IOCSPUBLISHER

Enrichment: Journal of Management

journal homepage: www.enrichment.iocspublisher.org

Analysis of Abuse and Fraud in the Legal and Illegal Online Loan Fintech Application Using the Hybrid Method

Febri Dolis Herdiani

Universitas Nasional Pasim

ARTICLE INFO

Keywords:
Digital Forensic Analysis, Hybrid Analysis, Fintech

ABSTRACT

Penetration of internet usage in Indonesia has increased by 10.12% from 2017 to 2021. This has led to very rapid technological growth, such as the growth of online loan services or Financial Technology (Fintech). This condition makes the emergence of illegal fintech services built by certain groups to reap profits. Illegal fintech service providers stand building applications with a lot of personal data requested at registration. Starting from personal data, family, work up to banking are accompanied by photo evidence and contact numbers. Hybrid analysis is needed to see the extent in which the fintech application treats customer data. In this technique, there are static analysis and dynamic analysis. Static analysis is used to see the extent in which the fintech application runs on Smartphone devices with required data and other policies. Dynamic analysis is used to view the activity of tiles and permissions of fintech applications from source code, malware analysis, and permission analysis. Hybrid analysis results show that all fintech applications have a huge potential for misuse of customer's personal data. This is indicated by the existence of a data collection URL that can be accessed by the public, there are malware activities, READ_PHONE_STATE and READ_CONTACS permissions so that fintech application providers freely monitor all contact activities, locations on the customer's Smartphone. The results of the analysis can be used to recommend fintech service users to be careful of fintech applications. Moreover, it can be used as a reference for making illegal fintech detection frameworks.

E-mail:
dolsfebri@gmail.com

1. INTRODUCTION

Indonesia is a developing country with a very high level of development compared to countries in Southeast Asia. Especially in the field of information technology and the internet. This can be seen from several government policies that encourage people to use technology, ranging from the education, business, transportation and other sectors. Even political phenomena cannot be separated from the linkage of information technology. The middle and lower levels of society must also be prepared for such rapid development. All of this is evident from a survey by the Indonesian Internet Service Providers Association (APJII) in 2019 - 2020 in terms of penetration and behavior of Indonesian internet users. In the report, there is an increase in changes in internet users from 73.7% in 2019 to 82.6% in 2020 As Table

Table 1.
Indonesian Internet User Penetration (Association of Indonesian Internet Service Providers (APJII), 2019-2020)

Year	2019	2020
Population Population (million)	267	269, 6
Internet users (million)	196,7	266,9
Percentage (%)	73,3 %	82,6%

Of the penetration of internet users, Java Island contributed 55.7% of the total distribution of internet users throughout Indonesia. From the same survey results, 93.9% of internet users in Indonesia connect with smartphones every day.

With this high number of internet users, many Financial Technology (Fintech) industries have emerged, where development has started since 2015. The presence of the Indonesian Fintech Association (AFI) aims to provide business partners and the establishment of a Bank Indonesia Fintech Office in 2016. In addition, it can also be a fintech regulatory forum that can be overseen by the Indonesian Financial Services Authority (OJK). The Financial Services Authority itself has issued regulation Number 77 / POJK.01 / 2016 concerning Information Technology-Based Lending and Borrowing Services, which contains operators, business activities, loan limits, and risk mitigation. This is what has become the speed of the fintech industry in Indonesia.

Over time, the fintech industry in Indonesia began to mushroom with the lack of strict supervision. The Financial Services Authority itself released 147 legal fintechs registered with the OJK in March 2021 and until April 2021 there were 3,198 illegal fintechs closed by the OJK, where in January 2021 there were 2,274 complaints of illegal fintech victims. With types of violations ranging from high late fees, high commissions / interest rates and terror committed by fintech companies. On the internet, there are already many free fintech applications. Even in the Android Playstore application, there are many fintech applications. The lack of public awareness of the vulnerability of misuse of personal data is the reason it is easy to apply for loans or online financing through fintech applications. The many scattered fintech applications can pose a potential risk of misuse of personal data uploaded at the time of submission of financing. Moreover, the process of making and developing applications is very easy to do without having programming experience. It was from this incident that problems emerged which became the big topic of this research. That is how the fintech application pattern in distributing customer personal information / data to third parties so that it can trigger cyber crime. The results of this analysis can later be used to create a security assessment framework in terms of personal data security in fintech applications. Apart from this, it can be used as a reference in identifying the characteristics of illegal fintech that can harm the community.

IOCSPUBLISHER

Enrichment: Journal of Management

journal homepage: www.enrichment.iocspublisher.org

2. LITERATURE REVIEW

An identifiable person is someone who can be identified directly or indirectly by identification number or based on specific factors from physical, psychological, mental, cultural or social identification. Protection of personal data in the banking sector has been regulated in Article 40 of Law Number 10 of 1998 concerning banking. Based on these provisions, banks are required to keep confidential information about customers (Dewi Rosadi & Gumelar Pratama, 2018).

It is very important to protect personal data relating to population and demographics in Indonesia such as NIK, E-KTP and KK so that they are not easily exploited. There are several forms of misuse of data such as data sales, profiling data, marketing purposes, research, even including monitoring / espionage. What is more dangerous is the misuse of personal data for criminal acts such as creating fake accounts, fraud, money laundering, extortion and illegal transactions (Sautunnida, 2018).

Based on a source from the Indonesian Financial Services Authority (OJK), illegal fintech has the following characteristics:

a. Do not have official permission
b. There is no management identity and address
c. Providing loans is very easy
d. Information on borrowing costs and fines is not clear
e. Unlimited interest / borrowing costs
f. Total returns (including penalties) are not limited
g. Billing has no time limit
h. There is no complaint service
i. Access to all data on the cellphone
j. Threats of violent terror, insults, defamation, spreading personal photos / videos, and spreading personal identity

The use of personal data that is managed for a specific purpose may not be without the consent of the data subject, be used for any other purpose than for the purpose for which the personal data was used. Personal data may not be treated or used contrary to the intended use. All necessary data access steps need to be taken by data managers to prevent data access, data processing, data changes, data disclosure and data destruction that can harm customers (Rosadi, 2017).

Reengineering software is an examination and change of a system subject to rearrange it into a new form according to the new form. This reengineering process includes 4 (four) objectives, namely Understanding (predictive), Repairing (corrective), Improving (perfective) and Evolving (adaptive). Meanwhile, Reengineering consists of two main processes, namely reverse and forward engineering. Reverse engineering is a process that does not involve system changes. A software system is analyzed to extract information from the software, so the choice that must be made is between static and dynamic analysis (Rahmadani, Raharjana, & Taufik, 2015).

Static analysis is a technique of collecting data manually. Where every system or application is opened its source code and string characteristics. Usually this static analysis technique only involves a few tools and produces little analytical data. Therefore, to reproduce the required data, another methodology is needed, namely dynamic analysis. Dynamic analysis involves the application or often referred to as the reengineering process. This analysis allows the system / application to run like a real situation and can analyze the patterns, data and techniques used (Lin, Chen, Zhu, Yang, & Wei, 2018).

In an application there are categories where the application is said to be safe from misuse of data (Mark, 2013), namely:

a. Application access control that ensures identity is authenticated and authorized to view protected data through the application.
b. The application must ensure the security of the connection between the user, database and application.
c. Audit and activity recording to provide valid and invalid reporting of every activity in the application.
d. Application code and configuration management that ensures the code is secure.

This category is the size of the application user data that is guaranteed its security from abuse from outside parties and in the application system.

Digital forensics is a scientific method used for information data collection, identification analysis, interpretation and presentation of digital evidence from digital sources, with the aim of facilitating reporting or anticipating cybercrime (Palmer, 2001).

3. RESEARCH METHODS

The method used to analyze fintech applications is to use a hybrid technique. Where this technique is inseparable from the basic techniques of Digital Forensics in conducting analysis as shown in Fig 1.The flow of the research method is shown in Fig 2.

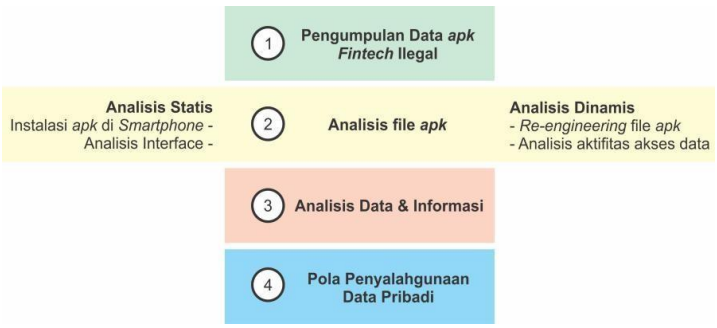


Fig 2. Hybrid Analysis Methods Illegal fintech apk file

IOCSPUBLISHER

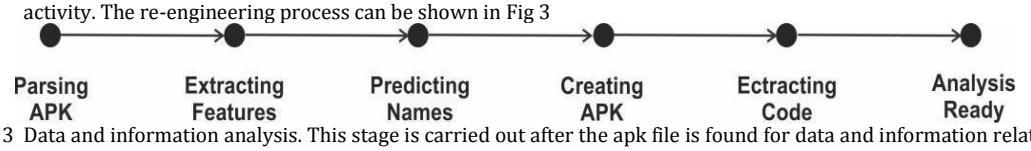
Enrichment: Journal of Management

journal homepage: www.enrichment.iocspublisher.org

The files being analyzed are files with the apk extension or the Android Package File package. Where the apk file is the file used by the Android Smartphone before installation. The stages of the hybrid analysis are:

Stage 1 Illegal fintech apk data collection. Application data retrieval is done by directly downloading the illegal fintech apk file released by the Indonesian Financial Services Authority (OJK). In this study, 5 samples of fintech application data with apk extension were used.

Stage 2 Analysis of the apk file. In the analysis process carried out using a hybrid model. Where in it there is a static analysis and dynamic analysis. At the static analysis stage, the apk application is tried to be installed directly on the Smartphone then an interface analysis is carried out and the data entered. Meanwhile, dynamic analysis is carried out by re-engineering the source code and analyzing the security of the fintech application process and malware activity. The re-engineering process can be shown in Fig 3



Stage 3 Data and information analysis. This stage is carried out after the apk file is found for data and information related to the misuse of customer / fintech application data. This data and information will describe the characteristics of each fintech application in the process of retrieving users' personal data. Starting from KTP data, family / family data, contact data on smartphones, banking data, personal data distribution models on the internet, to data and information on application behavior on smartphones.

Stage 4 Patterns of misuse of personal data. After finding the characteristics and models of fintech applications in stealing and disseminating their customers 'personal data, they will be grouped and conclusions can be drawn in the form of patterns of misuse of fintech customers' personal data.

4. RESULTS AND DISCUSSION

In this study, five sample data for illegal Android-based fintech applications were used which were obtained from the official release of the Financial Services Authority (OJK) and downloaded from the Web URL and Google Play Store. Some applications are no longer available or deleted from the Play Store by the Indonesian security authorities to minimize the occurrence of victims of misuse of personal data. But applications can still be obtained via the illegal fintech web URL or via apk bucket and apk pure.

4.1 Static Analyst Illegal Fintech Applications Android apk

The static analysis begins with installing the application on an Android Smartphone. This study did not use an emulator because it was possible that the analysis results were less accurate. Because in the emulator there is no phone number and location recording as the main requirement for verification of entry to the application. Interface analysis is needed to see the extent to which the application requests customer data in the online loan application process. The results of the static analysis are shown in Table 2 below:

From the results of the static analysis in Table 2 above, it can be concluded that there are important data and important processes that should go through verification and documentation. Privacy policies and data usage are the first measures that online loan service providers must prepare. This policy is an initial agreement in the use and transaction of data information provided by prospective borrowers. Of the five samples above, only 2 provide information on data privacy policies. However, this is not a definite measure that the service provider will properly safeguard the personal data. This policy will affect the confidentiality of personal data, family data, contact data, work data, banking data and social media data. In addition, video call verification services are also not provided in the online loan application. Video call verification is a way for service providers to ensure that prospective borrowers are sure of the services provided. In addition, the use of video call verification will minimize the use of online prospective borrower data.

4.2 Dynamic Analyst of Illegal Fintech Applications for Android apk

Dynamic analysis was carried out using 2 (two) methods. The first is to use the apk file re-engineering technique, which later converts the apk file into a source code file so that the system flow can be analyzed. While the second one uses genetic process analysis techniques, or is often called Genetic Malware Analysis. This technique will see the apk process whether it contains suspicious activity in information data theft or not.

4.3 Re-engineering apk file

The stages of the re-engineering process from the apk file to the source code can be seen in Fig 3. Re-engineering or Deobfuscation in this study using apk-deguard tools.

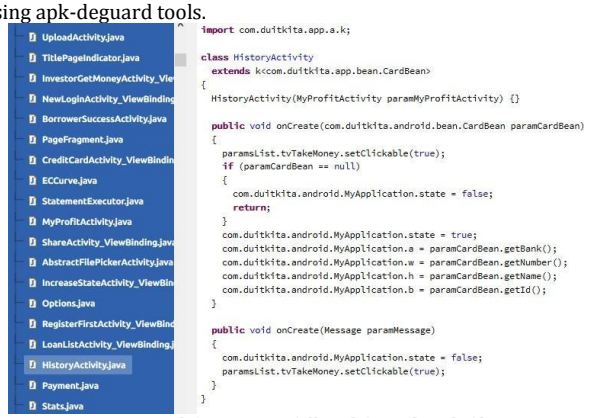


Fig 4. Deobfuscation of illegal fintech apk files

IOCSPUBLISHER

Enrichment: Journal of Management

journal homepage: www.enrichment.iocspublisher.org

The deobfuscation process shows that the sample application shows their admin URL address and even verifies banking data such as Credit Card data. Because some sample URL addresses of this application have been blocked, proxy access is required to enter them. Some URLs have also begun to be disabled for the safety of fintech customers.

4.4 Genetic Activity Analysis

Genetic analysis is conducted to see activities that resemble backdoor activity, malware and viruses. Where these activities can trigger data theft. Analysis using Intezer tools, and Virustotal. In addition, it can also be used to find out what activities the application does while running.

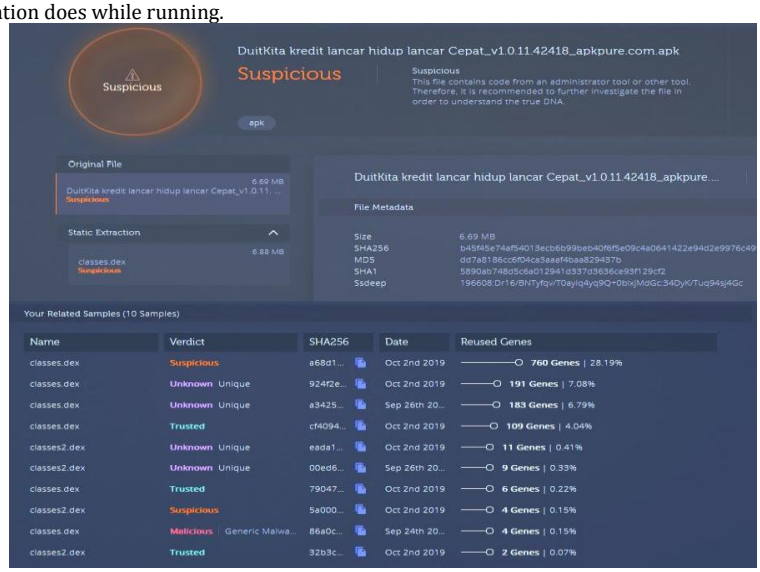


FIG 5. ANALYSIS OF GENETIC ACTIVITY WITH INTEGERS

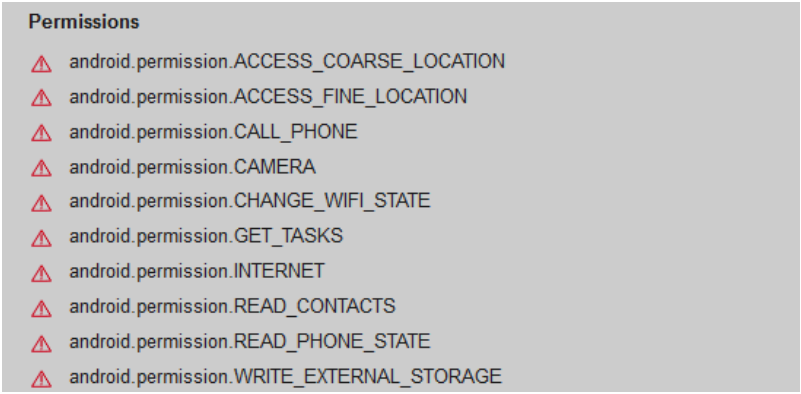


FIG 6. VIRUSTOTAL PERMISSION ANALYSIS

Based on the analysis of Fig 5 and Fig 6, it turns out that this illegal fintech application contains malware activity that was deliberately created by fintech administrators to be able to retrieve more data from fintech customers. This activity can be said to be illegal because the application vendor can open complete information / files from the customer's personal data. The conclusion of the dynamic analysis results can be shown in Table 3. In Table 3 it can be shown the comparison between fintech applications in terms of the extent to which the application is able to retrieve data / information from fintech users.

Permissions in a system are granting application permissions to the information and data on the Smartphone. From Table 3 it is known that all fintech applications request permission to read storage on a Smartphone, namely the READ_PHONE_CONTACTS permission. In addition, there is also a request for permission to read the telephone contact list stored on a Smartphone, namely READ_CONTACTS. It can be concluded that the information data stored on the Smartphone can be accessed by the fintech vendor / administrator, when the application is installed on the Smartphone. So that potentially, information data that should not be needed for loan application requirements can be taken by illegal fintech vendors.

5. Conclusions

From this research it can be concluded that:

a. An illegal online or fintech loan application makes it easy to transact with a lot of personal data required for registration. In addition, eliminating Video Calls as one of the requirements to replace direct verification with prospective customers as required by the Financial Services Authority (OJK) makes fintech applications rent for misuse of personal data.

b. It is easy for fintech vendors / administrators to retrieve customer data in addition to the data entered when registering fintech. This is evident from the fintech Android application Permission. All application samples provide

IOCSPUBLISHER

Enrichment: Journal of Management

journal homepage: www.enrichment.iocspublisher.org

READ_PHONE_STATE and READ_CONTACS permissions so that fintech application providers can freely monitor all contact activities on the customer's Smartphone.

6. REFERENCES

[1] Asosiasi Penyelenggara Jasa Internet Indonesia (APJII). (2020). *Infografis Penetrasi & Perilaku Pengguna Internet Indonesia*. Indonesia.
[2] Baryamureeba, V., & Tushabe, F. (2004). The Enhanced Digital Investigation Process Model. *Proceedings of the Digital Forensic Research Conference, DFRWS 2004 USA*, 1–9.
[3] Dewi Rosadi, S., & Gumelar Pratama, G. (2018). Urgensi Perlindungandata Privasidalam Era Ekonomi Digital Di Indonesia. *Veritas et Justitia*, *4*(1), 88–110. https://doi.org/10.25123/vej.2916
[4] Fisip, H. (2020, June). PROSIDING SLAMET RIYADI CONFERENCE ON PUBLIC ADMINISTRATION (SRIPA). In *PROSIDING: SLAMET RIYADI CONFERENCE ON PUBLIC ADMINISTRATION (SRIPA)* (Vol. 2, No. 1).
[5] Lin, X., Chen, T., Zhu, T., Yang, K., & Wei, F. (2018). Automated forensic analysis of mobile applications on Android devices. *Digital Investigation*, *26*, S59–S66. https://doi.org/10.1016/j.diin.2018.04.012
[6] Mark, R.-O. (2013). Information Security The Complete Reference, Second Edition.
[7] 896. Retrieved from www.it-ebooks.info/book/3340
[8] Palmer, G. L. (2001). A Road Map for Digital Forensic Research.
[9] Rahmadani, V. S., Raharjana, I. K., & Taufik, T. (2015). Penerapan Reverse Engineering Dalam Penentuan Pola Interaksi Sequence Diagram Pada Sampel Aplikasi Android. *Journal of Information Systems Engineering and Business Intelligence*, *1*(1), 25. https://doi.org/10.20473/jisebi.1.1.25-32
[10] Rosadi, S. D. (2017). Prinsip-Prinsip Perlindungan Data Pribadi Nasabah Kartu Kredit Menurut Ketentuan Nasional dan Implementasinya. *Sosiohumaniora*, *19*(3), 206– 212.
[11] Sautunnida, L. (2018). Urgensi Undang-undang Perlindungan Data Pribadi di Indonesia.
[12] Sudarmanto, E., Fitriana, A., Malau, M., Nainggolan, C. D., Zunaidi, A., Manurung, S., ... & Hidayat, G. (2021). PENGANGGARAN PERUSAHAAN.
[13] Kanun Jurnal Ilmu Hukum, 20(2), 369–384.