JEMBAR
Journal of Economic, Business & Accounting Research
JEMBAR 3(2): 164–179
ISSN 3024-9813

Institute for Advanced Science, Social and Sustainable Future
MORALITY BEFORE KNOWLEDGE

Readiness of regulation and cybercrime mitigation in syirkah-based securities crowdfunding for MSMEs acceleration

Putri Ruby Kohinoor[1,*], Devi Triananda Surya Putri[1], Anisa Nur Fatimah Karmun[1]
[1] *Department of Law, Faculty of Law, Universitas Sebelas Maret, Surakarta, Central Java 57126, Indonesia.*
*Correspondence: putrirubykohinoor@student.uns.ac.id

Received Date: September 22, 2025 Revised Date: January 7, 2026 Accepted Date: January 23, 2026

ABSTRACT

Background: This study addresses the urgent need for a robust legal and technical framework to support the acceleration of Micro, Small, and Medium Enterprises (MSMEs) through syirkah-based Securities Crowdfunding (SCF) in Indonesia. The modern economy's increasing reliance on information technology has created a new landscape for financial services, but this digitalization also introduces significant cyber risks that threaten the integrity and security of both investors and MSMEs. This study analyzed common cyber threats such as phishing, ransomware, and social engineering to identify key vulnerabilities within the SCF ecosystem. **Methods**: This article employs a comprehensive literature review to analyze the theoretical components of legal readiness and cybersecurity mitigation. The research procedure involved a systematic evaluation of various legal documents, academic literature, and official reports from government and cybersecurity agencies. **Findings:** The findings indicate that while Indonesia has established a foundational legal umbrella for Sharia SCF, the current regulatory framework remains general and normative, lacking detailed provisions on crucial technical aspects like dispute resolution mechanisms and optimal investor protection. Furthermore, cyber threats pose a significant risk, as evidenced by a substantial number of cyber traffic anomalies in Indonesia's cyberspace. These threats are not merely technical but also ethical, directly conflicting with the Islamic principles of amanah (trust) and justice. **Conclusion**: This study concludes that a significant gap exists between the general legal framework and the detailed technical requirements needed to ensure security and trust in the digital era. **Novelty/Originality of this article:** The novelty of this research lies in its integrated approach, which combines an analysis of the legal and regulatory gaps with a comprehensive review of cybercrime threats, and frames both issues within the ethical principles of Islamic law. It also highlights the lack of research on cyber threats targeting the Linux operating system, particularly within the Indonesian fintech sector.

KEYWORDS: cybercrime mitigation; regulatory readiness; syirkah-based securities crowdfunding.

1. Introduction

Micro, Small, and Medium Enterprises (MSMEs) play a strategic role in the Indonesian national economy, particularly in creating jobs and improving public welfare. According to data from the Indonesian Chamber of Commerce and Industry/*Kamar Dagang dan Industri Indonesia* (Kadin), MSMEs have experienced significant fluctuations over the past five years. In 2020, the number of MSMEs was recorded at approximately 64 million. In 2021, the number of MSMEs increased again to around 65.46 million, but decreased in 2022 to 65

Cite This Article:
Kohinoor, P. R., Putri, D. T. S. P., & Karmun, A. N. F. (2026). Readiness of regulation and cybercrime mitigation in syirkah-based securities crowdfunding for MSMEs acceleration. *Journal of Economic, Business & Accounting Research, 3*(2), 164–179. https://doi.org/10.61511/jembar.v3i2.2026.2295

million. The number of MSMEs continued to increase and stabilized in 2023-2025, reaching around 66 million units.

It is important to note that MSMEs are not simply economic actors but the backbone of the national economy. According to a report from the Directorate General of Treasury, Ministry of Finance of the Republic of Indonesia, in 2024, MSMEs contributed 61.07% to Gross Domestic Product (GDP), or IDR 8,573.89 trillion (Hapsari et al., 2024). This contribution demonstrates that MSMEs play a significant role not only quantitatively but also qualitatively for the national economy. Furthermore, MSMEs employ approximately 117 million workers, or 97% of the total workforce. This confirms that MSMEs are a crucial sector in absorbing labor, thereby reducing unemployment (Chairani et al., 2025). MSMEs are also a highly effective instrument for attracting investment, accumulating up to 60.4% of total national investment in the same year (Azzahra et al., 2024). According to a report from the Coordinating Ministry for Economic Affairs of the Republic of Indonesia, by 2025, MSMEs will contribute 15.7% to Indonesian exports. This will help Indonesia achieve its export growth target of approximately 9% over the next five years. This sector has been proven to contribute significantly to reducing unemployment, increasing GDP, and helping achieve export targets.

The development of MSMEs still faces a major obstacle: limited access to financing. MSMEs certainly require adequate financing sources for the sustainability of their businesses. Financing is challenging for MSMEs because many lack access to banking services (Billah, 2021). Furthermore, traditional loans require complex administrative procedures and collateral, which can be prohibitive for MSMEs. This contrasts with larger companies, which can choose to conduct an Initial Public Offering (IPO) through the Indonesia Stock Exchange (IDX) or obtain financing from banks (Hasan & Sinuraya, 2024). To address these challenges, funding innovations through financial technology (fintech), particularly Securities Crowdfunding (SCF), have emerged as a potential solution (Rahmawati et al., 2024). In Indonesia, the SCF sector has shown rapid growth. According to the Association of Major Crowdfunding Services/*Asosiasi Layanan Urun Dana Indonesia* (Aludi), by June 2025, funds raised from SCF had reached IDR 1.7 trillion, with the number of investors continuing to grow, supported by Financial Services Authority/*Otoritas Jasa Keuangan* (OJK) regulations governing mechanisms and legal protection, as stipulated in OJK Regulation Number 57/POJK.04/2020 concerning Securities Offerings Through Information Technology-Based Crowdfunding Services (Waluyo et al., 2022).

In the context of Islamic economics, Securities Crowdfunding, based on syirkah (a business partnership) that implements Sharia-compliant contracts such as musyarakah (business partnership), mudharabah (profit sharing), and murabahah (buying and selling with a profit margin), provides a financing alternative that adheres to halal principles, free from elements of usury (riba), gharar (uncertainty), and maysir (gambling) (Haedar et al., 2025). Securities Crowdfunding offers innovation in finance and technology that facilitates transactions and investments based on Sharia-compliant values. Although this system is a new breakthrough, it is experiencing rapid development (Nafiah & Faih, 2019). However, research on MSMEs' preferences for financing through the Islamic Securities Crowdfunding (I-SCF) model remains limited. Indonesia already has regulations regarding Islamic fintech, although they do not cover all types of Islamic fintech and are still evolving. One of the regulations related to I-SCF that the Financial Services Authority/*Otoritas Jasa Keuangan* (OJK) has prepared is Regulation 16/POJK.01/2021 concerning Amendments to Financial Services Authority Regulation No. 57/POJK.04/2020 concerning Securities Offerings Through Information Technology-Based Crowdfunding Services (POJK Securities Crowdfunding, hereinafter referred to as POJK No. 16/POJK.04/2021), which provides a legal basis for crowdfunding services, including those based on Islamic principles (Hidayah & Prakoso, 2023). However, improvements are still needed to accommodate the various contracts and specific needs of Islamic MSMEs.

On the other hand, the digitalization of funding poses security risks, particularly the threat of cybercrime, which can undermine trust and the stability of the Islamic financial system (Afifah et al., 2025). Crimes such as data theft, fraud, and even terrorism financing

using digital technology are becoming increasingly prevalent amidst massive digitalization. These risks create opportunities for interested parties to commit cybercrime online. Furthermore, the anonymous nature of the internet makes fraud highly likely. Fraud can occur within the platform's internal processes, be perpetrated by users, or even through collusion between internal parties and external actors. Fintech platform users need continuous education to raise awareness and prevent the risk of cybercrime. The risk of cyberattacks also requires serious attention from syirkah-based SCF providers, who provide multiple layers of security. Therefore, cybercrime mitigation is urgent to ensure customer data protection and system integrity are maintained in accordance with the principles of justice, welfare, and transparency in the Islamic economy. Cyberattacks have serious consequences because they can instantly halt platform operations and even destroy the information system applications used. These information system applications are the backbone of the platform's overall operations and therefore require adequate security investment (Bahtiar et al., 2021). Regulatory readiness also requires evaluation to integrate Sharia principles with digital risk governance and consumer protection.

Based on this description, further in-depth research is needed on "Regulatory Readiness and Cybercrime Mitigation in Syirkah-Based Securities Crowdfunding to Accelerate MSMEs." This research aims to discuss the MSME sector, which offers various benefits to advance the Indonesian economy, such as absorbing labor, increasing investment, and supporting export targets. However, MSMEs still face challenges in financing, leading to the emergence of financing solutions through the development of fintech through Securities Crowdfunding (SCF). Syirkah-based Securities Crowdfunding (SCF) is currently gaining popularity and can be a financing solution for MSMEs because it is providing a financing alternative that adheres to halal principles, free from riba, gharar, and maysir. However, it is undeniable that digital financial technology will give rise to new challenges, namely cybercrime and user data security. Therefore, regulatory preparedness is needed to protect user data and mitigate cybercrime. Based on the issues outlined, several research questions emerge: how is Indonesia's regulatory readiness to support MSME acceleration through syirkah-based Securities Crowdfunding and how to mitigate cybercrime in Indonesia by optimizing the security and trustworthiness of Securities Crowdfunding to accelerate MSME growth.

The primary objective of this study is to provide solutions to the problems arising from cybercrime in this new financing model, in order to accelerate MSME growth safely, reliably, and in accordance with the Sharia values embraced by Indonesian society. This research is also expected to provide evaluation material and recommendations for strengthening regulations and mitigation practices for Sharia-compliant fintech in the future.

2. Methods

2.1 Study design

In this section, this study explain the approach used to conduct a Systematic Literature Review (SLR). The SLR process focuses on two main topics, namely regulatory readiness and cybercrime mitigation in the context of syirkah-based securities crowdfunding (SCF). The questions to be answered in the framework of the Systematic Literature Review are as follows (1) RQ1: Regulatory readiness in Indonesia to support the acceleration of MSMEs through syirkah-based Securities Crowdfunding?, (2) RQ2: How can cybercrime be mitigated in FinTech to optimize the security and trustworthiness of Securities Crowdfunding?. The process of searching for relevant articles was carried out by determining the desired article search database for this SLR process. The specified databases will be used to collect the data and articles needed to review these two topics in depth. Database for searching data and related articles can be seen in Table 1.

Table 1. Database repositories

Source	URL
Science Direct	https://www.sciencedirect.com/
Emerlad Insight	https://www.emerald.com/
Springer	https://link.springer.com/
Google Scholar	Google Scholar
Database Peraturan JDIH BPK	https://peraturan.bpk.go.id/

The search for relevant articles and data is conducted by using specific keywords. The chosen keywords will revolve around "Sharia Securities Crowdfunding," "Cybercrime in FinTech," "Cyber Regulations," "Cybersecurity in FinTech," “Cybersecurity Awareness Training,” "cyber risk mitigation," and "Sharia Securities Crowdfunding Regulations in Indonesia." To maintain the relevance and quality of the selected papers, the following additional inclusion criteria were applied, (1) Papers published within the last ten years that remain relevant to the topic; (2) Keywords aligned with those used in search strategy, ensuring a strong correlation with research objectives; (3) Papers that explicitly discuss cybercrime in fintech and its mitigation strategies; (4) Papers that are accessible either through open access or via institutional subscriptions. This study based on academic experience and an in-depth literature analysis. To provide a visual overview of the most frequently discussed topics, a word cloud visualization presents the most common keywords and titles from search results (See Fig. 1).

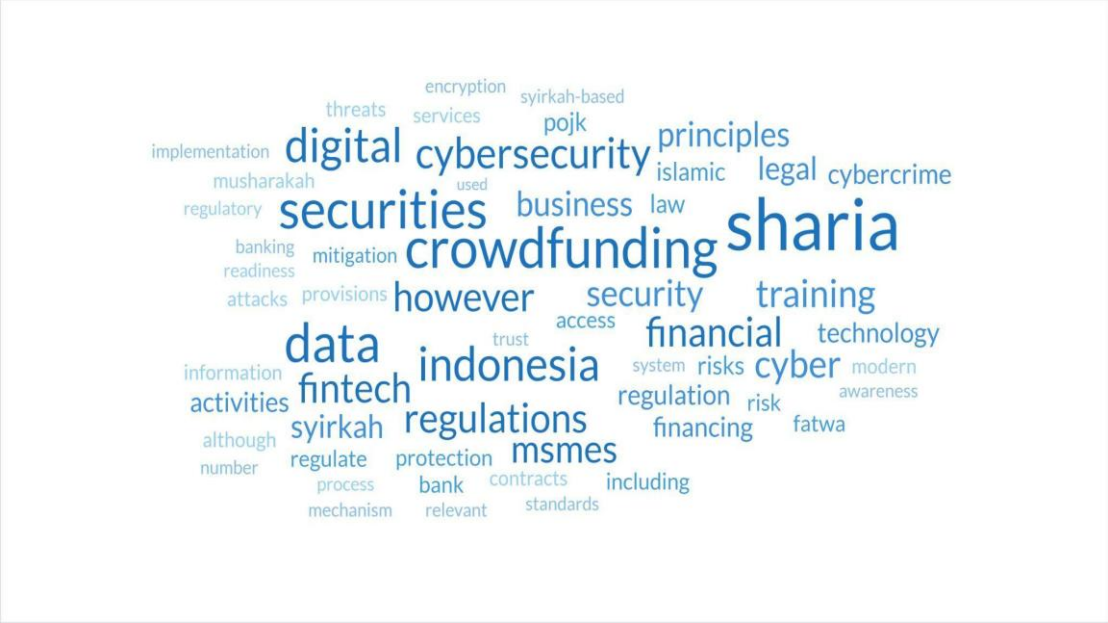

Fig.1. Word cloud generated from the most common keywords and titles

3. Results and Discussion

3.1 Regulatory readiness in Indonesia to support the acceleration of MSMEs through syirkah-based securities crowdfunding

Regulatory readiness in Indonesia to support the acceleration of MSMEs through syirkah-based securities crowdfunding still faces various legal challenges. Currently, a number of regulations do govern the principles of syirkah, although they generally still focus on traditional business practices, which do not fully accommodate modern and digital-based investment schemes. However, there are several regulations governing business activities based on syirkah contracts that can be used as a reference, including (Rosidah et al., 2025).

Compilation of Sharia Economic Law/*Kompilasi Hukum Ekonomi Syariah* (KHES), also regulates the general provisions of syirkah contracts, which are regulated in Chapter IV Articles 134-186. This is also confirmed in Supreme Court Regulation No. 2 of 2008 (Nuralim & Jawab, 2023). However, the provisions in the KHES mostly regulate conventional syirkah practices. Meanwhile, modern forms of business such as syirkah musahamah (partnership through shares) and the use of financial technology such as crowdfunding, which are more commonly used by large national and international companies, are not explained in detail. Furthermore, it does not include provisions on business cooperation that utilizes technological developments. Furthermore, the dispute resolution mechanism in KHES is often considered ineffective because the process takes place in religious courts, which tend to be lengthy and quite complex.

Law No. 21 of 2008 on Islamic Banking does not specifically discuss digital syirkah contracts (Harrieti & Suwandono, 2024). However, Article 1 paragraph 25 explains that financing includes the provision of funds or bills that are in principle in line with nisbah transactions such as mudharabah and musharakah. This provides a strong legal basis for the existence of musharakah financing as one of the main products of Islamic banking. However, although this Law mentions rules related to syirkah, it still does not regulate in detail the mechanism for using syirkah contracts. This condition creates legal uncertainty in the practice of syirkah contracts in Islamic banking. In addition, this Law does not yet provide a specific supervisory mechanism that comprehensively regulates syirkah activities. This is crucial, because the cooperation system between parties is vulnerable to the risk of fund misuse and dishonesty by partners. Similar to the Compilation of Islamic Economic Law, this Law has not yet accommodated regulations governing the use of digital technology innovations in the practice of syirkah contracts in Islamic banking. This legal vacuum has caused concerns about potential digital risks that may arise due to the lack of a legal umbrella.

In a fatwa issued by the National Sharia Council/*Dewan Syariah Nasional* (DSN), which serves as a legal guideline for business activities that use a partnership (*shirkah*) system. These include Fatwa No. 08/DSN-MUI/IV/2000 on Musharakah Financing, Fatwa No. 55/DSN-MUI/V/2007 on Sharia Current Account Financing, and Fatwa No. 73/DSN-MUI/XI/2008 on Musharakah Mutanaqisah. Although these fatwas provide a legal basis, they still have limitations similar to other legal regulations, namely that they do not contain clauses that specifically regulate the mechanism for resolving disputes if problems arise in the practice of shirkah. This has resulted in a lack of clear guidance for judges in resolving disputes that arise. In addition, there is also a relevant fatwa as a legal basis for digital business-based musharakah activities, particularly in crowdfunding instruments, namely DSN-MUI Fatwa No. 140/DSN-MUI/VIII/2021 concerning the Offering of Sharia Securities through Information Technology-Based Crowdfunding Services Based on Sharia Principles (Islamic Securities Crowdfunding), which in its implementation must not conflict with sharia principles, namely *riba, gharor, maysir, tadlis, dharar, zhulm,* and *maksiat*. It also details the provisions of the sharia securities trading mechanism (Kurnia et al., 2024). However, this fatwa is still general and normative in nature, and therefore does not discuss in detail practical aspects such as financial reporting mechanisms, profit distribution, and other technical aspects. These limitations pose challenges in optimally meeting investor protection needs, especially in the context of the ever-evolving digital business.

In order to regulate musharakah businesses in Islamic banking, the OJK has published a Musharakah Financing Product guideline book. The book discusses the sharia principles underlying musharakah financing, as well as explaining the relevant schemes, illustrations, and bookkeeping records. However, the guidelines still have several shortcomings, particularly in terms of the regulation of fair distribution of profits and losses, as well as the mechanism for resolving conflicts between partners, which has not been explained in detail. This condition indicates the need for updates so that syirkah business activities can run fairly and provide maximum benefits for all parties. In addition, in the course of digital business-based partnerships that use crowdfunding instruments, there are a number of relevant provisions in POJK, namely POJK No. 37/POJK.04/2018, and POJK No.

16/POJK.04/2021. However, these regulations do not yet comprehensively regulate screening standards through financial ratios, which are an important aspect of protecting the rights of sharia investors, while also maintaining the sustainability of the sharia economic cycle. In POJK No. 57/POJK.04/2020, it is mandatory to have adequate competence in reviewing Micro, Small, and Medium Enterprises (MSMEs) that are prospective issuers of securities. This assessment process is carried out by upholding the principle of prudence, covering several important points, namely (Kurnia et al., 2024); (a) Conducting a comprehensive evaluation of prospective MSME issuers before granting approval to issue sharia shares and/or sukuk through a digital platform managed by a Sharia SCF organizer, (b) Providing assistance to SME issuers in preparing prospectuses that comply with minimum regulatory standards while reflecting the actual business conditions of the SMEs, (c) Conducting ongoing supervision of SME issuers, particularly in terms of submitting periodic reports and managing the distribution of dividends or returns to investors.

To date, financial ratio screening standards in Indonesia are regulated in POJK No. 35 of 2017 concerning Criteria and Issuance of Sharia Securities Lists. However, according to Law No. 8 of 1995 concerning Capital Markets, the offering of securities through crowdfunding services is not included in the definition of securities offerings in the law, so legally these activities are not subject to the standards regulated in POJK No. 35 of 2017 (Ulum et al., 2025).

Bank Indonesia Regulation No. 7/46/PBI/2005 regulates agreements on the collection and distribution of funds for banks that conduct business activities based on sharia principles. This regulation contains provisions that explain the mechanisms of sharia-compliant business practices, including the principle of musharakah. However, as with other regulations, this regulation does not specifically regulate the mechanisms for resolving conflicts or disputes that may arise. The regulation only mentions that dispute resolution can be carried out through deliberation, other alternatives, or through the National Arbitration Board. The absence of provisions that specifically regulate this matter has the potential to cause uncertainty and new conflicts in decision-making by partners and third parties involved (Rosidah et al., 2025). However, this regulation is no longer valid.

Bank Indonesia explicitly facilitates the development of a technology-based inclusive financial ecosystem, including sharia services for MSMEs, through various policies and regulations. One of these is Bank Indonesia Regulation No. 19/12/PBI/2017 concerning the Implementation of Financial Technology, which regulates registration requirements and prudential principles for fintech operators. Bank Indonesia also encourages sharia innovation that uses sharia principles such as musyarakah and mudharabah for MSME financing, complemented by the application of technologies such as artificial intelligence and blockchain to improve efficiency and transparency.

Thus, Indonesia's regulatory readiness to support the acceleration of MSMEs through syirkah-based Securities Crowdfunding (SCF) shows progress with the existence of a legal umbrella that begins to accommodate sharia principles. However, existing regulations are still general and normative in nature, and do not yet regulate technical aspects in detail, such as dispute resolution mechanisms, profit distribution supervision, or optimal investor protection in the context of a rapidly growing digital business.

The Financial Services Authority through POJK No. 57/POJK.04/2020 regulates information technology-based crowdfunding services involving issuers of sharia securities such as stocks and sukuk. This regulation emphasizes the importance of the principles of prudence, transparency, and accountability in order to protect investor rights and maintain market integrity (Pribadi et al., 2020). In addition, the National Sharia Council-Indonesian Ulema Council (DSN-MUI) issued Fatwa No. 117/DSN-MUI/II/2018, which serves as a guideline for sharia compliance, so that crowdfunding activities are not only technically safe but also in accordance with sharia principles, such as the prohibition of usury and gharar. However, implementation challenges remain due to the lack of integrated oversight mechanisms and adequate sharia financial literacy among MSMEs and investors, as well as the need to adapt regulations to the risks of digital crime and fraud that are developing

alongside technological advances (Maulidi, 2024). Therefore, regulatory strengthening and collaboration among supervisory institutions are needed to ensure the security of digital transactions and optimal protection for all parties in the Sharia SCF ecosystem.

In addition to OJK, Bank Indonesia also encourages the development of an inclusive technology-based financial ecosystem, especially sharia fintech for MSMEs, through regulations such as Bank Indonesia Regulation Number 19/12/PBI/2017 concerning the Implementation of Financial Technology. BI emphasizes the principles of prudence, consumer protection, and the use of digital innovations, including artificial intelligence and blockchain, to improve efficiency and transparency in syirkah-based financing. However, several supporting regulations, such as Bank Indonesia Regulation Number 7/46/PBI/2005, which regulates fund collection agreements based on sharia principles, are no longer valid, necessitating continuous updates to accommodate digital-based business innovations. Thus, although Indonesian regulations have established a sufficiently robust legal foundation for accelerating MSMEs through Sharia Securities Crowdfunding, challenges in the field such as technical standards, integrated supervision, and Sharia financial literacy still need to be addressed in order to realize this potential to the fullest and in a sustainable manner.

3.2 Cybercrime mitigation in fintech to optimize the security and trust of securities crowdfunding

3.2.1 Cybercrime as a security threat to sharia-compliant securities crowdfunding

These days, information technology (IT) is a big part of the modern economy, being a key driver of growth. From small businesses to huge corporations, both government and private, they're all connected and rely heavily on IT, like cloud-based systems and artificial intelligence. No surprise, this also opens the door to more cyber risks. Privacy and cyber risks are important aspects that need to be considered when using IT to support any service (Aldasoro et al., 2022). The frequency of cyber risks in the financial sector is very high; in fact, it can be said that this sector is the most affected (Aldasoro et al., 2022). These types of crimes have existed for centuries, even before the advent of sophisticated technology. Fraudulent activities, theft, and swindles were common, even without high-tech equipment. However, using computers and the Internet has provided criminals with a tool to expand their pool of potential victims and evade detection. As a result, such crimes are committed frequently in the digital age (Adewopo et al., 2025).

Cybercrime covers a spectrum of malicious activities, ranging from sophisticated hacking and data breaches to social engineering and ransomware attacks. ENISA, the cybersecurity authority in the European Union, has compiled a classification of cyber threats, in which malware accounts for the largest share, contributing to 30% of all attacks. Beyond malware, the cyber threat landscape includes attacks on websites and domains aimed at stealing personal and banking data, as well as phishing schemes designed to impersonate identities and spread malicious software. These attacks target three fundamental security objectives, known as the CIA triad; confidentiality, integrity, and availability (Shankar et al., 2024). At the same time, internal risks are also a substantial source of vulnerability. ENISA (2020) reports that 77% of data breaches in companies are caused by incidents related to internal staff, whether intentional or unintentional. This shows that cyber risk management must include not only protection from external attacks, but also from internal threats (Fernandez De Arroyabe & Fernandez De Arroyabe, 2023).

Phishing is a social engineering tactic designed to trick individuals into voluntarily divulging sensitive and valuable personal information. The goal is to gain unauthorized access to data such as login credentials, financial account details, or other identity information. These attacks are typically carried out by malicious parties posing as trusted entities, utilizing a combination of psychological manipulation and technical methods. One method often used in phishing attacks is through the use of fake domains. These domains visually mimic the original website, creating a convincing duplicate to deceive users. When unsuspecting victims visit these fake sites, they are asked to enter personal information.

The data entered is then sent directly to the attacker, enabling a data breach (Rawla et al., 2025). With access to this sensitive information, attackers can carry out a series of malicious activities, including identity theft and financial fraud, by posing as legitimate users (See Fig 2).

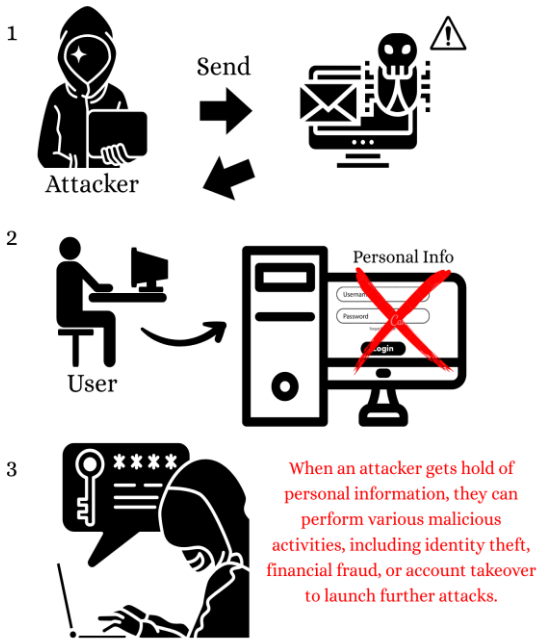

Fig. 2. Illustration of phishing attack workflow

Malicious software, commonly known as malware, is a category of programs deliberately designed to cause damage or disrupt operations on digital devices, networks, and computer systems. This term covers a wide range of cyber threats, such as worms, trojan horses, ransomware, spyware, adware, and viruses. Acorrding to Negi et al. (2023) as cited by Bakshi et al. (2025) Malware detection is a fundamental step in cybersecurity to prevent unauthorized access to devices and data, as well as mitigate potential financial losses or operational damage.

Ransomware has become a significant and evolving form of malware. As a denial-of-access attack, its primary function is to block a user's access to their system or data until a ransom is paid. Since its first appearance with the AIDS (PC Cyborg) variant, ransomware has developed into thousands of different versions. In 2023, there was a sharp increase in global ransomware attacks compared to the previous year. Today, the two main types are locker-ransomware, which locks the user out of their system by restricting screen access, and crypto-ransomware, which encrypts the user's data and demands a payment for the decryption key (Zhao et al., 2025).

Social engineering is a very dangerous and widespread cyber threat that targets individual privacy and security. These attacks exploit the natural human tendency to easily trust digital sources. Attackers exploit emotional and psychological weaknesses such as fear, greed, empathy, or curiosity to trick victims into clicking on fake links or URLs. Once victims are manipulated, they unknowingly grant attackers authorization to access personal and financial information, making the protection of digital platforms from these tactics an urgent challenge. In the broader context of cyber attacks, social engineering is often the most important first step in gaining unauthorized access to target systems (Rathod et al., 2025). In a social engineering attack, attackers begin with investigation, gathering information about the target through public data and social media profiles to identify vulnerabilities. Once the information is gathered, they enter the planning phase to devise a convincing strategy, such as creating phishing links or impersonation. The next stage is contact, where they interact with the target, usually via email, phone (vishing), or SMS (smishing) to build trust and persuade the victim to take the desired action. Finally, in the

execution phase, attackers secretly collect sensitive data such as login credentials or banking details, often by installing malware, while trying to avoid detection by security systems such as firewalls and antivirus software.

In the last five years, Indonesia's cyberspace has been a prime target for various types of cyber threats, underscoring the urgency of improving cybersecurity defenses. According to the National Cyber and Crypto Agency/*Badan Siber dan Sandi Negara* (BSSN), the total cumulative number of anomaly traffic identified during the 2020-2024 period reached 3,844,258,669 (See Table 2).

Table 2. Cyber traffic anomalies in Indonesia 2020-2024

Year	Total Anomalies	Most Frequent Anomaly	Source
2020	495,337,202	Trojan	BSSN (2020)
2021	1,637,973,022	Malware, Trojan Activity, Information Gathering	BSSN (2021)
2022	976,429,996	MyloBot Botnet (Enables full system control)	BSSN (2022)
2023	403,990,813	Generic Trojan RAT (Backdoor communication)	BSSN (2023)
2024	330,527,636	Mirai Botnet	BSSN (2024)
Total	3,844,258,669		

The bar chart shows cyber traffic anomalies in Indonesia from 2020 to 2024 (See Fig 3). The cumulative total of traffic anomalies identified during this period reached more than 3.8 billion. The data shows that 2021 experienced the highest anomalies, reaching 56.12% of the total incidents. This substantial number indicates that cyber attacks are no longer sporadic incidents, but rather a consistent and massive phenomenon. Therefore, the implementation of a comprehensive cybersecurity strategy, which includes detection, mitigation, and response to threats, is essential to maintain the integrity, confidentiality, and availability of data in cyberspace. This is especially true in the vital fintech sector, where financial data security is a top priority because fintech has a dynamic and complex network that interacts seamlessly to deliver a variety of financial products and services to end consumers (Muthukannan et al., 2020). According to the X-Force Threat Intelligence Index 2023 report, the financial and insurance sectors rank second among the industries most targeted by cybercriminals since 2018. Although FinTech-supported services have provided easy access and high availability, they have raised new cybersecurity concerns, especially for banks and businesses (Javaheri et al., 2024).

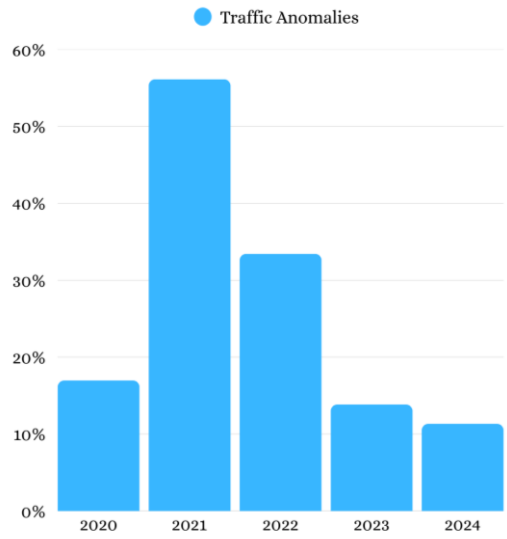

Fig. 3. Trafic anomalies in Indonesia

One form of FinTech is crowdfunding, known in Indonesia as urun dana. These days, to meet the long-term funding needs of MSMEs, there is an instrument called Securities Crowdfunding (SCF). All MSMEs rely on digital technology to varying degrees, whether for accounting and tax reporting, email, digital marketing, remote working, and so on. For more

and more businesses, digital technology is a key part of business operations (Cartwright et al., 2023). The presence of the FinTech crowdfunding industry has changed the way MSMEs obtain financing. This greatly facilitates MSMEs in remote areas, which no longer need to travel long distances to seek funding.

Securities crowdfunding operates in an online environment, which means that interactions between users are often affected by information asymmetry. This condition shows that building trust also involves a process of information verification by the platform. The perceived quality of information on the platform has been proven to facilitate the establishment of trust. Risks such as fraud, misuse of client data, digital signature forgery, and various other cybercrimes threaten user data security. The complexity of blockchain technology and uncertainty in security and trust are major obstacles (Javaheri et al., 2024). In this situation, legal protection plays a vital role in protecting all parties from potential crimes. Although FinTech-supported services have provided ease of access and high availability, these services have caused new cybersecurity concerns.

Cybersecurity is not only a technical issue, but also an ethical issue that is in line with Islamic principles. The Islamic principles referred to include *amanah* and justice. As caliphs and servants of Allah, humans have a great responsibility towards the amanah given to them. This responsibility requires humans not only to develop and prosper the earth in accordance with the rules set by Allah and His Messenger, but also to preserve and protect all of His creations. In the modern context, this trust includes the protection of personal data and digital assets, which are an integral part of human life these days. Given the role of *humans as 'abdun* (servants), obedience and submission to the commands of Allah and His Messenger is the essence of every action, including maintaining integrity and security (Qurratulaini, 2024). Therefore, fulfilling all religious and ethical obligations in full, without negligence, is key to fulfilling this mandate, including maintaining cybersecurity, which is now an integral part of human responsibility.

Allah SWT has established the principle of justice throughout the universe and commanded His servants to uphold it on earth. This command is not merely a request, but an obligation that must be carried out earnestly, even if it means sacrificing personal interests, parents, or close relatives (Akhmadi & Kholish, 2016). In the modern context, upholding this justice includes protection from cyber threats that can cause unfair financial losses to investors and MSMEs. Therefore, building a robust and strong security system in the digital world is a tangible manifestation of efforts to uphold justice, ensuring that the rights of all parties are optimally protected from losses caused by cybercrime. This action is in line with the divine teaching to always be fair in every aspect of life.

3.2.2 Securities crowdfunding risk mitigation strategy

Here are some key strategies for reducing cybersecurity risks in the FinTech industry, Cybersecurity Awareness Training. According to Disparte & Furlow (2017), as cited by Zhang et al. (2021), the most effective investment in cybersecurity is through stronger training for employees. FinTech companies should regularly provide cybersecurity awareness training to their employees and customers. This aims to reduce the risk of phishing and social engineering attacks. The training should cover topics such as identifying fraudulent emails, creating strong passwords, and avoiding the use of public Wi-Fi networks. Employees must be aware of the risks in their daily activities, such as phishing emails, unsecured devices, or inappropriate data sharing, so that they can mitigate them before they cause security breaches.

Cybersecurity awareness training can be categorized into three groups: traditional, technology-based, and innovative training methods (Qawasmeh et al., 2025). Traditional cybersecurity training methods, including passive, classroom-based, and video approaches, offer their own advantages and disadvantages. Passive methods such as posters and e-flyers are cost-effective and can reach a wide audience, but their static content is often ignored and less effective in the face of evolving threats (Potgieter, 2019). Classroom-based training, whether in-person or online, provides strong direct interaction and personalization, but has

challenges in terms of scalability and large content investment. Meanwhile, video-based training is highly scalable and flexible (Fyfield et al., 2019), ideal for remote employees, although its "one-size-fits-all" format can reduce engagement and fail to meet individual needs.

Technology-based and innovative cybersecurity training methods, such as simulations, applications, games, and VR/AR, offer a modern approach to raising awareness. Simulation-based training, such as simulated phishing attacks, is highly effective for providing experiential learning and is scalable. However, its effectiveness is highly dependent on a high level of realism in the simulation to reflect real threats. Application-based training offers flexibility and self-directed learning that is well-suited for a dispersed workforce (Abawajy, 2012). That said, the content is often uniform, lacks personalization, and may not be suitable for all learning styles. Game-based training can increase motivation and knowledge retention through elements of competition and storytelling, but it is expensive to develop and difficult to tailor to different roles in large organizations (Hill et al., 2020). Finally, VR/AR technology provides an unmatched immersive experience in knowledge acquisition and retention. However, this method is the least scalable due to the very high implementation costs for specialized hardware and personnel. MFA, a significant evolution in digital security, is a method of verifying a user's identity by requiring them to present two or more separate pieces of evidence, or 'factors' (See Fig 4).

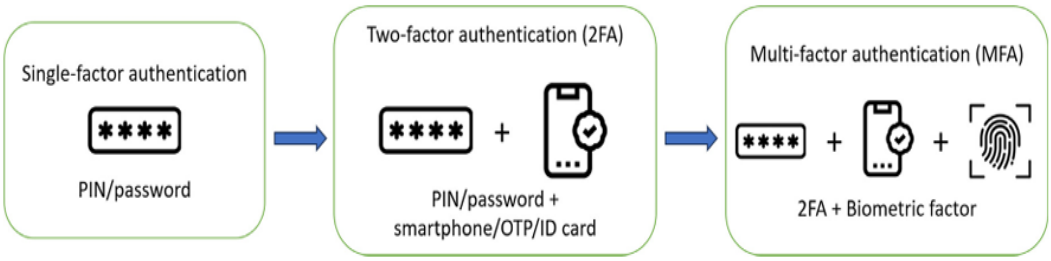

Fig. 4. The evolution of the authentication factor.
(Tran-Truong et al., 2025)

The main goal of MFA is to create a layered defense system. If one factor is compromised or breached, attackers still have at least one more barrier to overcome before successfully gaining access to the target. This makes MFA an effective tool in preventing unauthorized access to systems, data, and applications, thereby significantly improving an organization's overall security posture (Tran-Truong et al., 2025). It makes it more difficult for cyber attackers to gain access, even if they manage to obtain a user's password.

FinTech companies must implement strong encryption measures to protect data at rest and in transit. Encryption involves converting data into code that can only be deciphered with a key or password. This can help prevent data theft and unauthorized access to sensitive information. The implementation of encryption will focus on how encryption can secure data down to the row and field level while maintaining data integrity and the authority of each database user (Rahmadi & Yunita, 2020). FinTech companies must regularly assess the security measures of their third-party vendors to ensure that they meet the required standards (Ali et al., 2023).

4. Conclusions

Based on a comprehensive literature review, Indonesia's regulatory readiness to support the acceleration of MSMEs through *syirkah*-based Securities Crowdfunding (SCF) shows progress with the existence of various regulations, such as DSN-MUI Fatwas and OJK Regulations (POJK), that are beginning to accommodate sharia principles in crowdfunding services. However, the existing regulatory framework remains general and normative, lacking detailed provisions on crucial technical aspects like dispute resolution mechanisms, supervision of profit distribution, and optimal investor protection within a rapidly evolving

digital ecosystem. These regulatory weaknesses create legal gaps that can trigger uncertainty and risks, particularly concerning the potential misuse of funds and unethical practices. Therefore, continuous updates and strengthening of regulations are needed to accommodate digital innovation and ensure that all parties including investors and MSMEs are protected fairly and comprehensively in accordance with sharia principles.

On the other hand, the digitalization of the fintech sector introduces significant cyber risks, as evidenced by the high volume of cyber traffic anomalies in Indonesia. These threats are not only technical but also ethical, aligning with the Islamic principles of amanah (trust) and justice which mandate the protection of digital data and assets. To mitigate these risks and optimize the security and trustworthiness of SCF, implementing a comprehensive strategy is essential. Key recommended mitigation strategies include cybersecurity awareness training for all stakeholders, implementation of multi-factor authentication (MFA), strong encryption to protect data, and third-party vendor risk management. By integrating sharia principles into a robust and dynamic cybersecurity framework, Indonesia can build a Securities Crowdfunding ecosystem that is not only innovative and inclusive but also resilient and trustworthy, ensuring sustainable growth and continuity for MSMEs.

Acknowledgement
The authors would like to thank FILFEST 2025 for giving them the opportunity to publish this work.

Author Contribution
Conceptualization, P.R.K.; Methodology, P.R.K.; Software, P.R.K., A.N.F.K., and D.T.S.P.; Formal Analysis, A.N.F.K.; Investigation, C.C.; Resources, B.B.; Data Curation, B.B.; Writing – Original Draft Preparation, P.R.K., A.N.F.K., and D.T.S.P.; Writing – Review & Editing, P.R.K., A.N.F.K., and D.T.S.P.

Funding
This research received no external funding

Ethical Review Board Statement
Not available.

Informed Consent Statement
Not available.

Data Availability Statement
Not available.

Conflicts of Interest
The authors declare no conflict of interest.

Declaration of Generative AI Use
During the preparation of this work, the author used DeepL and AI *wordcloud* to help translate into English and edit the content as needed, and is fully responsible for the content of the publication.

References

Abawajy, J. (2012). User preference of cyber security awareness delivery methods. *Behaviour & Information Technology*, *33*, 237–248. https://doi.org/10.1080/0144929X.2012.708787

Adewopo, V. A., Azumah, S. W., Yakubu, M. A., Gyamfi, E. K., Ozer, M., & Elsayed, N. (2025). Comprehensive analytical review of cybercrime and cyber policy in West Africa. *Journal of Electrical Systems and Information Technology*, *12*(1). https://doi.org/10.1186/s43067-025-00216-x

Afifah, K., Abu-Hussin, M. F., & Zafar, M. B. (2025). Transforming Islamic social finance: determinants of blockchain technology adoption for zakat payment. *Journal of Islamic Accounting and Business Research*. https://doi.org/10.1108/JIABR-08-2024-0283

Akhmadi, S., & Kholish, A. (2016). Prinsip-prinsip fundamental ekonomi Islam. *El-Jizya: Jurnal Ekonomi Islam*, *4*(1), 97-118. https://ejournal.uinsaizu.ac.id/index.php/eljizya/article/view/976/787

Aldasoro, I., Gambacorta, L., Giudici, P., & Leach, T. (2022). The drivers of cyber risk. *Journal of Financial Stability*, *60*, 100989. https://doi.org/10.1016/J.JFS.2022.100989

Ali, M. N., Qualbi, M., & Sajjad, M.. (2023). Cybersecurity Risks and Mitigation Strategies in Fintech. *International Journal of Research Publication and Reviews,4*(4), 1395-1398. https://ijrpr.com/uploads/V4ISSUE4/IJRPR11519.pdf

Azzahra, N., Hotmian, H., Silalahi, B., Naibaho, H. S., Silaban, H. B., Sitio, F. M., & Lahagu, H. (2024). Analisis Koperasi Syariah Di Indonesia. *Jurnal Ilmiah Wahana Pendidikan*, *10*(11), 487–491. https://doi.org/10.5281/zenodo.12754894

Bahtiar, B., Lubis, E., & Harahap, H. (2021). Pengaturan Kaidah Manajemen Risiko Atas Penawaran Saham Berbasis Teknologi Informasi (Equity Crowfunding) untuk Pengembangan UMKM di Indonesia. *Jurnal Hukum Jurisdictie*, *3*(2), 65-98. https://doi.org/10.34005/jhj.v3i2.49

Bakshi, R., Lingwal, S., Bhatt, K. C., Thapliyal, S., Wazid, M., & Singh, D. P. (2025). A Robust Machine Learning-Based Mechanism for Detection and Analysis of Malware Attacks. *Procedia Computer Science*, *259*, 193–201. https://doi.org/10.1016/J.PROCS.2025.03.320

Billah, Z. I. T. (2021). Peran dan kendala fintech syariah pada UMKM. *Ar-Ribhu: Jurnal Manajemen dan Keuangan Syariah*, *2*(2), 256-266. https://doi.org/10.55210/arribhu.v2i2.671

BSSN. (2020). *Laporan Hasil Monitoring Keamanan Siber Tahun 2020.* Badan Siber dan Sandi Indonesia.

BSSN. (2021). *Laporan Hasil Monitoring Keamanan Siber Tahun 2021.* Badan Siber dan Sandi Indonesia.

BSSN. (2022). *Lanskap Keamanan Siber Indonesia 2022.* Badan Siber dan Sandi Indonesia.

BSSN. (2023). Lanskap Keamanan Siber Indonesia 2023. Badan Siber dan Sandi Indonesia.

BSSN. (2024). Lanskap Keamanan Siber Indonesia 2024. Badan Siber dan Sandi Indonesia.

Cartwright, A., Cartwright, E., & Edun, E. S. (2023). Cascading information on best practice: Cyber security risk management in UK micro and small businesses and the role of IT companies. *Computers & Security*, *131*, 103288. https://doi.org/10.1016/J.COSE.2023.103288

Chairani, N., Zasmin, N., Raisuli, R., & Rosidi, A. R. (2025). Peran sektor UMKM dalam menekan inflasi dan menyerap tenaga kerja di Surabaya. *Sammajiva: Jurnal Penelitian Bisnis dan Manajemen*, *3*(1), 57-66. https://doi.org/10.47861/sammajiva.v3i1.1651

Disparte, D., & Furlow, C. (2017). *The best cybersecurity investment you can make is better training.* Harvard Business Review, 5. https://hbr.org/2017/05/the-best-cybersecurity-investment-you-can-make-is-better-training

Fernandez De Arroyabe, I., & Fernandez de Arroyabe, J. C. (2023). The severity and effects of Cyber-breaches in SMEs: a machine learning approach. *Enterprise Information Systems*, *17*(3), 1942997. https://doi.org/10.1080/17517575.2021.1942997

Fyfield, M., Henderson, M., Heinrich, E., & Redmond, P. (2019). Videos in higher education: Making the most of a good thing. *Australasian Journal of Educational Technology*, *35*(5), 1-7. https://doi.org/10.14742/ajet.5930

Haedar, A. M., Ningrum, D. C., & Hidayanti, N. (2025). Pemikiran Ulama tentang Akad Mudharabah dari Mazhab Klasik Hingga Kontemporer serta Penerapannya dalam Ekonomi Syariah Digital. *SAUJANA: Jurnal Perbankan Syariah dan Ekonomi Syariah*, *7*(3), 89-108. https://doi.org/10.59636/saujana.v7i3.345

Hapsari, Y. A., Apriyanti, P., Hermiyanto, A., & Rozi, F. (2024). Analisa peran umkm terhadap perkembangan ekonomi di Indonesia. *Jurnal Manajemen Dan Ekonomi Kreatif*, *2*(4), 53-62. https://doi.org/10.59024/jumek.v2i4.464

Harrieti, N., & Suwandono, A. (2024). Peningkatan Pemahaman Akad-akad Perbankan Syariah dalam Mewujudkan Literasi Keuangan Syariah. *PROFICIO*, *5*(1), 198-205. https://doi.org/10.36728/jpf.v5i1.2946

Hasan, W., & Sinuraya, B. (2024). Securities Crowdfunding Sebagai Alternatif Pembiayaan Bagi UMKM Di Indonesia. *BULLET: Jurnal Multidisiplin Ilmu*, *2*(6), 1304-1308. https://journal.mediapublikasi.id/index.php/bullet/article/view/3959

Hidayah, Y. W., & Prakoso, B. (2023). Perlindungan Hukum Terhadap Investor Dalam Layanan Platform Securities Crowdfunding Sebagai Pendanaan Umkm Di Indonesia. *CLEAR: Criminal Law Review*, *1*(2), 1-16.

Hill Jr, W. A., Fanuel, M., Yuan, X., Zhang, J., & Sajad, S. (2020). A survey of serious games for cybersecurity education and training. In *KSU Proceedings on Cybersecurity Education, Research and Practice. 7.* https://digitalcommons.kennesaw.edu/ccerp/2020/Research/7/

Javaheri, D., Fahmideh, M., Chizari, H., Lalbakhsh, P., & Hur, J. (2024). Cybersecurity threats in FinTech: A systematic review. *Expert Systems with Applications*, *241*, 122697. https://doi.org/10.1016/J.ESWA.2023.122697

Kurnia, R., Melzatia, H. H., Rasyad, F. H. S., Sedera, R. M. H., & Mintra, R. R. M. (2024). The Role Of Financial Value Added In The Islamic Banking Sector. *Journal Of Accounting, Governance, And Organization*, *1*(1), 22-32. https://journal.uns.ac.id/index.php/jago/article/view/1873

Maulidi, M. A. (2024). Analisa Penerapan Sharia Compliance Securities Crowdfunding (Studi Kasus Fundex Platfom). *Jurnal Warta Ekonomi*, *7*(01), 219-232. https://jim.unisma.ac.id/index.php/jwe/article/view/24626

Muthukannan, P., Tan, B., Gozman, D., & Johnson, L. (2020). The emergence of a Fintech Ecosystem: A case study of the Vizag Fintech Valley in India. *Information & Management*, *57*(8), 103385. https://doi.org/10.1016/J.IM.2020.103385

Nafiah, R., & Faih, A. (2019). Analisis transaksi financial technology (fintech) syariah dalam perspektif maqashid syariah. *IQTISHADIA Jurnal Ekonomi & Perbankan Syariah*, *6*(2), 167-175. https://doi.org/10.19105/iqtishadia.v6i2

Negi, A., Rana, K., & Ranjan, R. (2023). Utilizing the CROPGRO Simulation Model to Optimize Management Practices for Achieving High Soybean Yields. *International Journal of Bio-resource and Stress Management*, *14*(9), 1214-1224. https://doi.org/10.23910/1.2023.3607b

Nuralim, A., & Jawab, A. R. (2023). Implementasi Mudharabah Dan Musyarakah Dalam Lembaga Perbankan Syariah. *Jurnal Ilmiah Multidisiplin*, *2*, 3-4. https://doi.org/10.56799/jim.v2i11.2417

Potgieter, P. (2019). The Awareness Behaviour of Students on Cyber Security Awareness by Using Social Media Platforms: A Case Study at Central University of Technology. In *ICICIS* (pp. 272-280). https://doi.org/10.29007/gprf

Pribadi, C., Sendrawan, T., & Salam, A. (2020). Implementasi Equity Crowdfunding Berbasis Teknologi Informasi Berdasarkan Peraturan Otoritas Jasa Keuangan Nomor

37/POJK.04/2018. *Indonesian Notary, 2*(5), 96-117. https://scholarhub.ui.ac.id/notary/vol2/iss3/5

Qawasmeh, S. A. D., AlQahtani, A. A. S., & Khan, M. K. (2025). Navigating cybersecurity training: A comprehensive review. *Computers and Electrical Engineering*, *123*, 110097. https://doi.org/10.1016/J.COMPELECENG.2025.110097

Qurratulaini, I. (2024). Nilai Kejujuran dan Amanah dalam Ekonomi dan Bisnis Islam. *Al-Iqtishadiah: Jurnal Hukum Ekonomi Syariah*, *5*(1), 80-100. https://journal.ar-raniry.ac.id/index.php/iqtishadiah/article/download/5240/2085

Rahmadi, P., & Yunita, H. D. (2020). Implementasi Pengamanan Basis Data Dengan Teknik Enkripsi. *Jurnal Cendikia*, *19*(1), 413-418. https://jurnal.dcc.ac.id/index.php/JC/article/view/331

Rahmawati, D., Apriady, M. N., & Wisudanto, W. (2024). Crowdfunding sebagai alternatif pembiayaan usaha mikro kecil dan menengah (UMKM), akibat meningkatnya jumlah pelaku UMKM di Indonesia. *Sebatik*, *28*(1), 33-40. https://doi.org/10.46984/sebatik.v27i2.2403

Rathod, T., Jadav, N. K., Tanwar, S., Alabdulatif, A., Garg, D., & Singh, A. (2025). A comprehensive survey on social engineering attacks, countermeasures, case study, and research challenges. *Information Processing & Management*, *62*(1), 103928. https://doi.org/10.1016/J.IPM.2024.103928

Rawla, A., Singh, S., Daniyal, M., & Dubey, P. (2025). Detection of Phishing Attacks in PhiUSIIL Dataset using Deep Learning. *Procedia Computer Science*, *259*, 543–552. https://doi.org/10.1016/J.PROCS.2025.04.003

Rosidah, A. I., Firmansyah, A., & Taufiqurrohman, M. (2025). Rekonstruksi Hukum Syirkah: Problematika Regulasi Dan Implementasinya Perspektif Qs Shaad (38): 24. *Al Maqashidi: Jurnal Hukum Islam Nusantara*, *8*(1), 236-256. https://doi.org/10.32665/almaqashidi.v8i1.4570

Shankar, D. D., Azhakath, A. S., Khalil, N., J. , S., T. , M., & K. , S. (2024). Data mining for cyber biosecurity risk management – A comprehensive review. *Computers & Security*, *137*, 103627. https://doi.org/10.1016/J.COSE.2023.103627

Tran-Truong, P. T., Pham, M. Q., Son, H. X., Nguyen, D. L. T., Nguyen, M. B., Tran, K. L., Van, L. C. P., Le, K. T., Vo, K. H., Kim, N. N. T., Nguyen, T. M., & Nguyen, A. T. (2025). A systematic review of multi-factor authentication in digital payment systems: NIST standards alignment and industry implementation analysis. *Journal of Systems Architecture*, *162*, 103402. https://doi.org/10.1016/J.SYSARC.2025.103402

Ulum, K. M., Fathoni, A. S., & Lia, L. W. I. (2025). Urgency of Financial Ratio Screening Regulation for Msmes Co-Funding on Securities Crowdfunding Service. *Mu'amalah: Jurnal Hukum Ekonomi Syariah*, *4*(2), 235-256. https://doi.org/10.32332/muamalah.e38hmp88

Waluyo, H., Sinaga, I. P. A., & Sugianto, F. (2022). Perlindungan hukum otoritas jasa keuangan terhadap penyelenggara layanan urun dana berbasis efek berdasarkan POJK Nomor 16/POJK. 04/2021. *DiH: Jurnal Ilmu Hukum*, 131-146. https://doi.org/10.30996/dih.v0i0.6241

Zhang, Z., He, W., Li, W., & Abdous, M. H. (2021). Cybersecurity awareness training programs: a cost–benefit analysis framework. *Industrial Management & Data Systems*, *121*(3), 613-636. https://doi.org/10.1108/IMDS-08-2020-0462

Zhao, L., Wang, Z., Wang, S., Zhang, Y., Hou, R., & Meng, D. (2025). Exploring the ransomware ecosystem and the active defense concept: Review of attacks and defense. *Journal of Information Security and Applications*, *94*, 104171. https://doi.org/10.1016/J.JISA.2025.104171

Biographies of Authors

Putri Ruby Kohinoor, is a seventh-semester undergraduate student at the Faculty of Law, Sebelas Maret University (UNS) in Surakarta.

- Email: putrirubykohinoor@student.uns.ac.id
- ORCID: N/A
- Web of Science ResearcherID: N/A
- Scopus Author ID: N/A
- Homepage: N/A

Devi Triananda Surya Putri, is a seventh-semester undergraduate student at the Faculty of Law at Sebelas Maret University (UNS).

- Email: devi11triananda04@student.uns.ac.id
- ORCID: N/A
- Web of Science ResearcherID: N/A
- Scopus Author ID: N/A
- Homepage: N/A

Anisa Nur Fatimah Karmun, is a law student from Madiun, East Java, at the Faculty of Law at Sebelas Maret University (UNS) in Surakarta.

- Email: anisa.karmun@student.uns.ac.id
- ORCID: N/A
- Web of Science ResearcherID: N/A
- Scopus Author ID: N/A
- Homepage: N/A