2023 17th International Conference on Ubiquitous Information Management and Communication (IMCOM) | 978-1-6654-5348-6/23/$31.00 ©2023 IEEE | DOI: 10.1109/IMCOM56909.2023.10035613

When social networks meet payment: a security perspective

Nivedita Singh
Computer Science and Engineering
Sungkyunkwan University
Republic of Korea
singhnivvy@g.skku.edu

Mohsen Ali Alawami
Electrical and Computer Engineering
Sungkyunkwan University
Republic of Korea
mohsencomm@skku.edu

Hyoungshick Kim
Computer Science and Engineering
Sungkyunkwan University
Republic of Korea
hyoung@skku.edu

***Abstract*—In the big data arena, opportunities and challenges are mixed. The volume of data in the financial institution is proliferating, which imposes a challenge to big data analytics to ensure safety during each transaction. Moreover, as more and more social networking sites (SNS) are integrating an inbuilt online payment system into their domain, an exponential surge in financial scams is expected in the upcoming days. These scenarios are alarming, and with the rapid growth in the daily addition of new end users and their increasing time spent on SNS, the situations become more vulnerable. With the existing trend of data mobilizations and rapid increase in volume, variety, and velocity of data being produced, big data has a significant role in detecting fraud incidents in financial transactions. However, in the framework of present followed international standards, there is a voluntary compliance obligation on domestic governing bodies, which is a significant source for such voluminous financial frauds on SNS. In order to strengthen the enforcement of international standards to combat financial transactions on SNS, the paper proposes that domestic legislation should comply with international standards with the further addition of machine learning encircled by domestic banking legislation. Eventually, this could solve the security and privacy governance difficulties arising from these financial frauds over SNS. We believe that with our approach of three-layer security i.e. by international standards, domestic legislation, and machine learning, the financial fraud arising due to the SNS payment system will be reduced to a larger extent.**

***Index Terms*—Social Networks, Online Payments, Big Data Analytics, Machine Learning**

I. Introduction

In a recent Federal Trade Commission (FTC) report, more than 95,000 people reported losing about $ 770 million to frauds initiated on social media in 2021 [1]. Social networking sites (SNS) have been a gold mine for scammers, and these losses are expected to surge exponentially as more and more new users join over the years. Jason et al. [2] discussed how profit-motivated cybercriminals target users for spam campaigns. They attract users to click on enticing posts, such as "free giveaways," to get gift cards and coupons. When a user finally clicks on the link, they are required to complete a survey before getting gifts, and thus they make an advertised video or spam-designed survey. Further, their study demonstrated that most spams happen on Facebook and Twitter.

978-1-6654-5348-6/23/$31.00 ©2023 IEEE

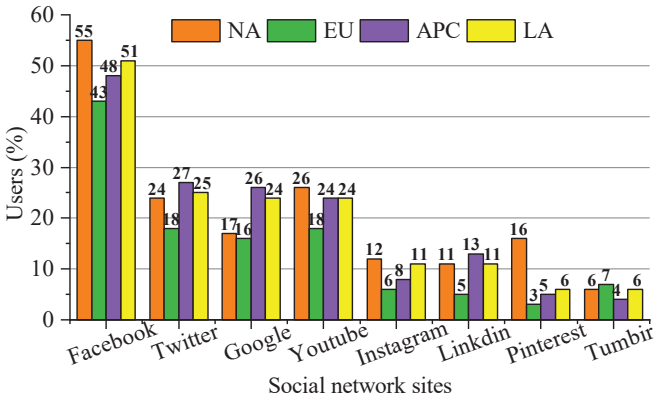

Fig. 1. SNS users continent-wise on different platforms (data in percentage).

Fig. 1 shows the continent-wise percentage of people using SNS of their own choice [3]. According to Fig. 1, Facebook captures the front position among the other social networking sites in all geolocations (in North America (NA), the European Union (EU), Asia Pacific countries (APC), and Latin America (LA). Based on these statistics, since Facebook captures the leading position in terms of social network market size, it is the first place for cybercriminals scammers too. In 2019, Facebook launched an inbuilt payment system, Whatsapp Pay was launched in 2018, and many others are in queue to launch, which motivated us to study the loopholes of the payment system integrated into SNS and find a solution to mitigate them.

Social media has been a ubiquitous part of the communications landscape and significantly contributes toward shaping a cashless and hassle-free transaction society by lucratively integrating an inbuilt online payment system on their domain. These SNS are sources of enormous big data information and produce a myriad of data that may be processed to produce intelligent information for end users [4]. These types of big data are cumbersome to model as time-critical systems due to their very complex data sources, and it consumes substantial computational time.

The messenger apps (e.g., Facebook Pay, WhatsApp Pay, Kakao Pay, etc.) have the linking of user's debit and credit

cards, and just inputting the amount and hitting the send button to send the money via SNS payment method [5]. Since these apps have the linking of debit cards and credit card information, security becomes the prime concern. Although these SNS deploy several layers of safeguards to protect public money and financial transactions information over their messenger apps, there always remains a chance that our security may be compromised. Cybercriminals and intruders can be ingenious, leading to several scams/online security breaches at big companies. Thus, it is high time to implement and adopt strong security measures to keep the end user data safe during these transactions. Pal et al. [6] discussed how the second-generation instant messaging application (SIMM) has revolutionized the mobile payment system. When mobile payment is compared to traditional online payment, the main benefit of mobile payment is its ubiquity. The end-users can use these services anywhere and at any time; therefore, it is free from all temporal and spatial constraints. However, there are several risks associated with these payments.

Several SNS providers, such as Facebook, have employed security solutions to keep their valuable end-user data safe. For example, Facebook asks users to re-enter their password once again to complete the transaction and offers protection from unauthorized access to open Facebook sessions. However, a security breach in 2018 exposed the personal information of nearly 87 million people, leading to some critical questions about the company's abilities to safeguard/protect customers' data [7], and this user data privacy breach makes an alarming situation for the SNS payment too. Banerjee et al. [8] investigated several studies to highlight the root causes of security incidents and some mitigation methods to prevent them. However, a complete solution is too far to reach. Hence there is an urgent need to safeguard the SNS payment method, and our paper aims to make this SNS payment system robust and trustworthy.

Financial security plays a prominent role for users; hence ensuring a safer transaction would be the highest priority. In this digitally connected world, payment over SNS has been a handy tool for users. However, integrating payment over SNS would raise users' concerns about new security breaches apart from other data breaches. To address this burning issue, our paper discusses the pervasive risk associated with the coupling/integration of SNS with digital payments and offers mitigation strategies to curb them to a certain extent.

Our research questions (RQs) and key contributions are summarized as follows:

- **RQ1:** What are the potential financial risks associated with SNS and the approach to mitigate them?
- **RQ2:** In the current era of increasing online financial fraud, is there any compliance between the international and domestic financial standards for SNS payment methods?

To answer RQ1, we elaborated on the different types of existing online financial fraud attacks. As SNS are easy to access by all, they act like a catalyst for financial fraud, and the situation can become grave with the integration of SNS and payment methods. The mitigation approach is explained collectively with the RQ2 answer.

TABLE I
MOST COMMON FINANCIAL FRAUD ATTACKS IN DIFFERENT REGIONS.

	NA	EU	APAC	LA
Card testing	1	5	5	2
Friendly fraud	2	2	2	1
Coupon discount refund	5	0	6	3
Phishing	3	1	1	4
Identity theft	4	0	4	0
Loyalty frauds	0	4	3	0
Account takeover	0	3	0	0
Affiliated frauds	0	0	0	5

Regarding RQ2, we emphasize that domestic and international financial norms work independently in the current SNS payment systems. Despite increasing fraud cases, this digitally connected world is welcoming the SNS payment system, which is alarming. Our key contribution lies in presenting a solution emphasizing that international standards and domestic norms must be coordinated. We propose that SNS payment methods should have securities of domestic/regional banks integrated with robust, ML-secure code. Our proposed fraud detection method avails this three-layered security to SNS payment, specifically international, domestic, and ML securities. The given algorithm considers two scams scenario, either the scammer makes all the withdrawals from the account or takes a tiny amount to check the users credentials validity. Our algorithm will check and ask users to confirm it and then proceed toward the transaction; for the same transaction, the regional banks will also provide their security to SNS users in the form of an app-specific secure keyboard and verify authenticity and legitimacy. Doing so ensures three-layer security to the SNS payment system.

II. CLASSIFICATION OF FRAUD ATTACKS

There is an urgent need to understand the fraud patterns and behavior of the various existing financial frauds occurring globally today. Based on the global fraud report 2021 [9], the major e-commerce financial fraud has been categorized as shown in Table I.

In card testing fraud, fraudsters use card testing to determine the validity of card numbers. Firstly, the scammers purchase or steal card details on the dark web or via phishing or spyware, and then they perform small purchases on the site to check card validity. Most of this type of financial fraud is happening in NA (see Table I). In the friendly fraud category, fraud is the charge-backs initiated by a customer who has not been subjected to fraudulent activity during a transaction. In LA, financial frauds are majorly happening through friendly frauds.

A scammer abuses a business's promotional campaigns in promo abuse or discount fraud. Scammers may also attempt to defraud a business by using promotion codes and discounts multiple times, or they may abuse coupons and return policies to obtain goods for free. This financial fraud category has a comparatively lower market area than other frauds.

Phishing is another cybercrime that favors deceptive emails, social networking sites, and text messages to steal confidential (financial) or personal and corporate information. These types of crimes are prevalent in the EU and APC. The phishing frauds occurring on various social media platforms are called social media phishing. In a social media phishing attack, scammers utilize our favorite social media sites like Facebook, Instagram, Twitter, and many more to steal our personal data [10]. In practice, the attacker makes a fake Facebook, Instagram, or Twitter website that looks similar to the original one and presents it before the user in the form of a link, post, or login page. The attacker steals sensitive information when users input their credentials to the fake website. Later, the attacker owns complete control of the account or withdraws all money through saved card details inside the account.

On the other hand, the intentional misrepresentation of identity details to deceive others are known as identity theft. In this type of fraud, someone else uses personal and financial details to commit fraud. Social media networks facilitate identity theft and fraud by stealing user information through these sites. Some preventive mechanisms like resetting passwords regularly, avoiding posting one's personal details, and many more exist; however, security breach is still a concern.

Loyalty fraud, also known as rewards fraud or points fraud, occurs when fraudsters exploit loyalty programs for personal gain. Account takeover, another type of fraud, is a form of identity theft. In this type of fraud, when a cyber attacker gains control of a legitimate account, the attackers can launch various attacks, such as internal phishing, supply-chain phishing, BEC-style attacks, and many more. The next financial fraud, affiliate fraud, is a type of advertising fraud that includes any fraudulent activity executed for the motive of fraudulently collecting commissions from an affiliate marketing program.

Out of the major financial fraud, SNS has become a one-stop platform for scammers to access personal details and decode financial information quickly. Like, in card testing frauds, scammers try to steal the user's card information and validate the authenticity for their purpose. Big data analytics are being used for social media marketing campaigns. In other words, big data is used by marketers as a fuel that energizes their digital campaigns toward success. Big data analytics helps marketers better understand their online communities and predict their behaviors so they can perform personalized services as well as quickly. Big data helps to make a robust decision by taking the volume of data through social media. This is one side of big data's role in social media. However, as every coin has two sides (i.e., advantages and disadvantages), the massive size of social media data helps scammers, too, to make vital decisions to decode their details and perform illegitimate actions. Therefore every security researcher has an obligation to find the best solution out of the disadvantages of social media big data analytics. When we think about making the financial system robust and trustworthy, there are many benefits of using big data. Big data helps banks to make their offers beyond the typical bank credit card and debit card, transforming digital payments and making payments more secure and straightforward for their customers. The benefits of big data analytics for business are not only for financial and retail, but this big data analytics improves work efficiency, better performance, and productivity for the banking organization. Through this voluminous and valuable information, the answer to every security-related question can be solved. The data should be analyzed thoroughly to get insights, and necessary steps should be raised based on this.

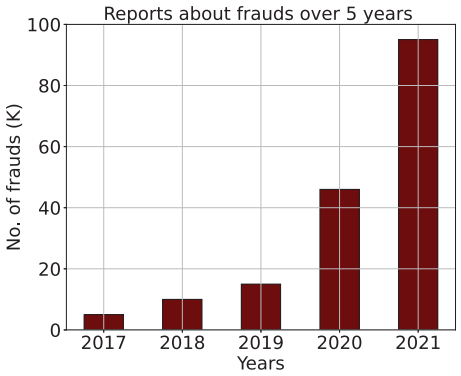

Fig. 2. Statistics based on fraud reports directly by FTC indicating a monetary loss, identifying through social media platforms.

Out of many available solutions, security is still a big concern. Since the SNS is open to all, it makes the financial system more fragile, which is why every year, financial fraud over social media increases exponentially, as shown in Fig. 2. The classification of fraud attacks shown in Table I gives a quick view of financial fraud's behavior, pattern, and occurrence rate. This classification turns the design of the solution strategy for the future robust model. For example, in Facebook Pay, the payment can be made either by linking debit/credit card details or by PayPal; if in any unfortunate circumstances, the attacker performs the phishing to an account, it can be disastrous.

Why is the SNS more prone to scams? The simple and easy answer is its independence and lack of coordination between international and domestic standards. This increasing rate of fraud on social media platforms warns us of the future havoc, and this alarming situation motivates us to avail practical and best solutions. Since the integration of SNS and online payment is new, it is expected to accelerate financial scams further. Eventually, this is the prime time we must sincerely find the loopholes in the SNS payment system and make the concrete decision to safeguard financial transactions over SNS. To make the financial system robust, we need to strengthen the standards and technical loopholes to reduce the emerging new arena of financial fraud. Our paper aims to draw attention to the upcoming havoc and mitigate it to a larger extent.

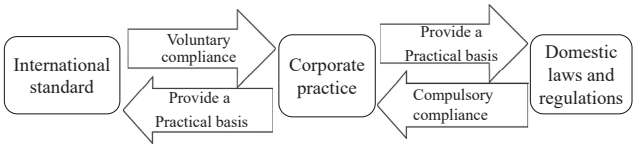

Fig. 3. Relationships showing international standard and domestic norms.

III. Discussion

A. No more secrets in the big-data era – A privacy risk

Certainly, SNS, such as Facebook, Instagram, Twitter, etc., has changed how people communicate with each other [11]. However, they have also opened up the secrets of their financial status, which invites the scammers to a more significant extent. In numerous cases, security breaches have been identified due to personal internet of things (IoT) devices when the end user sometimes has remained logged in. Scammers steal useful information, which increases the risk of financial vulnerabilities. These financial vulnerabilities are getting more prone with the evolution of more sophisticated electronic devices [12]. Thus there is an urgent need to make our electronic devices smarter to get logged out after a specific predefined time, as in banking systems.

B. Lack of uniform norms and legislation

Major SNS owners are restricted to a specific region of the world. However, their services are distributed all across the globe. For instance, the IT experts of Facebook sitting at the headquarter in the USA handle the backhand operation of an end user's account enjoying social media in some parts of Kenya or Ghana.

As shown in Fig. 3, there is a mismatch between the international and the regional/domestic standards. Corporate practices enjoy voluntary compliance with international standards, while domestic laws are mandatory. Thus, security relies on the mercy of the relationship between voluntary and mandatory compliance. The financial transactions primarily abide by the domestic norms of that nation; however, in the absence of domestic norms being followed, whenever a financial transaction occurs over SNS, it is guaranteed that there would be a mismatch between the international norms/standards. This becomes the hot spot for scammers for a security breach (Fig. 3.) [13]. It is often in the news that local financial governing bodies refuse to handle the scams/frauds that occur over SNS as these frauds are out of their jurisdictions. It is primarily due to a lack of uniform or cooperative standards for financial losses. Our paper addresses this critical issue and proposes a method to combat it.

C. Technical loopholes

In the era of digital civilization, machine learning (ML) and artificial intelligence (AI) stand at the forefront of data security and privacy governance, known as technical governance. ML/AI can boost security via digital certification, authentication, secure encryption, and with the addition of additional hidden layers in deep neural networks. However, technological loopholes exist, like theft, adversarial attacks, encryption decode, secure data storage, transaction logs, endpoint validation, real-time security, data-centric security, the granularity of access controls, audits, and data provenance. Thus there is a perpetual need to upgrade and implement enhanced securities through ML/AI.

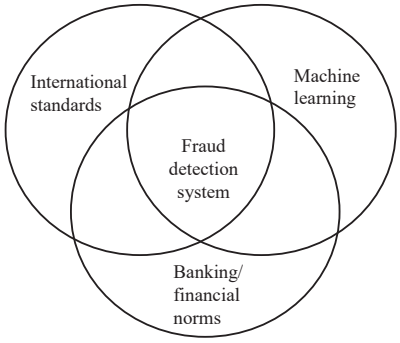

Fig. 4. Position of the proposed fraud detection system.

IV. Proposed approach

Domestic banking securities are considered to be the safest means of financial transactions due to their app-specific secure keyboard for passwords [14] and auto-logged-off features. Since SNS use their specific merchandise for financial transactions, they are more prone to security breaches. Social networking sites keep independent ownership, and the regulation of domestic laws applies to them very restrictively; thus, there is a lack of coordination between international and domestic laws. However, in the financial system, the domestic laws provide the best security measures, but the SNS has a voluntary obligation to comply with them. Thus there is an urgent need to implement a uniform financial international standard irrespective of the region. Keeping these vulnerabilities in consideration, we propose that the most effective path could be the combination of comprehensive regulation by international standards in terms of service provided by SNS and concrete implementation of financial transactions security by regional/domestic banking systems in terms of norms and technologies. In addition, machine learning will provide enhanced security. This way, our encircled fraud detection system approach will provide three-layer security to the SNS payment system (see Fig. 4).

Algorithm 1 shows the overall process of the proposed method. When a payment is initiated over SNS, the visualized data should create a unique id that should be sent to banks for cross-verification and authorization. Here, the bank should also improvise their security to that payment. On the other hand, the ML secure code also provides additional security to that payment. After getting the triple security check, the test prediction will be performed to decide whether to proceed with the further transaction or reject it.

The proposed ML system would significantly reduce payment fraud over SNS to a more considerable extent. To

Algorithm 1: Overall process of the proposed method.

Input : ID and Password to pay
Output: Secure payment

```
1  UID: User ID for payment
2  PW: User password for payment
3  SK: Secure Keyboard
4  VU: Validate URL
5  TB: Total available balance in user account
6  PA: Payment authorization
7  SA: SNS administrator
8  AT: Amount transfer
9  MLs: Machine-learning side
10 BSs: Bank security side
11 foreach user do
12     - User visits SNS website;
13     - Login to SNS Pay;
14     - Input UID and PW;
15     MLs do - Execute models → VU;
16     SA do - Encrypting → UID and PW;
17     - Get unique Id;
18     BSs do - Send unique Id → Bank;
19     - Bank → SK;
20     - Input password;
21     MLs do - Data visualizing and feature engineering;
22     - if AT >= (TB+$1) || AT <= $1 then
23         - Bank executes → PA;
24         - Bank asks user to confirm;
25         - if user accepts then
26             - Payment DONE.
27         else
28             - Payment REJECT.
29         end
30     else
31         - Payment DONE.
32     end
33 end
```

ensure better financial security, we need to consider a co-operative relationship between international-national-banking standards. In addition, implementing machine learning with these standards should boost financial transactions over SNS to a much larger extent. This approach will ensure an additional safety layer and detect fraudulent cases under international and national legislation.

V. System Methodology

The proposed methodology is presented in Algorithm 1. We assume that the SNS payment security must be three-layer security, provided by the SNS itself, the regional bank side security, and through machine learning. We represented the bank side security as an acronym of BSs, the existing security by SNS as SA, and machine learning security by the acronym MLs. In **line** 1 to 10, we have defined the various acronym used in our proposed algorithm.

To start the process, a user visits the SNS page to log in. The user enters his/her account and password. These steps are already performed by the user and administered by the SNS administrator, i.e., SA. This process is shown from **line** 11 to 13. After login to the account, the machine learning execution is performed. Here we hypothesized phishing attack fraud to provide machine learning security. We find that social media phishing is mostly performed by clicking a fake URL.

In our approach, the MLs analyze a given URL before performing the payment process shown in **lines** 14 to 15. After validating the URL, the user initiates a payment by sending his/her account to a bank. After getting the unique id, the BSs starts their security services. This process is shown from **line** 17 to 18. As it is already known, regional banks provide the best security compared to other methods, so we assume that banking standards will be applied to our system. The user will get the app-specific secure keyboard to re-enter the password. The user will do so as shown in **lines** 19 to 20. On the same side, machine learning security is running in the back end; it will collect the visualized data and do some feature engineering like the total amount needed to be transferred, the destination details authenticity, and many more. In short, it will collect the user data and do some security engineering. If everything goes well, the payment processing will start **line** 21 to 26.

Next, after analyzing some common cyber fraud patterns, there are two hypotheses: the scammer will either withdraw the whole amount from the victim's account or withdraw a small Penny to check credential validity. These are both fraud patterns we are taking to assume in our paper. If these two hypotheses appear in **line** 22, then the banking authorization action will be performed by BSs. In the current scenario, payment authorization is being performed in many ways. It depends on their region. We assume three basic authorization techniques, i.e., knowledge factor, inference factor, and user location. In knowledge factor authorization, banks have security questions like what is your pet name? and so on. The inference factor accepts bio-metric recognition like voice messages, iris recognition, and many more. In user location authentication, banks need reliable location confirmation. The transaction may be rejected if a user's location does not match a record in their bank file. Therefore, the next step is to provide banking side authorization shown in **lines** 23 to 25; if banks get a positive response from the users, then the next step is to proceed with the payment processing shown in **line** 26; otherwise, it will be declined in case of failed authentication **line** 28. At last, if everything goes well in normal circumstances, the payment will be made as shown in line **line** 31, and hence the process is ended as shown in **line** 33.

VI. Conclusions and Future Work

Shortly, we will face financial fraud happening on SNS. In addition to the existing financial fraud over SNS, the integration of payment methods has further increased security concerns. Thus, our paper tries to draw attention to this

alarming situation and the loopholes that assist the scammers in performing it quickly and easily in spite of having anti-fraud technology. In this paper, we presented a suggestive approach in the form of a relationship chart and algorithm that focuses on addressing the emerging financial risks tied to SNS and payment system integration, which has brought us challenges in terms of utilizing big and multi-modal data. Our approach implies that when the domestic legislation complies with international standards by adding machine learning encircled by the domestic banking legislation, there will be a high chance of making the SNS financial transactions robust and secure. This will not only solve the security and privacy governance difficulties arising from SNS financial frauds to a more significant extent but will also make the payment system more trustworthy.

Machine learning algorithms would be the best solution to detect financial fraud and secure online financial transactions to a larger extent. Our future work will be to develop an implementation for secure payment transactions over SNS without compromising its usability.

ACKNOWLEDGMENT

This work was supported by Institute of Information & communications Technology Planning & evaluation (IITP) grants (No. 2022-0-00495 and No. 2019-0-01343) funded by the Korean government.

REFERENCES

[1] Keith B Anderson. To whom do victims of mass-market consumer fraud complain? *Available at SSRN 3852323*, 2021.

[2] Jason W. Clark and Damon McCoy. There are no free iPads: An analysis of survey scams as a business. In *6th USENIX Workshop on Large-Scale Exploits and Emergent Threats (LEET 13)*, Washington, D.C., August 2013. USENIX Association.

[3] Kelly L Gabrielsen. Instagram Is The Fastest-Growing Social Site Globally, Mobile Devices Rule Over PCs For Access.

[4] Hsinchun Chen, Roger HL Chiang, and Veda C Storey. Business intelligence and analytics: From big data to big impact. *MIS quarterly*, pages 1165–1188, 2012.

[5] Rachel Morgan Cautero. How Social Media Payments Are Changing the Way We Buy.

[6] Debajyoti Pal, Suree Funilkul, and Syamal Patra. Paying by your messaging application? a trust model. In *Proceedings of the 11th International Conference on Advances in Information Technology*, IAIT2020, New York, NY, USA, 2020. Association for Computing Machinery.

[7] Salvador Rodriguez. Facebook says hackers were able to access millions of phone numbers and email addresses.

[8] Arpita Banerjee, C Banerjee, and A Poonia. Security threats of social networking sites: An analytical approach. *network*, 13(12):16, 2014.

[9] Anonymous. 2021 Global fraud report.

[10] Anonymous. What Is Social Media Phishing?

[11] Antoine Boutet, Hyoungshick Kim, and Eiko Yoneki. What's in twitter, i know what parties are popular and who you are supporting now! *Social network analysis and mining*, 3(4):1379–1391, 2013.

[12] Xueqi Cheng, Shenghua Liu, Xiaoqian Sun, Zidong Wang, Houquan Zhou, Yu Shao, and Huawei Shen. Combating emerging financial risks in the big data era: A perspective review. *Fundamental Research*, 1(5):595–606, 2021.

[13] XinRui Wang, Wei Luo, XiaoLi Bai, and Yi Wang. Research on big data security and privacy risk governance. In *2021 International Conference on Big Data, Artificial Intelligence and Risk Management (ICBAR)*, pages 15–18. IEEE, 2021.

[14] Xinyue Liang and Jun Ma. A study on screen logging risks of secure keyboards of android financial apps. In *2022 IEEE International Conference on Software Analysis, Evolution and Reengineering (SANER)*, pages 101–111. IEEE, 2022.