Jurnal Informatika Medis (J-INFORMED)
Universitas Muhammadiyah Muara Bungo
DOI: 10.52060/im.v4i1.4196
Vol. 4, No. 1, Juni-2026, hlm. 16-22
e-ISSN: 2987-9337

Forensic Analysis of Trojan Backdoor (Gacor) Attacks on Private Cloud Environments using KUAD Method

Hero Wintolo*[1]
[1] Institut Teknologi Dirgantara Adisutjipto
[1]herowintolo@itda.ac.id

Mohammad Faiq Badruz Zaman[2]
[2]Institut Teknologi Dirgantara Adisutjipto

Haruno Sajati[3]
[3]Institut Teknologi Dirgantara Adisutjipto

Imam Riadi[4]
[4]Universitas Ahmad Dahlan

Anton Yudhana[5]
[5]Universitas Ahmad Dahlan

Tri Rochmadi[6]
[6]Universitas Alma Ata

Puspa Ira Dewi Candra Wulan[7]
[7]National Taiwan University Science and Technology

ABSTRACT

This research examines the impact of a Trojan Backdoor Attack, referred to as a Gacor attack, on the security and service integrity of a private cloud environment based on OwnCloud. The experimental environment was deployed ubuntu server 22.04 using OwnCloud version 10.15.2 and supported by a Mikrotik CCR1016-12G network device. Application level and network level activities were monitored through Apache web server logs and Snort Intrusion Detection System (IDS) version 2.9.15.1, respectively. The investigation adopts the knowledge Understanding assessment defence (KUAD) framework, which structures the analysis into initiation, acquisition, execution, mitigation, and digital evidence disposition stages. The attack scenario focuses on exploiting a file upload vulnerability in the OwnCloud service to deploy and execute a malicious PHP-based Trojan Backdoor. The results show that the Gacor attack demonstrates highly repetitive and centralized behaviour, originate from a limited number of highly active IP addresses. This behaviour exploits weaknesses in application security configuration and results in system takeover and service defacement. Correlation between log analysis and IDS alerts confirms 10 distinct attack events and reveals a structured intrusion pattern rather than random probing activity. The data visualization reveals a structured and centralized attack pattern, resulting in 100% defacement of the OwnCloud index page, which highlights the severe security risk faced by private cloud environments that lack a adequate file upload protection mechanisms. The findings demonstrate that the application of the KUAD method, when combined with log analysis and intrusion detection systems (IDS) is effective in identifying, analyzing, and systematically documenting Trojan Backdoor attacks in private cloud computing environments.

Keywords: Netowork Forensic, Trojan Backdoor, Gacor, Private Cloud, KUAD Method

1. INTRODUCTION

The rapid advancement of cloud computing technologies, particularly private cloud environments, has introduced serious security challenges related to data protection and service reliability. Although private clouds are designed to offer greater control and isolation than public clouds, their dependence on internet connectivity makes them vulnerable to a wide range of cyberattacks. One emerging and increasingly concerning threat is the so called gacor attack, which exploits trojan-based techniques to infiltrate systems and abuse existing security weaknesses. Such attacks can disrupt service availability, degrade system performance, and compromise the confidentiality and integrity of user data. A lack of in depth understanding of the operational impact of gacor attack on private cloud infrastructures offer leaves organization is needed to

assess how gacor attacks affect the security, performance, and reliability of private cloud computing environments.

Previous studies have extensively explored network security and cyber forensics from various perspectives; however, several important gaps remain. Research works such as (Indrianingsih et al., 2023), (Lasaharu, Dahlan and Riadi, 2022), and (Wintolo, Riadi and Yudhana, 2025b) focus on vulnerability assessment and intrusion detection in web-based services using OWASP standards and network forensic development life cycle (NFDLC), emphasizing incident identification and response. Meanwhile, network forensic studies (Umar, Riadi and Surya Kusuma, 2021; Wijayanto et al., 2022; Zakiyaturrahma and Riadi, 2022; Retno, Sembiring and Riadi, 2023; Wijayanto, Riadi and Prayudi, 2023) primarily concentrate on post incident investigations involving attacks such as ARP spoofing, ransomware, fake Wi-Fi, and phising. Although methodologies such as TAARA and NFDLC have proven effective in forensic analysis, most of these studies adopt a reactive approach and are limited to conventional network environments or specific applications. Notably, there is a lack of research that explicitly examines the characteristics, attack patterns, and operational impacts of gacor or trojan based attacks within private cloud computing environments, which have distinct architectures and security mechanisms.

On the other hand, studies addressing online gambling or gacor related attacks on websites, such as (Erawan et al., 2024) and (Alim et al., 2024) mainly emphasize content monitoring, attack pattern identification, and prevention using OSINT based techniques and application-level monitoring. While these approaches are effective for publicly accessible web application, they do not sufficiently address infrastructure level concerns, particularly in private cloud systems where internal control mechanisms differ significantly. Research on Trojan and malware attacks, including works in (Kanaker et al., 2022), (Darmawan and Aprilia, 2024), and (Wang et al., 2025) has investigated machine learning based detection(Ayuningtyas, Riadi and Yudhana, 2025), backdoor analysis, and advanced Trojan behaviours. However, most of these studies adopt a general perspective on cloud or distributed system environments, which differ from mobile or private cloud architectures (Samani and Khayyambashi, 2020), and do not explicitly frame gacor attacks as a distinct phenomenon that combines Trojan infiltration, anomalous traffic behaviour and potential service disruption, This gap indicates a clear disconnect between existing studies on gacor attacks at the application level and technical analyses of trojan behaviour at the cloud infrastructure level.

Recent research in cloud security (Min, Mei and Weiping, 2022; Ali et al., 2023; 2024; Mohammed et al., 2023; Ranganatha Rao and Sujatha, 2023; Abdullayeva and Suleymanzade, 2024; El-Sofany, Bouallegue and Abd El-Latif, 2024; Ouhssini et al., 2024) have largely concentrated on strengthening protection mechanisms, including cryptographic schemes, biometric authentication, data classification, AI based DDoS detection, and general attack prevention frameworks. While these contributions are substantial, most of the existing work assumes generic cloud threat models, primarily focusing on public or hybrid cloud environments. Research that specifically addresses private cloud systems remains limited and is generally confined to deployment strategies and security policy design (Zhong, 2023), without examining the operational impact of gacor attacks on system performance, service availability or data security. As a result, a clear research gap exists due to the lack of an integrated analysis that investigates the impact of trojan based gacor attacks (Haga et al., 2025) in private cloud computing environments. Such attacks differ fundamentally from DDoS attacks (Rafiee and Shirmarz, 2022)(Owaid and Hammood, 2024)(Subrmanian et al., 2024), both in terms of attack mechanisms and their effects on system behaviour and security posture, addressing this gap forms the core contribution of this research.

The solution proposed in this research is the adoption of an integrated security approach for private cloud computing environments that combines network forensic based attack detection, traffic behaviour analysis and adaptive mitigation mechanisms. The approach begins with real time network traffic monitoring to identify anomalous patterns that may indicate trojan based gacor attacks, followed by the application of the KUAD method (Wintolo, Riadi and Yudhana, 2025a)(Wintolo, Riadi and Yudhana, 2025c) to obtain valid and well-structured digital evidence. The results of the forensic analysis are used to assess the impact of the attack on system performance, service availability and data security within the private cloud. To strengthen preventive measures, the system is enhanced with dynamic security rules implemented at the firewall and intrusion detection system levels, along with service isolation mechanisms for affected components. Through this approach, private cloud infrastructures are expected to improve their resilience against gacor attacks, while also providing a more effective and sustainable basis for security decision making.

The primary objective of this research is to analyse and evaluate the impact of trojan based gacor attacks on the security, performance, and service availability of private cloud computing environments. This is achieved by identifying attack patterns and network traffic characteristics that emerge during gacor attacks, as well as assessing the extent to which such attacks affect data integrity and confidentiality. In addition, this research aims to apply and evaluate the KUAD method as a systematic approach for detecting, analysing and documenting gacor attack incidents in private cloud infrastructures. Another objective is to derive effective mitigation and prevention strategies based on forensic analysis results, with the goal of enhancing the overall resilience of private cloud systems against similar attack scenarios. Through these objectives, the research is expected to provide both scientific and practical contributions to the field of private cloud security management.

The novelty of this research lies in its comprehensive analysis of the impact of trojan based gacor attacks specifically within private cloud computing environments, an area that remains largely

underexplored in existing literature, rather than focusing on attack detection or prevention, this research integrates network forensic analysis using the KUAD method to examine changes in system performance, traffic behaviour and data security implications resulting from gacor attacks. Furthermore, this research extends the concept of gacor attacks which has previously been examined mainly at the web application level, to the infrastructure level of private cloud systems. Another novel contribution is the development of an impact analysis model that links forensic evidence, network anomaly indicators and cloud service performance metrics. This integrated approach is expected to serve as a useful reference for future research and practical implementations in private cloud security.

2. RESEARCH METHOD

This research applies the KUAD method to detect gacor attacks within a private cloud computing environment used as the research object. The private cloud was deployed on a computer running ubuntu version 22, with OwnCloud installed as the cloud service platform, as illustrated in Figure 1.

Figure 1. KUAD Method

Figure 1 illustrates the systematic and sequential workflow of network security incident handling, which is structured from the initiation stage through to disposition. The initiation stage represents the initial phase in which potential indicators of security attacks or incidents within the system are identified. Next, the acquisition stage focuses on the collection of relevant data and digital evidence, including network logs, traffic records, and system activity data. The execution stage describes the process of analysis and the application of forensic techniques to understand attack patterns, employed methods, and their impact on the system. Following the analysis, the mitigation stage aims to implement response actions to stop the attacks, reduce system damage, and prevent recurrence. The final stage, Disposition, involves documenting and reporting the investigation results, as well as supporting followup decision making for system evaluation and future security improvement

3. RESULT AND DISCUSSION

The result of this research demonstrates the successful implementation of a network forensic application designed to analyse Trojan Backdoor attacks, particularly those categorized as gacor attacks, within a private cloud computing environment. The developed application, which is based on the KUAD method, can support the entire forensic process in an integrated manner, ranging from data acquisition to the disposition of digital evidence. The testing environment was established using owncloud as the private cloud platform, with controlled attack scenario designed to generate realistic forensic artifacts. Through this implementation, the application was able to effectively identify attack sources, network activity patterns, and the impact of the attacks on the system.

The first stage, initiation, involved preparing the devices and tools required for the experiment. Several computers were configured to support the private cloud environment, attack monitoring using snort, and attack simulation using the gacor method. As illustrated in Figure 2, the gacor attack pattern was executed by uploading two PHP files, namely a shell file and a PHP based payload. Both files pose a serious security risk, which required the attack simulation process to be conducted with a high level of precision and caution to avoid unintended system damage.

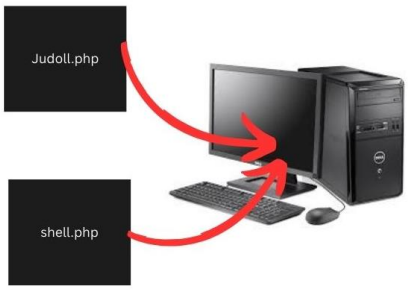

Figure 2. The attack process uploading 2 malicious file

During the acquisition stage, this research successfully collected network traffic data from Apache server log files and alerts generated by the snort intrusion detection system (IDS). The Apache logs recorded detailed information for each incoming HTTP request, including the source IP address, access timestamp, request method, and target URL. Analysis of the acquired data revealed many repeated POST requests targeting malicious PHP files such as shell.php, which indicates automated and persistent attack activity. This behaviour is consistent with the characteristics of gacor attacks, which are known for their intensive and repetitive nature. The structured format of Apache logs facilitated efficient parsing and data correlation, ensuring that the integrity and reliability of the digital evidence were maintained. These findings highlight the importance of proper logging mechanisms as a fundamental component of network forensic investigations in private cloud environments. The execution stage played a critical role in validating the forensic findings. At this stage, a cross-correlation analysis was performed between the Apache log data and snort alerts using shared parameters such as IP address, timestamp, protocol, and attack classification. The validation results, as presented in Table 1, show a strong correlation between the network activities recorded in the logs and the alerts generated by the IDS. Alerts categorized as web application attack and possible reverse shell connection were directly associated with repeated access attempts to the uploaded backdoor

files on the server. This validation process significantly reduced the likelihood of false positives and effectively filtered out irrelevant network activity.

Table 1. Validation of Log File Data Using Snort IDS

No	Date and Time of Incident	Log File Screenshot Evidence	Snort Alert Screenshot Evidence	Validated
1	2025-07-15 22:53:24	125.160.99.68	125.160.99.68	✔
2	2025-07-15 22:53:59	125.160.99.68	125.160.99.68	✔
3	2025-07-15 22:59:56	182.4.101.92	182.4.101.92	✔
4	2025-07-15 23:00:07	182.4.101.92	182.4.101.92	✔
5	2025-07-15 23:01:01	182.4.101.92	182.4.101.92	✔
6	2025-07-15 23:11:39	140.213.174.164	140.213.174.164	✔
7	2025-07-15 23:12:22	140.213.172.86	140.213.172.86	✔
8	2025-07-15 23:20:02	182.4.103.106	182.4.103.106	✔
9	2025-07-15 23:27:32	140.213.128.191	140.213.128.191	✔
10	2025-07-15 23:26:29	140.213.138.175	140.213.138.175	✔

Table 1 presents the validation results of the observed network attack incidents based on event timestamps, source IP addresses and the consistency between server log data and snort detection outputs. Each entry confirms that the source IP address recorded in the server logs matches the IP address identified by snort. The check marks in the validation column indicate that all recorded incidents were successfully and consistently verified. During the execution stage, the attack simulation clearly demonstrates how misconfigurations in the OwnCloud service can be exploited by an attacker. The absence of MIME type validation and file extension restrictions allowed malicious PHP files to be uploaded and executed without obstruction. Once the shell.php file was accessed, the attacker gained the ability to execute remote commands through the web shell interface. This capability enabled unauthorized modification of the server's directory structure, including the replacement of critical application files with defacement content, as shown in Figure 3. Forensic evidence further indicates that the file judoll.php was successfully renamed to index.php, resulting in the complete takeover of the OwnCloud homepage by the attacker. These findings highlight the weakness of the application's security controls and emphasize the significant risk faced by private cloud environments when file upload protection mechanisms are not properly enforced.

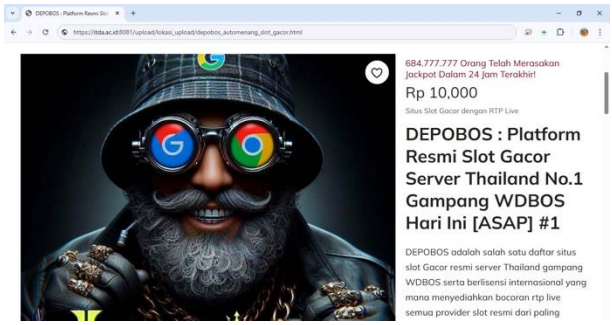

Figure 3. Appearance of the OwnCloud Index Page after the Attack

Figure 3 illustrated that the impact of the attack was not limited to technical system behaviour, but also directly affected the appearance and functionally of the OwnCloud service. A comparison between the interface before and after the attack reveals significant changes to the login page, clearly indicating defacement and loss of application integrity. The complete visual alteration of the interface serves as strong evidence that the attacker successfully accessed and modified core system files. From a cloud security perspective, this condition reflects an escalation from an initial exploitation phase to a full-service takeover. These findings emphasize the importance of early detection and rapid response to trojan backdoor attacks in order to prevent more extensive damage. The next phase addressed in this research is post incident mitigation. After successfully bypassing the file upload mechanism on the server, the attacker uploaded a PHP shell file that could be accessed via the URL http://itda.ac.id:8081/upload/lokasi_upload/shell.php . This PHP shell granted the attacker the ability to execute remote commands with web server privileges (www-data). Using this access, the attacker subsequently created an additional file in the form of an online gambling web page, place within the upload directoryhttp://itda.ac.id:8081/upload/lokasi_upload/cara-menang-jackpot.html. The presence of this file not only violated server usage policies, but also posed reputational risks to the institution and increased the likelihood of the server being blacklisted by search engines. As a post incident mitigation measure, the system administrator developed a PHP based script to detect newly added files on the server within a specified time window. This approach focuses on the incident response phase, aiming to identify malicious artifacts that have already entered the system rather than preventing the initial attack. The script performs a recursive scan of the main web server directory (/var/www/html/) using RecursiveDirectoryIterator. Each file's modification time (mtime) is examined and compared against a defined threshold, such as files created or modified within the last 1 – 10 days. Only files that meet this criterion are reported to the administrator. To reduce analysis overhead and minimize false detections, the script applies exclusion rules for specific directories and file extensions. Internal application directories and system data paths are excluded, as are static files such as images and documents. This design allows the detection process to focus on higher risk files, particularly PHP and HTML files that appear within upload directories. The following section presents the core part of the script responsible for detecting newly modified files based on their modification time see Figure 4.

```
1.  $minTime = strtotime("-$days days");
2.  foreach ($rii as $file) {
3.  if ($file->isDir()) continue;
4.  $filePath = $file->getPathname();
5.  if (!is_readable($filePath))
    continue;
6.  $mtime = $file->getMTime();
7.  if ($mtime < $minTime) continue;
8.  $ownerId = fileowner($filePath);
9.  $ownerInfo =
    posix_getpwuid($ownerId);
10. $ownerName = $ownerInfo['name'] ??
    'Unknown';
11. // only new files that pass the time
    filter are logged
12. }
```

Figure 4. part of the script responsible for detecting newly modified files

The logic described above indicates that files are classified as suspicious not based on their name or content, but rather on their relatively recent creation or modification time. This time-based approach is effective for identifying exploitation artifacts, as backdoor files or web shells are typically created shortly after an attacker successfully gains access to the system. Another important aspect of the script is file ownership validation. The detection process focuses on files owned by www-data user, which is the account used by the web server and PHP processes. This assumption is based on the observation that files created through upload mechanisms or PHP shell exploitation are almost always written with www-data privileges. In contrast, files owned by rood or other system users are generally considered part of legitimate system or application components and are therefore excluded from this mitigation process. By applying this restriction, the risk of accidentally removing critical system files can be significantly reduced. In addition, the script verifies that the running PHP process has the same effective user (www-data) before presenting any file removal options. This layered validation mechanism ensures that the mitigation process remains controlled and safe, minimizing the potential for unintended system disruption. Figure 5 presents the results of the newly uploaded file inspection on the server. Two suspicious files were identified, namely shell.php and how to win the jackpot.html, both of which are owned by the www-data user and located within the upload directory.

No.	Date	Owner	Action
1	2025-12-30 13:38:56	/var/www/html/upload/lokasi_upload/shell.php	Delete
2	2025-12-30 13:39:15	/var/www/html/upload/lokasi_upload/cara-menang-jackpot.html	Delete

Figure 5. Detection of Newly Uploaded Files on the Server

Figure 5 shows that file removal was performed manually through the provided interface. This semi manual approach was intentionally selected to reduce the risk of false positives, where legitimate files might be mistakenly identified as malicious. BY adopting this approach, the administrator retains full control over file deletion decisions, ensuring that only confirmed malicious artefacts are removed. The disposition stage serves as the final phase of the forensic process, focusing on the preparation of a structured and accountable digital evidence report. This report documents key findings, including the origin of the attack, exploitation methods, validation results, and the total number of identified attacks, which amounted to 1149 gacor type attack events. The resulting documentation is not only valuable as a technical record, but also serves as a foundation for security decision making the improvement of system protection policies. Overall, the results and discussion of this research demonstrate that integrating the KUAD method with log analysis, intrusion detection systems, and data visualization provides an effective approach for investigating trojan backdoor attacks in private cloud computing environments. Moreover, this integration helps reveal critical security weaknesses that require immediate attention, as illustrated in Figure 6.

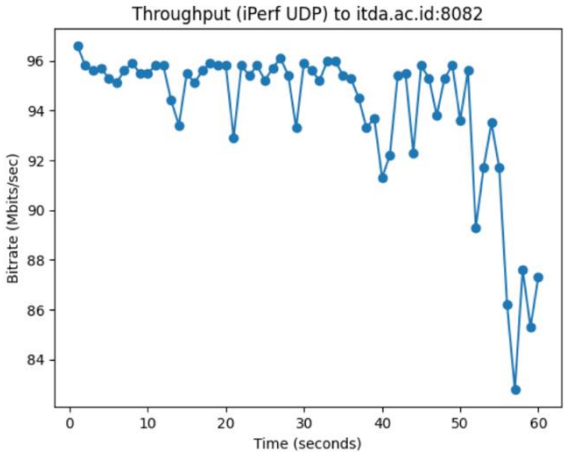

Figure 6. Throughput Graph (Bitrate Vs Time) Based on UDP Iperf Test Result After Mitigation

Figure 6 presents the network throughput graph obtained from an iPerf UDP test directed to itda.ac.id on port 8082, conducted over a duration of approximately 60 seconds. The horizontal axis represents time, while the vertical axis shows the bitrate in Mbps. From the beginning of the test until around the 40-second mark. The throughput remains relatively stable, ranging between 94 and 96 Mbps, with minor fluctuations that reflect normal variations in UDP transmission behaviour. After this point, a more noticeable performance degradation becomes apparent. Several data points drop to around 90 Mbps with some values approaching 83-85 Mbps toward the end of the test. This decline may indicate the presence of network congestion, increased packet loss, bandwidth limitations, or temporary disturbances affecting the destination network.

4. CONCLUSION

Trojan backdoor attacks categorized as gacor attacks have a significant impact on the security, integrity and service availability of OwnCloud based private cloud computing environments. Through the application of the KUAD method, this research successfully identified, analysed and validated attack activities in a systematic manner, covering all stages from data acquisition to digital evidence disposition. The analysis of Apache server logs and alerts generated by the snort intrusion detection system (IDS) confirms that the attacks were active, repetitive, and primarily focused on exploiting file upload vulnerabilities that lacked adequate validation mechanisms. Cross validation between these two data sources improved the accuracy of incident identification and reduced the likelihood of analytical

errors. Data visualization further revealed that most attack activities originated from a small number of highly active IP addresses, indicating a structured and coordinated attack pattern. The impact of the attacks was not limited to technical system behaviour, but also directly affected the appearance and functionality of the cloud service through defacement actions, reflecting the attacker's successful control over core application files. In addition, the findings highlight that weak application security configurations in private cloud environments can facilitate attack escalation from initial exploitation to full-service takeover. The throughput remains relatively stable, ranging between 94 and 96 Mbps, with minor fluctuations that reflect normal variations in UDP transmission behaviour. After this point, a more noticeable performance degradation becomes apparent. Several data points drop to around 90 Mbps with some values approaching 83-85 Mbps toward the end of the test. Overall, this research demonstrates that integrating the KUAD method with log analysis, intrusion detection systems, and data visualization provides an effective and reliable approach for network forensic investigations in private cloud computing environments. Moreover, the proposed approach offers a strong foundation for the development of mitigation strategies and future security enhancements.

5. REFERENCE

Abdullayeva, F. and 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*, [online] 15. https://doi.org/10.1016/j.rico.2024.100423.

Ali, M., Tang Jung, L., Hassan Sodhro, A., Ali Laghari, A., Birahim Belhaouari, S. and Gillani, Z., 2023. A Confidentiality-based data Classification-as-a-Service (C2aaS) for cloud security. *Alexandria Engineering Journal*, [online] 64, pp.749–760. https://doi.org/10.1016/j.aej.2022.10.056.

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

Alim, E.S., Nuroji, N., Rizkiawan, M.A., Anhari, T. and Sobari, B., 2024. Monitoring and Prevention of Online Gambling Attacks (Gacor Slots) on Websites. *Edumatic: Jurnal Pendidikan Informatika*, 8(1), pp.75–83. https://doi.org/10.29408/edumatic.v8i1.25267.

Ayuningtyas, A., Riadi, I. and Yudhana, A., 2025. A Comparative Evaluation of Drone Detection Models on Aerial Imagery across Varying Training Epochs. *JUITA: Jurnal Informatika*, 13(3), pp.277–286.

Darmawan, W. and Aprilia, T., 2024. Analysis of the Metasploit Framework 'msfvenom' Backdoor Trojan and Fully Undetected (FUD) Trojan. *Techno.COM*, 23(1), pp.112–124. https://doi.org/https://doi.org/10.62411/tc.v23i1.9741.

El-Sofany, H., Bouallegue, B. and Abd El-Latif, Y.M., 2024. A proposed biometric authentication hybrid approach using iris recognition for improving cloud security. *Heliyon*, [online] 10(16). https://doi.org/10.1016/j.heliyon.2024.e36390.

Erawan, E., Satria, R.P., Nastiti, A.D., Juniardi, W., Anbiya, D.R. and Go Reinnamah, D.A., 2024. A Lightweight Design Approach to Detect Malicious Injections in Government Websites: Combating Hidden Online Gambling Pages. In: *2024 Beyond Technology Summit on Informatics International Conference (BTS-I2C)*. pp.365–369. https://doi.org/10.1109/BTS-I2C63534.2024.10942063.

Haga, R., Kaji, S., Fujimoto, D. and Hayashi, Y., 2025. Detection of Hardware Trojans Using a Capacitance Sensor Focused on Parasitic Coupling Between Wires. In: *2025 23rd IEEE Interregional NEWCAS Conference (NEWCAS)*. pp.104–107. https://doi.org/10.1109/NewCAS64648.2025.11107121.

Indrianingsih, Y., Pamungkas, A.G., Wintolo, H., Sajati, H., Gunawan and Nugraheny, D., 2023. Descriptive Analysis of Web Security Vulnerabilities at Airport Servers Using The Open Web Application Security Project Security Standard. In: *Proceedings - IEIT 2023: 2023 International Conference on Electrical and Information Technology*. Institute of Electrical and Electronics Engineers Inc. pp.6–11. https://doi.org/10.1109/IEIT59852.2023.10335586.

Kanaker, H., Karim, N.A., Awwad, S.A.B., Ismail, N.H.A., Zraqou, J. and Al ali, A.M.F., 2022. Trojan Horse Infection Detection in Cloud Based Environment Using Machine Learning. *International Journal of Interactive Mobile Technologies*, 16(24), pp.81–106. https://doi.org/10.3991/ijim.v16i24.35763.

Lasaharu, S., Dahlan, U.A. and Riadi, I., 2022. *Network Forensic on Web-based Applications using Network Forensic Development Life Cycle Method*. [online] *International Journal of Computer Applications*, https://doi.org/10.5120/ijca2022921869.

Min, X., Mei, G. and Weiping, Z., 2022. Research and Implementation of Network Security Deployment Based on Private Cloud Security Platform. In: *Procedia Computer Science*. [online] Elsevier B.V. pp.565–569. https://doi.org/10.1016/j.procs.2022.10.078.

Mohammed, S., Nanthini, S., Bala Krishna, N., Srinivas, I. V., Rajagopal, M. and Ashok

Kumar, M., 2023. A new lightweight data security system for data security in the cloud computing. *Measurement: Sensors*, [online] 29. https://doi.org/10.1016/j.measen.2023.100856.

Ouhssini, M., Afdel, K., Agherrabi, E., Akouhar, M. and 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*, [online] 36(2). https://doi.org/10.1016/j.jksuci.2024.101938.

Owaid, M.A. and Hammood, A.S., 2024. Evaluating Machine Learning and Deep Learning Models for Enhanced DDoS Attack Detection. *Mathematical Modelling of Engineering Problems*, 11(2), pp.493–499. https://doi.org/10.18280/mmep.110221.

Rafiee, M. and Shirmarz, A., 2022. Self-Organization Map (SOM) Algorithm for DDoS Attack Detection in Distributed Software Defined Network (D-SDN). *Journal of Information Systems and Telecommunication (JIST)*, 10(2). https://doi.org/10.52547/jist.15644.10.38.120.

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

Retno, R., Sembiring, R. and Riadi, I., 2023. *Wireless Implementation on Fake Wifi using Network Forensic Development Life Cycle Method*. [online] *International Journal of Computer Applications*, Available at: <https://doi.org/10.5120/ijca2023922042> [Accessed 15 April 2025].

Samani, Z.N. and Khayyambashi, M.R., 2020. Reliable resource allocation and fault tolerance in mobile cloud computing. *Journal of Information Systems and Telecommunication (JIST)*, 7(2). https://doi.org/10.7508/jist.2019.02.002.

Subrmanian, K., Thangarasu, G., Zhao, Y. and Kannan, K.N., 2024. Enhancing Detection and Prediction of DDoS Attacks Through Regression Modeling. *2024 IEEE 6th Symposium on Computers & Informatics (ISCI)*, [online] null, pp.253–257. https://doi.org/10.1109/ISCI62787.2024.10668039.

Umar, R., Riadi, I. and Surya Kusuma, R., 2021. Network Forensics Against Ryuk Ransomware Using Trigger, Acquire, Analysis, Report, and Action (TAARA) Method. *Kinetik: Game Technology, Information System, Computer Network, Computing, Electronics, and Control*. https://doi.org/10.22219/kinetik.v6i2.1225.

Wang, R., Lin, H., Luo, Z., Cheung, K.C., See, S., Ma, J. and Wan, R., 2025. Meme Trojan: Backdoor Attacks Against Hateful Meme Detection via Cross-Modal Triggers. *Proceedings of the AAAI Conference on Artificial Intelligence*, [online] 39. https://doi.org/https://doi.org/10.1609/aaai.v39i8.32845.

Wijayanto, A., Riadi, I. and Prayudi, Y., 2023. TAARA Method for Processing on the Network Forensics in the Event of an ARP Spoofing Attack. *Jurnal RESTI (Rekayasa Sistem dan Teknologi Informasi)*, 7(2), pp.208–217. https://doi.org/10.29207/resti.v7i2.4589.

Wijayanto, A., Riadi, I., Prayudi, Y. and Sudinugraha, T., 2022. Network Forensics Against Address Resolution Protocol Spoofing Attacks Using Trigger, Acquire, Analysis, Report, Action Method. *Register: Jurnal Ilmiah Teknologi Sistem Informasi*, 8(2), pp.156–169. https://doi.org/10.26594/register.v8i2.2953.

Wintolo, H., Riadi, I. and Yudhana, A., 2025a. Enhancing Private Cloud Security Using Knowledge Understanding Assessment Defense Method for Distributed Denial of Service Attack Mitigation. *International Journal of Safety and Security Engineering*, [online] 15(11), pp.2323–2331. https://doi.org/10.18280/ijsse.151112.

Wintolo, H., Riadi, I. and Yudhana, A., 2025b. Intrusion Detection Analysis on Open Journal System Services Using Network Forensic Development Life Cycle Method. *SKANIKA: Sistem Komputer dan Teknik Informatika*, [online] 8(1), pp.133–144. Available at: <https://doi.org/10.36080/skanika.v8i1.3284> [Accessed 15 April 2025].

Wintolo, H., Riadi, I. and Yudhana, A., 2025c. 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*. [online] https://doi.org/10.22219/kinetik.v10i4.2279.

Zakiyaturrahma and Riadi, I., 2022. Email Forensic from Phishing Attack using Network Forensics Development Life Cycle Method. *International Journal of Computer Applications*, [online] 183(46), pp.975–8887.https://doi.org/10.5120/ijca2022921865

Zhong, L., 2023. A convolutional neural network based online teaching method using edge-cloud computing platform. *Journal of Cloud Computing*, 12(1). https://doi.org/10.1186/s13677-023-00426-6.