attacks, an area that has not been thoroughly explored thus far. The literature indicates that while many studies have enhanced cloud security via encryption schemes, intrusion detection systems, and AI-driven models, the majority of approaches are confined to either preventive or reactive mechanisms. Limited frameworks offer a cohesive lifecycle that integrates attack detection, forensic analysis, and active recovery into a single workflow. Furthermore, current methodologies frequently neglect the feedback dynamics between forensic investigation and real-time mitigation. This gap leads to the current study, which presents the KUAD framework as a comprehensive method that identifies and analyzes DDoS attacks while also restoring system functionality through adaptive mitigation. This research seeks to fill a methodological gap, contributing to both theoretical and practical advancements in cloud security resilience. This paper is structured as follows. Section 2 outlines the research methodology, detailing the KUAD framework and its integration into the OwnCloud-based private cloud environment. Section 3 presents the experimental setup, attack simulation, and analysis results related to the Goldeneye DDoS mitigation process. Section 4 discusses the disposition phase and its significance in improving post-attack recovery and system resilience. Section 5 concludes the paper by summarizing the key findings and proposing directions for future research. This research introduces a methodological innovation by integrating a mitigation and recovery stage within the KUAD framework, thereby establishing a continuous feedback loop that connects attack detection, forensic validation, and system stabilization. Previous studies utilizing the Network Forensic Development Life Cycle (NFDLC) or related frameworks reach conclusions focused on fact-finding, lacking mechanisms for real-time response or service restoration.

2. RESEARCH METHOD

Previous research that underlies this research examined the creation of a method utilizing the NFDLC, with the Open Journal System (OJS) as the subject of investigation, specifically targeting a Trojan variant identified as Gacor [38]. Early forensic models, especially the NFDLC, prioritize systematic approaches for recognizing attack patterns, collecting evidence, and verifying digital artifacts. NFDLC,

while effective in forensic investigation, concludes with evidence analysis and lacks integration of real-time mitigation or system recovery. Research utilizing NFDLC, including forensic analysis of OJS, has shown effective detection capabilities; however, it has not addressed the need for mechanisms to stabilize system performance during attacks.

The second research paper employed the same research subject and attack type but utilized a different methodological approach, transitioning from NFDLC to the KUAD method. This research illustrates that integrating the mitigation phase before disposition significantly enhances the field of digital forensics.

In contrast to previous methods that generally concluded with fact-finding, KUAD innovatively integrates a system recovery phase aimed at restoring the environment to its pre-attack condition. Figure 1 illustrates that the mitigation phase follows the execution stage. The KUAD method [39] integrates the execution and implementation phases due to the similarity of activities performed in both stages. This research presents the KUAD framework, which offers a hybrid approach that integrates forensic acquisition, attack validation, mitigation, and recovery into a single lifecycle. Integrating a dedicated mitigation phase into the forensic workflow enables KUAD to establish a closed-loop system that effectively analyzes the attack and restores service conditions. This innovation addresses the methodological gap in current research, which often distinguishes forensic investigation from active defense measures. This consolidation simplifies the process and enhances the efficiency and effectiveness of the digital forensic investigation workflow.

Figure 1. Proposed method framework design

As illustrated in Figure 1, this research employs OwnCloud, configured as private cloud computing, as the primary research object. The framework proposed in this research is original, as it has not been previously introduced by other scholars in the domain of cloud security. The proposed KUAD framework demonstrates effectiveness through its systematic integration of knowledge understanding, assessment, and defense stages, adhering to the principles of the NFDLC. The KUAD method has a sequence of processes for handling cyberattacks, as follows:

1. Initiation

This stage primarily involves conducting an initial risk assessment of end devices and intermediary devices concerning potential attack faults. This assessment aids in decision-making concerning the software and hardware utilized, along with their susceptibility to attacks.

2. Acquisition

This stage aims to collect data used in the investigation, thus requiring several tools in the form of software. With established standards applied to the tools used, the evidence obtained can be utilized in subsequent processes.

3. Execution

The execution stage represents the integration of the implementation and operation stages within the NFDLC method. At this stage, data is collected to be used as evidence of criminal activity. This process also includes documentation so that the acquired data can be utilized without having to repeat the process from the beginning. In addition, any remediation of an attack must be properly documented as a form of preparation and anticipation in case a similar attack occurs with the same impact or an even higher level of damage.

4. Mitigation

This stage addresses the effects of attacks resulting in loss and damage to the targeted objects. At this stage, various techniques for mitigating cyberattacks are employed, categorized into repair and recovery methods.

5. Disposition

The final stage is disposition, in which the documents that have been prepared and created as part of security measures and protective actions for the attacked devices are submitted to the top management responsible within the relevant institution where the devices were attacked and have been mitigated.

The inclusion of the mitigation phase introduces a feedback mechanism that shortens the response loop between detection and recovery. This dynamic adaptation aligns with control theory, where system stability is maintained through corrective feedback when anomalies are detected. The relationship among traffic load, jitter variation, and packet loss can be described mathematically: an increase in attack intensity correlates with a nonlinear increase in both the variance of packet arrival time (jitter) and the percentage of packet loss. The application of the mitigation stage, specifically IP blocking, demonstrates the KUAD method's effectiveness in reducing deviations towards equilibrium, thereby affirming its ability to restore system performance to a steady state. Therefore, the proposed framework is theoretically justified as a closed-loop system that enhances resilience by combining forensic investigation principles with adaptive defense control.

3. RESULT AND DISCUSSION

This research simulates an attack on an OwnCloud service hosted on a server operating Ubuntu Server 22.04 at IP address 10.10.10.4. The simulated attack is a DDoS executed using the Goldeneye tool from a computer located on a different network segment than OwnCloud. The simulation aimed to replicate a real-world testing scenario and assess the effectiveness of the proposed framework in mitigating these attacks. During the network forensics stage, the preparation phase for method deployment begins with initiation, as illustrated by the specifications of the equipment in Figure 2.

The attack on the OwnCloud service was carried out from a computer located on a different network segment connected via a MikroTik CCR1016-12G router. The server hosting the OwnCloud service and the computer running Wireshark were connected to the router within the same network segment, utilizing the router's switch ports to establish a local network. More than 1,000 attack attempts were directed toward the

server hosting OwnCloud, and the events were recorded by the Snort intrusion detection system installed on the test server. The attack simulation was executed from an external computer outside the 10.10.10.0 network using a Python script named GoldenEye.py with the command:python3 GoldenEye.py http://8081/OwnCloud/index.php/-w250-s 250.

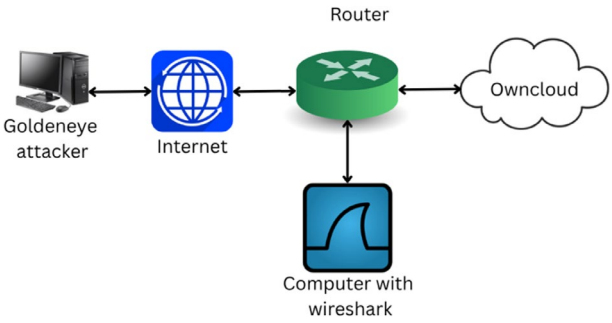

Figure 2. Devices used in the research

The attack activity was successfully captured by Snort, indicating that the IP address 125.160.99.68 launched an attack against 10.10.10.4, utilizing the Goldeneye tool. It should be noted that there is a discrepancy between the port specified in the simulation command (port 8081) and the port recorded in the log; this is recommended to be reverified in the test configuration. Snort's detection capability was enhanced through the customization of rules to identify HTTP GET flood patterns and the Goldeneye User-Agent signature. These custom rules were added to the Snort configuration file, allowing the system to automatically recognize the attack pattern and record it in the log swiftly and accurately for validation and mitigation purposes.

The rule was specifically designed to detect HTTP GET flood-type DDoS attacks targeting the OwnCloud service at IP address 10.10.10.4 on port 8081. The detection results from Snort were used as acquisition data and subsequently validated using Wireshark to confirm the involvement of the attacker's IP address, as illustrated in Figure 3. This research utilized Wireshark on a distinct computer within the same network segment as the server to monitor both inbound and outbound traffic from the cloud server.

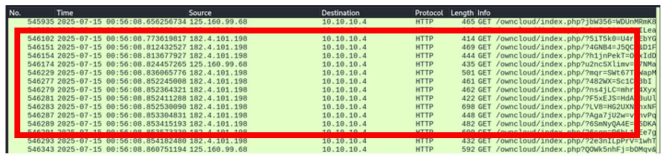

Figure 3. Network traffic captures using Wireshark

The data traffic to and from the server hosting the OwnCloud service reflects the communication between cloud users and the active server, which was captured using Wireshark. The attacks on the research object were identified as originating from IP addresses 125.160.99.68 and 182.4.101.198; both addresses were recorded not only by Snort but also detected through Wireshark. The detection data were then validated and presented in tabular form, as shown in Table 1.

The Goldeneye attack's impact on the OwnCloud service was analyzed using nload, a Command Line Interface (CLI)-based bandwidth monitoring tool operating on the Linux system. The execution phase involved simulating an attack in the form of a DDoS aimed at the OwnCloud server. The network activity during the attack was analyzed using Wireshark and Apache2 log records.

Table 1. Attacker data validation

No.	Time and Date	Capture from Wireshark	Capture from Snort	Valid
1	2025-07-15 00:53:36.875954190	125.160.99.68	125.160.99.68	✓
2	2025-07-15 00:53:36.876311011	125.160.99.68	125.160.99.68	✓
3	2025-07-15 00:53:36.880768949	125.160.99.68	125.160.99.68	✓
4	2025-07-15 00:53:36.888148780	125.160.99.68	125.160.99.68	✓
5	2025-07-15 00:53:36.888243423	125.160.99.68	125.160.99.68	✓
6	2025-07-15 00:53:54.540158025	182.4.101.198	182.4.101.198	✓
7	2025-07-15 00:53:54.540434310	182.4.101.198	182.4.101.198	✓
8	2025-07-15 00:53:54.541075860	182.4.101.198	182.4.101.198	✓
9	2025-07-15 00:53:54.541292005	182.4.101.198	182.4.101.198	✓
10	2025-07-15 00:53:54.541424551	82.4.101.198	82.4.101.198	✓

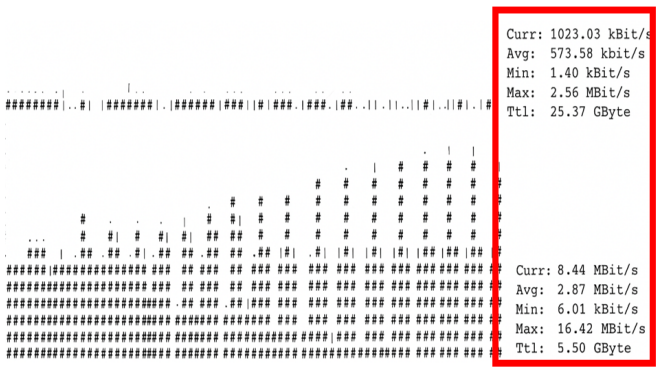

Figure 4. Graphical display of the server's load monitoring results during the Goldeneye attack

This analysis sought to identify attack patterns, trace attacker IP addresses, and assess the impact on OwnCloud's service performance. Through nload, bandwidth usage could be monitored in real time, facilitating network issue diagnosis and supporting data traffic management. Server performance monitoring utilizing nload was performed as part of the attack impact analysis, with the results presented in Figure 4.

Figure 4 illustrates a significant increase in network traffic during the attack period. The incoming traffic shows a sharp spike compared to normal conditions, while the outgoing traffic remains relatively stable. This pattern indicates an intensification of external communication toward the target server OwnCloud at IP address 10.10.10.4. Traffic measurement was performed using iPerf, where the iPerf server was executed on the OwnCloud server and the iPerf

client on a separate computer that also ran Wireshark. The main performance parameter analysed was jitter, representing variations in packet arrival times from the expected interval. This parameter is essential for preserving service quality in latency-sensitive applications, including video conferencing and IP-based voice services. Previous studies addressed packet delay and jitter issues in heterogeneous wireless networks through the Flag-Based Multi-Path Retransmission (FBMRTX) approach [40]. This research calculates the jitter parameter using Eq. (1), and packet loss is calculated using Eq. (2), both referring to the total number of lost packets during transmission. These two parameters are essential indicators for evaluating network quality, especially for continuous data flow applications that require minimal disruption. In the UDP test using iPerf, jitter is computed based on the variation in delay between consecutive packets, as defined in RFC 3550 (RTP/RTCP).

$$J = J + \frac{|(D_{i-1,i})| - J}{16} \quad (1)$$

$$D_{i-1,i} = (t_i - t_{i-1}) - (T_i - T_{i-1}) \quad (2)$$

J is the current jitter (Eq. (1)) value (ms), $D_{i-1,i}$ is the difference in delay variation between two consecutive packets, t_i is the time the packet is received at the receiver side, and T_i = the timestamp of the packet when it is sent. In Eq. (2), t_i and t_{i-1} denote the actual or observed times at the i-th and (i−1)-th events, respectively, while T_i and T_{i-1} represent the expected, ideal, or reference times for the same events. The term $t_i - t_{i-1}$ describes the actual time interval between two consecutive events, whereas $T_i - T_{i-1}$ defines the ideal time interval. The resulting value $D_{i-1,i}$ quantifies the difference between these two intervals, where a value of zero indicates perfect alignment, a positive value indicates a delay relative to the reference interval, and a negative value indicates an earlier occurrence than expected. Along with the calculation of the jitter value, which provides insights into the stability of the delay between data packets during the Goldeneye attack, a comparison was also conducted between the number of packets sent and the number of packets received. This comparison, known as Loss/Total Datagram, is calculated using the following Eq. (3):

$$Packet\ Loss(\%) = \frac{N_{sent} - N_{receive}}{N_{sent}} \times 100\% \quad (3)$$

N_{sent} is the number of packets sent, and $N_{receive}$ is the number of packets received. The jitter and Loss/Total Datagram values were calculated based on ping data collected before and during the Goldeneye attack on the cloud service. The results of these calculations are presented in Table 2 for further analysis.

Table 2. Results of jitter and loss / total datagram calculations

No.	Before the Attack		After the Attack	
	Jitter	Loss / Total Datagram (%)	Jitter	Loss / Total Datagram (%)
1	0.1986	0.0020	0.1465	0.0032
2	0.2638	0.0025	0.1513	0.0055
3	0.1333	0.0035	0.1013	0.0054
4	0.1277	0.0058	0.1118	0.0093
5	0.1715	0	0.0979	0.0134
6	0.1006	0.0034	0.2652	0.0191
7	0.1159	0.0041	0.1277	0.0100
8	0.1715	0.0019	0.1048	0.0019
9	0.2229	0.0027	0.0951	0
10	0.1548	0.0002	0.2826	0
11	0.1368	0.0031	0.0888	0
12	0.1236	0.0031	0.1347	0.0001
13	0.0902	0.0034	0.1027	0
14	0.0944	0.0022	0.3097	0.0038
15	0.2062	0.0015	0.1715	0.0098
16	0.1854	0	0.13819	0.0075

Table 2 presents 16 data rows obtained through iPerf. Data analysis shows that the jitter before the attack ranged from 0.198 ms to 0.185 ms, with an average of 0.156 ms. After the attack occurred, the jitter increased slightly, ranging from 0.146 ms to 0.138 ms, with the average remaining around 0.1519 ms. This increase indicates a higher degree of time fluctuation in the network during the attack, although the difference is not significant. The average jitter under both conditions can be calculated using the standard mean calculation method as follows:

1. Before the attack
• Jitter = 0.1561 ms
• Loss/total = 0.24%
2. After the attack
• Jitter = 0.1519 ms
• Loss/total = 0.89%

Before the attack occurred, the packet loss rate was relatively low, with the Loss/Total Datagram percentage ranging from 0% to 0.15%. After the Goldeneye attack, a significant increase in packet loss was observed, peaking at 1.9% during specific intervals, such as between the 6th and 7th seconds. This condition can be observed in Figure 5.

The Loss/Total Datagram values before and after the attack were calculated to illustrate the change in network quality. In terms of jitter, a slight increase was recorded after the attack, although the average value did not show a substantial difference. Conversely, the increase in Loss/Total Datagram was more pronounced, indicating a degradation in overall data transmission quality. While the jitter values remained within acceptable tolerance limits, the rise in packet loss suggests potential issues in data delivery, particularly affecting applications that require high speed and consistency. Figure 5 illustrates the fluctuations of jitter values and the Loss/Total Datagram ratio during the first 16 intervals before the attack,

whereas Figure 6 shows the jitter values after the attack, represented by the light blue line.

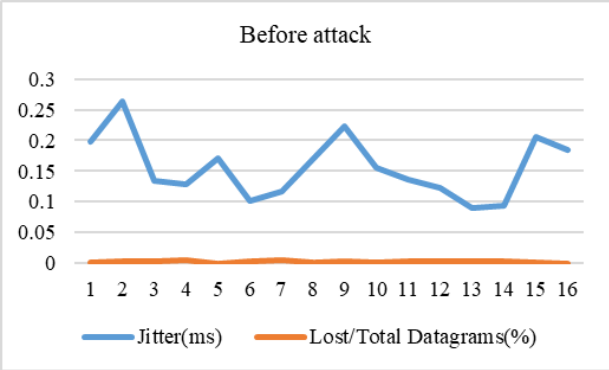

Figure 5. Graphical representation of jitter and loss/total datagram on the OwnCloud service before

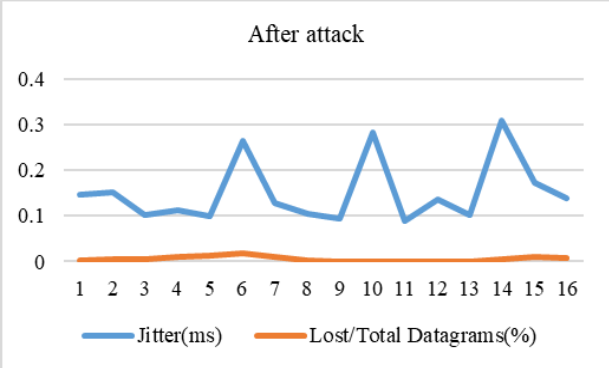

Figure 6. After the mitigation phase was implemented

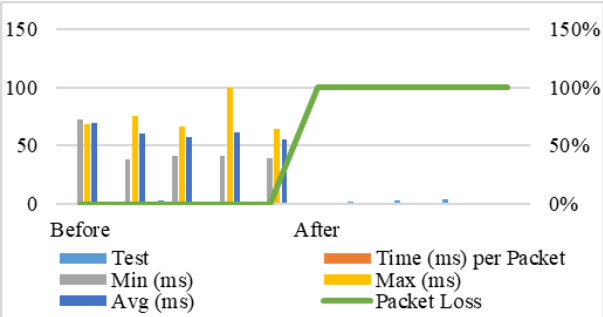

Figure 7. The impact of the attack as observed through packet loss during the ping process

The red line indicates the Loss/Total Datagram values prior to the attack, while the orange line illustrates these values subsequent to the attack. The graph indicates that lower values of jitter and Loss/Total Datagram correlate with improved network quality. An increase in these indicators indicates the occurrence of a Goldeneye attack, facilitating effective detection of the attack. In addition to monitoring jitter and Loss/Total Datagram using iPerf, the ping utility was also employed to observe the impact of the attack on the OwnCloud service. These observations confirm that the private cloud used in this research, which employs the OwnCloud service, is vulnerable to Goldeneye attacks, as shown in Figure 7.

Based on the observations, a mitigation phase is required to restore the jitter and Loss/Total Datagram values to their pre-attack conditions. This recovery is achieved by blocking the IP addresses identified as sources of the Goldeneye attack using Wireshark. The mitigation phase serves as an active defense mechanism within the developed framework. Once the attacker IP addresses have been validated through data analysis from Wireshark and Snort, the system provides a "Block All" function that enables administrators to block all IP addresses or subnets involved in the attack directly. The blocking process is executed through a shell script using the iptables DROP command. This IP blocking procedure constitutes a crucial component of the KUAD method implemented in this research. The impact of this blocking demonstrates that the OwnCloud service condition can be restored to its pre-attack state, as shown in Figure 8.

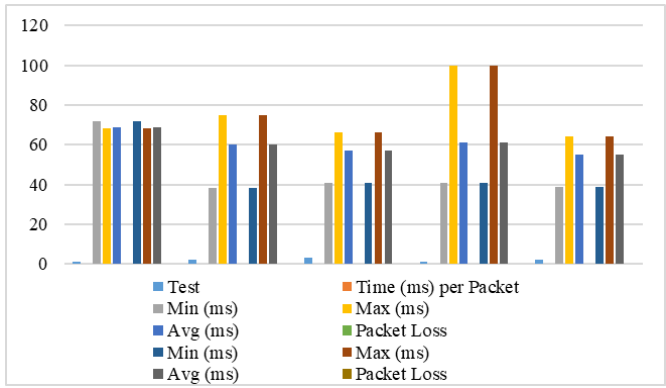

Figure 8. The impact of Goldeneye attack mitigation as observed through packet loss during ping testing

The final stage of this research focuses on the preparation of a comprehensive disposition document, which follows a standardized format previously applied in related published studies. This stage is crucial as it integrates all research findings, analytical results, and recommendations obtained from the experimental phase. The disposition is not merely a summary of results but functions as a strategic guideline that can be adopted by decision-makers and system administrators in designing effective policies for IT management.

This research offers actionable insights for preventive and corrective measures to improve the security posture of private cloud environments. It provides a systematic method for identifying vulnerabilities, executing mitigation strategies, and assessing recovery processes following an attack. The documentation highlights the necessity of ongoing monitoring and adaptive defense mechanisms, essential for sustaining service reliability and system performance during and following cyberattacks, exemplified by the Goldeneye denial-of-service (DoS) incident.

Moreover, this framework highlights the role of proactive risk assessment and incident response planning as integral components of organizational resilience. By integrating these strategies, organizations can ensure that their IT infrastructure remains stable, secure, and capable of sustaining operational efficiency even under potential attack scenarios. Ultimately, the disposition developed in this research not only serves as a practical tool for operational improvement but also contributes to the broader academic discourse on cybersecurity resilience in cloud computing systems. It provides a reproducible model that other researchers and practitioners can adapt to evaluate and strengthen their own defensive architectures against evolving threats.

SDN has been widely adopted as a standard approach for mitigating DDoS attacks due to its centralized control and dynamic traffic management capabilities. SDN-based

mitigation frameworks typically rely on flow-level monitoring and controller-driven policies to detect and block malicious traffic in real time. These approaches are effective in large-scale and highly dynamic networks; however, they introduce architectural complexity and dependency on a centralized controller, which may itself become a target during an attack. Although the experimental evaluation in this research primarily focuses on descriptive performance metrics such as jitter and packet loss, the results can be contextualized with respect to existing DDoS mitigation frameworks. DeepDefend and SDN-based models, for instance, rely heavily on predefined learning patterns or flow-based policies to detect and neutralize attacks. In contrast, the KUAD framework, see Table 3, adopts a feedback-oriented approach that not only detects anomalies but also triggers immediate corrective actions through its integrated mitigation phase. This adaptive mechanism minimizes system downtime without requiring extensive model retraining or centralized controller dependency.

Table 3. Comparison between SDN and KUAD

Aspect	SDN-Based Mitigation	KUAD Framework
Architecture	Centralized controller	Host centric
Detection	Flow based	Forensic validation
Mitigation	Flow rule enforcement	IP blocking
Evidence	Limited	Integrated
Recovery	Implicit	Explicit
Feedback	Partial	Closed loop
Suitability	Large scale network	Private cloud

Note: SDN = Software-Defined Networking; KUAD = Knowledge Understanding Assessment Defense.

From a performance perspective, SDN-based frameworks prioritize rapid traffic rerouting and filtering, whereas KUAD focuses on stabilizing service-level parameters such as jitter and packet loss after an attack is identified. Experimental results demonstrate that KUAD effectively restores network performance close to normal operating conditions following a Goldeneye DDoS attack. Although KUAD does not provide global traffic optimization as in SDN architectures, it offers a lightweight, adaptive, and evidence-oriented mitigation mechanism suitable for private cloud environments. The mitigation process in KUAD functions as a closed-loop control system that dynamically stabilizes network parameters, including jitter and packet loss, during active attacks. Subsequent research could improve this study by performing comparative benchmarking between KUAD and established frameworks to measure its benefits in terms of response time, recovery efficiency, and mitigation accuracy.

This research examines the feasibility and effectiveness of the KUAD framework through the application of fundamental mitigation techniques and a restricted set of performance metrics. Future research will enhance the evaluation by integrating advanced mitigation mechanisms, utilizing larger datasets, exploring multiple attack scenarios, and conducting thorough statistical benchmarking against established frameworks, including SDN-based mitigation models.

4. CONCLUSIONS

This research examined the use of the KUAD framework to reduce Goldeneye-based DDoS attacks within a private cloud setting, utilizing OwnCloud. The experimental findings demonstrate that Goldeneye attacks substantially impair service availability through heightened packet loss and destabilization of network performance. The integration of a mitigation phase within the forensic workflow allows the KUAD framework to facilitate prompt defensive actions that restore essential performance metrics to baseline conditions. This research primarily contributes by illustrating that digital forensic processes can be expanded beyond post-incident analysis to facilitate real-time mitigation and recovery efforts. In contrast to conventional forensic models that prioritize evidence acquisition, KUAD presents a closed-loop lifecycle integrating attack detection, validation, mitigation, and system stabilization. The experimental results indicate that a fundamental mitigation strategy, when integrated into this structured framework, can significantly diminish the effects of DDoS attacks while maintaining forensic traceability. This research is constrained by its dependence on a singular attack type, a fundamental IP-blocking countermeasure, and a limited range of performance metrics. The results should be viewed as evidence of feasibility rather than as a complete performance benchmark. This research will be further developed in three specific directions. Initially, advanced mitigation techniques, including rate limiting, behavioral filtering, and SDN-assisted control, will be integrated into the defense phase of KUAD. The framework will undergo evaluation against various DDoS attack variants and larger traffic datasets to facilitate comparative benchmarking and enhance statistical validation. Third, the integration of adaptive thresholding and automated rule generation will improve the framework's responsiveness and scalability within dynamic cloud environments. These extensions enable KUAD to develop into a more comprehensive and flexible forensic-mitigation framework for the security of private cloud infrastructures.

REFERENCES

[1] Ali, S., Wadho, S.A., Yichiet, A., Gan, M.L., Lee, C.K. (2024). Advancing cloud security: Unveiling the protective potential of homomorphic secret sharing in secure cloud computing. Egyptian Informatics Journal, 27: 100519. https://doi.org/10.1016/j.eij.2024.100519

[2] Min, X., Mei, G., Weiping, Z. (2022). Research and implementation of network security deployment based on private cloud security platform. Procedia Computer Science, 208: 565-569. https://doi.org/10.1016/j.procs.2022.10.078

[3] Xu, H., Hu, L., Li, Q., Liu, S., Yan, D., Liu, X. (2026). Point geometrical Coulomb force: An explicit and robust embedding for point cloud analysis. Pattern Recognition, 170: 112025. https://doi.org/10.1016/j.patcog.2025.112025

[4] Dhaka, P., Sehrawat, R. (2026). IntHDCNN: IoT-driven remote cardiac health monitoring with interactive hunt-based deep convolutional neural network. Biomedical Signal Processing and Control, 112: 108467. https://doi.org/10.1016/j.bspc.2025.108467

[5] Ranganatha Rao, B., Sujatha, B. (2023). A hybrid elliptic curve cryptography (HECC) technique for fast encryption of data for public cloud security. Measurement: Sensors, 29: 100870. https://doi.org/10.1016/j.measen.2023.100870

[6] Zhang, C., Pan, Z., Hou, C. (2023). Marketing data security and privacy protection based on federated

gamma in cloud computing environment. International Journal of Intelligent Networks, 4: 261-271. https://doi.org/10.1016/j.ijin.2023.09.003
[7] Abdullayeva, F., Suleymanzade, S. (2024). Cyber security attack recognition on cloud computing networks based on graph convolutional neural network and graphsage models. Results in Control and Optimization, 15: 100423. https://doi.org/10.1016/j.rico.2024.100423
[8] El-Sofany, H., Bouallegue, B., Abd El-Latif, Y.M. (2024). A proposed biometric authentication hybrid approach using iris recognition for improving cloud security. Heliyon, 10(16): e36390. https://doi.org/10.1016/j.heliyon.2024.e36390
[9] Riadi, I., Yudhana, A., Pramuja, G., Fanani, I. (2023). Mobile forensic tools for digital crime investigation: Comparison and evaluation. International Journal of Safety and Security Engineering, 13(1): 11-19. https://doi.org/10.18280/ijsse.130102
[10] Nasim, S.S., Pranav, P., Dutta, S. (2025). A systematic literature review on intrusion detection techniques in cloud computing. Discover Computing, 28(1). https://doi.org/10.1007/s10791-025-09641-y
[11] Ouhssini, M., Afdel, K., Agherrabi, E., Akouhar, M., Abarda, A. (2024). DeepDefend: A comprehensive framework for DDoS attack detection and prevention in cloud computing. Journal of King Saud University - Computer and Information Sciences, 36(2): 101938. https://doi.org/10.1016/j.jksuci.2024.101938
[12] Ali, M., Tang Jung, L., Hassan Sodhro, A., Ali Laghari, A., Birahim Belhaouari, S., Gillani, Z. (2023). A confidentiality-based data classification-as-a-service (C2aaS) for cloud security. Alexandria Engineering Journal, 64: 749-760. https://doi.org/10.1016/j.aej.2022.10.056
[13] Eddermoug, N., Mansour, A., Azmi, M., Sadik, M., Sabir, E., Bahassi, H. (2023). A literature review on attacks prevention and profiling in cloud computing. Procedia Computer Science, 220: 970-977. https://doi.org/10.1016/j.procs.2023.03.134
[14] Mohammed, S., Nanthini, S., Bala Krishna, N., Srinivas, I.V., Rajagopal, M., Ashok Kumar, M. (2023). A new lightweight data security system for data security in the cloud computing. Measurement: Sensors, 29: 100856. https://doi.org/10.1016/j.measen.2023.100856
[15] Mallidi, S.K.R., Ramisetty, R.R. (2025). Advancements in training and deployment strategies for AI-based intrusion detection systems in IoT: A systematic literature review. Discover Internet of Things, 5(1). https://doi.org/10.1007/s43926-025-00099-4
[16] Pothireddy, S., Peddisetty, N., Yellamma, P., Botta, G., Gottipati, K.N. (2024). Data security in cloud environment by using hybrid encryption technique: A comprehensive study on enhancing confidentiality and reliability. International Journal of Intelligent Engineering and Systems, 17(2): 159-170. https://doi.org/10.22266/ijies2024.0430.14
[17] Wang, J., Wang, X., Shi, Y., Yang, H., Jia, B., Zhang, X., Lin, L. (2025). A review of the application prospects of cloud-edge-end collaborative technology in freshwater aquaculture. Artificial Intelligence in Agriculture, 15(2): 232-251. https://doi.org/10.1016/j.aiia.2025.02.008
[18] Fadlil, A., Riadi, I., Fachri, F. (2022). Mitigation web server for cross-site scripting attack using penetration testing method. International Journal of Safety and Security Engineering, 12(2): 201-208. https://doi.org/10.18280/ijsse.120208
[19] Bilgili, S., Demir, A.K., Alam, S. (2024). IfNot: An approach towards mitigating interest flooding attacks in named data networking of things. Internet of Things, 25: 101076. https://doi.org/10.1016/j.iot.2024.101076
[20] Yadav, S., Hashmi, H., Vekariya, D., N, Z.A.K., J, V.F. (2024). Mitigation of attacks via improved network security in IOT network environment using RNN. Measurement: Sensors, 32: 101046. https://doi.org/10.1016/j.measen.2024.101046
[21] Rozam, N.F., Riasetiawan, M. (2023). XGBoost classifier for DDOS attack detection in software defined network using sFlow protocol. International Journal on Advanced Science, Engineering and Information Technology, 13(2): 718-725. https://doi.org/10.18517/ijaseit.13.2.17810
[22] Zhou, L., Zhu, Y., Xiang, Y., Zong, T. (2022). A novel feature-based framework enabling multi-type DDoS attacks detection. World Wide Web, 26(1): 163-185. https://doi.org/10.1007/s11280-022-01040-3
[23] Hnamte, V., Hussain, J. (2024). Enhancing security in software-defined networks: An approach to efficient ARP spoofing attacks detection and mitigation. Telematics and Informatics Reports, 14: 100129. https://doi.org/10.1016/j.teler.2024.100129
[24] Aleisa, M.A. (2025). Enhancing security in CPS industry 5.0 using lightweight MobileNetV3 with adaptive optimization technique. Scientific Reports, 15(1). https://doi.org/10.1038/s41598-025-00496-3
[25] Hajjouz, A., Avksentieva, E.Y. (2025). Enhancing and extending CatBoost for accurate detection and classification of DoS and DDoS attack subtypes in network traffic. Scientific and Technical Journal of Information Technologies, Mechanics and Optics, 25(1): 114-127. https://doi.org/10.17586/2226-1494-2025-25-1-114-127
[26] Inayat, U., Farzan, M., Mahmood, S., Zia, M.F., Hussain, S., Pallonetto, F. (2024). Insider threat mitigation: Systematic literature review. Ain Shams Engineering Journal, 15(12): 103068. https://doi.org/10.1016/j.asej.2024.103068
[27] Amoujavadi, S., Nemati, A. (2024). Developing sustainability, resiliency, agility, and security criteria for cloud service providers' viability assessment: A comprehensive hierarchical structure. Sustainable Futures, 7: 100219. https://doi.org/10.1016/j.sftr.2024.100219
[28] Gorva, S.K., Anandachar, L.C. (2022). Effective load balancing and security in cloud using modified particle swarm optimization technique and enhanced elliptic curve cryptography algorithm. International Journal of Intelligent Engineering and Systems, 15(2): 190-199. https://doi.org/10.22266/ijies2022.0430.18
[29] Patwal, A., Wazid, M., Singh, J., Singh, D.P., Das, A.K. (2025). An authenticated key agreement method for secure big data analytics in next-generation wireless networks-enabled smart farming. Journal of Systems Architecture, 168: 103552. https://doi.org/10.1016/j.sysarc.2025.103552
[30] Sefati, S.S., Arasteh, B., Fratu, O., Halunga, S. (2025). SSLA: A semi-supervised framework for real-time injection detection and anomaly monitoring in cloud-based web applications with real-world implementation

and evaluation. Journal of Cloud Computing, 14(1). https://doi.org/10.1186/s13677-025-00765-6

[31] Rahmawati, S.N.E., Hasanah, M., Rohmah, A., Pratama, R.A.P., Anshori, M.I. (2023). Privacy and ethics in digital human resource management. Lokawati: Journal of Management Research and Innovation, 1(6): 1-23. https://doi.org/10.61132/lokawati.v1i6.328

[32] Casino, F., Lopez-Iturri, P., Patsakis, C. (2025). Cloud continuum testbeds and next-generation ICTs: Trends, challenges, and perspectives. Computer Science Review, 56: 100696. https://doi.org/10.1016/j.cosrev.2024.100696

[33] Song, C., Sohn, Y. (2022). The influence of dependability in cloud computing adoption. The Journal of Supercomputing, 78(10): 12159-12201. https://doi.org/10.1007/s11227-022-04346-1

[34] Wang, R., Li, C., Zhang, K., Tu, B. (2025). Zero-trust based dynamic access control for cloud computing. Cybersecurity, 8(1). https://doi.org/10.1186/s42400-024-00320-x

[35] Liang, J., Chen, X., Chen, M. (2026). Delay-sensitive compound service function chain deployment in multi-provider edge cloud: A learning-based approach. Expert Systems with Applications, 296: 129157. https://doi.org/10.1016/j.eswa.2025.129157

[36] Musarat, M.A., Alaloul, W.S., Khan, M.H.F., Ayub, S., Guy, C.P.L. (2024). Evaluating cloud computing in construction projects to avoid project delay. Journal of Open Innovation: Technology, Market, and Complexity, 10(2): 100296. https://doi.org/10.1016/j.joitmc.2024.100296

[37] Singh, G., Singh, P., Motii, A., Hedabou, M. (2024). A secure and lightweight container migration technique in cloud computing. Journal of King Saud University - Computer and Information Sciences, 36(1): 101887. https://doi.org/10.1016/j.jksuci.2023.101887

[38] Wintolo, H., Riadi, I., Yudhana, A. (2025). Intrusion detection analysis on Open Journal System services using the network forensic development life cycle method. SKANIKA: Computer Systems and Informatics Engineering, 8(1): 133-144. https://doi.org/10.36080/skanika.v8i1.3284

[39] Wintolo, H., Riadi, I., Yudhana, A. (2025). Post attack mitigation on Open Journal System services using knowledge understanding assessment defense (KUAD) method. Kinetik: Game Technology, Information System, Computer Network, Computing, Electronics, and Control, 10(4). https://doi.org/10.22219/kinetik.v10i4.2279

[40] Raghavendra Rao, K., Ramya Kalangi, R., Balaji, B., Agarwal, V. (2026). Adaptive and optimized scheduling mechanism for heterogeneous wireless networks using an explicit flag based reinjection approach. International Journal of Engineering, 39(2): 534-546. https://doi.org/10.5829/ije.2026.39.02b.19