Improving Dynamic Archive Security Based Biometric System for Identification and Authentication with Personal Fingerprint

Yahya Nur Ifriza[1]✉, Sudarno[2]

DOI: 10.15294/eeaj.v10i3.49877

[1]Department of Computer Science Universitas Negeri Semarang, Semarang, Indonesia
[2]Faculty of Economics, Universitas Negeri Semarang, Semarang, Indonesia

Abstract

Pandemic has impacted many areas of life and led to the development of much new behaviour due to people's efforts to adapt, including adaptation in the workplace. The WFO (Work from Office) and WFH (Work from Home) rules will be enforced during the Covid-19, and this is one of the adaptive steps taken. Some employees are required to work from the office, while others are allowed to work from home under this rule. The author aimed to investigate the development of a microcontroller-based dynamic archive security system to address archive security during the WFH and WFO periods. With security system, the goal was to develop security tools that can serve two functions simultaneously, namely protecting data from loss while making it easier for workers to access the dynamic archives they need. This research was conducted by using research and development methods and the object of research was education staff at the Faculty of Economics, UNNES, using research and development strategies, this study succeeded in making a Dynamic Archive Security System product based on Biometric System Identification. Suggestions in this research on security systems can also be added with variations with RFID cards or NFC cards to implement various security systems.

How to Cite

Ifriza, Y. N. & Sudarno, S. (2021). Improving Dynamic Archive Security Based Biometric System for Identification and Authentication with Personal Fingerprint. *Economic Education Analysis Journal*, 10 (3), 467-476.

✉ Correspondance Address:
Jl. Raya Ngijo, Gunungpati, Semarang, Jawa Tengah
Email: yahyanurifriza@mail.unnes.ac.id

INTRODUCTION

The world is experiencing a Covid-19 pandemic, and Indonesia is no exception (Susilo et al., 2020). This pandemic impacts all aspects of life and has created many new habits as a step for human adaptation, including adaptation in the world of work (Li et al., 2013).

One of the adaptation steps during the Covid-19 pandemic is maintaining a distance between humans. These impacts work greatly, giving raise to the WFO (Work From Office) and WFH (Work From Home) rules. This rule requires some workers to work from the office while others work from home. This follows the Circular Letter of the Minister of State Civil Apparatus Empowerment and Bureaucratic Reform Number 58 of 2020 concerning the Work System of State Civil Apparatus Employees in the New Normal Order (Barokati et al., 2013). This rule explains that the maximum quota of employees is 50% of the total number of employees to enter and work in the office. This means that the number of employees or ASN is divided equally into two groups in one office. On the same day, group 1 works from the office (WFO) while group 2 results from home (WFH), so it keeps changing every week (Fitria, 2020).

Especially in the past two decades, the advancement of information technology has been unavoidable. Information used to be tough to get by, but because to technological advancements, it has now become something that is easily accessible to the general population (Bhanu et al., 2000). The Internet is one of the most visible manifestations of technological development, having altered almost every aspect of human society. The Internet, which includes information that can be accessed by anybody anywhere in the globe, is the primary source of information for the vast majority of people on the planet when it comes to addressing the information issue. IT is extensively used for job administration because of its efficiency and effectiveness, which have been shown to enhance performance, both

professionally and in the network. The ease of access, the speed with which information can be obtained, and the ability to save both time and money are the main reasons for people to utilize the Internet. Thus, it should come as no surprise that humans are unable to function without the aid of electronic devices and the Internet (Jain et al., 2000). The Internet, as one of the greatest inventions, has evolved into a forum for any digital activity that has been hazy as a result of the privacy restrictions that are now available to everyone (Rizkyantha, 2018).

The application of WFH and WFO rules has both positive and negative sides (Fitria, 2020). Employees can work more flexibly, but it also brings some obstacles. One of them is in the archives field, whose main task is to process and store documents (Oo & Aung, 2019). Constraints that often arise are related to document security and the difficulty of finding documents if they are needed at any time (Ekayana, 2018) (Oktaviani, N.S., & Sumardi, 2016). Often records are lost or scattered, so it will take a long time and hinder other work (Sam & Ifriza, 2021).

Fingerprint identification is the process of making imprints on the fingers by using the formations or patterns of small strokes that may be found on the fingertips. Neither two individuals nor one individual has the same arrangement of ridge patterns, and the design of one individual remains constant throughout life (Sokop et al., 2016).

Fingerprints are an indestructible method of establishing personal identity (Roth et al., 2020). Other aspects of a person's personality may change, but fingerprints remain constant (Februariyanti, 2006). Depending on the situation, the fingerprint can be captured on a conventional fingerprint card, or it can be digitally recorded and sent electronically to the technology for comparison(Zhang et al., 2010). A fingerprint is an imprint made by the friction ridges of a human finger on a piece of paper or other surface. Forensic science relies heavily on the recovery of partial fingerprints from crime scenes, which is an essential

technique of investigation (Ito et al., 2005). Fingerprints left on surfaces such as glass or metal are caused by moisture and grease on the fingertip. A flat surface such as paper may be used to create deliberate imprints of complete fingerprints by transferring ink or other substances from the peaks of friction ridges on the skin to a smooth surface such as paper. It is customary for fingerprint records to include impressions taken from the pad on the final joint of the fingers and thumbs, but fingerprint cards are also often used to capture parts of the lower joint regions in the fingers (Gao & Ding, 2020). Records maintainers can establish valid evidence of a person's presence in a dynamic archive by matching fingerprints (Sun et al., 2019).

As precise and virtually unique as human fingerprints are, they are difficult to change and remain stable throughout the course of a person's life, making them ideal for use as long-term identifiers of human identity. They may be used by law enforcement or other authorities to identify persons who want to remain anonymous, as well as to identify people who are disabled or dead and therefore unable to identify themselves, such as in the aftermath of a catastrophe (Sun et al., 2019).

We are now doing research on the design and implementation of an archive system security. As previously stated, the main objective of an archive system is to ensure the long-term availability and secrecy of data even in the event of storage server failures or breaches. The ability to adjust to the addition or removal of servers is another objective. Throughout this article, we describe a design for an archive system that achieves those objectives, as well as a protocol for secret redistribution, which is a critical component of the overall architecture (Wong et al., 2003).

A clear indication that greater attention should be given to biometrics is the growing need for dependable and secure recognition systems, which are currently being utilized in a wide range of fields. Biological and behavioural characteristics (such as fingerprints, iris, face, and palm print) as well as physiological characteristics (such as gait, signature, and typing) that are unique and cannot be lost or forgotten are used in biometric systems to provide accurate and reliable automatic personal recognition (Thai & Tam, 2010). In a variety of applications, such as passport verification, airport security, building access control, mobile phone unlocking, and identification cards, biometric recognition systems are utilized. Unimodal biometric systems are those that measure and analyze just a single feature of the human body, such as height. A number of disadvantages are associated with this approach, including: I noise in sensed data: in this case, the recognition rate of a biometric system is highly dependent on the quality of the biometric sample (Tan & Bhanu, 2006).

A biometric modality is said to be universal if each person in a population is capable of providing it for a particular system. If a modality is not universal, it is said to be non-universal. Not all biometric modalities, on the other hand, are really global. A third problem is that there is a lack of uniqueness in the characteristics derived from biometric modalities of different people; these traits may be almost similar. Within-class variation: The biometric information collected from a person during the training phase for the purpose of creating a template will not be identical to the template produced from the same user's biometric information during the testing process (Sha et al., 2006). It is possible that these differences are caused by insufficient interaction between the user and the sensor. In spite of the fact that it seems difficult to steal a person's biometric modalities, it is always feasible to bypass a biometric system by employing spoofing of the person's biometric modalities. In order to address these drawbacks, one option is the integration of several biometric modalities into a single system, which is referred to as a multi-biometric system (Ammour et al., 2020).

Based on the description of the work constraints on applying WFH and WFO rules, the authors initiated the idea of researching the Development of a Microcontroller-Based Dynamic Archive Storage Safe System as a

Solution for Ease of Working During WFH and WFO for Archives Employees (Carminati, 2019). This security system aims to create a security device that can perform two purposes at once: preventing files from being lost or damaged and making it easier for employees to access the files they need (Roth et al., 2020).

METHODS

Implementation of research using research and development methods (Research and Development) (Sumrahyadi, 2020). Research and development methods (Research and Development) are research methods used to produce certain products and test the effectiveness of these products (Prastya et al., 2015).

The research design used in this study is the ADDIE development model. The ADDIE development model is a programmatically structured model with a systematic sequence of activities to solve product development problems (Prastya et al., 2015). According to Prasetya, ADDIE Model stands for Analysis - Design - Development - Implementation - Evaluation.

Design, this stage aims to design a security system for dynamic archive storage vaults based on a microcontroller. The following is a tool design that has been made, as shown in Figure 1.
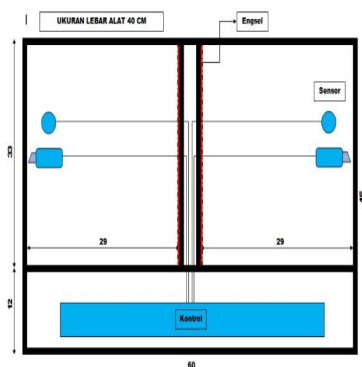

Figure 1. Design Biometric System for Identification

The development stage aims to create a security system following what has been previously defined in the design stage. The development stage will produce a product. Furthermore, the product that has been made will be validated by an expert validator. This aims to provide validation that the product created is suitable for use. Activities at this stage are followed by a series of revision activities and limited trials.

When it comes to security systems, they are a collection of various components that are responsible for preventing and removing interference from any dangers or barriers that may arise. Another objective of a security system may be to provide simple access to protected devices. Specifically, in the context of archives, the security system is primarily concerned with preventative measures, in order to reduce the likelihood of lost or damaged archives being preserved. However, this approach is designed to make it simpler for workers to access the archive without creating major problems for the organization as a whole. Securing your home may be accomplished via the use of a variety of security systems. With each, there are benefits and drawbacks depending on the intended purpose for which it is being considered. One of these systems is a fingerprint-based security system (Roth et al., 2020). Some of the components we used in developing this research:

Fingerprint Sensor. Fingerprints are a unique kind of identification that no one else can duplicate. Unlike other forms of identification, fingerprints in the form of strokes linked to human fingers have unique features that will not change throughout one's life (Sun et al., 2019). Based on the above-mentioned distinguishing features, there is one device that can be used to identify each individual's fingerprint, which is the fingerprint sensor as shown in Figure 2.

Figure 2. Fingerprint Sensor

The fingerprint sensor operates by scanning and reading the surface of the fingerprint, and then converting the analog readings into digital data via the use of an ADC (Analog to Digital Converter) device to complete the process. This device is in charge of storing and transmitting digital read data to and from the processor unit (microcontroller).

Microcontroller. A microcontroller may be thought of as a controller that is smaller than a standard controller. In general, a micro controller may be thought of as a miniaturized computer on a silicon chip. A variety of components, including a CPU, memory, input, and output, are housed in a single compact container. Micro controllers are small, low-power devices that are cheap and simple to acquire. The microcontroller works at a clocking speed of one Mega Hertz or less, depending on the model (Sun et al., 2019). As shown in Figure 3 microcontroller arduino type.
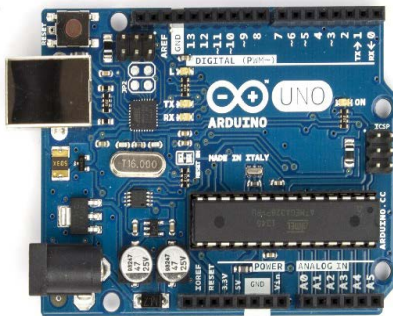

Figure 3. Microcontroller Arduino

To be specific, a microcontroller differs from a microprocessor found in a personal computer in that it contains only the bare minimum of system support components found in a microprocessor; in fact, some types of microcontrollers are equipped with ADC, PLL, and EEPROM facilities all in one compact package. Arduino is one of a number of different kinds of microcontrollers that contain the features listed above. This component is an open source physical computing platform based on basic input/output circuits, as well as a programming environment that implements a processing language for use in physical computing applications (Sokop et al., 2016).

In this case, the Arduino microcontroller is responsible for receiving input data from the fingerprint sensor and processing it. A collection of programming languages is required by the microcontroller in order for it to be able to handle data. The output device will then be instructed to execute the instruction as a result of this language.

Electric Door Lock. An electric door lock is the output device of a set of security systems that are connected together. This component is in charge of receiving and executing instructions that are sent by the microcontroller, among other things. It works by utilizing an electromagnet as a solenoid to open and shut a door lock or a safe, and it is quite simple, which is the electric door lock as shown in Figure 4.

Figure 4. The Electric Door Lock

The voltage required to operate an electric door lock is 12 volts. There are two terminals: one that is positive and one that is negative. Assuming that the positive leg of this component is powered by 12V and the negative leg is powered by zeroV, then this component will function to unlock. Meanwhile, if these two polarities are removed from the equation, the lock will be closed once again, and so on (Ekayana, 2018).

Validation activities are carried out by asking for consideration from experts to assess the feasibility of the developed product by filling out an assessment instrument in the form of a product validation sheet for a microcontroller-based dynamic archive storage safe system (Ifriza & Sam, 2021). This assessment was carried out by a lecturer in the Department of Electrical Engineering, State University of Semarang and the Head of the

Archives Section of the State University of Semarang (Sam & Ifriza, 2021). Product revisions are made based on advice from experts during validation (Ekayana, 2018).

Implementation. The implementation phase was carried out after the microcontroller-based dynamic archive storage safe system product underwent trials and revisions several times and was declared feasible based on experts' assessment. This stage is a field trial or application of the product to the actual archival work.

Several interconnected activities must be completed in an orderly manner in order for a system to be properly implemented and tested. The use of an established implementation methodology and the solicitation of professional assistance can be beneficial, but it is often the sheer number of tasks, insufficient planning, and inadequate resources that cause problems with an implementation project, rather than any of the tasks themselves being particularly difficult to complete. In the same manner, when it comes to cultural problems, it is often a lack of appropriate consultation and two-way communication that prevents the intended outcomes from being achieved.

Evaluation. The final stage in the ADDIE research model is evaluation. At this stage, an assessment of the results of field trials can be carried out. Evaluation is also carried out by revising the final product so that it is truly feasible to support archival work (Fitria, 2020).

Evaluation is the systematic interpretation and imparting of meaning to anticipated or actual effects of proposals or outcomes, as determined by a defined process. It examines the initial goals, as well as what may be anticipated, as well as what has been achieved and how it has been accomplished. Evaluating an idea or proposal, a project, or an organization may be formative, meaning that it occurs during the development of a concept or proposal, a project, or an organization with the goal of increasing the value or effectiveness of the proposal, project, or organization. Also possible is a summative approach, in which lessons are drawn from a finished activity or project or from an organization at a later point in time or under different circumstances.

The instrument used to collect data was an expert validation sheet. An expert validation sheet is an instrument used to obtain data about the validity of the developed product. This validation is carried out by media (development) experts. After getting assessment data from media (product) experts, the data is analyzed descriptively to determine the feasibility of the developed product (Ifriza et al., 2017).

When it comes to research, data collection is described as the process of gathering, measuring, and analyzing correct insights via the use of established, proven methods. A researcher may assess their hypothesis on the basis of the data that they have gathered. In the majority of instances, data collecting is the

Table 1. Instrument Grid for Experts

No.	Assessment Aspect	Indicator	Number of Items
1	Appearance	Attractive design	1
		Colour match	1
		Place the components accordingly	1
2	Size	Suitable size	1
3	Utilization	Easy to use	1
		Comfortable to use	1
4	Completeness	Audio Clear	1
		Image Clear	1
Amount			8

Source: Primary data processed, 2021

first and most essential stage in any research project, regardless of the subject matter being studied. According to the information that is needed, the method of data collecting differs for various areas of research.

After data from all sources is collected, the next step is to process or analyze the data (Roth et al., 2020). The data analysis carried out is Expert Validation Data Analysis. Analytical techniques such as data collecting, data cleansing, and data organization are usually used in conjunction with other operations such as statistical testing. These procedures, which often involve the use of data analysis tools, are required in order to prepare the data for use in business operations. Data analysis, often known as data analytics, is defined as the science of evaluating raw data in order to make educated conclusions based on the information included in the data.

Analysis of the data used was a quantitative descriptive analysis technique. Expert validation data analysis was carried out by using the eligibility percentage with the following formula (Ammour et al., 2020). Because the essence of quantitative data is numerical, quantitative data analysis entails dealing with numerical variables such as statistics, percentages, computations, measurements, and other data, as well as other types of data. Algorithms, mathematical analytical tools, and software are usually used in conjunction with quantitative data analysis methods to alter data and discover insights that have significant commercial value. When a whole is divided into its constituent parts for individual study, this is referred to as analysis. Information retrieval and conversion into information helpful for decision-making is the act of gathering raw data and turning it into information beneficial to users. Data is gathered and processed in order to answer questions, test hypotheses, or refute ideas, among other things.

Eligibility Percentage (%) = ($\sum$validation score)/($\sum$ideal score) x 100%

Furthermore, the percentage is categorized as an assessment on a Likert scale to determine the feasibility of the product being developed and decide whether or not to revise the visual media. The Likert scale is categorized by (Oktaviani, N.S., & Sumardi, 2016).

RESULTS AND DISCUSSION

Following the Biometric system's design for identification, the following is a ready-made tool, which can be seen in Figure 5.

Figure 5. Biometric System for Identification

Four minutes features, terminations, bifurcation, short lines, and dots are retrieved from each fingerprint picture, for a total of four minutes features per fingerprint image. Crossing Number is utilized to identify minutiae points in a fingerprint picture while extracting terminations since the terminations

Table 2. Product Feasibility Assessment By Expert Validators

Percentage (%)	Value Scale	Validity Criteria	Information
81 – 100	5	Very Valid	No Revision
61 – 80	4	Valid	No Revision
41 – 60	3	Quite Valid	No Revision
21 – 40	2	Less Valid	Revision
0 – 20	1	Invalid	Revision

Source: Primary data processed, 2021

Table 3. Eligibility Result By Expert

Code	Rating Indicator	Result
A1	Attractive Dynamic Archive Security System Design	100%
A2	Dynamic Archive Security System Color Match	100%
A3	Component Location in Dynamic Archive Security System Appropriately	93%
A4	Dynamic Archive Security System Size Appropriate	100%
A5	Easy to Use Dynamic Archive Security System	93%
A6	Dynamic Archive Security System Convenient to Use	87%
A7	Audio on Dynamic Archive Security System Clear	87%
A8	Image on Dynamic Archive Security System Clear	100%

Source: Primary data processed, 2021

that are located at the outside borders are not taken into consideration. When two adjacent pixels have different intensity values from one another, the Crossing Number is half of the total of the disparities between the two adjacent pixels. Minutiae points are categorized as Termination if their crossing numbers are 1, 2, and 3 or more than 3. The rest of the time, they are just regular ridges or bifurcation.

Based on tool validation by experts selected by the research team to validate the Biometric system for identification through boring dynamic archive security system validation sheets, the results of product feasibility from experts show valid and very valid results, starting from A1 with 100% results, A2 with 100% results. A3 results in 93%, A4 results in 100%, A5 results in 93%, A6 results in 87%, A7 results in 87%, and A8 results 100%, if

the overall validity component is obtained on average, 95% of the products are very valid. These results can be presented in the form of Table 3.

We also present expert validity data into the graph of each component, which can be seen in Figure 6.

CONCLUSION

Based on the study results, it can be concluded that the use of the Biometric system for identification in dynamic archive security has proven to be very valid. Before applying the Biometric System for Identification Method at the planning stage, the security system used was still manual. After implementing the biometric identification method, the security system is more secure, and access to dynamic archives can be restricted. The validity test of the Biometric system for identification proved to be very valid, with an average validity of the expert team reaching 95%.

Based on input from experts, it is necessary to create a larger Biometric system for identification and backup security. Future research on security systems can also be added with variations with RFID cards or NFC cards to apply various security systems. In addition, researchers can use biometric systems for identification for security in other fields.

	A1	A2	A3	A4	A5	A6	A7	A8
Ahli 1	5	5	5	5	5	5	4	5
Ahli 2	5	5	4	5	4	4	5	5
Ahli 3	5	5	5	5	5	4	4	5

Figure 6. Expert Validity of Each Component

ACKNOWLEDGEMENT

REFERENCES

Ammour, B., Boubchir, L., Bouden, T., & Ramdani, M. (2020). Face–iris multimodal biometric identification system. *Electronics (Switzerland),* 9(1). https://doi.org/10.3390/electronics9010085

Annisah, S. (2014). Siti Annisah. *Jurnal Tarbawiyah,* 11(1), 1–15.

Barokati, N., & Annas, F. (2013). Pengembangan Pembelajaran Berbasis Blended Learning pada Mata Kuliah Pemrograman Komputer (Studi Kasus: UNISDA Lamongan). *Sisfo,* 4(5), 352–359. https://doi.org/10.24089/j.sisfo.2013.09.006

Bhanu, B., Boshra, M., & Tan, X. (2000). Logical templates for feature extraction in fingerprint images. *Proceedings - International Conference on Pattern Recognition,* 15(2), 846–850. https://doi.org/10.1109/icpr.2000.906207

Carminati, L. (2019). Dead ends in and out of the archive: an ethnography of Dar al Watha'iq al Qawmiyya, the Egyptian National Archive. *Rethinking History,* 23(1), 34–51. https://doi.org/10.1080/13642529.2018.1494933

Ekayana, A. A. G. (2018). Implementasi Sistem Penguncian Pintu Menggunakan RFID Mifare Frekuensi 13.56 Mhz dengan Multi Access. *Jurnal Pendidikan Teknologi Dan Kejuruan,* 15(2), 244–253. https://doi.org/10.23887/jptk-undiksha.v15i2.14361

Februariyanti, H. (2006). Standar dan Manajemen Keamanan Komputer. *Teknologi Informasi DINAMIK*, XI(2), 134–142.

Fitria, N. J. L. (2020). Penerapan Work From Home Dan Work From Office Dengan Absensi Online Sebagai Implikasi E-Government Di Masa New Normal Implementation of Work From Home and Work From Office With Online Absence As an E-Government. *Civil Service,* 14(1), 69–84.

Gao, L., & Ding, Y. (2020). Disease prediction via Bayesian hyperparameter optimization and ensemble learning. *BMC Research Notes,* 13(1), 1–6. https://doi.org/10.1186/s13104-020-05050-0

Ifriza, Y. N., Edi, C. E., & Suseno, J. E. (2017). expert system irrigation management of agricultural reservoir system using analytical hierarchy process (AHP) and forward chaining method. 74–83.

Ifriza, Y. N., & Sam, M. (2021). Irrigation management of agricultural reservoir with correlation feature selection based binary particle swarm optimization. *Journal of Soft Computing Exploration*, 2(1), 40–45. https://doi.org/10.52465/joscex.v2i1.23

Ito, K., Moritat, A., Aoki, T., Higuchi, T., Nakajima, H., & Kobayashi, K. (2005). A fingerprint recognition algorithm using phase-based image matching for low-quality fingerprints. *Proceedings - International Conference on Image Processing,* ICIP, 2, 33–36. https://doi.org/10.1109/ICIP.2005.1529984

Jain, A. K., Prabhakar, S., Hong, L., & Pankanti, S. (2000). *Filterbank-Based Fingerprint Matching.* 9(5), 846–859.

Li, N. N., Liu, Y. B., & Liu, K. (2013). Primary discussion on LNG terminal fire prevention system design. *Procedia Engineering*, 52, 181–185. https://doi.org/10.1016/j.proeng.2013.02.124

Oktaviani, N.S., & Sumardi, Y. (2016). Unnes Physics Education Journal. *Physics Education*, 5(3), 1–8.

Oo, A. K., & Aung, Z. L. (2019). A Robust Fingerprint Recognition Technique Applying Minutiae Extractors and Neural Network. *International Journal of Engineering Research and Advanced Technolog*y, 5(3), 78–87. https://doi.org/10.31695/ijerat.2019.3402

Prastya, I. G. H., Pudjawan, K., & Suartama, I. K. (2015). Pengembangan Multimedia Pembelajaran Interaktif Mata Pelajaran Bahasa Indonesia dengan Model ADDIE untuk

Siswa Kelas VII Semester Genap Tahun Ajaran 2014-2015 di SMP Negeri 1 Banjar. *E-Journal Edutech Universitas Pendidikan Ganesha Jurusan Teknologi Pendidikan,* 3(1), 1–11. https://ejournal.undiksha.ac.id/index.php/JEU/article/view/5605

Rizkyantha, O. (2018). The Roles of Archive Institution on Indonesia Public Information Disclosure In Digital Era. *Pustabiblia: Journal of Library and Information Science*, 1(2), 139. https://doi.org/10.18326/pustabiblia.v1i2.139-154

Roth, S., Barron, T., Calzavara, S., Nikiforakis, N., & Stock, B. (2020). Complex Security Policy? A Longitudinal Analysis of Deployed Content Security Policies. February. https://doi.org/10.14722/ndss.2020.23046

Sam, M., & Ifriza, Y. N. (2021). A combination of TDM and KSAM to determine initial feasible solution of transportation problems. *Journal of Soft Computing Exploration,* 2(1), 17–24. https://doi.org/10.52465/joscex.v2i1.16

Sha, L., Zhao, F., & Tang, X. (2006). Minutiae-based fingerprint matching using subset combination. *Proceedings - International Conference on Pattern Recognition*, 4, 566–569. https://doi.org/10.1109/ICPR.2006.802

Sokop, S. J., Mamahit, D. J., & Sompie, S. (2016). Trainer Periferal Antarmuka Berbasis Mikrokontroler Arduino Uno. *Jurnal Teknik Elektro Dan Komputer,* 5(3), 13–23.

Sumrahyadi. (2020). Archive Human resources in The ASEAN Economic Community Era. 1(1), 38–46.

Sun, X., Wu, C., Gao, X., & Li, G. Y. (2019). Fingerprint-Based Localization for Massive MIMO-OFDM System with Deep Convolutional Neural Networks. *IEEE Transactions on Vehicular Technology,* 68(11), 10846–10857. https://doi.org/10.1109/TVT.2019.2939209

Susilo, A., Rumende, C. M., Pitoyo, C. W., Santoso, W. D., Yulianti, M., Herikurniawan, H., Sinto, R., Singh, G., Nainggolan, L., Nelwan, E. J., Chen, L. K., Widhani, A., Wijaya, E., Wicaksana, B., Maksum, M., Annisa, F., Jasirwan, C. O. M., & Yunihastuti, E. (2020). Coronavirus Disease 2019: Tinjauan Literatur Terkini. *Jurnal Penyakit Dalam Indonesia,* 7(1), 45. https://doi.org/10.7454/jpdi.v7i1.415

Tan, X., & Bhanu, B. (2006). Fingerprint matching by genetic algorithms. *Pattern Recognition,* 39(3), 465–477. https://doi.org/10.1016/j.patcog.2005.09.005

Thai, L. H., & Tam, H. N. (2010). Fingerprint recognition using standardized fingerprint model. 7(3), 11–17.

Wong, T. M., Wang, C., & Wing, J. M. (2003). Verifiable secret redistribution for archive systems. *Proceedings - 1st International IEEE Security in Storage Workshop*, SISW 2002, 94–105. https://doi.org/10.1109/SISW.2002.1183515

Zhang, K., She, J., Gao, M., & Ma, W. (2010). Study on the embedded fingerprint image recognition system. *Proceedings - 2010 International Conference of Information Science and Management Engineering, ISME* 2010, 2, 169–172. https://doi.org/10.1109/ISME.2010.281