Indonesian Legal Framework of the Misuses of Financial Technology as A Means of Child Sexual Exploitation Amidst the Innovation of Cryptocurrency

Uni Tsulasi Putri
Universitas Ahmad Dahlan, Yogyakarya, Indonesia

uni.putri@law.uad.ac.id

Abstract. *In the current era of financial technology (fintech) development, the misuse of financial service providers for transactions involving sexual exploitation becomes a new challenge. The illicit activities related to child sexual exploitation may involve buying, selling, or trading children's sexual services, as well as live streaming child sexual abuse. Offenders might exploit the pseudonymity and decentralization of blockchain and cryptocurrency to facilitate that crime. This is normative legal research involving a library study of the primary, secondary, and tertiary legal sources. This article examines Indonesian legal framework concerning the misuse of fintech as a means to child sexual exploitation. This paper will also elaborate on the potential challenges and strategies for preventing the misuse of financial technology for child sexual exploitation amidst the development of cryptocurrency. The paper identifies key regulatory gaps and explores strategies to address these challenges, including mandatory Know Your Customer (KYC) procedures, Anti-Money Laundering (AML) compliance, and enhanced blockchain forensic tools. A strengthened legal framework that balances the protection of vulnerable children with the benefits of financial innovation is required nowadays. Without robust regulatory measures, cryptocurrency's potential for misuse will continue to pose a significant threat to child protection efforts.*

Keywords*: Financial Technology, Child, Sexual, Exploitation, Cryptocurrency.*

1. Introduction

The rapid advancement of financial technology (fintech) has revolutionized the financial services industry, offering unparalleled convenience, efficiency, and accessibility. [1] In Indonesia, as in many other countries, fintech has become an integral part of everyday financial activities, driving economic growth and inclusion. However, alongside these benefits, fintech also introduces significant challenges, particularly concerning its potential misuse for illicit activities. One of the egregious of these illicit activities is the commercial sexual exploitation of children (CSEC).

ECPAT International prepared a document submitted for the United Nations General Assembly's 79th session, addresses the increasing complexity and prevalence of sexually exploitative practices against children facilitated by digital technology. It highlights how advancements such as instant communication platforms, social media, smart devices, and artificial intelligence have diversified the ways in which children are targeted online. Notably, there has been a surge in child sexual abuse material (CSAM) and grooming across multiple platforms, with offenders using encrypted channels to evade detection. Emerging threats like deepfakes, AI-generated CSAM, and the potential misuse of augmented and virtual reality further complicate efforts to protect children. Financial sexual extortion targeting children has also re-emerged, emphasizing the need for a robust response [2].

The commercial sexual exploitation of children (CSEC) is a grave and growing concern globally, with offenders increasingly exploiting advancements in digital technologies to carry out and conceal their crimes. As financial transactions move from traditional banking systems to fintech platforms, the opportunities for perpetrators to misuse these technologies for illegal

A. Sofian et al. (eds.), *Proceedings of the ASEAN Conference on Sexual Exploitation of Children (ACOSEC 2024)*, Advances in Social Science, Education and Humanities Research 876,
https://doi.org/10.2991/978-2-38476-325-2_8

activities, including CSEC, have expanded. Blockchain technology and cryptocurrencies, in particular, have become attractive tools for criminals due to their ability to facilitate anonymous, cross-border transactions. This raises urgent concerns about the ability of existing legal frameworks to protect children from exploitation in this new technological landscape.

In Indonesia, the legal framework addressing child protection is relatively robust, with various laws in place aimed at preventing and penalizing sexual crimes against children. Laws such as the Act No. 23 Year 2002 concerning the Child Protection, the Act No. 44 Year 2008 concerning Pornography, and the recently enacted Act No. 12 Year 2022 concerning the Sexual Violence Crimes provide a foundation for safeguarding children's rights. However, these laws were designed to address more traditional forms of exploitation and abuse and may not fully encompass the complexities introduced by modern financial technologies, particularly blockchain and cryptocurrencies. The urgent need to update and strengthen these legal frameworks to cover the misuse of these emerging technologies for CSEC is crucial for preventing exploitation and ensuring justice for victims.

Based on the background above, this article examines Indonesian legal framework concerning the misuse of fintech as a means to child sexual exploitation. This paper will also elaborate on the potential challenges and strategy potential challenges and strategies for preventing the misuse of financial technology for child sexual exploitation amidst the development of cryptocurrency.

2. Literature Review

Financial technology, while offering numerous benefits, also presents opportunities for misuse, particularly in facilitating child sexual exploitation. Various online platforms are increasingly being utilized for exploitative purposes, resulting in a significant rise in technology-facilitated child abuse[3]. Internet bulletin boards, chat rooms, and peer-to-peer networks are commonly exploited by perpetrators to connect with unsuspecting children, creating avenues for child sexual exploitation [4]. Additionally, live streaming technologies have become a troubling tool for facilitating child sexual abuse. There is growing evidence that individuals, often in their 50s or 60s, engage in financial transactions related to the live streaming of child sexual abuse, highlighting the severe misuse of these technologies [5], [6].

Addressing the misuse of financial technology for child sexual exploitation is complicated by several regulatory challenges. The laissez-faire regulatory frameworks influenced by neoliberal policies have inadvertently aligned the interests of child sexual abusers with the economic goals of some online service providers. This alignment has increased opportunities for child sexual exploitation and weakened both formal and informal control mechanisms [6]. Anti-exploitation professionals have pointed out that technology companies often deprioritized online child protection, especially during the COVID-19 pandemic, suggesting a complicity within the tech industry regarding the online sexual exploitation of children[7]. Moreover, investigating and prosecuting cases of child sexual abuse material is hindered by technological issues, inadequate laws, limited resources, and the mental health and well-being of service providers [5].

Despite these challenges, financial technology can also be harnessed to combat child sexual exploitation effectively. One of the key strategies is enhancing international cooperation and coordination, which includes legal protection measures, awareness-raising campaigns, and capacity-building for law enforcement agencies [8]. Multidisciplinary teams and specialized training programs are crucial facilitators in investigating and prosecuting child sexual abuse material. These teams bring together diverse expertise and resources, improving the effectiveness of legal actions against perpetrators [5].

The use of financial technology to address child sexual exploitation raises significant ethical considerations. Discussions about harm reduction technologies, such as sex robots, haptic devices, and synthetic child pornography, highlight the potential to reduce harm to real children [9]. However, these technologies also pose complex ethical and moral questions.

Ensuring the protection of children's rights is paramount, as the commercial sexual exploitation of children constitutes a fundamental violation of their rights. A multifaceted approach that integrates legal, social, and technological measures is necessary to address this issue comprehensively [10].

3. Methodology

This study is normative legal studies. The research is structured to address two main objectives: (1) To elaborate the Indonesian legal framework concerning the misuse of fintech as a means to child sexual exploitation and (2) to identify the potential challenges and strategy in tackling the child sexual exploitation amidst the development of cryptocurrency. This research uses secondary data which consist of primary and secondary legal sources. Primary legal sources are the official legal documents that constitute the law.

For this research, primary sources include: the Act No. 4 Year 2023 concerning the Developing and Strengthening the Financial Sector, Act No. 11 Year 2008 concerning the Electronic Information and Transaction and Its Amendment of the Act No. 19 Year 2016 and Act No. 1 Year 2024, the Act No. 12 Year 2022 concerning Sexual Crimes, the Act No. 23 Year 2022 concerning the Child Protection and Its Amendment of the Act No. 35 Year 2014, the Act No. 44 Year 2008 concerning the Pornography, FSA Regulation No. 3 Year 2024 concerning the Establishment of Technology Innovation of Financial Sector, and Bank Indonesia Regulation No. 18/40/PBI/2016 concerning Payment Transaction Processing. Secondary legal sources provide interpretation, commentary, and analysis of primary sources. These include: legal textbooks, journal articles, reports and publications. The data collected from primary, secondary, and tertiary sources are analysed using qualitative methods.

4. Discussion and Findings

A. Overview of Financial Technology Regulation and Children Protection in Indonesia Concerning The Misuse of Fintech as a Means to Child Sexual Exploitation

Indonesia's fintech sector operates under a comprehensive regulatory framework designed to ensure the integrity, security, and reliability of financial transactions. The primary regulatory bodies overseeing this sector are Bank Indonesia (BI) and the Financial Services Authority (OJK). These institutions are responsible for developing and enforcing regulations that govern the fintech industry, addressing issues such as payment systems, peer-to-peer lending, and anti-money laundering (AML) and countering the financing of terrorism (CFT) measures.

The first regulation governing about Fintech is Bank Indonesia Regulation No. 18/40/PBI/2016 concerning Payment Transaction Processing. This regulation is pivotal in governing the operations of payment system operators within Indonesia. It underscores the importance of security and reliability in processing payment transactions, ensuring that all payment system providers adhere to stringent standards. The regulation mandates that these operators implement robust security measures to protect the integrity of transactions and prevent fraud. This includes requirements for encryption, secure authentication methods, and regular audits to ensure compliance with security protocols. By enforcing these standards, Bank Indonesia aims to build a secure and trustworthy payment ecosystem that can effectively support the growing fintech industry.

In 2023, Indonesia issued the Act No. 4 Year 2023 concerning the Developing and Strengthening the Financial Sector. The regulation introduces comprehensive measures aimed at protecting consumers, particularly in the realms of e-commerce and digital financial services. This legislation establishes stringent consumer protection standards to ensure that individuals engaging in online transactions receive high-quality services and their rights are well-protected. The Act underscores principles such as fairness, equality, honesty,

transparency, consumer education, and corporate responsibility. These principles are crucial in fostering a safe and trustworthy environment for digital financial activities.

Key areas of regulation under the Act include robust data protection measures to prevent the misuse of consumer information and stringent security protocols to safeguard financial transactions from fraud. The Act also mandates that companies provide clear and transparent information about their products and services, helping consumers make informed decisions. Moreover, it establishes effective mechanisms for handling consumer complaints and resolving disputes, ensuring that grievances are addressed promptly and fairly. Compliance with these regulations is mandatory, reinforcing the commitment to protecting consumer rights in the evolving digital marketplace.

The Financial Services Authority (OJK) plays a pivotal role in implementing and enforcing these regulations. The OJK is responsible for developing policies that protect consumer rights, employing both proactive and reactive approaches. Proactively, the OJK focuses on preventing fraud through consumer education and appropriate regulatory measures, thereby enhancing public trust in financial services. Reactively, it provides legal protection and facilitates consumer complaints. This dual approach ensures that consumers are well-protected in their financial transactions, supporting a stable and secure e-commerce and financial environment in Indonesia.

OJK further issued Regulation No. 3 Year 2024 concerning the Establishment of Technology Innovation of Financial Sector. The regulation covers the principle of Consumer Protection as one of the principles in conducting the regulating and surveillance process. The regulation, effective since February 19, 2024, updates the previous POJK No. 13 of 2018, enhancing the regulatory sandbox's scope and eligibility criteria. It provides a more structured approach for testing and developing innovations, clear exit policies, and post-trial business licensing processes. These improvements not only offer legal certainty for businesses but also encourage responsible innovation with effective risk management. AFTECH, representing 53 fintech companies across various business models, urges all stakeholders, including regulators and the fintech community, to collaborate in leveraging the opportunities presented by this regulation to enhance financial inclusion and deliver greater benefits to the Indonesian society.

The regulations related to financial technology, both from the OJK or BI level and the Act level do not govern about the possibility or prevention to the misuse of fintech for the CSEC. It might only fall to the rules of know-your-customer principles, surveillance on the suspicious transaction, but no specific regulation governing about the said sexual crime. However, as the fintech is correlated to the Electronic Information and Transaction, the Act No. 11 Year 2008 concerning the Electronic Information and Transaction and Its Amendment of the Act No. 19 Year 2016 and Act No. 1 Year 2024 shall be applicable.

The key provisions of this law target the distribution, transmission, and accessibility of electronic information or documents containing immoral content, as stated in Article 27(1). This article is particularly significant in combating the spread of child sexual abuse material (CSAM) and other exploitative content online. Additionally, Article 27(4) addresses cyber harassment and threats by prohibiting the dissemination of electronic information that contains threats of violence or intimidation, which is essential for protecting children from online grooming and harassment. Article 29 further reinforces this protection by targeting the dissemination of electronic information with threats aimed at instilling fear, thus supporting the safeguard against coercion and blackmail related to online sexual exploitation.

The Electronic Information and Transaction Act provides a comprehensive framework for both preventive and reactive measures to combat online sexual crimes against children. Preventive measures include public education and awareness campaigns aimed at informing children, parents, and educators about the risks and signs of online sexual exploitation. The law also mandates the implementation of stringent cybersecurity measures to monitor and block access to websites and online platforms that distribute CSAM or facilitate sexual exploitation. Reactive measures enable victims to report incidents of online sexual

exploitation through accessible and secure channels, and provide legal and psychological support to victims throughout the investigation and legal proceedings. Cooperation between law enforcement agencies, including the police, judiciary, and specialized cybercrime units, is facilitated to ensure a swift and effective response to reports of online sexual crimes.

The Act No. 44 Year 2008 concerning Pornography establishes comprehensive legal measures to combat the production, distribution, and consumption of pornographic content, particularly focusing on protecting children from exploitation. According to Article 1, pornography encompasses images, sketches, illustrations, photos, writings, sounds, videos, conversations, gestures, or any other messages containing obscenity or sexual exploitation that violates moral norms. This broad definition includes various forms of content that may be used to exploit children.

One of the crucial articles, Article 4, explicitly prohibits any person from producing, creating, duplicating, distributing, broadcasting, importing, exporting, offering, trading, renting, or providing pornographic content. This article details specific prohibited content, including sexual intercourse (including deviant practices), sexual violence, masturbation, explicit nudity, genitalia, and child pornography. The inclusion of child pornography emphasizes the law's intent to safeguard minors from sexual exploitation through digital and physical media. In terms of penalties, Article 29 stipulates severe punishments for offenders, with imprisonment of up to 12 years and fines reaching six billion rupiahs. These stringent measures reflect the law's robust approach to deterring individuals from engaging in or facilitating the production and dissemination of pornographic material, especially involving children.

The Act No. 12 Year 2022 concerning Sexual Crimes imposes stringent penalties on perpetrators to create a deterrent effect [11]. Article 12 addresses unlawful actions involving the exploitation of another person's sexual organs for self-satisfaction or the satisfaction of others, penalizing such offenses with imprisonment for up to 15 years and fines up to one billion rupiahs. Article 13 targets those who, unlawfully and with the intent to sexually exploit, place someone under their control and render them powerless, carrying the same severe penalties as Article 12. Additionally, Article 28 mandates legal protection for those accompanying victims and witnesses, ensuring their safety throughout the investigation process. Article 30 outlines the rights of victims to restitution and recovery services, including compensation for financial loss, medical and psychological care, and other damages caused by the crime. Articles 42 to 47 stipulate immediate protection measures for victims, including the provision of temporary protection by the police within 24 hours of receiving a report, and coordination between police and other authorized institutions to restrict the movements of perpetrators and ensure comprehensive victim protection.

The Act No. 35 Year 2014 concerning the Child Protection complements the Sexual Crimes Act by providing a specific focus on children's rights and protection measures. Article 76I prohibits acts of child exploitation, including sexual exploitation, and Article 88 prescribes penalties for violations, with offenders facing up to 10 years of imprisonment and fines up to 200 million rupiahs. Article 71 emphasizes special protection measures for child victims of mistreatment and neglect, including supervision, prevention, care, counselling, social rehabilitation, and social assistance. Furthermore, Article 71D grants child victims the right to claim restitution from perpetrators, ensuring they receive compensation and support for the harm suffered. This article outlines the procedural details for claiming restitution, governed by specific government regulations to facilitate the process.

Together, these laws provide a comprehensive legal framework to combat child sexual exploitation. They not only impose severe penalties on offenders but also ensure that victims receive the necessary support and protection. By integrating immediate protection measures, legal restitution, and a focus on recovery services, these laws strive to create a safer environment for children and a robust deterrent against perpetrators of such heinous crimes. While these laws collectively offer a framework to combat online sexual crimes against children, there is a need for more targeted regulations specifically addressing the misuse of

fintech for CSEC. Strengthening the legal framework with explicit provisions and enhancing coordination among regulatory bodies, law enforcement, and fintech companies can help address this gap. By doing so, Indonesia can better protect its children from the dangers of online sexual exploitation and ensure a safer digital environment.

B. Potential Challenges and Strategies for Preventing The Misuse of Financial Technology for Child Sexual Exploitation Amidst The Development of Cryptocurrency

The rise of blockchain technology and cryptocurrencies presents significant challenges in preventing CSEC. The pseudonymous nature of blockchain transactions makes it difficult for law enforcement to trace offenders, while the decentralized structure of cryptocurrency platforms prevents regulators from freezing assets or halting illegal activities in real-time. Moreover, the global reach of these technologies often means that illegal transactions cross multiple jurisdictions, creating further enforcement difficulties.

The global nature of blockchain transactions complicates matters further, as they often cross jurisdictions, limiting the reach of national law enforcement. Additionally, the complexity of blockchain platforms, such as decentralized applications (DApps), makes it harder for traditional regulatory methods to detect illegal activities like CSEC. The difficulties for mandatory implement Know-Your-Customer (KYC) and Anti-Money Laundering (AML) compliance on crypto platforms allows offenders to operate anonymously, with little fear of detection. Criminals can also use multiple wallets to compartmentalize transactions, making it even more difficult to trace their activities.

To combat these challenges, Indonesia must implement robust regulatory frameworks that enforce mandatory KYC/AML policies for cryptocurrency exchanges. However, this requires substantial investment in technological infrastructure and capacity-building, particularly in the area of blockchain forensics. Additionally, international cooperation is critical to address cross-border crimes, and blockchain forensics tools should be used to trace illicit transactions. A balance between privacy and regulation must be struck, ensuring legitimate use of blockchain while preventing exploitation. Public awareness campaigns, victim support services, and strict penalties will further strengthen the fight against the misuse of blockchain for CSEC.

The collaboration between financial institutions and law enforcement is crucial in addressing the complex issue of child sexual exploitation facilitated by financial technology [12]. This collaboration involves navigating various legal and regulatory challenges, implementing technological solutions, considering ethical implications, and understanding the potential impacts of such partnerships [3]. The rapid development of financial technologies poses significant challenges for regulators and law enforcement agencies in adapting to the criminal exploitation of these innovations [13]. As new financial technologies emerge, they create opportunities for perpetrators to exploit gaps in the legal framework. The COVID-19 pandemic highlighted a lack of prioritization for online child protection by technology companies, underscoring the need for regulatory intervention to ensure child safety [7]. European law recognizes the importance of international collaboration to prevent and prosecute online child exploitation, yet these crimes continue to escalate with technological advancements [14]. This highlights the necessity for robust legal and regulatory measures to keep pace with the evolving landscape of financial technology and criminal activities.

Financial technologies are evolving at a rapid pace, presenting new opportunities for detecting and preventing financial crimes, including child sexual exploitation. Emerging technologies in regulatory technology (*regtech*) offer promising avenues for enhancing supervision and compliance efforts. These technologies can be leveraged to monitor and analyse financial transactions, thereby identifying suspicious activities that may indicate child exploitation[13]. For instance, a study of financial transactions related to child sexual abuse live streaming in the Philippines revealed identifiable patterns that could inform the

development of technological solutions to prevent such crimes [5]. These insights highlight the potential of financial technology to support law enforcement efforts in combating child exploitation.

The intersection of economic interests within the technology sector and the sexual interests of online child abusers necessitates careful ethical considerations and regulatory intervention [7]. Protecting children from exploitation must take precedence over economic gains. Law enforcement agencies increasingly collaborate with child welfare organizations and service providers to enhance responses to the commercial sexual exploitation of children [15]. This collaboration emphasizes the importance of maintaining ethical standards and ensuring consistent international operational activities to safeguarding children's rights and well-being.

5. Conclusion

In conclusion, Indonesia's regulatory framework for financial technology, while comprehensive, lacks specific measures addressing the misuse of fintech for the commercial sexual exploitation of children (CSEC) especially in its correlation to the misuse of crypto currency as the payment method. The rise of blockchain and cryptocurrency technologies presents significant challenges, including anonymity, decentralization, and cross-border transactions, which complicate law enforcement efforts. Strengthening the legal framework with mandatory Know-Your-Customer (KYC) and Anti-Money Laundering (AML) policies, alongside enhanced cooperation between financial institutions, law enforcement, and international bodies, is crucial. These measures, combined with public awareness and technological advancements in blockchain forensics, are essential to preventing and addresing CSEC in the digital age.

6. Acknowledgement

I would like to express my sincere gratitude to the Law Study Program, Faculty of Law, Universitas Ahmad Dahlan (UAD), for their generous financial support, which enabled the presentation of this paper. This support has been instrumental in allowing me to share this research findings and contribute to the academic discourse on the critical issue of preventing child sexual exploitation through financial technology amidst the development of cryptocurrency. I am also grateful to my colleagues and mentors at the Faculty of Law for their invaluable guidance and encouragement throughout this research project. I would like to also extend my heartfelt thanks to the committee of the conference for providing a platform to present and discuss my research.

References

[1] D. W. Arner, J. N. Barberis, and R. P. Buckley, "The Evolution of Fintech: A New Post-Crisis Paradigm?," *SSRN Electron. J.*, no. January, 2015, doi: 10.2139/ssrn.2676553.

[2] ECPAT International, "Call for input: Existing and Emerging Sexually Exploitative Practices against Children in the Digital Environment," 2024.

[3] R. J. Peters, "Technology-Facilitated Child Abuse," in *Handbook of Interpersonal Violence and Abuse Across the Lifespan: A Project of the National Partnership to End Interpersonal Violence Across the Lifespan (NPEIV)*, 2021, pp. 953–973.

[4] S. Kierkegaard, "Cybering, online grooming and ageplay," *Comput. Law Secur. Rep.*, vol. 24, no. 1, pp. 41–55, 2008, doi: 10.1016/j.clsr.2007.11.004.

[5] R. Brown, S. Napier, and R. G. Smith, "Australians who view live streaming of child sexual abuse: An analysis of financial transactions," *Trends Issues Crime Crim. Justice*, no. 589, 2020.

[6] O. Cullen, K. Z. Ernst, N. Dawes, W. Binford, and G. Dimitropoulos, "'Our Laws

Have Not Caught up with the Technology': Understanding Challenges and Facilitators in Investigating and Prosecuting Child Sexual Abuse Materials in the United States," *Laws*, vol. 9, no. 4, 2020, doi: 10.3390/laws9040028.

[7] M. Salter, D. Woodlock, and T. Wong, "The sexual politics of technology industry responses to online child sexual exploitation during COVID-19: 'This pernicious elitism,'" *Child Abus. Negl.*, 2023, doi: 10.1016/j.chiabu.2023.106559.

[8] T. Rebhi and I. Bouderbala, "Challenges and Prospects in Enforcing Legal Protection of Children from Online Sexual Exploitation," *Kryt. Prawa*, vol. 15, no. 4, pp. 21–33, 2023, doi: 10.7206/kp.2080-1084.636.

[9] J. M. Appel, "Unconventional harm reduction interventions for Minor-attracted persons," *Clin. Ethics*, vol. 18, no. 2, pp. 183–191, 2023, doi: 10.1177/14777509221117981.

[10] B. Gerbaka, S. Richa, and R. Tomb, "Commercial Sexual Exploitation of Children and Trafficking," in *Child Maltreatment: Contemporary Issues in Research and Policy*, vol. 13, 2021, pp. 101–154.

[11] S. W. Kartika and I. P. Hapsari, "Sanksi Pemidanaan Terhadap Pelaku Eksploitasi Seksual Anak Dibawah Umur Menurut UU TPKS Dan UUPA Dalam Kacamata Hukum Pidana Di Indonesia," *UNES Law Rev.*, vol. 6, no. 1, pp. 2840–2847, 2023, doi: 10.31933/unesrev.v6i1.1061.

[12] J. E. B. Coster Van Voorhout, "Combatting Human Trafficking Holistically through Proactive Financial Investigations," *J. Int. Crim. Justice*, vol. 18, no. 1, pp. 87–106, 2020, doi: 10.1093/jicj/mqaa013.

[13] D. Goldbarsht and L. de Koker, "From Paper Money to Digital Assets: Financial Technology and the Risks of Criminal Abuse," *Law, Gov. Technol. Ser.*, vol. 47, pp. 1 – 15, 2022, doi: 10.1007/978-3-030-88036-1_1.

[14] E. Quayle, "Prevention, disruption and deterrence of online child sexual exploitation and abuse," *ERA Forum*, vol. 21, no. 3, pp. 429 – 447, 2020, doi: 10.1007/s12027-020-00625-7.

[15] A. Farrell, C. Wills, and C. Nicolas, "Police engagement in multidisciplinary team approaches to commercial sexual exploitation of children," *Adv. Sci. Technol. Secur. Appl.*, pp. 195 – 214, 2020, doi: 10.1007/978-3-030-41287-6_10.