Volume 3, No. 8 August 2024 (1883-1894)
p-ISSN 2980-4868 | e-ISSN 2980-4841
https://ajesh.ph/index.php/gp

The Concept of Cloud Computing for Notary Protocol Storage Reviewed from the Secrets of the Notary Position

Nadine Cristalia Gautama[1]*, Tjhong Sendrawan[2]
[1,2]Universitas Indonesia, Depok, West Java, Indonesia
Email: ncristalia@gmail.com[1*], tjhong_sendrawan@ui.ac.id[2]

ABSTRACT:
This research is motivated by the problems and difficulties in storing the Notary Protocol, where it must provide a sufficient place and protect it from the risk of loss or damage due to fire, theft, or force majeure. Cloud computing-based Notary Protocol Storage is the solution to the problem. This study aims to analyze the implementation of the Notary Protocol based on cloud computing associated with the Secrets of the Notary Position regulated in Law Number 2 of 2014 concerning Amendments to the 2004 Law on the Notary Position (UUJN). This research was conducted using a doctrinal approach, with an explanatory type of research that used secondary data obtained from literature and document studies. The data obtained is analyzed qualitatively; the collected data is systematically calcified according to each category and then analyzed to answer the main problem. The results of this study show that the cloud computing system will facilitate and overcome the risk of loss or damage to archives stored in the Notary Protocol, and the use of cloud computing can be done without violating the Notary Secret, but it is better than the service provider is the party organized by the Notary Supervisory Council (MPN), and for the weaknesses and risks owned by the cloud computing system, the storage of the Notary Protocol should be carried out in conjunction with manual storage either by conventional (paper) and/or by backing up on a private server.
Keywords: Notary Protocol Storage, Cloud Computing, Office Secrets.

INTRODUCTION

The authority of the notary in making and storing deeds is an obligation mandated by Article 16 paragraph (1) of the UUJN; in carrying out his position, the notary is obliged to make a deed in the form of a deed and keep it as part of the notary protocol. The minuta deed itself is part of the notary protocol that is mandatory to be kept by the notary because it may be needed for the benefit of the judicial process, where the minuta deed itself can be shown according to

the procedures determined by the regulations. The notary must really store and maintain the notary protocol because it is the power to copy the deed (Nadhiro, 2019).

Minuta deeds and other documents that are part of the notary protocol contain important, confidential information and personal data of individuals and legal entities (Delafare et al., 2023). Therefore, the trust given by the public to notaries must be firmly held and is a secret of the position that should not be known by anyone other than those who are interested and authorized. The notary official pledged his promise during the oath of office to keep the contents of the deed and the information he obtained confidential as stipulated in Article 4 paragraph 2 of the UUJN so that In addition to being able to protect the deeds he makes from theft, fire, and disasters, the notary must also keep them from reaching parties who are not interested and not authorized to know the contents of the deed or control copies beyond their authority.

Notaries need to keep up with global and technological developments to fulfil their functions and responsibilities. According to (Hetharie et al., 2022), the existence of notaries is inseparable from the community's needs. It needs someone (figure) whose testimony is reliable and trustworthy, whose signature and seal (its stamp) provide strong assurance and evidence, an impartial expert and an unblemished advisor (onkreukbaar) or (unimpeachhable), who shut up and make a covenant that can protect in the days to come.

The problem today is that notary protocol storage is still done conventionally. This causes many difficulties and problems for notary officials in fulfilling their obligations because they require a large enough space. Besides that, the notary must also follow the protocol received from the notary who has stopped serving. Article 63, paragraph 5 of the UUJN also explains that the submission of the notary protocol to another notary whose protocol age is 25 years or more is submitted by the recipient of the protocol to the Regional Supervisory Council (MPD) for safekeeping. However, the fact is that none of these Protocols has been submitted to the MPD until now, and this is a national problem, which means that it occurs in the territory of Indonesia due to the absence of facilities and infrastructure. This causes material losses both to the notary and also to the public who need evidence related to the deed kept by the Notary (Permana et al., 2024). as in research by Putri in 2019 entitled "Electronic Storage of Notary Protocol in the Concept of Cyber Notary", shows that archives in the form of paper archives cause various problems related to storage places, maintenance costs, management personnel, facilities and other factors that can cause damage to archives, so it is necessary to utilize existing technology. The existence of technology with the concept of Cyber Notary allows the creation and storage of notarized deeds online through the Cyber platform (Alkatiri et al., 2023).

Basically, the use of information technology for notaries in Indonesia is not something unfamiliar; notary offices are already commonly using computers and e-mail ¬to send and receive data and store data in the form of Portable Document Format (PDF). However, the records, authentic deeds, deed lists, lists of letters under the notarized hand, protest lists, will books, and

other things that notaries must keep are very many and complicated. Notaries need a reliable system to help notaries, one of which is an electronic system with the concept of Cloud Computing.

The development of the form of society into an information society (information society) triggered the development of information technology (Information Technology Revolution). It is becoming increasingly rapid, so increasingly sophisticated information devices and information system networks are becoming increasingly complex and reliable and able to meet the demands of all levels of society. The countries of Indonesia and France have started to develop applications based on cloud computing to meet the needs of the community, especially in this study, which is the need for notaries. In Indonesia, there is an application called CNOT (Kumar et al., 2024). CNOT, which is a notary office application system and PPAT, was created by the Indonesia Notary Association (INI) in collaboration with PT Averin Teknologi in 2018. However, the development to date, most notaries still keep the protocol in conventional form. Meanwhile, in France, MICEN (Minutier Central Électronique des Notaries de France), where all authentic deeds made by a notary in France must be sent, registered, and entered in the MICEN system managed by the Conseil Supérieur du Notary (CSN) where the institution is the Notary High Council

This cloud-based electronic system provides advantages for notaries, such as no longer needing to provide a room or building to store stacks of notary protocol archives and no need to invest heavily in applications or IT systems when managing their own storage servers. In addition, there is a guarantee of data security from the service provider Cloud (because the data is stored in encrypted form), and the application will always be updated in accordance with technological developments and related rules/regulations (Verma et al., 2023). However, using Cloud Computing still has shortcomings and risks, such as data leakage or theft and problems related to the confidentiality of the notary position. So, it is necessary to study the storage of the Notary-based Protocol Cloud Computing System more deeply, especially in maintaining the Confidentiality of the Notary Position.

Based on the background and problem formulation mentioned above, the objectives of this study are to explore how Cloud Computing can provide solutions to the challenges and difficulties faced by notary officials in storing and maintaining notary protocols and serving the community's needs. Additionally, this study aims to analyze how the implementation of cloud-based notary protocol storage relates to the confidentiality of the notary position as mandated by the Notary Law (UUJN).

RESEARCH METHODS

Legal research is a scientific activity based on certain methods, systematics, and thinking that aims to study one or several specific legal phenomena by way of galacis, except that an in-depth examination of the legal facts is held to try to solve the problems that arise in the phenomenon concerned.

This research was carried out with a doctrinal approach by researching legal rules and doctrines that involved a review of the Notary Office Law, which regulates the confidentiality of the notary office and the storage of notary protocols. The object of research is the problem notary officials face in storing notary protocols with the concept of cloud computing associated with the Secret of Position (Makhdoom et al., 2024). This type of research is an explanatory type of research, describing and explaining more deeply the symptoms arising from the subject matter in this study and trying to find answers to the problem by examining the sources of sukum related to the subject matter, as well as finding answers to the problem by examining sources related to the subject matter and detailing several new information that Found.

While the type of data used in this study is secondary data in the form of primary and secondary legal entities, the primary legal material in this case is Law Number 30 of 2004 and its amendments, namely Law Number 2 of 2014 concerning the Notary Position, and secondary legal entities, in this case, consist of books, research or legal writing in the form of theses or dissertations and legal journals that are relevant to this research. This method approach can provide knowledge related to the features and utilization of cloud computing that can be used to store notary archives (Kleinaki et al., 2018). This study compares with the French state, which has a great role in and influence on the history of the notary institution in Indonesia.

RESULTS AND DISCUSSION

The Problem of Notary Protocol Storage in Indonesia.

The Notary Protocol, which is a collection of documents in the form of state archives, must be kept and maintained by a notary in accordance with the provisions of laws and regulations (Toruan, 2022). The notary is responsible for keeping his or notary deeds and protocols during his or her tenure and will be continued by the next notary who replaces him or her. In accordance with the current rules, the Notary Protocol archives are in the form of paper. Therefore, the notary, as the holder of the Protocol, faces the difficulty of providing a large place and organizing the documents properly; as a result of not enough space to accommodate the protocol that must be accepted, is: minute books are scattered in the office and the house of the protocol recipient. So, it is very vulnerable to loss and damage due to unexpected things (force majeur) such as animal pest bites (termites), floods, fires, and earthquakes (Srivastav & Srivastav, 2019). In addition, the storage period of the notary protocol is not short, and in the process, there is often a risk of damage or loss.

The storage of notary protocols that are 25 years old or older should be handed over by the notary who received the protocol to the MPD. Still, its implementation has not been able to be done due to the limitations of the Regional Supervisory Council, which does not have a warehouse or building to store it. This is a big and national problem caused by inadequate facilities and infrastructure for the storage of notary protocols, which are state archives (Ibrahim et al., 2021). In 2014, this matter was discussed by the Head of Information Technology of the Central Board of the Indonesia Notary Association, namely Ismiati Dwi Rahayu. One of the reasons was that the Notary Regional Supervisory Council alone was doubtful of having an office, let alone having to keep many Notary Protocols (Lewinbuk, 2020).

In addition, there are many problems due to the storage of the Notary Protocol which is still conventional, such as the first in Zahra's research in 2021 which examined the jurisprudence of the Surabaya District Court Decision Number 943/Pdt.G/2019/PN SBY in 2019, showed a problem related to the Notary who could not provide a copy of the deed of Transfer and Transfer of Rights (Cessie) dated December 1, 2003 Number 5 made before the Notary HC. S.H. In this case, as the defendant, the Notary could also not be contacted and met. Due to the negligence of the Notary, the heirs had difficulty handling the name change at the land office because they needed a copy of the deed as a document that must be completed (Dewi, 2022).

Second, in Indonesia, there has also been a disaster that caused big problems and the loss of notary archives. In 2004, notaries in Aceh lost the protocol and all supporting documents for doing deeds that were stored due to the tsunami that hit the area. This incident harmed many parties and caused notaries, especially the public, difficulty obtaining the required documentary evidence (Habibah et al., 2024).

Examples of the two cases above show the importance of storing notary protocols in an electronic system (Kencana et al., 2023). The discourse to switch the notary protocol from the conventional one using paper (paper-based) to electronic (digital-based) will provide considerable benefits for the notary profession itself, including the fact that notaries will be more optimal in carrying out their obligations and duties. The filing of documents in the notary protocol will be able to run more effectively and efficiently. Electronic storage of minutes or notary protocol is not only to minimize document damage but also to facilitate access to find the file or file sought and to reduce the use of excess paper; the electronic storage of deed minutes is an important thing to be implemented by notaries in carrying out their positions. However, although technology allows the role of notaries online and remotely, legally, this does not seem to be possible because the paradigm underlying the UUJN is built with a conventional mechanism (Catur, 2023)**.**

Notary Protocol Storage with Cloud Computing Concept

Cloud computing is a computing paradigm that allows the access, storage, and management of computing resources and data through the Internet network (Agarwal &

Srivastava, 2017). NIST defines Cloud Computing as a model that allows convenient and flexible network access to customizable computing shared resources (such as networks, servers, storage, applications, and services) that can be quickly installed and released with minimal management effort or interaction with service providers. This means that the user of cloud computing can access the desired data through any network, anywhere, and anytime to the data set managed by a certain party to obtain and use it quickly (Botta et al., 2016).

Cloud computing-based Notary Protocol Storage can solve the problems described above. Here are some of the advantages of using Cloud Computing:

1. Cost savings in the use of cloud computing, where there is no need to invest in rooms/warehouses or even buildings that need to be provided, cabinets, and even departing. It also does not require hardware in the form of a production server or IT professional to manage the software and supporting network because everything already exists and is installed online when using cloud computing.
2. An easy and fast search, equipped with a search engine in the software used, will make it easier for Notary Officials to find the deeds the public needs quickly and accurately. This can be a solution to meeting the demand for document discovery, especially for making copies of old deeds. This is a problem for notaries because finding and rediscovering documents is not easy.
3. Cloud users can determine the storage capacity as needed, eliminating the need for computer memory upgrades.
4. The backup and recovery of existing data will be stored on the server of the cloud computing service provider online, so theft, fire, or natural disasters will not cause the loss or damage of documents stored in the Notary Archive.
5. It can be accessed anywhere because it is internet-based, so Notary officials can meet the community's needs online and remotely.

However, of all the advantages and advantages outlined earlier, the use of cloud computing is inseparable from its drawbacks and risks (Chiregi & Jafari Navimipour, 2018). The shortcomings found in cloud computing, namely:

1) An internet connection is an obligation in cloud computing because the internet is the only door to cloud computing. Adequate and stable bandwidth is needed to support this.
2) Cloud computing service tenants do not have direct access to resources, and also regarding the confidentiality and security of user data. Data confidentiality and security are still a serious consideration in cloud computing services.
3) Server quality is also a consideration before using cloud computing services. Users will suffer greatly if the server or program access goes down at any time. Server problems must be handled well, and there must be a backup (recovery) system. If not handled properly, users will suffer huge losses.

The main risk associated with the use of cloud computing is data security. It is recorded that many large companies providing cloud computing services have experienced data leaks that result in losses for service providers and users who store data, including personal data. The following are the things that cause risks in the use of cloud computing systems (Suroso & Sriratnasari, 2018), such as:

1) Only the provider knows physically what is happening with the user's data, so it is the provider's full responsibility.
2) When a disaster occurs, sometimes the provider's ability to recover data is still a concern for users.
3) Uncertainty regarding the provider's compliance with regulations and in the event of bankruptcy.

The Storage of Notary Protocols Based on Cloud Computing is reviewed from the Position Secrets regulated in the UUJN.

Notary-based Protocol Storage Cloud Computing needs to pay attention to one of the main things: not violating the Notary Secret (Mauri & Verticale, 2017). The trust given by the public to the Notary must be firmly held and is a secret of the position that should not be told to anyone, both everything written in the deed and everything that the Notary obtains from the parties to do the deed, except to people who have a direct interest in the deed, such as heirs. Based on the provisions of the UUJN, notaries who violate the secrecy of their positions can be subject to sanctions in the form of warnings up to dishonourable dismissal from their positions.

The Notary must firmly hold the secret of this position in carrying out his position. This can be seen in Article 4 paragraph (2) paragraph 4, Article 16 paragraph (1) letter f, and Article 54 paragraph (1) of the UUJN. A violation of the Notary Secret can give rise to accountability for the notary profession, be it administrative liability, compensation for losses in the civil realm, or criminal liability. So, there are things that need to be ensured that the use of Cloud Computing In keeping the notary protocol, it is reviewed from the secrecy of the position, including:

1. The location where the server is located is very important, considering that notary protocols are state archives whose storage must not violate office secrecy, so notary protocols cannot be stored on general cloud computing, such as iCloud, where the servers and hardware that collect data are stored in the United States. The application model of the cloud computing system used is preferably Private Cloud. The private cloud has the most guaranteed data security because it is managed by itself and is located in Indonesia. It's just that it requires workforce infrastructure to maintain and ensure that services run well. As a service provider, of course, the IT department must be responsible so that the service can run well in accordance with the service quality standards that have been determined by the company, including infrastructure, platforms, and existing applications.

2. Storage on cloud computing so as not to violate the Job Secrets must only be accessible to authorized persons.
3. Cloud computing service providers can offer security mechanisms to users. These security mechanisms are configured based on user requests and needs, such as keeping documents confidential and storing them in the cloud. The security mechanisms that can be implemented in cloud computing are process authentication and encryption-decryption processes.
4. Cloud service users for notaries, each given 1 (one) virtual server so that the data between one notary and the other is not mixed and there is minimal threat of risk from the outside, which often takes advantage of loopholes in the cloud system where 1 (one) server stores several tenants.
5. Although only the user, namely the Notary and/or his assistant, can access the data, the data stored on the server is owned by the service provider. This can potentially violate the confidentiality of the Notary position because it can be accessed or read by the data manager. Therefore, the service provider who stores data in the form of a Notary Protocol must be held by the authorities, such as under the Notary Supervisory Board.
6. Notary protocols stored in the cloud, in addition to being encrypted, are also stored in Portable Document Format (PDF), where PDF files can be encoded so that certain keywords are required to open or edit them.

Take the example of the notary office system based on cloud computing in Indonesia, which is in collaboration with the Indonesia Notary Association, organized and managed by PT. Averin Informatics Technology is called CNOT. If the Notary decides to use this cloud-based electronic system, the Notary can contact this service provider and register himself as a user to obtain a username and password (Camley, 2020). To use this service, the Notary must pay a subscription fee according to the platform determined by the service provider. After that, the Notary can access the service from anywhere, including from outside the office, so that he can do his work remotely and mobile. If the Notary wants his assistant to be able to access one of the modules from outside the office, the Notary can arrange it by contacting the service provider to register a specific IP Address so that it can be connected to the cloud system. A regulated security system restricts free access to the cloud, and Notaries and PSEs have log-in data to know who can access data from the cloud and when which is a way of securing data stored in the cloud.

An encryption system also protects data security in the CNOT cloud system; each notary who subscribes to this service is given 1 (one) virtual server so that the data between one notary and the other is not mixed and there is minimal threat of risk from the outside which often takes advantage of loopholes in the cloud, where generally 1 (one) server stores several tenants. In addition, all documents, in addition to encryption, are stored in Portable Document Format (PDF) format, where PDF files can be encoded so that certain keywords are required to open or edit them.

Another country that has used the concept of cloud computing to store notary protocols is France. A country that has played an important role in the history of notarization in Indonesia has established the Minutier Central Électronique des Notaries de France (MICEN), where all authentic deeds made by the French Notary must be sent, registered, and entered in the MICEN system which is a secure server dedicated to centralizing the national storage of notary documents provided by the government. Deeds uploaded in MICEN can only be accessed by the notary who signed the deed, and only an authorized notary can modify or make a copy of the deed.

MICEN is managed by the Conseil Supérieur du Notary (CSN), the Higher Council of Notaries, an organization formed by the Ordinance of November 2, 1945, and the Decree of December 19, 1945. CSN is authorized as a representative of the French Notary to speak on behalf of the Notary before the Notary, determine general policy, contribute to the development of the notary profession, and provide collective services to Notaries. As of October 2021, there are already 20 (twenty) million Electronic Authentic Act (AAE) registered in MICEN, and 90% of Authentic Deeds have been signed electronically and stored in MICEN, and starting in 2022, 85% have carried out notary work remotely using a video-conferencing system.

To ensure the confidentiality of deeds and other documents stored in a notary protocol, such as in France, it is recommended that the service provider that manages and stores the notary protocol in a cloud computing system is organized by an authorized organization or institution. Because the notary protocol is a state archive, it is recommended that the service provider be organized by the Notary Supervisory Council (MPN) as the only body formed by the Minister of Law and Human Rights, as contained in Article 67 of the UUJN, to supervise the behavior and implementation of notary positions, one of which is the authentic deed made. MPN has the authority to examine deeds made by a notary and take samples from deeds made by a notary to check if there is a violation of the authenticity of the deed. As previously described, deeds already 25 (twenty-five years old) will be submitted to the MPD for safekeeping. If the service provider stores the notary protocol organized by MPN, the risk of violating office secrets can be minimized to the maximum.

While there are all preventive measures in place for violations of office secrets, both the service user in this case, the notary, and the service provider need to monitor each other's activities to ensure compliance with the regulations and contracts entered into between the parties such as customer and end-user compliance with the AUP and IP license, as well as the provider's compliance with SLAs, data protection policies and so on, the contract may include a clause that will discuss the audit rights of both parties, the scope of the audit, formalities and costs. Contractual rights or legal obligations for audits and security tests may need to be supplemented in the contract with binding obligations from the other party to facilitate the exercise of those rights or the fulfilment of those obligations. Monitoring such activities can also

address the user's ambiguity over the physical location of their data as it depends on the service provider, which results in difficulties in overcoming disasters due to dependence on service providers for data recovery, with disciplined monitoring and regular audits. Users can recognize the risk of leakage, loss, or other things that cause the breach of the confidentiality of the Notary Office.

CONCLUSION

The use of cloud computing systems by notaries for storing protocols by uploading documents and deeds into the system allows quick access to data anytime and anywhere via the Internet while reducing costs since there is no need for physical storage space. Additionally, this system minimizes the risk of lost or leaked documents due to theft, fire, or natural disasters. However, to ensure security and confidentiality, certain key aspects must be considered, such as the server location, access rights, security mechanisms, separation of documents among notaries, management by the Notary Supervisory Council (MPN), and the use of encryption and passwords to protect the documents. By adhering to these provisions, storing notary protocols using cloud computing systems can be effectively implemented, as has been successfully done in France.

REFERENCES

Agarwal, M., & Srivastava, G. M. S. (2017). Cloud computing: A paradigm shift in the way of computing. *International Journal of Modern Education and Computer Science*, *9*(12), 38.

Alkatiri, N. H., Putra, M. F. M., & Ongko, K. (2023). A Legal Perspective: Implementing an Electronic Notarization System in Indonesia in the Post-Pandemic Era. *Jambura Law Review*, *5*(2), 332–355.

Botta, A., de Donato, W., Persico, V., & Pescapé, A. (2016). Integration of Cloud computing and Internet of Things: A survey. *Future Generation Computer Systems*, *56*, 684–700. https://doi.org/10.1016/j.future.2015.09.021

Camley, P. R. (2020). *Mobile Identity, Credential, and Access Management Framework*.

Catur, R. (2023). Comparison of Legal System Related to Implementation of Cyber Notary in Indonesia With Common Law And Civil Law System. *Jhbbc*, 41–52.

Chiregi, M., & Jafari Navimipour, N. (2018). Cloud computing and trust evaluation: A systematic literature review of the state-of-the-art mechanisms. *Journal of Electrical Systems and Information Technology*, *5*(3), 608–622. https://doi.org/10.1016/j.jesit.2017.09.001

Delafare, M. W., Suhartono, S., & Prasetyawati, E. (2023). LEGAL PROTECTION FOR NOTARY THAT DOESN'T ATTACH LETTER AND DOCUMENT TO MINUTA DEED. *Russian Law Journal*, *11*(3), 571–581.

Dewi, S. P. (2022). Responsibility of Notary/Land Deed Official on Joint Title Deed Based on Incompatible Inheritance Certificate. *Authentica*, *5*(2), 201–212.

Habibah, N. M., Masykur, M. H., & Wardhani, D. A. W. (2024). Force Majeure And Notary Responsibility: The Case of the Destruction of Deed Minutes. *Iblam Law Review*, *4*(1), 71–80.

Hetharie, Y., Tjoanda, M., & Uktolseja, N. (2022). Fungsi Pengawasan Majelis Pengawas Daerah Terhadap Penegakan Kode Etik Notaris. *PAMALI: Pattimura Magister Law Review*, *2*(2), 161–171.

Ibrahim, I., Daud, D., Azmi, F. A. M., Noor, N. A. M., & Yusoff, N. S. M. (2021). Improvement of land administration system in Nigeria: A blockchain technology review. *International Journal of Scientific & Technology Research*, *10*(08), 33–39.

Kencana, V., Syaufi, A., & Erliyani, R. (2023). The Urgency of Electronic Notary Protocol Storage in E-Notary Perspective. *International Journal of Social Science and Human Research*, *6*(08).

Kleinaki, A.-S., Mytis-Gkometh, P., Drosatos, G., Efraimidis, P. S., & Kaldoudi, E. (2018). A Blockchain-Based Notarization Service for Biomedical Knowledge Retrieval. *Computational and Structural Biotechnology Journal*, *16*, 288–297. https://doi.org/10.1016/j.csbj.2018.08.002

Kumar, R., Jain, V., Yie, L. W., & Teyarachakul, S. (2024). *Convergence of IoT, Blockchain, and Computational Intelligence in Smart Cities*. CRC Press.

Lewinbuk, K. P. (2020). True Perestroika or Still Perfunctory: A Decade of Developments in Russian Law Practice Reform. *Fla. J. Int'l L.*, *32*, 301.

Makhdoom, I., Abolhasan, M., Lipman, J., Piccardi, M., & Franklin, D. (2024). PrivySeC: A secure and privacy-compliant distributed framework for personal data sharing in IoT ecosystems. *Blockchain: Research and Applications*, 100220. https://doi.org/10.1016/j.bcra.2024.100220

Mauri, G., & Verticale, G. (2017). Up-to-date key retrieval for information centric networking. *Computer Networks*, *112*, 1–11. https://doi.org/10.1016/j.comnet.2016.10.018

Nadhiro, E. (2019). A Notary's Authority In Issuing Copies of Acts From Minutes of Deeds of Other Notaries' Protocol Parts. *YURISDIKSI: Jurnal Wacana Hukum Dan Sains*, *13*(2), 107–116.

Permana, B. I., Al Farizy, M. R., & Manggala, F. P. (2024). Responsibility of Notary for Registered Private Deed in the Perspective of Law of Evidence. *Jurnal Justiciabelen*, *7*(1).

Srivastav, A., & Srivastav, A. (2019). Natures' reaction to anthropogenic activities. *The Science and Impact of Climate Change*, 79–109.

Suroso, J. S., & Sriratnasari, S. R. (2018). A Literature Review on The Challenges of Adopting Cloud Computing for Startup in Indonesia. *2018 Indonesian Association for Pattern Recognition International Conference (INAPR)*, 315–321.

Toruan, H. D. L. (2022). The Importance of Using Electronic Deeds to Facilitate The Service and Storage of Notary Archives. *Jurnal Penelitian Hukum De Jure*, *22*(4), 483–498.

Verma, H., Chauhan, N., & Awasthi, L. K. (2023). A Comprehensive review of 'Internet of Healthcare Things': Networking aspects, technologies, services, applications, challenges, and security concerns. *Computer Science Review*, *50*, 100591. https://doi.org/10.1016/j.cosrev.2023.100591