

Understanding Digital Signature through a Conceptual Approach to Improve Efficiency, Access, and Quality of Fintech

Rasmuddin¹, Wahyudi Umar², Sudirman³

rasmuddin@yahoo.com, wahyudi.umar@umkendari.ac.id, sudirman@umkendari.ac.id

¹Faculty of Law, Universitas Halu Oleo

²³Faculty of Law, Universitas Muhammadiyah Kendari

Article Info

Received: 2022-08-12

Revised: 2023-02-21

Accepted: 2023-03-31

Keywords:

Digital Signature;
Conceptual Approach;
Fintech

Abstract

This study aims to deepen the understanding of the concept of digital signature in the context of the fintech industry, focusing on efforts to improve the efficiency, accessibility, and quality of fintech services. Digital signatures are a key component in modern fintech transactions and services, which are important in securing information and maintaining data integrity in a digital environment. This research method involves a conceptual approach consisting of literature analysis, case studies, and an in-depth understanding of digital signature technology and its impact on the fintech ecosystem. Basic concepts such as cryptography, algorithms, and digital security principles will be carefully examined to understand the foundations of digital signature technology. In addition, this research will also explore the latest developments in the use of digital signatures in the fintech industry, as well as their impact on operational efficiency, service accessibility, and transaction quality. The results of this research are expected to provide in-depth insights into the role of digital signatures in changing the fintech landscape. By understanding this concept better, stakeholders in the fintech industry can optimize the use of digital signatures to improve their speed, security, and quality of service. This is expected to help create a more efficient, accessible, and reliable fintech environment for consumers and businesses. This research can also be the basis for further research in the field of fintech security and related technological innovations.

I. Introduction

Coffee is one of the most popular drinks in the world. So it is not strange that until now the coffee business is mushrooming both in big cities and in small towns. Coffee is a food commodity that is enjoyed by people from various types of circles. The history of the discovery of coffee itself, was discovered by the Ethiopians on the African continent since 800-850 BC. The people of the African continent, especially the Ethiopians, claim that coffee is a nutritious drink that can provide energy. They consume coffee by mixing coffee beans with animal fat and also wine to meet their protein needs.

Fintech, short for financial technology, is one of the industries that has experienced rapid growth in recent years. It is an industry that combines information and financial technology to create innovative and advanced financial services.¹ In this context, digital signatures are one of the key elements in financial transactions carried out online. Digital signatures play an important role in ensuring security, authentication, and data integrity in online transactions.² Understanding the concept of digital signature and how it can be used to improve the efficiency, accessibility, and quality of fintech is very important in this context.

A digital signature is an electronic authentication method used to verify the identity of a user and the integrity of a signed document or message. It is one of the key technologies in the fintech world as it allows financial transactions to be carried out online with a high level of security.³ In an era where online transactions are increasingly common, a deep understanding of digital signatures is essential.

A few previous studies have explored the issue of using digital signatures in the context of fintech. This research has covered various aspects, including the concept of digital signatures, laws, and regulations related to digital signatures in financial transactions. Previous research has discussed the implementation of digital signatures in online payment systems, risk management, and other security aspects.

One of the relevant previous studies is research that highlights the legal strength of digital signatures as evidence.⁴ Most countries have issued guidelines and regulations regarding the use of digital signatures in financial transactions. This research has

¹ Miswan Ansori, "Development and Impact of Financial Technology (Fintech) on the Islamic Financial Industry in Central Java," *Wahana Islamika: Journal of Islamic Studies* 05, no. 01 (2019): 32–45.

² Thalís Noor Cahyadi, "Legal Aspects of Digital Signature Utilization in Improving Efficiency, Access and Quality of Sharia Fintech," *Journal of Rechts Vinding: Media for National Legal Development* 9, no. 2 (2020): 219, doi:10.33331/rechtsvinding.v9i2.424.

³ Trihastuti Yuniati and Muhammad Fajar Sidiq, "Literature Review: Electronic Document Legalization Using Digital Signatures as an Alternative to Document Attestation During a Pandemic," *Journal of RESTI (Systems Engineering and Information Technology)* 4, no. 6 (2020), doi:10.29207/resti.v4i6.2502.

⁴ Eman Sulaiman, Nur Arifudin, and Lily Triyana, "The Power of Digital Signature Law as Legal Evidence in Review of Civil Procedure Law," *Legal Minutes* 16, no. 02 (2021): 95–105, doi:10.30872/risalah.v16i2.207.

tried to understand the concept of digital signatures to improve the efficiency, accessibility, and quality of fintech services.

Although much previous research has been done in this area, there are still some research gaps that need to be filled. Some possible research gaps are identified such as deep conceptual understanding where there is a need for a deeper conceptual understanding of what a digital signature is, how it functions, and why it is important in the context of fintech. This research can help in providing a solid foundation of understanding for stakeholders in the fintech industry. Related use cases in fintech are also a research gap where further research can explore case studies of using digital signatures in certain fintech applications. This can help in understanding how these technologies can improve the efficiency, accessibility, and quality of financial services.

This research is expected to make a major contribution in the understanding of digital signatures in the context of fintech. With a better understanding of this technology, the fintech industry can integrate digital signatures more effectively in its operations. It can also help in increasing user confidence in fintech services, which in turn can drive industry growth.

In addition, this research can also have implications in the development of fintech-related regulations. With a better understanding of digital signatures, regulators can formulate more precise guidelines for their use in financial transactions. The research is expected to provide valuable insights into how this technology can be used to improve the efficiency, accessibility, and quality of fintech services, while also identifying research gaps that still need to be filled.

2. Research Method

Doctrinal or normative legal research, which uses law as a fundamental norm, is used in this type of research. The norm system in question relates to principles, norms and legislation regarding the case quo.⁵ The first stage of normative research consists of research with the aim of achieving objective laws, by conducting research on legal issues. The second stage of normative legal research is aimed at obtaining subjective law.⁶ It also deals with a critical review of rules relevant to the case quo in Indonesia.

This research uses a conceptual approach which is a type of approach in legal research that provides an analytical point of view on problem solving in legal research seen from the aspects of the legal concepts behind it, or even can be seen from the values contained in the norming of a regulation in relation to the concepts used.⁷

⁵ Ming-Hsi Sung and Wahyudi Umar, "A New Industry and Tax Base on Taxing Esports in Indonesia," *Jurnal Media Hukum* 27, no. 2 (2020), doi:10.18196/jmh.20200148.

⁶ Ahmad Rustan, Ju-lan Hsieh, and Wahyudi Umar, "Maladministration on Mining Business Licenses : Case Study " Mining Business License Production Operation PT . Aneka," *Varia Justicia* 17, no. 3 (2021): 246–57.

⁷ Peter Mahmud Marzuki, *Legal Research* (Jakarta: Prenada Media, 2011).

3. Results and Discussion

Legal Aspects of Using Digital Signatures

Electronic signature

An electronic signature refers to a form of signature created by embedding, associating, or linking electronic information with other electronic data, such as an electronic contract.⁸ It is commonly used as a means of authentication or verification. Electronic documents, in the form of electronic contracts or hard copies, are considered legally valid evidence in most cases.⁹

Electronic contracts refer to legal relationships established by computer-based information systems and communication networks, which are further facilitated by the Internet. This type of contract is made through electronic devices or information technology and is usually documented in electronic form.¹⁰

In accordance with Law Number 19 of 2016 concerning Amendments to Law Number 11 of 2008 concerning Electronic Information and Transactions (ITE Law), an electronic contract is defined as an agreement between parties formed through an electronic system. It is important that the agreement meets the requirements for a demonstrable agreement to be considered valid. In addition, an electronic system refers to a set of electronic devices and procedures used to prepare, collect, process, analyze, store, display, announce, transmit, and/or disseminate electronic information.¹¹

Digital Signature (Digital *Signature*)

In Indonesia, electronic signature and digital signature are two different terms. An electronic signature is a legal term defined by a country's laws and regulations, while a digital *signature* is an electronic authentication method that secures and certifies digital documents or transactions.¹² It is a modern alternative to the physical signature we are familiar with. *Digital signatures* create a unique digital footprint that can be used to verify the authenticity of documents or an individual's identity. It serves to protect transactions and documents from counterfeiting, fraud, and unauthorized alteration.¹³

There are three key components of a digital signature: *private key*, *public key*, and

⁸ Ahmad Farisi, "Development of Digital Signature Applications with Hash Method Using Custom Core System Class in CodeIgniter Framework," *Journal of Information System Technology (JTST)* 02, no. 01 (2021): 137–49.

⁹ Ni Luh Putu Sudarini and Dewa Gede Pradnyana Yustiawan, "Electronic Contract Validity as a Tool of Evidence in Civil Law Review," *Journal of Law and Social Politics* 01, No. 04 (2023): 266–75.

¹⁰ David Herianto Sinaga and I Wayan Wiryawan, "The Validity of Electronic Contracts (E-Contracts) in Business Agreements," *Kertha Semaya : Journal of Legal Sciences* 8, no. 9 (2020): 1385, doi:10.24843/ks.2020.v08.i09.p09.

¹¹ Ranita Gustisia Janis, Elko Lucky Mamesah, and Debby Telly Antow, "Criminal Aspects of Online Fraud with Investment Mode," *Lex Privatum* 11, no. 4 (2023): 145–54.

¹² Sulaiman, Arifudin, and Triyana, "The Power of Digital Signature Law as Legal Evidence in Review of Civil Procedure Law."

¹³ Merry Dahlia and Wasis Susetio, "Juridical Review of the Use of Digital Signatures in Sale and Purchase Agreements," *Indonesian Multidisciplinary Journal* 2, no. 8 (2023): 2277–89, doi:10.58344/jmi.v2i8.442.

*Certificate Authority (CA).*¹⁴ A *private key* is a confidential component known only to its owner and used to create a digital signature. A *public key*, on the other hand, is a publicly available component made available to third parties and used to verify digital signatures created with private keys. Finally, a *Certificate Authority (CA)* is a trusted entity that issues digital certificates that bind public keys to the identity of their owners.¹⁵

By utilizing *the public key attached to the electronic certificate, the system can verify whether the public key corresponds to the individual named in the certificate, and decrypt the encryption with the private key.* If the encryption can be decrypted, then it means that the *public* and *private* keys are related, and we can confirm that the information and identity specified in the electronic certificate are genuine. The entity responsible for issuing electronic key pairs and certificates is known as an Electronic Certification Operator (PSE) or Certificate Authority (CA).

In accordance with Article 58 of Government Regulation Number 82 of 2012, which relates to the implementation of electronic systems and transactions, digital signatures require a combination of at least two authentication factors to prove the identity of the signatory. These factors can be chosen from three types – something individually owned (such as an ATM card), something individually known (such as a PIN/password or cryptographic key), and something that is characteristic of an individual (such as voice patterns, handwriting dynamics, or fingerprints).¹⁶

To use a digital signature, the user creates a key pair where the *private key* is stored securely and the *public key* can be shared freely. When a user wants to sign a message or document, cryptographic algorithms are used to generate a unique digital signature based on the private key. The message or document is signed and the digital signature is then sent to the recipient. The recipient can verify the digital signature using the user's public key. If the digital signature matches the message or document, it confirms that the message has not been tampered with and that it came from a legitimate user.¹⁷

Digital signature is a technology that provides security to electronic documents by identifying the owner of the document and ensuring the authenticity and integrity of the document. There are different types of digital signatures, as follows:¹⁸

1. Basic Electronic Signature (BES)

BES or Basic Electronic Signature is a direct digital signature method used to certify

¹⁴ Alwin Indra Fatra, R. Rizal Isnanto, and Enda Wista Sinuraya, "Public Key Infrastructure Design with the Implementation of Making Digital Receipts for English Course Payments," *Transient* 2, no. 3 (2013): 799–804, <https://ejournal3.undip.ac.id/index.php/transient/article/view/3977>.

¹⁵ Hermawan Setiawan and Adek Muhammad Zulkham Ristiawan Kertanegara, "Public Key Infrastructure Design with the Implementation of Web-Based Online Examination System Development," *Computer Based Information System Journal* 11, no. 1 (2023): 1–11, doi:10.33884/cbis.v11i1.6504.

¹⁶ Aleksandr Ometov et al., "Multi-Factor Authentication: A Survey," *Cryptography* 2, no. 1 (2018): 1–31, doi:10.3390/cryptography2010001.

¹⁷ Mark Twain, "Security in Wireless Systems," in *Tom Sawyer Abroad*, 2020, 97–106, doi:10.1525/9780520950610-015.

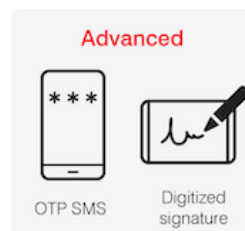
¹⁸ Rizki Dermawan, "The Utilization of Certified Digital Signatures in the Pandemic Era," *Lex Generalis Law Journal* 2, no. 8 (2021): 762–81, doi:10.56370/jhlg.v2i8.95.

electronic documents. The technology uses simple encryption techniques that allow users to sign electronic documents by clicking a checkbox or sign directly on a touchscreen device and save the signature as an image. It's a quick and easy way to add a layer of security to your electronic documents.



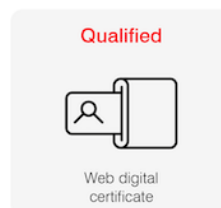
2. Advanced Electronic Signature (AES)

The AES encryption algorithm uses more advanced technology compared to BES, thus providing a superior level of security. In addition, AES often includes digital certificates issued by reputable certificate authorities, such as SMS or signatures from trusted authorities. This further increases the security and reliability of the encryption process.



3. Qualified Electronic Signature (QES)

QES is considered the most secure and legally valid type of digital signature. It uses strong encryption technology and digital certificates issued by government-recognized digital certificate providers. This ensures that all digital signatures are authenticated and protected from potential security threats.



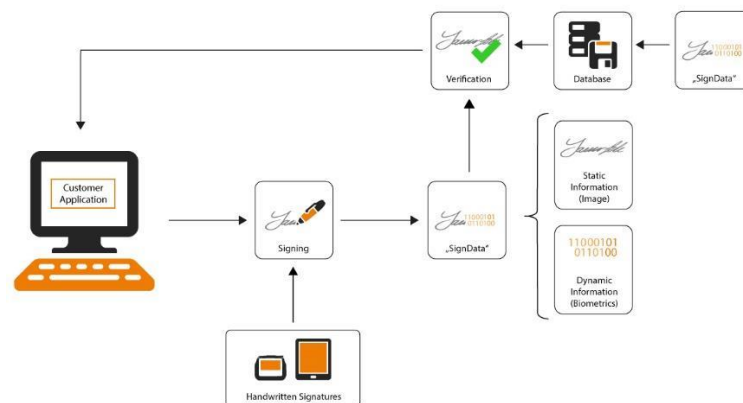
4. Digital Certificate Signature (DCS)

Digital signature technology (DCS) uses digital certificates to verify the authenticity and integrity of electronic documents and user identity. By combining the power of digital certificates with public key encryption, DCS provides a high level of security that guarantees confidentiality and non-rejection of electronic transactions.



5. Biometric Signature

Biometric signature uses biometric technology, such as fingerprint or facial recognition, to identify the owner of an electronic document. This technology provides a high level of security because it is difficult to forge or duplicate biometric signatures.



Implementation of Electronic Certification Providers

As mentioned earlier, to perform a digital signature, one must have a key pair and an electronic certificate issued by a Certification Authority (CA) or Public Service Entity (PSE). PSE identification guidelines are generally regulated by the ITE Law, and more precisely, by PP PSTE and Minister of Communication and Information Regulation Number 11 of 2018 concerning Electronic Certification Providers (PSrE Candy).

An Electronic Certificate is a digital certificate that includes an Electronic Signature and Identity, indicating the legal status of the parties involved in an electronic transaction.¹⁹ It is issued by a trusted legal entity, known as an Electronic Certification Operator, which provides and verifies electronic certificates.

Electronic certification providers are required to provide precise, clear, and conclusive information to each user of the service, detailing the methods used to identify the signer, the means for obtaining the necessary information about the

¹⁹ Kominfo, "Electronic Certification Organizer (PSrE) Indonesia," *Tte.Kominfo.Go.Id*, 2023, <https://tte.kominfo.go.id/apaitu>.

electronic signature generator, and how the electronic signature can be authenticated for its validity and security. In addition, the authority of electronic certification providers includes examination of prospective owners and/or holders of electronic certificates, issuance of electronic certificates, extension of the validity period of electronic certificates, and blocking or revocation of electronic certificates if necessary.²⁰

Validity and Strength of Law in Evidence

For an electronic signature to have legal force and effect, certain requirements must be met. These include that the electronic signature generation data relates only to the signer, that the electronic signature generation data is under the control of the signer during the electronic signing process, that any changes made to the electronic signature after signing can be detected and that any changes made to the electronic information associated with the signature can also be detected. In addition, there must be a reliable way to identify signatories and demonstrate that they have given their consent to the relevant electronic information.

For an electronic signature to be legally binding and effective, it must satisfy the six conditions mentioned above. Although only in the form of a code, electronic signatures have the same legal weight as manual signatures, as explained in Article 11 of Law Number 19 of 2016 which amends Law Number 111 of 2008 concerning Electronic Information and Transactions.²¹

According to Article 5 paragraph 1 of the ITE Law, Electronic Information, Electronic Documents, and printouts are considered valid legal evidence. This implies that its existence is binding and can be submitted as valid evidence to ensure legal certainty in the implementation of electronic systems and transactions, especially in cases related to legal acts carried out through electronic means.

In accordance with paragraph 2 of Article 5 of the ITE Law, Electronic Information, Electronic Documents, and printouts can be used as valid evidence in accordance with the applicable Procedural Law in Indonesia. However, wiretapping, wiretapping, or recording of Electronic Information or Electronic Documents may only be carried out in the context of law enforcement, at the request of the police, prosecutors, and other agencies authorized by law.

According to Article 5 paragraph 4 of the ITE Law, Electronic Information and/or Electronic Documents and/or printouts are considered valid legal evidence, except for letters required by law in written form and letters and documents that must be made in the form of notarial deeds or deeds made by deed making officials. The explanation of this paragraph explains that papers that must be made in writing pursuant to law include, but are not limited to, securities, securities, and letters used in civil, criminal, and state administrative procedures.

Article 6 of the ITE Law states that accountability must be provided to clarify a

²⁰ Laura Helena Wiryana and Benny Djajaputra, "Electronic Certificate SWOT Analysis of Land Dispute Resolution in Indonesia," *Adigama Law Journal* 4, no. 2 (2021): 4392–4410.

²¹ Sulaiman, Arifudin, and Triyana, "The Power of Digital Signature Law as Legal Evidence in Review of Civil Procedure Law."

situation. As far as criminal evidence is concerned, digital signatures incorporated in electronic documents are considered valid evidence, in addition to the evidence specified in the Code of Criminal Procedure, as per article 44 of the ITE Law.

The Role of Digital Signature in Fintech

Digital signatures play an important role in the fintech industry, significantly improving security, efficiency, accessibility, and quality of service.²² They enhance security by providing strong authentication for electronic transactions, thereby reducing the risks associated with fraud, forgery, and unauthorized access. In addition, digital signatures enable careful tracking of document changes, ensure data integrity, and transparency, which are critical for regulatory oversight and auditing in the financial sector.

In terms of efficiency, they speed up the verification process, an important factor in fintech where time is of the essence. Traditional methods of identity verification and physical signatures often take days, if not weeks, while digital signatures can complete the same task in seconds or minutes, greatly improving the speed and efficiency of fintech operations.²³ In addition, its implementation results in reduced costs, eliminating the costs associated with printing, shipping, handling, and storing physical documents. This not only streamlines operations but also promotes environmental sustainability by reducing paper usage. In addition, digital signatures increase accessibility, allowing financial services to be accessed remotely from almost anywhere at any time, a boon for those in remote areas or lacking access to traditional financial services.²⁴

The overall quality of service in the fintech industry is also improving as digital signatures facilitate transactions and smoother approval processes, minimizing bureaucratic hurdles.²⁵ This, coupled with the ability for users to digitally sign and access documents and contracts, empowers users to efficiently manage and oversee their financial information. Lastly, digital signatures drive innovation in fintech, offering a flexible platform for the development of a diverse range of financial products and services while fostering continuous innovation in risk management, customer identification, and data utilization.

Although digital signatures offer many benefits to the fintech industry, there are some hurdles that need to be overcome. These include challenges related to user trust, legal sustainability, technology security, and reliance on internet connections. To adopt digital signatures, users must have confidence in this technology, which requires fintech providers to invest resources in user education. In addition, fintech

²² Habib Ullah Khan et al., "Role of Authentication Factors in Fin-Tech Mobile Transaction Security," *Journal of Big Data* 10, no. 1 (2023), doi:10.1186/s40537-023-00807-3.

²³ Cahyadi, "Legal Aspects of Digital Signature Utilization in Improving Efficiency, Access and Quality of Sharia Fintech."

²⁴ Colleen E. Lawrence et al., "A REDCap-Based Model for Electronic Consent (EConsent): Moving toward a More Personalized Consent," *Journal of Clinical and Translational Science* 4, no. 4 (2020): 345–53, doi:10.1017/cts.2020.30.

²⁵ Annisa Noor El Izzah and Wasis Sugandha, "The Use of Electronic Signatures in the Administration of E-Government to Realize Efficient Public Services," *Journal of Law, Society, and Islamic Civilization* 9, no. 1 (2021): 1, doi:10.20961/jolsic.v9i1.52836.

companies must comply with applicable regulations in the regions in which they operate and must address the vulnerability of digital signatures to cyberattacks and security breaches using robust security technologies. Finally, reliance on internet connections is a challenge in the use of digital signatures, especially in areas with limited internet access.

In the realm of fintech, digital signatures find their application in various fields. First, digital signatures can be used by borrowers to sign loan contracts when applying for online loans, thus making the loan approval process faster and more efficient. Secondly, investors can use digital signatures to sign documents related to their investments on online investment platforms, thus streamlining the investment process and enabling better portfolio management.

4. Conclusion

Digital signature is an important concept in the fintech world that provides great benefits in improving efficiency, accessibility, and quality of service. With the increasing use of this technology, fintech has become safer, faster, and more efficient than traditional banking. However, some challenges need to be overcome, including user trust, legal regulations, technology security, and reliance on internet connections. To fully utilize the potential of digital signatures, fintech companies must be committed to maintaining data security and user privacy, complying with applicable regulations, and continuing to innovate in service development. Thus, digital signature technology will continue to play an important role in the evolution of the fintech industry and support the growth of a more modern, efficient, and secure financial sector.

References

- Ansori, Miswan. "Perkembangan Dan Dampak Financial Technology (Fintech) Terhadap Industri Keuangan Syariah Di Jawa Tengah." *Wahana Islamika: Jurnal Studi Keislaman* 05, no. 01 (2019): 32–45.
- Cahyadi, Thalish Noor. "Aspek Hukum Pemanfaatan Digital Signature Dalam Meningkatkan Efisiensi, Akses Dan Kualitas Fintech Syariah." *Jurnal Rechts Vinding: Media Pembinaan Hukum Nasional* 9, no. 2 (2020): 219. doi:10.33331/rechtsvinding.v9i2.424.
- Dahlia, Merry, and Wasis Susetio. "Tinjauan Yuridis Penggunaan Tanda Tangan Digital Dalam Perjanjian Jual Beli." *Jurnal Multidisiplin Indonesia* 2, no. 8 (2023): 2277–89. doi:10.58344/jmi.v2i8.442.
- Dermawan, Rizki. "Pemanfaatan Tanda Tangan Digital Tersertifikasi Di Era Pandemi." *Jurnal Hukum Lex Generalis* 2, no. 8 (2021): 762–81. doi:10.56370/jhlq.v2i8.95.
- Farisi, Ahmad. "Pengembangan Aplikasi Tanda Tangan Digital Dengan Metode Hash Menggunakan Custom Core System Class Pada Framework CodeIgniter." *Jurnal Teknologi Sistem Informasi (JTSI)* 02, no. 01 (2021): 137–49.
- Fatra, Alwin Indra, R. Rizal Isnanto, and Enda Wista Sinuraya. "Perancangan Infrastruktur Kunci Publik Dengan Implementasi Pembuatan Kuitansi Digital Pembayaran Kursus Bahasa Inggris." *Transient* 2, no. 3 (2013): 799–804. <https://ejournal3.undip.ac.id/index.php/transient/article/view/3977>.
- Herianto Sinaga, David, and I Wayan Wiryawan. "Keabsahan Kontrak Elektronik (E-Contract) Dalam Perjanjian Bisnis." *Kertha Semaya: Journal Ilmu Hukum* 8, no. 9 (2020): 1385. doi:10.24843/ks.2020.v08.i09.p09.
- Izzah, Annisa Noor El, and Wasis Sugandha. "Penggunaan Tanda Tangan Elektronik Dalam Penyelenggaraan E-Government Guna Mewujudkan Pelayanan Publik Yang Efisien." *Journal of Law, Society, and Islamic Civilization* 9, no. 1 (2021): 1. doi:10.20961/jolsic.v9i1.52836.
- Janis, Ranita Gustisia, Elko Lucky Mamesah, and Debby Telly Antow. "Aspek Pidana Dalam Penipuan Online Dengan Modus Investasi." *Lex Privatum* 11, no. 4 (2023): 145–54.
- Khan, Habib Ullah, Muhammad Sohail, Shah Nazir, Tariq Hussain, Babar Shah, and Farman Ali. "Role of Authentication Factors in Fin-Tech Mobile Transaction Security." *Journal of Big Data* 10, no. 1 (2023). doi:10.1186/s40537-023-00807-3.
- Kominfo. "Penyelenggara Sertifikasi Elektronik (PSrE) Indonesia." *Tte.Kominfo.Go.Id*, 2023. <https://tte.kominfo.go.id/apaitu>.
- Lawrence, Colleen E., Leah Dunkel, Mark McEver, Tiffany Israel, Robert Taylor, Germán Chiriboga, Karin Valentine Goins, et al. "A REDCap-Based Model for Electronic Consent (EConsent): Moving toward a More Personalized Consent." *Journal of Clinical and Translational Science* 4, no. 4 (2020): 345–53. doi:10.1017/cts.2020.30.
- Marzuki, Peter Mahmud. *Penelitian Hukum*. Jakarta: Prenada Media, 2011.
- Ometov, Aleksandr, Sergey Bezzateev, Niko Mäkitalo, Sergey Andreev, Tommi Mikkonen, and Yevgeni Koucheryav. "Multi-Factor Authentication: A Survey." *Cryptography* 2, no. 1 (2018): 1–31. doi:10.3390/cryptography2010001.

- Rustan, Ahmad, Ju-lan Hsieh, and Wahyudi Umar. "Maladministration on Mining Business Licenses : Case Study " Mining Business License Production Operation PT . Aneka." *Varia Justicia* 17, no. 3 (2021): 246–57.
- Setiawan, Hermawan, and Adek Muhammad Zulkham Ristiawan Kertanegara. "Perancangan Infrastruktur Kunci Publik Dengan Implementasi Pembangunan Sistem Ujian Daring Berbasis Web." *Computer Based Information System Journal* 11, no. 1 (2023): 1–11. doi:10.33884/cbis.v11i1.6504.
- Sudarini, Ni Luh Putu, and Dewa gede pradnyana Yustiawan. "Keabsahan Kontrak Secara Elektronik Sebagai Alat Pembuktian Di Tinjau Secara Hukum Perdata." *Jurnal Hukum Dan Sosial Politik* 01, no. 04 (2023): 266–75.
- Sulaiman, Eman, Nur Arifudin, and Lily Triyana. "Kekuatan Hukum Digital Signature Sebagai Alat Bukti Yang Sah Di Tinjau Dari Hukum Acara Perdata." *Risalah Hukum* 16, no. 02 (2021): 95–105. doi:10.30872/risalah.v16i2.207.
- Sung, Ming-Hsi, and Wahyudi Umar. "A New Industry and Tax Base on Taxing Esports in Indonesia." *Jurnal Media Hukum* 27, no. 2 (2020). doi:10.18196/jmh.20200148.
- Twain, Mark. "Security in Wireless Systems." In *Tom Sawyer Abroad*, 97–106, 2020. doi:10.1525/9780520950610-015.
- Wiryana, Laura Helena, and Benny Djajaputra. "Analisis Swot Sertifikat Elektronik Terhadap Penyelesaian Sengketa Pertanahan Di Indonesia." *Jurnal Hukum Adigama* 4, no. 2 (2021): 4392–4410.
- Yuniati, Trihastuti, and Muhammad Fajar Sidiq. "Literature Review: Legalisasi Dokumen Elektronik Menggunakan Tanda Tangan Digital Sebagai Alternatif Pengesahan Dokumen Di Masa Pandemi." *Jurnal RESTI (Rekayasa Sistem Dan Teknologi Informasi)* 4, no. 6 (2020). doi:10.29207/resti.v4i6.250