Journal of Computer Networks, Architecture and High Performance Computing
Volume 6, Number 3, July 2024
https://doi.org/10.47709/cnapc.v6i3.4256

Submitted : 9 July 2024
Accepted : 29 July 2024
Published : 31 July 2024

Implementation of Intrusion Detection System with Rule-Based Method on Website

Try Firdyanta[1)*], **Rushendra**[2)]
[1)*2)] Universitas Mercu Buana, Indonesia
[1)*] 41520110040@student.mercubuana.ac.id, [2)] rushendra@mercubuana.ac.id

ABSTRACT

The aim of this research is to implement an intrusion detection system using rule-based methods on websites. Th approach in this research is the development of an intrusion detection system (IDS). research results afte implementation, testing, and acceptance of test results, conclusions can be drawn. The detection system can b implemented well in website-based applications using a rule-based method.

Keywords: Cyber Security; Intrusion Detection System (IDS); Attack Detection

1. INTRODUCTION

In the current digital era, the existence of a website has become a crucial element for various organizations, be it companies, educational institutions, or even government agencies. Websites are not only a communication and promotional tool, but also a platform for carrying out transactions, storing data, and providing services to users. However, as website use increases, threats to cyber security also become more complex and diverse. Cyberattacks such as hacking, malware, phishing, and distributed denial of service (DDoS) have become a significant challenge that can result in financial, reputational, and operational losses for organizations that are unprepared to deal with them(Heni, 2023).

Website security is a top priority in maintaining the integrity and confidentiality of managed data. One solution that is widely adopted to overcome this threat is the Intrusion Detection System (IDS). IDS functions to monitor and analyze network traffic and activity on websites to detect suspicious actions that could indicate a cyber attack. The intrusion detection methods used can vary, but one that is often applied is the rule-based method(Fauzi et al., 2023).

Rule-Based Methods in Intrusion Detection Systems work by defining a series of rules that can identify patterns or signs of attacks. These rules are based on prior knowledge of known attack techniques and normal network traffic characteristics. When the system detects activity that complies with one of these rules, it will display a warning or mitigation action to prevent potential damage. The implementation of this method allows fast and responsive detection of attacks, considering that the rules used have been specifically designed to identify certain threats(Riza, 2023).

An Intrusion Detection System (IDS) is a computer security system designed to detect unauthorized, suspicious, or malicious activity on a network or system. A rules-based IDS works by observing events in a system and applying a set of rules that lead to a decision on whether or not a particular pattern of behavior is considered suspicious. These rules contain conditions that IDS uses to analyze traffic and are stored on servers and sensors(Ulfa, 2015). Rule-based IDS can be used on various network stack layers, such as the application layer, where HTTP traffic headers and payloads are analyzed for possible intrusion(Alamsyah et al., 2020).

However, rule-based IDS has some limitations, such as the inability to detect new or unknown threats that do not match predefined rules. Rule-based IDS can also generate false positives or negatives if the rules are not defined correctly or traffic patterns change. To overcome these limitations, some IDS systems combine rule-based detection with other methods, such as anomaly detection or machine learning(Wicaksono, 2023)

Implementation of IDS with a rule-based method requires the creation of a set of rules that group the rules according to any attribute. The rule set can be active or inactive, and IDS checks the rules in the set as they load. When a condition defined in an active rule is detected in traffic, IDS logs the event that triggered the rule(Kurniawan et al., 2024)

Implementation of an Intrusion Detection System using the Rule-Based method is expected to make a significant

* Corresponding author

Submitted : 9 July 2024
Accepted : 29 July 2024
Published : 31 July 2024

contribution in strengthening cyber security on websites, reducing the risk of attacks, and protecting high-value data and information. With better website security, organizations can run their operations with greater peace of mind and focus on developing services and innovations that provide added value for users. Therefore, research and development in this field has become very relevant and urgent to carry out, as cyber threats in the digital world continue to grow increasingly complex.

2. LITERATURE REVIEW

Debi Setiawan's research (2023) with the title Implementation of a Network Security System Using Rule-Based Ids at Pt Netkrida Tuah Cakrawala. As a result of this research, it can be concluded that implementing Rule-Based IDS is the right step to improve corporate network security. This system can prevent cyber attacks and protect company data and information systems

Faizal Riza's research (2023) entitled Realtime Intrusion Detection System on Servers Using Feature Selection and Firebase Cloud Messaging. The results show that ELM outperforms other approaches. Utilization of Firebase Cloud Messaging because it can work with many platforms and there is a file store that can store all logs created by the JALA application

Endah Octaviana Nasution's research (2021) with the title Implementation of the C5.0 Algorithm for Classifying DDoS Attacks. The accuracy, precision and recall evaluation test results of the C5.0 algorithm were 98.38%, 98.39% and 98.37% and the required running time was 16.84 seconds.

Research gap in this research Although previous research has shown the effectiveness of various methods in improving network security, such as the implementation of Rule-Based IDS which can prevent cyber attacks on companies (Setiawan, 2023), the use of Firebase Cloud Messaging to detect intrusions in real time with the advantage of working on Various platforms (Riza, 2023), and the C5.0 algorithm for classifying DDoS attacks with high accuracy (Nasution, 2021), there are still irregularities in the specific implementation of the Rule-Based Intrusion Detection System (IDS) on websites. This research will focus on the application of Rule-Based IDS in the context of website security, which has not been widely explored in previous studies, to assess its effectiveness in detecting and preventing cyber attacks targeting websites.

3. METHOD

The quantitative research approach in this study emphasizes the collection of numerical data to analyze and measure the effectiveness of intrusion detection systems. The quantitative approach allows researchers to use statistical techniques to analyze the numerical data obtained, such as hypothesis testing to measure the significance of experimental results. The research design chosen for this study is an experiment. Within the framework of this experiment, the research will involve the direct implementation of IDS with rule-based methods in a controlled environment(Al Hilmi & Khujaemah, 2022)

Sampling in this context can include variations of attacks relevant to the cyber environment. For example, testing can involve samples of DDOS attacks, SQL Injection, cross-site scripting (XSS), or unauthorized access attempts. This research approach requires the use of data that shows the description of the attack and the payload or data used by the attacker in attacking a website-based application. The dataset used in this study is sourced from Github and several other sources on the internet

The research stages in implementing an intrusion detection system using a rule-based method on a website begin with identifying needs and analyzing security risks on the website to be tested. The next step is to design specific detection rules based on common attack patterns, such as SQL injection, cross-site scripting (XSS), and others. After that, the intrusion detection system is developed and configured using software that supports rule-based methods, such as Snort or Suricata. The system is then tested in a real website environment to detect potential attacks, where the detection results are analyzed to evaluate the effectiveness and efficiency of the system. Finally, adjustments and optimization of detection rules are made based on field findings, and a research report is prepared which includes an evaluation of the performance, advantages and disadvantages of the intrusion detection system that has been implemented(Fachri & Harahap, 2020).

4. RESULT

This study aims to detail the achievement of research objectives focused on implementing an Intrusion

* Corresponding author

Submitted : 9 July 2024
Accepted : 29 July 2024
Published : 31 July 2024

Detection System (IDS) on a website by applying a rule-based method. IDS is an urgent need in an increasingly complex online environment, where potential cyber security threats are becoming increasingly serious. Therefore, this research is committed to investigating and developing an effective and efficient system for detecting and responding to security threats at the web application level.

The first step in achieving this goal involves an in-depth understanding of rule-based methods in the context of IDS. An in-depth analysis of the different types of security threats that the website can face will be the basis for formulating relevant rules. In addition, the implementation of IDS must consider technical aspects such as response speed, detection accuracy, and minimizing false positives.

Thus, developing this IDS system refers to applying specific rules that can identify suspicious behavior patterns in website traffic. The objectives of this research also involve testing the IDS system that has been implemented using a dataset that covers various possible attack scenarios, which is obtained from several sources such as Github.

Furthermore, the evaluation of IDS performance is carried out by considering critical metrics such as detection accuracy, response speed, and the ability to overcome variations in threats. The results of this evaluation serve as the basis for assessing the extent to which the proposed IDS system can make a positive contribution to improving security at the web application level(Ramli et al., 2021).

Thus, through the achievement of the objectives of this research, a significant contribution can be made to the understanding and implementation of rules-based IDS in the web environment. The conclusions and findings of this study are expected to provide a foundation for further developments in the field of cybersecurity, especially in the context of intrusion detection at the web application level.

The achievement in the implementation of the Intrusion Detection System (IDS) on the website using the rule-based method has made a significant contribution to the field of Information Technology. In this context, the main contribution is the development of a security system that enables early detection and effective response to security threats at the web application level. Implementing the rule-based method reflects a systematic and directed approach to formulating specific rules that can identify suspicious behavior patterns. This contribution focuses not only on the technical aspects but also on the aspects of in-depth security analysis, resulting in rules that can provide proactive protection against evolving cyber-attacks(Alamsyah et al., 2020).

By presenting a rules-based IDS in the website environment, the contribution to the field of Information Technology is manifested in improving the security of the overall information system. Successful implementation of this will reduce the risk of cyber threats that can include SQL injection attacks, cross-site scripting (XSS), and various other attacks that can harm the integrity and availability of data. Thus, this contribution supports efforts to provide safe and reliable online services

In addition, implementing rule-based methods in IDS contributes to developing and understanding intrusion detection methods that the broader Information Technology community can adopt. The findings and methodologies from this study can be a valuable reference for further research in cybersecurity, enriching the literature and practical understanding related to intrusion detection at the web application level. Thus, this contribution creates a foundation for continuous improvement in efforts to counter the ever-evolving cybersecurity threats in the era of Information Technology.

5. DISCUSSIONS

Implementing the Intrusion Detection System (IDS) based on the rule-based method on websites has substantial implications and applications in cybersecurity and information risk management. The main implications of this research lie in improving the system's ability to detect and respond effectively to security threats that may threaten the integrity and availability of data at the web application level. With the adoption of specific rules developed through in-depth analysis of different types of possible attacks, these IDSs provide a more specialized and adaptive layer of defense.

This IDS implementation can be applied in practical cybersecurity management scenarios, where the security policies implemented become more dynamic and responsive to changes in the cyber environment. The system allows managers to detail and adjust detection rules according to the characteristics and evolving attack trends. Thus, the IDS application on the website has a real impact in mitigating risks and providing more effective protection against evolving cyberattacks.

* Corresponding author

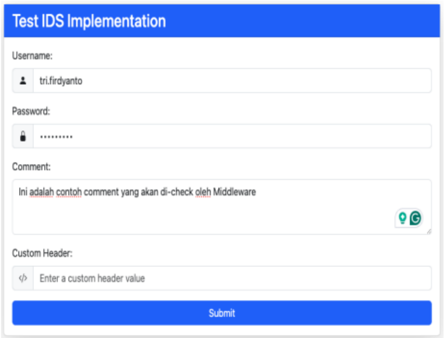
In terms of implementation, the results of this research can be applied to various organizational contexts, ranging from small companies to large companies with varying levels of complexity. Information system managers can integrate these IDSs as an integral part of their security strategy, ensuring holistic protection against potential security threats at the web application level. As an adaptive tool, the IDS application can be implemented in a variety of web-based environments, including e-commerce platforms, content management systems, and other web-based applications.

Thus, the implementation of IDS based on the rule-based method on the website not only contributes to the management of cybersecurity risks but also provides practical solutions that various organizations can adopt and adjust. The implications and applications of this research strengthen the proactive, adaptive, and measurable cybersecurity paradigm in dealing with the dynamics of cyber threats in the era of Information Technology.

This study created a system using the C# programming language (ASP .Net Core). Rule-based algorithms will be applied to the middleware in this web application. The implementation of this system design is divided as follows.

Test Page View

This section has a page to test the Middleware from user input.



Test IDS Implementation

Username: tri.firdyanto

Password: ••••••••••

Comment: Ini adalah contoh comment yang akan di-check oleh Middleware

Custom Header: Enter a custom header value

Fig.1 Test Page Display

The process of checking user input is a critical step in implementing the Intrusion Detection System (IDS) with a rule-based method on the website. This process involves analyzing any input received from the user to detect and identify suspicious or malicious activity. Using predefined rules, IDS can check input patterns against a list of known attack signatures, such as SQL injection, cross-site scripting (XSS), and various other exploits. This check ensures that every data received is valid and does not contain elements that can compromise the system's security.

System Testing

System testing is the next step after the system is implemented. The purpose of such testing is to show how well the system built can work properly and can repel attacks such as SQL Injection, XSS Injection, and so on.
Implementing the Intrusion Detection System (IDS) with the rule-based method using Regex in C# consists of several important stages that must be carried out sequentially to ensure the effectiveness of attack detection on web applications. Here are the stages:

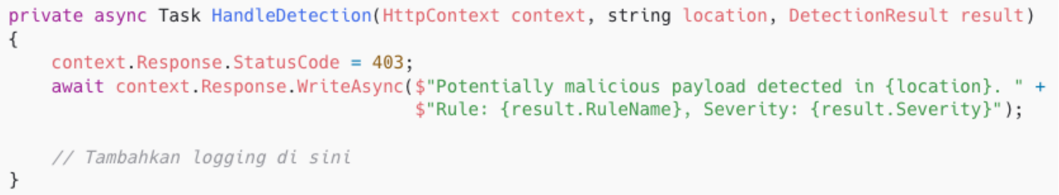
Initialization and Rule Creation

The first stage in implementing IDS is initializing and creating attack detection rules. These rules are written in the form of regular expressions (regex) that are able to detect common attack patterns, such as SQL injection, cross-site scripting (XSS), and other injection attacks. These rules are structured based on the specific known signs of different types of cyberattacks.

Once the attack detection rules are in place, the next step is to collect and process user feedback. Input data received from various sources, such as forms, URLs, or query parameters, is collected and prepared for analysis.

* Corresponding author

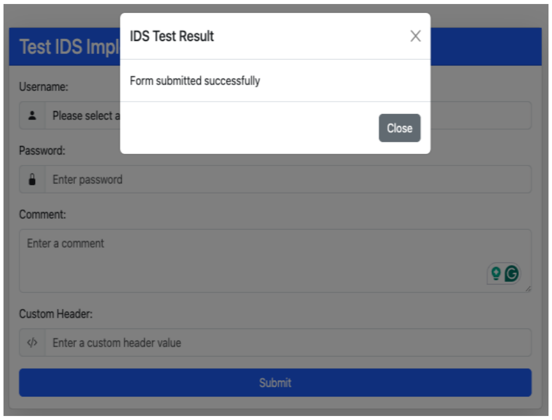
The final stage is reporting and taking corrective actions. When IDS detects an attack based on the rules applied, the system will create a log of the suspicious activity. System administrators will be notified to take necessary corrective action, such as blocking the attacker's IP address, fixing vulnerabilities, or tightening security rules.



```
private async Task HandleDetection(HttpContext context, string location, DetectionResult result)
{
    context.Response.StatusCode = 403;
    await context.Response.WriteAsync($"Potentially malicious payload detected in {location}. " +
                                      $"Rule: {result.RuleName}, Severity: {result.Severity}");

    // Tambahkan logging di sini
}
```

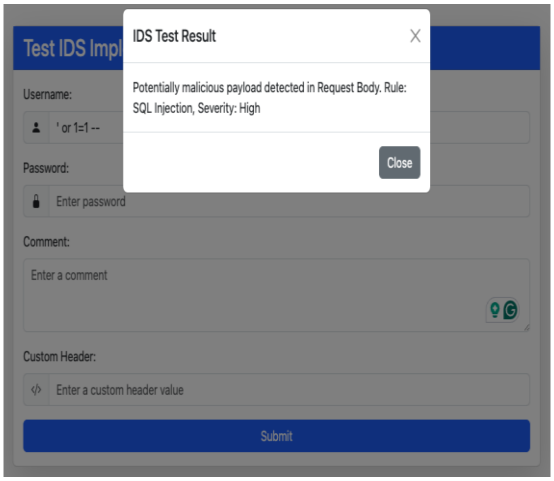
The testing process will simulate a web application that has implemented IDS using a rule-based method.



IDS Test Result

Form submitted successfully

Fig. 2 SQL Injection Not Detected



IDS Test Result

Potentially malicious payload detected in Request Body. Rule: SQL Injection, Severity: High

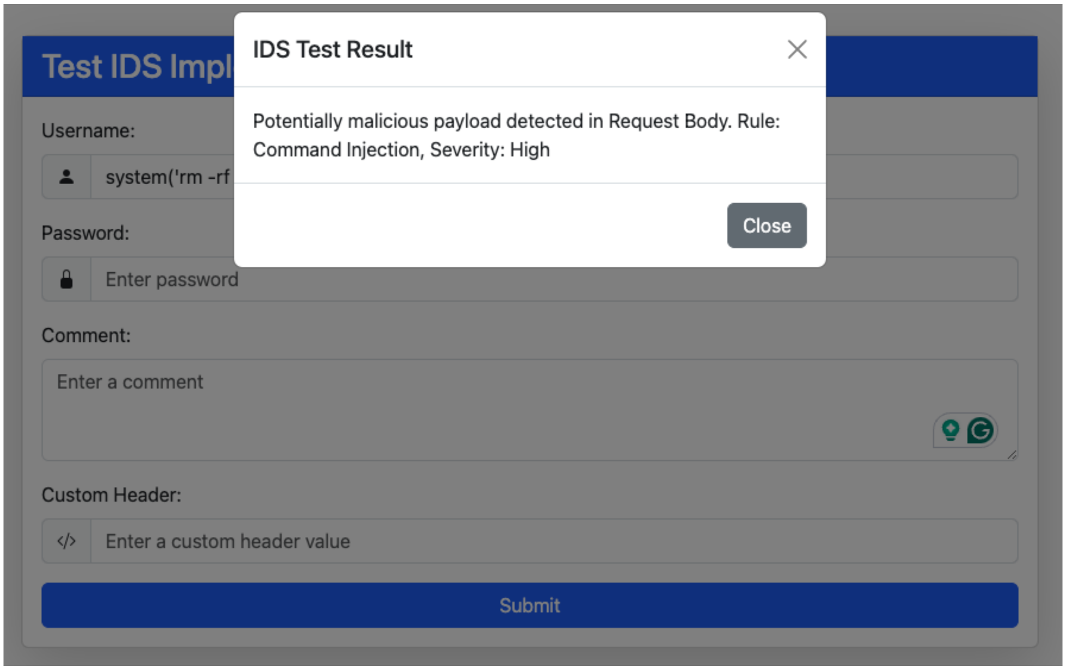
Username: ' or 1=1 --

Fig. 3 SQL Injection Detected

* Corresponding author

Journal of Computer Networks, Architecture and High Performance Computing
Volume 6, Number 3, July 2024
https://doi.org/10.47709/cnapc.v6i3.4256

Submitted : 9 July 2024
Accepted : 29 July 2024
Published : 31 July 2024



Potentially malicious payload detected in Request Body. Rule: Command Injection, Severity: High

Username: system('rm -rf

Password: Enter password

Comment: Enter a comment

Custom Header: Enter a custom header value

Fig. 5 Command Injection Detected

Implementing the Intrusion Detection System (IDS) with a rule-based method on the website is important in maintaining cyber security in this digital era. IDS is a surveillance system that detects and responds to suspicious or unauthorized activity in computer networks. By using rule-based methods, IDS can identify attacks based on a predefined set of rules, allowing for faster and more accurate detection(Cahyanto et al., 2022).

First of all, the rule-based method works by relying on a set of rules defined by the network administrator. These rules are typically based on common signs of an attack, such as suspicious network traffic patterns, repeated login attempts, or access attempts to sensitive pages. By defining these rules, IDS can compare the activity that occurs on the network with existing rules and flag suspicious activity as a potential threat. The main advantage of this method is its ability to detect known attacks quickly and efficiently(Saputra et al., 2023).

One of the key advantages of rule-based IDS is its ability to provide real-time responses to threats. In a dynamic website environment, attacks can occur at any time, and a quick response is essential to prevent further losses. For example, if IDS detects an attempted SQL injection, the system can immediately block the attacker's IP address, thus preventing further damage to the database. This capability provides an additional layer of protection that is critical to maintaining data integrity and availability(Pramudita & Rushendra, 2024)

However, rule-based methods also have some limitations. One of them is the dependence on predefined rules. This means that IDS can only detect attacks that are already known and recorded in the rules. If there is a new attack or a new variant of an existing attack, the IDS may not be able to detect it. Therefore, regular updates to the rules are essential to maintaining the effectiveness of the IDS. In addition, if the rules are too strict or numerous, IDS can generate many false positives, i.e., detect normal activity as a threat, which can interfere with network performance and require unnecessary handling(Lazuardo, 2022).

To overcome these limitations, integrating rule-based IDS with other detection methods, such as machine learning or anomaly-based detection, can be an effective solution. By combining various detection techniques, security systems can be more adaptive in the face of evolving threats. For example, machine learning methods can detect new patterns not covered by existing rules, while rule-based IDS still serves as the first line of defense for familiar(Rushendra et al., 2021)

In addition, the implementation of rule-based IDS also requires constant monitoring and maintenance. Network administrators should regularly check the logs and reports generated by IDS to identify threats and update existing

* Corresponding author

Submitted : 9 July 2024
Accepted : 29 July 2024
Published : 31 July 2024

rules. This requires human resources and time, but it is critical to ensure that the system remains effective and responsive to evolving threats(Nasution & Basuki, 2021).

Implementing the Intrusion Detection System with a rule-based method on the website provides significant advantages in improving cybersecurity. Despite its limitations, with good maintenance and integration with other detection methods, rule-based IDS can be an important component in a comprehensive security strategy. In an era where cyberattacks are increasingly sophisticated and frequent, having a reliable and responsive detection system is a must for any organization looking to protect its digital assets.

6. CONCLUSION

After the implementation, testing, and acceptance of the test results, conclusions can be drawn. The Detection System can be applied well to website-based applications by using rule-based methods. The results of the implementation of the Intrusion Detection System resulted in some user input such as "<script>alert('XSS')</script>" detected as XSS Injection. Aspiring web application builders can use the results to implement regex templates as a reference to avoid cyberattacks. This research contributes significantly to improving cyber security on websites through implementing a rule-based intrusion detection system. By developing and testing a system that is able to detect and respond to security threats in real-time, this research provides practical solutions for website managers in protecting data and information from cyber attacks.

7. REFERENCES

Al Hilmi, M. A., & Khujaemah, E. (2022). Network Security Monitoring With Intrusion Detection System. *Jurnal Teknik Informatika (Jutif)*, *3*(2), 249–253.

Alamsyah, H., Riska, A. A. A., & Al Akbar, A. (2020). Analisa Keamanan Jaringan Menggunakan Network Intrusion Detection And Prevention System. *Jointecs (Journal Of Information Technology And Computer Science)*, *5*(1), 17.

Cahyanto, K. A., Al Hilmi, M. A., & Mustamiin, M. (2022). Pengujian Rule-Based Pada Dataset Log Server Menggunakan Support Vector Machine Berbasis Linear Discriminat Analysis Untuk Deteksi Malicious Activity. *Jurnal Teknologi Informasi Dan Ilmu Komputer (Jtiik)*, *9*(2).

Fachri, B., & Harahap, F. H. (2020). Simulasi Penggunaan Intrusion Detection System (Ids) Sebagai Keamanan Jaringan Dan Komputer. *Jurnal Media Informatika Budidarma*, *4*(2), 413–420.

Fauzi, A., Utami, E., & Hartanto, A. D. (2023). Ddos Penerapan Random Forest Dan Adaboost Untuk Klasifikasi Serangan Ddos. *Journal On Education*, *5*(3), 7925–7937.

Heni, S. (2023). *Implementasi Berbagai Metode Kecerdasan Buatan (Artificial Intelligence) Pada Masalah Gangguan Kepribadian (Narcissistic Personality Disorder: Npd)*.

Kurniawan, I., Djumhadi, D., Alimyaningtias, W. N., & Budi, D. S. (2024). Analisis Komparasi Intrution Detection System Berbasis Snort Dengan Suricata Untuk Keamanan Jaringan (Studi Kasus: Astara Hotel Balikpapan). *Forbis*, *1*(1), 1–7.

Lazuardo, J. (2022). *Implementasi Hybrid Intrusion Detection Prevention System Sebagai Upaya Meningkatkan Keamanan Jaringan Pada Uptd Instalasi Farmasi Kab. Tangerang*. Univeristas Komputer Indonesia.

Nasution, E. O., & Basuki, A. (2021). Implementasi Algoritme C5. 0 Untuk Klasifikasi Serangan Ddos. *Jurnal Pengembangan Teknologi Informasi Dan Ilmu Komputer*, *5*(1), 389–395.

Pramudita, A., & Rushendra, R. (2024). Implementation Of Load Balancing With Per Connection Classifier And Failover And Utilization Of Telegram Bot (Case Study: Pt Tujuh Media Angkasa). *Jurnal Teknik Informatika (Jutif)*, *5*(1), 273–282.

Ramli, K., Hayati, N., Ihsanto, E., Gunawan, T. S., & Halbouni, A. H. (2021). Development Of Intrusion Detection System Using Residual Feedforward Neural Network Algorithm. *2021 4th International Seminar On Research Of Information Technology And Intelligent Systems (Isriti)*, 539–543.

Riza, F. (2023). Sistem Deteksi Intrusi Pada Server Secara Realtime Menggunakan Seleksi Fitur Dan Firebase Cloud Messaging. *Jurnal Sistim Informasi Dan Teknologi*, 7–15.

Rushendra, M. Y., Hidayat, R., Liklikwatil, Y., & Subrata, D. S. (2021). Rancang Bangun Sistem Deteksi Dini Ketinggian Air Banjir Berbasis Iot Dengan Sensor Ultrasonik. *Jurnal Ict: Information Communication & Technology*, *18*(2), 93–101.

* Corresponding author

Submitted : 9 July 2024
Accepted : 29 July 2024
Published : 31 July 2024

Saputra, D. A., Deris, S., & Tata, S. (2023). Implementasi Sistem Deteksi Ransomware Menggunakan Deep Packet Inspection Pada Layanan Smk Negeri 1 Palembang. *Indonesian Journal Of Multidisciplinary On Social And Technology*, *1*(2), 176–183.

Ulfa, M. (2015). Perancangan Dan Implementasi Sistem Keamanan Berbasis Ids Di Jaringan Internet Universitas Bina Darma. *Jurnal Nasional Pendidikan Teknik Informatika: Janapati*, *4*(2), 45–49.

Wicaksono, A. (2023). *Perancangan Dan Implementasi Ids Suricata, Snort, Dan Fail2ban Pada Raspberry Pi*. Sekolah Tinggi Teknologi Terpadu Nurul Fikri.

* Corresponding author