Jurnal Teknik Informatika (JUTIF)
Vol. 4, No. 6, Desember 2023, pp. 1287-1293

DOI: https://doi.org/10.52436/1.jutif.2023.4.6.1052
p-ISSN: 2723-3863
e-ISSN: 2723-3871

ASSESSMENT OF INFORMATION SECURITY RISKS USE FUZZY INFERENCE MODEL (FIS)

Lutfi Nukman*[1], Rahmat Kurniawan[2], Achmad Solichin[3]

[1,2,3]Faculty of Information Technology, Universitas Budiluhur, Indonesia
Email: [1]2111602047@student.budiluhur.ac.id, [2]211602039@student.budiluhur.ac.id, [3]solichin@budiluhur.ac.id

(Article received: May 17, 2023; Revision: May 31, 2023; published: Desember 23, 2023)

Abstract

Risk analysis is the process of systematically using information to identify and assess risks. This process how to analyze potential information security failure scenarios and the consequences of loss of confidentiality, integrity and preservation Availability of stored information values. Risk assessment is the process of comparing estimated risks against predetermined risk evaluation criteria to determine the level and priority of risk. This operation is performed using the retrieved data Risk analysis results for informed decision making future risk management measures; It is said that this cyber attack could lead to cyber warfare and cyber interference that disrupt national security and sovereignty. All of the above cyber threats are said to have the potential to threaten national assets. Institutions/companies around the world, especially those stored in his ISMS.

Keywords: *Cyber Crime, Fuzzy Inference Model (FIS) Law, Information Security.*

1. INTRODUCTION

Application of current development of information technology, security of information assets is an important issue for organizations that need to protect themselves from security threats from outside and inside the organization. But the reality is that today's security issues don't get much attention from IT managers. Currently, there are many so-called cybercriminals in cyberspace that exploit the weaknesses of IT administrators. For example: hacking systems to obtain important documents and jeopardize an organization's reputation [1].

A risk assessment mechanism based on fuzzy logic allows you to consider the quality of the input data and the credibility of the source. It adapts to different application profiles and has a rich set of features that allow you to build your own risk management system. [2]

Information security management includes routine protection, known as managing information security and disaster preparedness is known as business continuity management. Threats can be accidental or intentional. Risks may include unauthorized disclosure, use, modification, theft, destruction and denial of service [3].

Information security is the protection of computer hardware, computing and non-computer equipment, data, and information from misuse by unauthorized persons. Information security aims to achieve three main goals. Security of company seeks to protect data and information from being disclosed by unauthorized persons. The purpose of availability is to ensure that an organization's information infrastructure makes data and information available to authorized users. And finally, the integrity of all systems. The information must provide an accurate representation of the physical system it represents. In today's world, many organizations are increasingly aware of the importance of maintenance.

Protect all your resources, virtual and physical, against internal and external threats. Early computer systems provided little protection, but that changed as many computer security facilities were vandalized by protesters during the Vietnam War. This experience has led the industry to adopt security measures that eliminate or minimize the risk of damage or destruction and ensure business continuity after disruptions [4].

It provides the correct choices approximately the uncertainties of the occasion and the correct rules to take after. [5] Finding out what can cause risks within the work environment will offer assistance make choices to dodge those risks. The likelihood of such an occasion is scaled based on the score to decide the likelihood of the occasion. It moreover makes a difference survey the safeguards or activities required to ensure work environment resources. In this way, conceivable results are communicated to choice producers inside the organization so that they can take particular steps to dodge dangers [6].

Quantitative methods that utilize calculations to analyze information. For illustration, methodologies such as affectability investigation, Monte Carlo reenactment, Disappointment modeling, and impacts examination are utilized in this strategy. The assessment of most cases underpins a cost-benefit investigation of the dangers included and the conceivable courses of activity [7]. It calculates the likely result of a misfortune occasion which makes a

difference evaluate the probability of accomplishing the objectives set for a specific venture or commerce. On the other hand, subjective procedures depend more on the appraisal of an occasion than factual information, such as situation examination. It gives the proper choices approximately the uncertainty of an occasion and the correct guidelines to take after. An examination of what can cause hurt within the work environment ought to be carried out to help decision-making approximately ways to maintain a strategic distance from these dangers. [8] The likelihood of such an occasion is evaluated on a rating to decide the probability of the occasion happening. It moreover makes a difference assess any safety measures or activities required to protect property within the work environment. In this manner, conceivable comes about are passed on to the choice producers of an organization to assist them start exact steps to dodge dangers.

Additionally, semi-quantitative strategies are utilized when risk presentation is not one or the other tall nor moo. This evaluation employments a set of standards, strategies or rules to assess an occasion employing a scale or number that has esteem but isn't kept up in other circumstances [9]. This gives the benefits of utilizing both subjective and quantitative chance evaluation strategies. In expansion, a few of the strategies utilized by semi-quantitative appraisals are layers of assurance or line of defense procedures and chance lattices. Among these different approaches, the Fluffy Induction Framework (FIS) can be connected to analyze the Risk of an occasion [10]. The reason is since the investigation is subjective to misfortunes and is related with vague data [10].

FIS was presented in 1965 by Lotfy Zadeh to assist overcome the issues that had vague data [11]. Hence, correct values are broadly utilized to assess profound thinking occurrence. As of late, a fluffy rationale approach has been utilized within the handle of assessing dangers in challenging circumstances distinctive. It is an critical apparatus utilized to analyze the security of a put. For illustration, approach based on deduction motor is utilized to distinguish conceivable dangers to the framework based computer. The comes about appear its adequacy in performing risk modeling. In expansion, master based fluffy rules decide the dangers related with a specific computer program some time recently its establishment. Moreover, government offices have utilized the fluffy chance assessment strategy.

For case, it has been connected to the organize security Risk appraisal that makes a difference distinguish potential dangers related with systems in government organizations [12]. In expansion, Multi Fluffy Induction Framework (MFIS) is combined in a fluffy Risk assessment framework. Typically utilized to decide the level the chance of an occasion with the assistance of different components related with a specific occasion. [13] Concurring to Sallam, FIS may be a computer demonstrate including a collection of participation capacities, a set of rules and thinking [14]. Three commonly known deduction frameworks are the Sugeno Fluffy Demonstrate, the Fuzzy Model Mamdani, and Show Fluffy Tsukamoto. For this approach, the Mamdani show will be utilized assess and assess Risk. This includes employing a variety of steps to supply assessment comes about. Our paper will utilize the FIS approach to leverage the Fluffy Mamdani model which is the foremost well-known approach that's appropriate for executing our strategy.

2. RESET METHODS

In this area, we are going seek after and search among different thoughts proposed within the writing audit on the subject 'Risk Evaluation Management' counting evaluation modeling and we'll attempt to use our chance evaluation variables utilizing fluffy rationale. The chance demonstrate portrays the dangers to be assessed and the different connections they have with one another. This makes a difference to classify dangers that are likely to be comparable inside one bunch. As a result, Risk relief techniques are utilized effectively with the same sort of dangers. Chance variables, on the other hand, are characteristics that are utilized in models as input factors. They offer assistance decide the level of Risk amid the Risk evaluation handle. These factors incorporate impacts, dangers, conditions, probability of event, and vulnerabilities. They are more often than not decayed into more factors. For illustration, dangers can be broken down into risk sources or risk occasions.

Risk examination makes a difference individuals oversee questionable occasions with recognize Risk components. These variables incorporate dangers, powerless get to focuses, impacts, and the likelihood of the occasion happening. Examination can be done by different strategies, such as strategy quantitative, subjective, or semi-quantitative. It depends on whether the factual approach, levelappraisal, or both are required to evaluate Risk. Security chance administration is done byutilizing the SRFT show, which employments fluffy set hypothesis to decide dangers and countermeasures. Chance assessment evaluates how much Risk an data framework can have happens as a result of a misfortune occasion. It is decided by increasing the in general probabilities of an thing occasions, capabilities, and the affect of misfortunes on the framework. In expansion, the focusing on likelihood for the framework depends on the likelihood of advance, vulnerabilities, and conceivable manhandle of these vulnerabilities. The chance evaluation technique is survey the level of Risk as an component of capability, affect, and probability.

3. RESULT AND DISCUSSION

3.1. Result

The literature review on related themes can be summarized by researchers as follows.

1) A study by Al-Kausar et al. When looking at fuzzy applications to assess leakage risk, it became clear that the biggest risk was fuel migration within the pipelin2) A study by J. Wang et al. Based on existing evidence from system security assessments, there are recommendations for new methods of security analysis and integration of complex technical systems with unclear logic to account for some of the ambiguities that cause fatal problems.
2) The study Case by Orooji et al study also provides recommendations as to how to assess construction worker risk using fuzzy rule-based safety analysis to overcome the uncertainty of insufficient data. . From the above related studies, researchers can conclude that the application of fuzzy inference models is also suitable as a research tool for finding information arising from technology development and the activities of people working in the field. Work appears as an important organization [15].

Data security administration incorporates schedule assurance, known as overseeing data security and catastrophe readiness is known as trade coherence administration. Dangers can be coincidental or deliberateness. Dangers may incorporate unauthorized divulgence, utilize, adjustment, burglary, devastation and refusal of benefit [16].

Data security is the assurance of computer equipment, computing and non-computer hardware, information, and data from abuse by unauthorized people. Data security points to realize three primary objectives: security, i.H. The Company looks for to secure information and data from being uncovered by unauthorized people. The reason of accessibility is to guarantee that an organization's data framework makes information and data accessible to authorized clients. And at last, the keenness of all frameworks. The data must give an exact representation of the physical framework it speaks to. In today's world, numerous organizations are progressively mindful of the significance of upkeep [17].

Ensure all your assets, virtual and physical, against inner and outside dangers. Early computer frameworks given small assurance, but that changed as numerous computer security offices were vandalized by dissidents amid the Vietnam War. This involvement has driven the industry to embrace security measures that kill or minimize the hazard of harm or annihilation and guarantee trade progression after disturbances [18].

In its basic form, information security management consists of four stages: (1) Identify threats that can attack corporate information assets, (2) identify the potential risks posed by this threat, (3) Define data security policies, (4) implement controls to overcome these risks

The risk assessment process model is very simple and does not fully cover all aspects of cyber security and cybercrime. Then, the proposed modification model starts with vulnerable object detection (data or hardware) and then proceeds through the risk assessment model. The risk assessment model evaluates objects according to some calculation method, then passes it on to the next model, which either approves it or proceeds in the other direction.

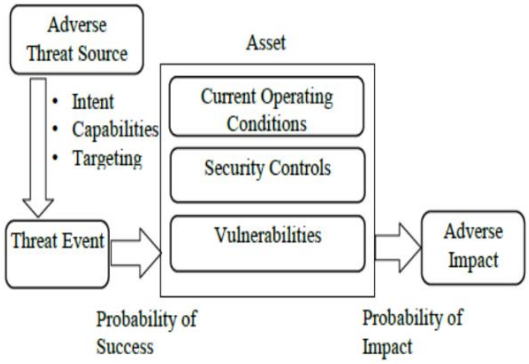

Figure 1. Risk Assessment Model

If an object is approved, the process ends, which means the object is safe. ÷ If an object is deprecated, it will switch to other models and estimate the vulnerability by computing probabilities based on fuzzy theory, then pass all the information to the tester to decide how minimize the risk and fix its vulnerability. The subject then undergoes vulnerability testing again. This process will update the model of people without human interaction to decide whether to oppose the risk assessment and accept the threats. The review process can be done by one or a group of actors, and at any time these days, many organizations deploy people to monitor the security in their businesses almost all the time; they are part of Operation Security.

Fuzzy Inference System "FIS" Receive incoming clips and then send a knowledge base with n fuzzy rules in an "if-then" format. membership level/ The antecedent or α is searched for each rule. If you have multiple rules, Aggregation of all rules. Then the aggregation result is performed DeFuzzification to get the Crips score as the output of the fuzzy inference system.

One of the FIS methods that can be used for decision making is Fuzzy Tsukamoto Inference Method. In Tsukamoto's fuzzy reasoning, each meaning is Rules take the form of "if-then" or "if-then" implications placed between antecedents.

So there is a relationship. Each rule is described using a fuzzy set with a monotonic membership function. As a result, the inference output of each rule

is given strictly (crips) based on the α predicate (fire intensity). A final score is obtained using a weighted average.

In Tsukamoto's fuzzy reasoning, the implication of each rule takes the form of an ``if-then" or ``if-then" implication, which is the relationship between the antecedent and the result. every day of ules are written using fuzzy sets with monotonic membership functions. As a result, the inference output of each rule is given strictly (crips) based on the α predicate (fire intensity). A final score is obtained using a weighted average [17].

The proposed method calculates the risk rating using the Mamdani method, which is one of the most widely used in the entire fuzzy logic theory, and then extends the work to include Sugeno's method. The differences between Mamdani and Sugeno's approaches are explained in Table 2 and Table 3.

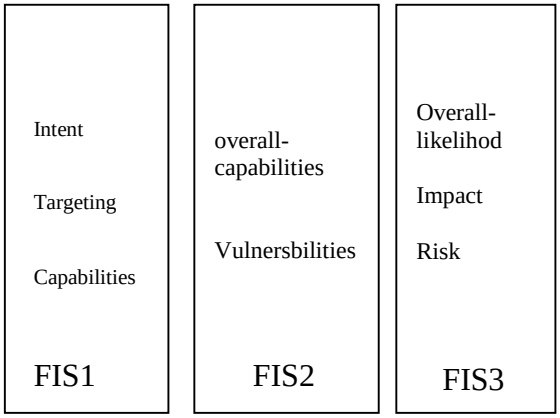

Figure 2. Proposed Risk Assessment Model

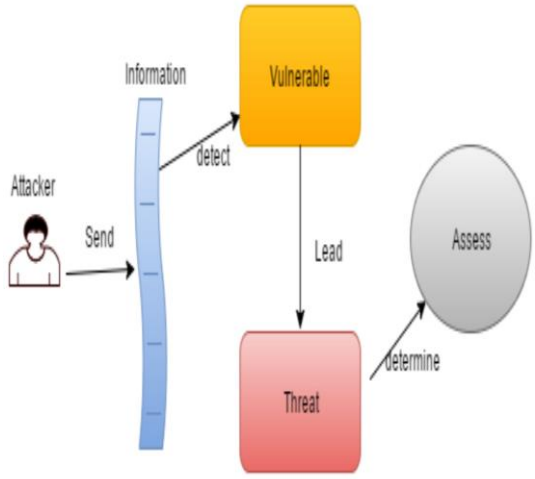

Figure 3. F1 Parameters and Settings

The proposed SIF applies this model to get the total risk for the system using the following formula.

1) F1=Overall Capability= (Ability, Intent, Target)
   The result obtained from F1 should be the combination of all possible intentions, goals and possibilities for all n=1 to n=n member groups.
2) F2=Overall probability= (Vulnerability, Overall likelihood)
   The result obtained from F2 should be the combination of all possible global possibilities and vulnerabilities for all member groups n=1 to n=n
3) F3=Staking= (overall probability, impact)
   The result obtained from F3 should be the combination of all probabilities and possible global effects for all member groups n=1 to n=n

From the above, it can be seen that three inputs and outputs are used in the proposed model and these inputs have many variables, members and values. Input values start from 0 to 1 and are divided into 3 or 5 segments, respectively. The output of F1 in 3D consists of three variables, and we can see that targeting and intent have a greater impact on skill, as attacks are malicious. Mostly from sophisticated attackers who are updating their tools while limiting their skills Limit the attacker's power and the power of the victim's system through updates as the table 4 the bellow:

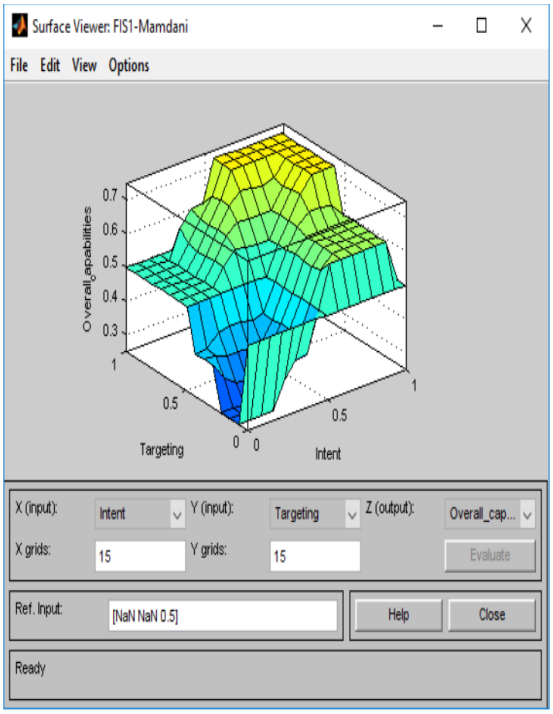

Figure 4. FIS1 Surface Output

3.2. Discussion

The dynamics of the development of the world's strategic environment are constantly increasing A variety of threats that have become more complex and affect national defense systems, including Indonesia. The form of threat that emerges from the development of the strategic environment is the threat cyber attack.

Risk analysis is the process of systematically using information to identify and assess risks. This process how to analyze potential information security failure scenarios and the consequences of loss of

confidentiality, integrity and preservation Availability of stored information values.

Risk assessment is the process of comparing estimated risks against predetermined risk evaluation criteria to determine the level and priority of risk. This operation is performed using the retrieved data Risk analysis results for informed decision making future risk management measures;

It is said that this cyber attack could lead to cyber warfare and cyber interference that disrupt national security and sovereignty. All of the above cyber threats are said to have the potential to threaten national assets. Institutions/companies around the world, especially those stored in his ISMS.

This threat is occurring worldwide and continues to be experienced significant year-on-year increase. Website attacks target organizations that use websites to provide services, provide information, make payments, and perform other essential functions. Web-oriented attacks are a top priority for cybercriminals. Especially organizations that cannot sanitize or validate the size of user input and the removal of variables.

This activity identifies vulnerabilities that cybercriminals use to perform exploits, such as cross-site scripting, cross-site hijacking, and SQL injection. destruction and Website hacking, also known as cybervandalism, determines the circumstances under which an attacker modifies the content of her website. Attackers tend to exploit such vulnerabilities through local file mounting, SQL injection, or cross-site scripting prior to obfuscation. DoS and Distributed Denial of Service (DDoS) describe attacks in which cybercriminals attempt to compromise a network or website by preventing legitimate users from entering.

Using or accessing certain Internet services. DoS attacks can target functionality Limit your organization's service bandwidth by sending too many ICMP or UDP packets to interfere with your bandwidth goals. DoS can be further described as protocol attacks that utilize various TCP/IP procedures with a highly standardized design such as UDP, ICMP and TCT. For example, a SNY flood leads to asymmetric resource exhaustion, where the attacker uses her TCP SYN packets to overwhelm the victim. DoS attacks, on the other hand, can appear as software vulnerability attacks that exploit vulnerabilities in network resources such as web servers.

Attacks can be exploit or smurf attacks, SYN/ACK floods, or ping floods. Consume bandwidth intended for organizational services and cause damage Or freeze the system in question. DoS typically serves three main purposes:

a) to change or destroy the information set;
b) consume scarce, renewable or finite resources; again
c) physically altering or destroying network elements.

Spam is defined as unsolicited email sent with the recipient's consent. Spammers typically use information available on social media and the web, as well as phishing techniques designed to steal banking information and credentials using social engineering. Phishing is best understood as a criminal activity that seeks direct access to sensitive information such as credit card information, usernames and passwords.

There are two types of phishing attacks: malware-based phishing and fraudulent phishing. It launches a phishing campaign that exploits vulnerabilities in the targeted computer's security software to launch malware that distributes the malware via email (the malware then acts as a keylogger and saves user input). Phishing scammers, on the other hand, use deceptive emails to trick users into revealing sensitive information such as passwords and bank accounts.

4. CONCLUSION

Administrators are expected not only to protect information assets, but also to keep the business functioning after a disaster or security breach. Activities to protect business assets and information assets are called information security management. It can be concluded that information security is used to describe the protection of computers and non-computer devices, as well as non-computer devices, facilities, data and information from misuse by unauthorized persons. increase. Information security is primarily aimed at achieving three goals: Confidentiality, Availability, Integrity.

In today's world, many organizations are increasingly realizing the importance of protecting all assets, both virtual and physical, from internal and external threats. The term system security is used to describe the protection of computers and non-computer devices, equipment, data and information from misuse by unauthorized persons. Activities to protect information assets are called Information Security Management (ISM), and activities to protect an organization and its information assets after a disaster occurs are called Business Continuity Management (BCM). The term risk management was coined to describe this approach of comparing the security level of a company's information assets and the risks to which they are exposed. An information system security threat is any person, organization, mechanism, or event that has the potential to harm an organization's information assets. Threats consist of internal and external threats. Information security risk can be defined as the unintended consequences of information security breaches by information security threats. All risks represent fraudulent activity. There are many ways to control threats and information security risks.

Fuzzy inference system is a rule system based on fuzzy logic that is used as a tool to represent various information about a problem and to model the interactions and relationships between these

variables. Therefore, the research process undertaken consists of evaluating the information flow of a company or organization using a Fuzzy Inference System (SIF), whose framework relies on the ability of its components to effectively proceed in a multitasking communication environment. and ascertain customer requests for repairs. This requires that the components of each framework operate under margin, manageable risk (servers, workstations, VMware devices, cloud capacity.

REFERENCES

[1] I. P. Galang Persada Nurani Hakim, S.T., M. T., Ir.Diah Septiyana, S.T., M.T., I. P. P., Ahmad Firdausi, S.T., M. T., Fajar Rahayu Ikhwannul Mariati, S.T., M. T., & Dr. Ir. Setiyo Budiyanto, S.T., M.T., *Sistem Fuzzy : Panduan Lengkap Aplikatif | Perpustakaan STIKOM Bali*. 2021. [Daring]. Tersedia pada: http://library.stikom-bali.ac.id/10054/sistem-fuzzy-panduan-lengkap-aplikatif

[2] C. T. Sanjaya, "Implementasi Logika Fuzzy Pada Aplikasi Pemasaran Udang Vaname Berdasarkan Skala Prioritas Di Ud. Mega Jaya Kab. Pacitan," hal. 1–58, 2021, [Daring]. Tersedia pada: http://eprints.umpo.ac.id/id/eprint/7564

[3] J. Al-kausar dan A. S. Handayani, "Perbandingan Type-1 Fuzzy Logic System (T1FLS) dan Interval Type-2 Fuzzy Logic System (IT2FLS) pada Mobile Robot," *Annu. Res. Semin.*, vol. 4, no. 1, hal. 978–979, 2018.

[4] M. F. Saifuddien, "Implementasi algoritma Fuzzy type-2 untuk menentukan perilaku NPC dalam game Virtual Reality Survival Shooter," hal. 1–100, 2018, [Daring]. Tersedia pada: http://etheses.uin-malang.ac.id/id/eprint/11023

[5] A. M. Mohammed, E. I. Morsy, dan F. A. Omara, "Trust model for cloud service consumers," hal. 122–129, 2018, doi: 10.1109/itce.2018.8316610.

[6] P. S. D. Ragavendiran dan N. M. E. Sowmiya, "Analysis of Trust Score of CSPS by Comparing Service Broker Policies and Load Balancing Policies using Cloud Analyst and Fuzzy Inference System," 2021, [Daring]. Tersedia pada: www.ijert.org

[7] T. Jensen, M. M. H. Khan, Y. Albayram, M. A. Al Fahim, R. Buck, dan E. Coman, "Anticipated Emotions in Initial Trust Evaluations of a Drone System Based on Performance and Process Information," *Int. J. Hum. Comput. Interact.*, vol. 36, no. 4, hal. 316–325, 2020, doi: 10.1080/10447318.2019.1642616.

[8] H. Kurdi *et al.*, "A lightweight trust management algorithm based on subjective logic for interconnected cloud computing environments," *J. Supercomput.*, vol. 75, no. 7, hal. 3534–3554, 2019, doi: 10.1007/s11227-018-2669-y.

[9] F. Topaloğlu dan H. Pehlivan, "Comparison of Mamdani type and Sugeno type fuzzy inference systems in wind power plant installations," *6th Int. Symp. Digit. Forensic Secur. ISDFS 2018 - Proceeding*, vol. 2018-Janua, hal. 1–4, 2018, doi: 10.1109/ISDFS.2018.8355384.

[10] A. K. Mehar dan S. Kotni, "A Study on Performance of Hydroxyapatite-Filled Polycarbonate and Polysulfone Composites Under Two-Body Abrasive Wear," 2021. doi: 10.1007/978-981-15-7779-6_24.

[11] S. De Capitani Di Vimercati, S. Foresti, G. Livraga, V. Piuri, dan P. Samarati, "A Fuzzy-Based Brokering Service for Cloud Plan Selection," *IEEE Syst. J.*, vol. 13, no. 4, hal. 4101–4109, 2019, doi: 10.1109/JSYST.2019.2893212.

[12] D. Novitasari, M. Asbari, L. M. Wijayanti, C. C. Hyun, dan M. Farhan, "The Role of Religiosity, Leadership Style, Job Satisfaction and Organizational Citizenship Behavior Mediation on Woman Teachers' Performance," *Solid State Technol.*, vol. 63, no. 6, hal. 2953–2967, 2020, [Daring]. Tersedia pada: http://solidstatetechnology.us/index.php/JSST/article/view/3380

[13] R. P. Sharma, D. Ramesh, P. Pal, S. Tripathi, dan C. Kumar, "IoT-Enabled IEEE 802.15.4 WSN Monitoring Infrastructure-Driven Fuzzy-Logic-Based Crop Pest Prediction," *IEEE Internet Things J.*, vol. 9, no. 4, hal. 3037–3045, 2022, doi: 10.1109/JIOT.2021.3094198.

[14] L. Van Der Werff, C. Real, dan T. G. Lynn, "Individual trust and the internet," *Routledge Companion to Trust*, hal. 391–407, 2017, doi: 10.4324/9781315745572.

[15] A. Orooji, M. Langarizadeh, M. Hassanzad, dan M. R. Zarkesh, "A Comparison Between Fuzzy Type-1 and Type-2 Systems in Medical Decision Making: A Systematic Review," *Crescent J. Med. Biol. Sci.*, vol. 6, no. 3, hal. 246–252, 2019.

[16] A. Nhlabatsi *et al.*, "Threat-specific security risk evaluation in the cloud," *IEEE Trans. Cloud Comput.*, vol. 9, no. 2, hal. 793–806, 2021, doi: 10.1109/TCC.2018.2883063.

[17] F. Deng, Y. Li, H. Lin, J. Miao, dan X. Liang, "A bwm-topsis hazardous waste inventory safety risk evaluation," *Int. J. Environ. Res. Public Health*, vol. 17, no. 16, hal. 1–18,

2020, doi: 10.3390/ijerph17165765.

[18] D. Serdar, "Analisis Sistem Manajemen Keamanan Informasi Menggunakan Standar ISO/IEC 27001 Dan ISO/IEC 27002 Pada Kantor Pusat PT Jasa Marga," *Sustain.*, vol. 11, no. 1, hal. 1–14, 2019, [Daring]. Tersedia pada: http://scioteca.caf.com/bitstream/handle/123456789/1091/RED2017-Eng-8ene.pdf?sequence=12&isAllowed=y%0Ahttp://dx.doi.org/10.1016/j.regsciurbeco.2008.06.005%0Ahttps://www.researchgate.net/publication/305320484_SISTEM_PEMBETUNGAN_TERPUSAT_STRATEGI_MELESTARI.