Exploring bank account information of nominees and scammers in Thailand

Patsita Sirawongphatsara[1], Phisit Pornpongtechavanich[2], Pakkasit Sriamorntrakul[3], Therdpong Daengsi[3]

[1]Department of Computer Science, Faculty of Science and Technology, Rajamangala University of Technology Tawan-ok, Chonburi, Thailand
[2]Department of Information Technology, Faculty of Industry and Technology, Rajamangala University of Technology Rattanakosin, Prachuap Khiri Khan, Thailand
[3]Department of Sustainable Industrial Management Engineering, Faculty of Engineering, Rajamangala University of Technology Phra Nakhon, Bangkok, Thailand

Article Info

Article history:

Received Dec 18, 2023
Revised Mar 30, 2024
Accepted May 17, 2024

Keywords:

Cyber fraud
Fraudsters
Online banking
Online scams
Victims

ABSTRACT

In today's digital era, people heavily depend on the internet for various tasks, such as online banking and e-commerce. While online transactions offer convenience, they also expose vulnerable individuals to potential exploitation by online scammers. The analysis and inquiry presented herein rely on data sourced from ChaladOhn, a system developed by academics and law enforcement, covering the period from February 2022 to January 2023. The comprehensive investigation reveals that each case resulted in losses under 10 million Thai Baht, accumulating to a staggering 3,100 million in damages. Notably, the fraudulent activities were traced back to the top two banks in the Thai market, referred to as the first and second bank. These banks were found responsible for; i) 28.2% and 16.0% of all scam accounts, ii) 25.6% and 20.5% of all transactions, and iii) 35.7% and 14.9% of all victim losses, respectively. The results of the inquiry must be shared with appropriate organizations and regulators due to the predicted worsening of this situation. This proactive approach aims to facilitate the development, recommendation, and implementation of effective strategies to address the escalating threat of online scams.

Corresponding Author:

Therdpong Daengsi
Department of Sustainable Industrial Management Engineering, Faculty of Engineering
Rajamangala University of Technology Phra Nakhon
Pibul Songkhram Road, Bangsue, Bangkok, Thailand
E-mail: therdpong.d@rmutp.ac.th

1. INTRODUCTION

Background and significance; in the past, network security was a major concern, with attacks focusing on communication and data networks, such as man-in-the-middle (MTM) attacks [1], [2]. However, the term "cybersecurity" is now widely used, encompassing all security areas, particularly addressing threats and attacks within the internet channel. Furthermore, the advance of the internet and computer technology has led to the widespread use of computers and networks in various aspects of daily life, resulting in cyber threats and attacks becoming commonplace [3], [4]. Most people now use computers and the internet in their transactions, including for e-commerce, which is already a common practice. This is particularly true in Asia, which holds the title of the world's largest retail e-commerce market. It is predicted to generate $2,055 billion in revenue, in 2023 [5]. The coronavirus disease 2019 (Covid-19) pandemic that occurred between 2020 and 2022 is one of the factors accelerating the expansion of e-commerce, including the trend of online shopping

[6]. The convenience of online shopping allows people to shop more easily, effectively, and efficiently [6], [7]. But with the increasing number of websites for e-commerce, it is essential to be aware of phishing attempts that aim to collect sensitive information [8]-[10]. Carelessly clicking on uniform resource locator (URL) links created by attackers, user data might be stolen, including login information and monetary account details [8]. However, one issue with e-commerce is the prevalence of online frauds. It has been shown that scammers use a variety of cunning methods to obtain the personal data of their victims, including:

- Create a false identity as a bank or government representative, then phone the victim and demand personal information.
- Call or solicit victims to click on phony links that contain malware or other harmful software.
- Create listings on an e-commerce site, but fail to fulfill the victims' orders for the products.
- Request investments from the victims in phony securities that offer extremely high returns.
- Promotion of an online casino.
- Romance scams.

Once the scammers have the victims' personal information, they use it to gain unauthorized access to their bank accounts and transfer money to money mules' accounts, also known as Banshee Ma (literally, “horse accounts” in Thai), which are individuals who move or transfer illegally acquired money on behalf of another [11], [12]. The first layer of mules then passes the victims' money to the second and upper tiers of mules, as indicated in Figure 1 [13], respectively. The money will then be given to the boss who has an electronic wallet and/or a cryptocurrency wallet. Practically, all of the accounts used by scammers are those of money mules that are dispersed throughout numerous Thai banks and financial organizations.

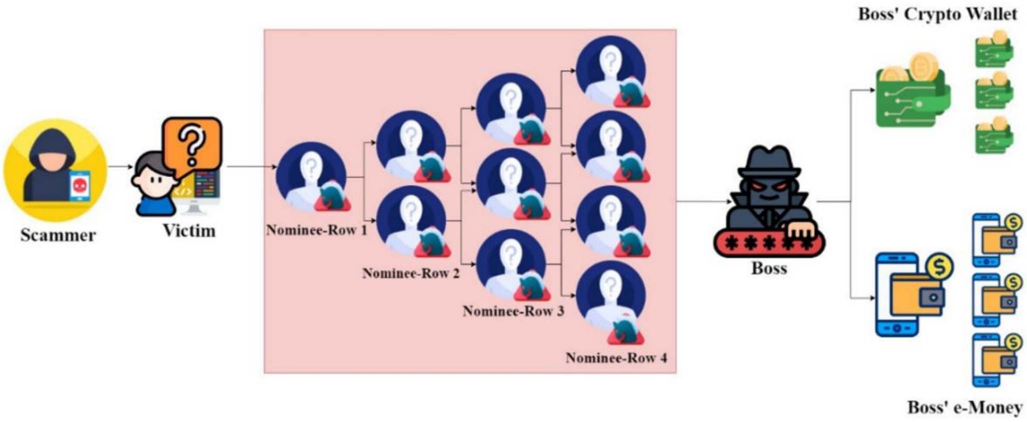


Figure 1. Typical money flow in well-organized online frauds

Unlike other prior studies that did not emphasize in bank accounts belonging to scammers and money mules, to investigate the nominees and scammers’ bank accounts used for online scams, this study used data from the ChaladOhn database, a website created in partnership with the Thai metropolitan police bureau, to examine the characteristics of the spread of money mule accounts in the group of Thai banks [14]. This article has been extended from [13]. The major contribution of this study is the disclosure of Thailand's top five banks with the most accounts belonging to money mules and scammers, as well as the loss amounts from victimization. The structure of this article is as follows: section 1 presents the background data. Next, section 2 presents previous related works. The method is then demonstrated in section 3. Sections 4 and 5 provide interesting figures and discussions to describe the findings and analyses, respectively. Finally, as in section 6, the conclusion is stated.

Online scams; as referenced in [15], scammers employ various methods to deceive individuals and perpetrate fraud, particularly targeting those who utilize bank accounts, mobile banking applications, internet banking web-applications, and credit cards. These methods include but are not limited to:

- Fake website: users can first examine the URL of the financial institution to gain confidence and prevent online attacks. Some URLs can be used to determine the nation where a website is registered; for instance, https://www.scb.co.th indicates that the website was created in Thailand. Users can verify the website information for URLs with suffixes like.com, .net, or others without country suffixes at https://www.whois.com/whois/, which reveals where that website is registered and who the owner is. When users click it, if it's phony, they will be prompted to enter extensive personal data. Users should not believe it is unusual as a result. Typically, the bank simply asks for the most basic data, like name, last name, email, and phone number.

- Fraud SMS: in this method, scammers send phony SMS messages to their victims under the guise of a financial institution, a reputable company, or a well-known phone number. However, some suspicions are obvious because the text messages frequently induce fear and apprehension in the recipients or excitement and contentment as if they will receive some in privilege or award, and they press the recipients to act quickly before their accounts expire. They may also tempt recipients to click an attached link to enter personal information in exchange for a gift. Complete information, such as a person's ID, bank account number, credit card number, birthdate, ATM code, and/or password, will be requested in fake mail. Additionally, users will reach fraudulent websites if they click the link included in the SMS.
- Fake line: in Thailand, banks or other businesses sometimes use official line profiles. As a result, scammers use this channel of contact to obtain personal data from bank customers to gain access to their bank accounts. Typically, a false line account will start by adding and welcoming people. Users can see "Add friends" at the top, indicating that they have not yet become friends with this account. In contrast, a real line account requires the user to manually add friends. Additionally, since most bank employees communicate with consumers using chatbots rather than personally, the line account is unable to initiate the first conversation with any customer. Naturally, detailed personal information may be requested during the chat, or the user may be prompted to visit a phony link, website, or application to hijack their bank account. The victim's real friend's line account can also be hacked, before requesting a loan with a false justification.
- Facebook fraud: in this instance, scammers create a phony Facebook page for a bank or other financial institution. Because it frequently resembles a legitimate Facebook page and the submitted content also appears authentic, many bank customers may not realize it is a scam if they are not paying close attention. If they look closely, though, they might be able to spot suspicious items. The fake Facebook may utilize names that are nearly identical to the genuine Facebook but contain specific indicators (e.g., commas or other uncommon characters) that may confuse the bank customer. Moreover, the fake Facebook page might only have a few hundred fans, in contrast to the millions of fans on the actual page. Additionally, every post on the phony page receiving none or a small number of likes, whereas each post on the actual page usually receives hundreds or thousands of likes.
- Spam email: in general, Thai banks don't email clients to request confidential or sensitive information (such as a customer ID or citizen ID, pin code, or essential information over email). There is no bank policy to contact a customer directly from a bank officer to ask for secret personal information or to do things that may be risky to be hacked, so customers should be aware of emails that ask them to disclose sensitive or personal information, change passwords, or click external links.
- Scam app: it is currently taking off and becoming popular among scammers. They use line or fraudulent SMS to deliver links to malicious applications that can be downloaded. They frequently use numerous offers that are scams to trick their victims, such as loans with extremely cheap interest rates. The victim will be taken directly to the program if they choose to download rather than going through the play store, App store, or Huawei app gallery. There is no application information provided for this type of application notice, such as the number of reviewers, the number of downloads, rating information, or file size.

It is imperative for users and bank clientele utilizing such applications to exercise caution, vigilance, and awareness to mitigate potential risks posed by fraudsters or scammers. Strengthening cybersecurity awareness stands pivotal in fortifying their defenses against evolving threats.

Predicted worldwide cybercrime loss; according to [4], [13], the estimated global loss from cybercrime in 2025 would be over 17.7 trillion USD (as shown in Figure 2 [13]), which is a significant increase from the estimated loss of 10.5 trillion USD in 2025 given in the cybercrime magazine. Even though the two anticipated numbers differ, they show that cybercrime is a major global problem. The estimated cost from cybercrime was based on previous cybercrime data, which also included statistics on organized crime actions by hacking groups. The damage or destruction of data lost productivity, theft of financial, intellectual, and personal data, fraud, embezzlement, and theft of money are just a few examples of the losses that can result from cybercrime [13]. Most cyberattacks target financial institutions. This reduces the number of intermediaries an attacker needs to hit to reach the target [16]. Other losses might include forensic investigation, reputational harm, and post-attack business disruption.

Overview of online scams in Thailand; online fraud has recently become a significant problem in Thailand as a result of the proliferation of fraud tactics used by scammers, such as false loan applications, phony call centers, remote access malware for smartphones, and misleading text messages. According to online police reports from March to December 2022, fraudulent listings accounted for 32.6% of all online scams, followed by misleading online employment, false online loans, online investment fraud, and scam call centers (see Table 1 [13]). This is in keeping with what was previously mentioned in [13]. The Bank of

Thailand (BOT) claimed that it continually develops and implements procedures to stop these internet scams. BOT has also worked together with the relevant authorities to put these safeguards in place to combat cybercrime. Almost twenty banks are among the financial institutions that the bank regulator has ordered to regularly update their systems to combat cybercrime and improve joint operations with the appropriate parties to prevent such crimes.

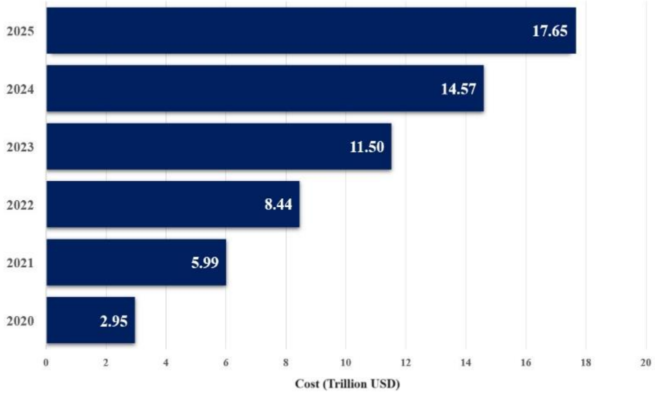


Figure 2. Estimated cost of worldwide cybercrime between 2020 to 2025

Table 1. Statistic of online police complaints

	Online sales	Online employment	Online faulty loans	Online investment	Call center
No. of cases	53,080	22,781	19,349	14,313	13,178
Percentage	32.6%	14.0%	11.9%	8.8%	8.1%
Loss value (million THB)	750	2,562	819	6,977	2,620

2. PREVIOUS RESEARCH WORKS

Following a study of prior studies, numerous articles with strong arguments and insightful debates about online fraud were discovered. They fit the description given in Table 2 (in Appendix) [6], [10], [17]-[35]. As shown in the table, those previous works demonstrate that the majority of earlier works, particularly, concentrated on the financial sector because banks are the main target of fraudsters and/or scammers when they try to steal money. As a result, it would be helpful to evaluate the data from ChaladOhn [14] to identify problems and weaknesses related to the bank sectors.

3. METHOD

The data set for this investigation was exported from the database of the ChaladOhn website, a collaborative project between the Faculty of Engineering at Rajamangala University of Technology Phra Nakhon (RMUTP) and the investigation division of metropolitan police division 8. The project was funded by the broadcasting and telecommunications research and development fund for public interest [14]. The information spans the months of February 2022 and January 2023 and was gathered from actual online fraud victims and perpetrators. However, only information related to online scammers was used in this study. That dataset of information was processed as shown in Figure 3, which is similar to the processes conducted in [13].

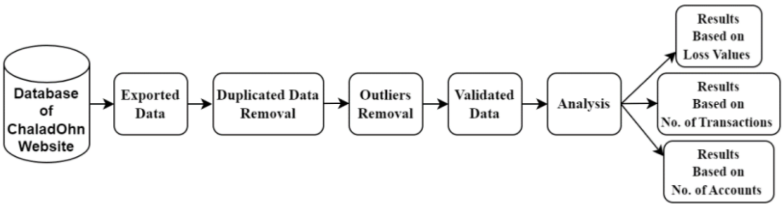

Database of ChaladOhn Website
Exported Data
Duplicated Data Removal
Outliers Removal
Validated Data
Analysis
Results Based on Loss Values
Results Based on No. of Transactions
Results Based on No. of Accounts

Figure 3. Data processing overview

The data processing as shown in the figure was started from exporting the data from the database of ChaladOhn website. Then, the duplicated data, which are duplicate information from the con artist and/or money mules with identical names and bank account numbers, was taken into consideration and eliminated. Next, the outliers, including the transactions of the loss values with less than 100 THB and more than 10,000,000 THB, were removed. Next, the validated data, which consists of more than 87,500 records, were analyzed. Lastly, the analyzed results were issued. The results are presented in the next section.

4. RESULTS

This study used data from the ChaladOhn website's database, with losses ranging from 100 THB to 10,000,000 THB. The total losses amounted to 4,685,252,172 THB, with a total of 87,943 transactions and 61,805 scammers or money mules accounts. The following three major points associated with Thai banks (hereafter called Bank1, Bank2, Bank3 instead of each bank name) are highlighted as follows:

4.1. Statistics based on loss values

Following the deletion of duplicate bank accounts, situations with a wide range of loss values were considered. Then the data associated with the number of loss values per transaction divided into five categories, for convenience when mention hereafter, that can be described as follows: i) 100-1,000 THB per transaction, or category A, ii) 1,001-10,000 THB per transaction, or category B, iii) 10,001-100,000 THB per transaction, or category C, iv) 100,001-1,000,000 THB per transaction, or category D, and v) 1,000,001-10,000,000 THB per transaction, or category E.

According to the above mentioned, the processed data obtaining from the database of the ChaladOhn website were then utilized to produce pie charts as displayed in Figures 4(a) to (e). The following details are derived from the results associated with the loss values shown in Figure 4:

- As shown in Figure 4(a), Bank1 is ranked first in category A with 26.1% of the loss values between 100 and 1,000 THB per transaction, followed by Bank2, Bank4, Bank5, and Bank6, which are ranked second through fifth, with respective loss values of 20.0%, 13.1%, 11.2%, and 8.3%.
- The position changed when category B, the loss values between 1,001 and 10,000 THB per transaction, were considered. In Figure 4(b), Bank2 is ranked first with 23.0% of the loss values, slightly higher than Bank1, which is in second place with 22.9%. Bank3, Bank4, and Bank5 are in third through fifth place, respectively, with 11.5%, 11.3%, and 9.5% of the loss values.
- On the other hand, for category C, the loss values between 10,000 and 100,000 THB per transaction, as shown in Figure 4(c), Bank1 reclaimed the top spot with 26.9% of the loss values, followed by Bank2, Bank3, Bank4, and Bank5 with 20.8%, 14.1%, 11.9%, and 8.3%, respectively.
- In Figure 4(d), among transactions involving 100,000 THB or more, or category D, Bank1 is rated first with 30.9% of the loss values, followed by Bank2, Bank4, Bank3, and Bank5, which are ranked second through fifth, with 16.6%, 12.1%, 11.7%, and 11.1% of the loss values, respectively.
- Contrary to other data, Figure 4(e) shows that for category E, the loss values between 100,000 and 1,000,000 THB per transaction, Bank1 still holds the top spot with 25.4% of the loss values, but Bank4, Bank5, Bank2, and Bank6 are surprisingly in the second to fifth positions with 21.8%, 19.8%, 10.4%, and 8.3% of the loss values, respectively.
- Lastly, the overall figure in Figure 4(f) may be seen to be identical to Figure 4(a). Bank1 is placed highest with 35.7% of the loss values, followed by Bank2, Bank4, Bank5, and Bank6 in that order, with respective loss values of 14.9%, 13.2%, 11.3%, and 8.4%.

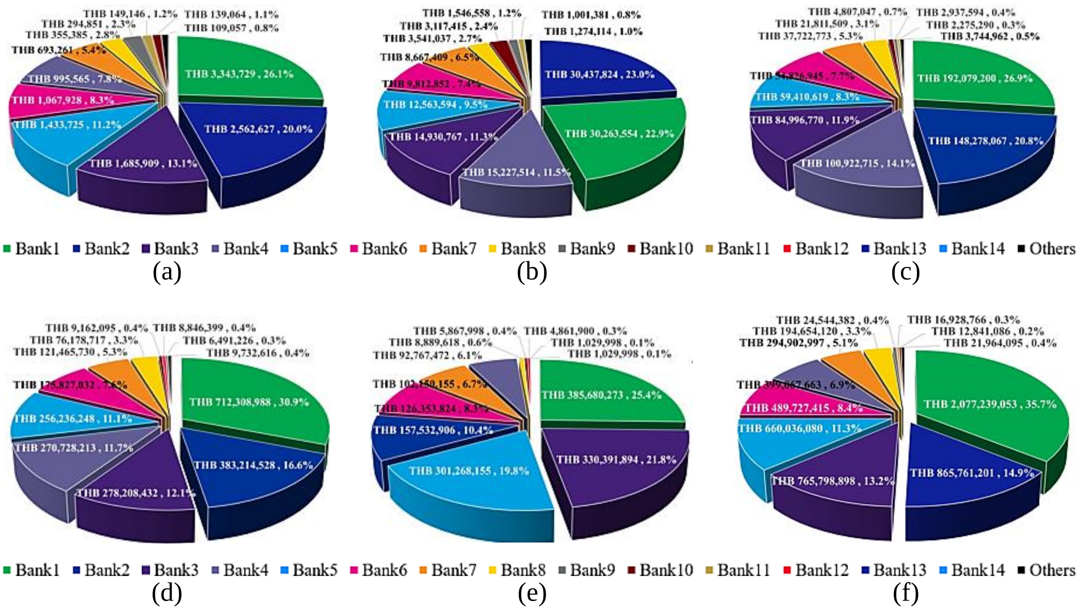
4.2. Statistics based on number of transactions

The processed data associated with the transactions obtained from the ChaladOhn website's database can be succinctly summarized by analyzing the outcomes corresponding to the transaction numbers illustrated in Figure 5. This approach offers a clear and concise overview of the data's implications.

- From Figure 5(a), it can be seen that Bank1 is placed first with 27.6% of the transactions linked with losses of between 100 and 1,000 THB per transaction, or category A, while Bank2, Bank4, Bank5, and Bank6 are ranked as the second to fifth position with 18.2%, 14.1%, 11.9%, and 8.6%, respectively.
- When transactions with loss values between 1,001 and 10,000 THB per transaction, or category B, were considered, it can be seen in Figure 5(b) that Bank1 is ranked first with 22.7% of the transactions with loss values, slightly higher than Bank2, who is in second place with 22.3%. Bank4, Bank3, and Bank5 are in third through fifth places, respectively, with 11.3%, 10.9%, and 9.9% of the loss values.
- However, as shown in Figure 5(c), for transactions associated with category C, the loss values range from 10,001 to 100,000 THB per transaction. Bank1 takes the top spot with 25.8% of the transactions associated with the loss values, followed by Bank2, Bank3, Bank4, and Bank5 with 21.8%, 14.1%, 11.8%, and 8.1%, respectively.
- The situation is comparable to Figure 5(c), for Figure 5(d), Bank1 is ranked first with 29.8% of the transactions belonging to category D, or the loss values between 100,001 and 1,000,000 THB per

transaction. Bank2, Bank3, Bank4, and Bank5 are ranked second through fifth, with 17.3%, 13.2%, 11.8%, and 9.7% of the loss values, respectively.

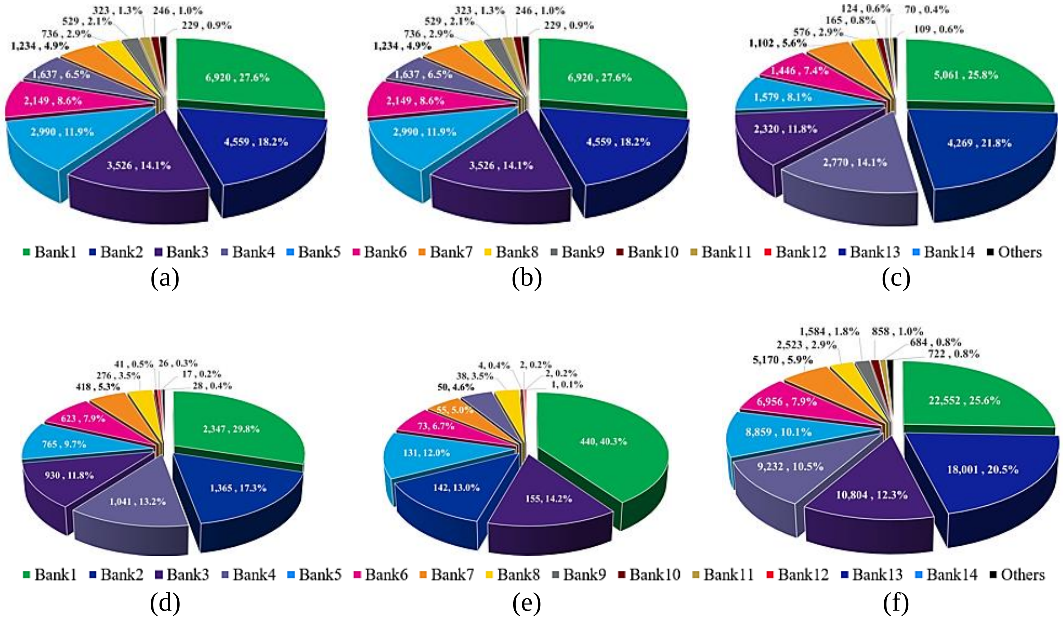
- According to Figure 5(e), the first place is still held by Bank1 with 40.3% of the loss values, but surprisingly, Bank4, Bank2, Bank5, and Bank6 are in the second through fifth places with 14.2%, 13.0%, 12.0%, and 6.7% of the loss values, respectively. For category E, the loss values between 100,001 and one million THB per transaction, it is different from other figures.
- Finally, the overall figure, shown in Figure 5(f), is comparable to Figure 5(b). With 25.6% of the transactions linked to loss values, Bank1 is rated top, followed by Bank2, Bank4, Bank3, and Bank5 in that order, with respective rankings of 20.5%, 12.3%, 10.5%, and 10.1%.



(a) (b) (c)

(d) (e) (f)

Figure 4. The statistics based on loss values (THB) per transaction by bank; (a) 100-1,000; (b) 1,001-10,000; (c) 10,001-100,000; (d) 100,001-1,000,000; (e) 1,000,001-10,000,000; and (f) overall (100-10,000,000)



(a) (b) (c)

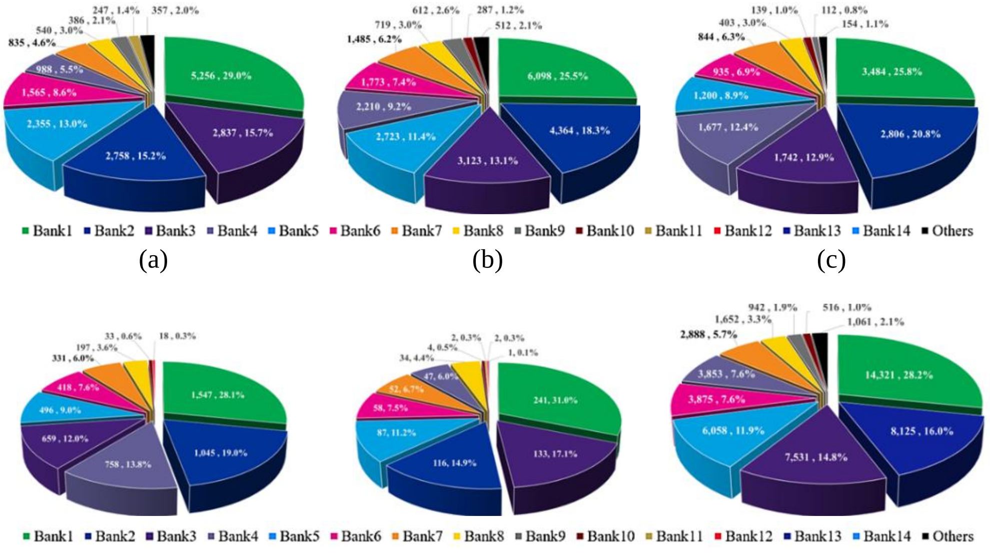
(d) (e) (f)

Figure 5. The statistics based on numbers of transactions (THB per transaction) by bank; (a) 100-1,000, (b) 1,001-10,000, (c) 10,001-100,000, (d) 100,001-1,000,000, (e) 1,000,001-10,000,000, and (f) overall (100-10,000,000)

4.3. Statistics based on numbers of accounts

In addition, the processed data derived from the results correlated with bank account numbers sourced from the ChaladOhn website's database can undergo analysis and synthesis. Subsequently, these findings can be depicted graphically, as illustrated in Figure 6, and described as follows:

- According to Figure 6(a), Bank1 is rated first with 29.0% of the bank accounts linked to category A, category A, or loss values between 100 and 1,000 THB each transaction, while Bank4, Bank2, Bank5, and Bank6 are ranked second through fifth, with 15.7%, 15.2%, 13.0%, and 8.6%, respectively.
- When bank accounts associated with category B or loss values between 1,001 and 10,000 THB per transaction were considered, it can be seen in Figure 6(b) that Bank1 is ranked first with 25.5% of the accounts associated with the loss values, higher than Bank2, which is in second place with 18.3%. Bank4, Bank3, and Bank5 are in third through fifth place, respectively, with 13.1%, 11.4%, and 9.2% of the loss values.
- However, Bank1 is in first place with 25.8% of the accounts associated with the loss values for the transactions associated with category C, or the loss values between 10,001 and 100,000 THB, as shown in Figure 6(c). This is almost the same percentage as shown in Figure 6(b), the transactions of Bank1 associated with the loss values of 1,001 to 10,000 THB. While Bank2, Bank3, Bank4, and Bank5 are in second through sixth place, respectively, with 20.8%, 12.9%, 12.4%, and 8.9%.
- In Figure 6(d), with 28.1% of the accounts linked with category B, or the loss values between 100,001 and 1,000,000 THB per transaction, Bank1 is rated first. Bank2, Bank3, Bank4, and Bank5 are listed from second to fifth with 19.0%, 13.8%, 12.0%, and 9.0% of the loss values, respectively.
- For category E, the loss values between 100,000 and 1,000,000 THB per transaction, it is like Figure 6(a), Figure 6(e) shows that Bank1 is still in first place with 31.0% of the loss values, but Bank4, Bank2, Bank5, and Bank6 are surprisingly in second to fifth place with 17.1%, 14.9%, 11.2%, and 7.5% of the loss values, respectively.
- Finally, Bank2, Bank4, Bank5, and Bank6, as shown in Figure 6(e) are rated as the second to fifth position with 16.0%, 14.8%, 11.9%, and 7.6% of the transactions connected with the loss values, respectively. Bank1 is placed first with 28.2% of the transactions related to the loss.



(a) (b) (c)

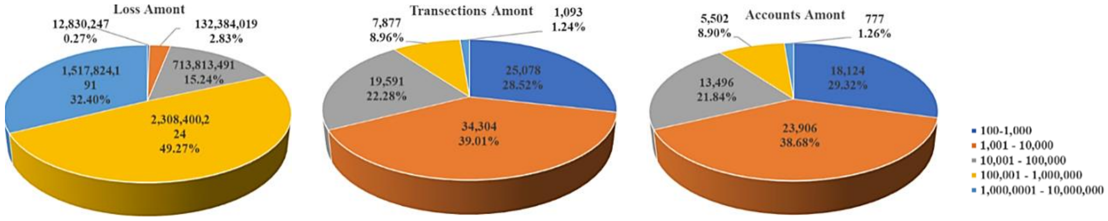
(d) (e) (f)

Figure 6. The statistics based on numbers of accounts (THB per transaction) by bank; (a) 100-1,000; (b) 1,001-10,000; (c) 10,001-100,000; (d) 100,001-1,000,000; (e) 1,000,001-10,000,000; and (f) overall (100-10,000,000)

4.4. Comparison among five categories of loss value per transactions

According to Figures 4 to 6, the ranges of loss value per transaction were divided into five groups: A (100–1,000 THB per transaction), B (1,001–10,000 THB per transaction), C (10,001-100,000 THB per transaction), and E (1,000,001–10,000,000 THB per transaction). As a result, in this subsection, those five categories-which are related to lost values, transactions, and bank accounts-were taken into account and presented as follows:

- According to loss values, as shown in Figure 7(a), category D (100,001-1,000,000 THB per transaction) occupies the largest portion of the graph with 49.3% (2,308,400,224 THB), followed by category E in second place with 32.4% (more than 1.517 billion THB), Category C in third place with 15.2% (more than 713 million THB), and category B in fourth place with 2.8% (more than 132 million THB). The smallest section, category A, only makes up 0.3% of the chart (or 12.8 million THB).
- In Figure 7(b), the largest category by number of transactions is category B, which accounts for 39.0% (34,304 transactions). Categories A and C are in second and third place, respectively, with 28.5% (25,078 transactions) and 22.3% (19,591 transactions). While category D and E make up the fourth and final portions with respective percentages of 9.0% (7,877 transactions) and 1.2% (1,093 transactions).
- By bank accounts, Figure 7(c) is comparable to Figure 7(b), category B occupies the largest percentage, accounting for 38.7% (23,906 accounts), while category A and C come in second and third, accounting for 29.3% (18,124 accounts) and 21.8% (13,496 accounts), respectively. While the fourth and final portions are category D transactions between 100,000 and 1,000,000 THB and category E, with rates of 8.9% (5,502 accounts) and 1.3% (777 accounts), respectively.



(a) (b) (c)

Figure 7. Portion of each category assiciated with total; (a) loss values (b) transactions (c) accounts

5. DISCUSSION

The findings outlined in section 4, which include statistical analyses of loss values, transaction volumes, and account numbers, reveal noteworthy insights. These insights encompass comparisons across loss value per transaction categories, offering valuable avenues for discussion and analysis as follows:

- From Figures 4 to 6, Bank1 and Bank2 were ranked top and second overall, respectively, highlighting the reliability of the findings. These statistics also show that both banks are the most frequently used in online fraud and scams.
- Bank1 and Bank2 accounted for roughly 28.2%+16.0%=44.2% of scammer accounts, which is more than 22,000 accounts, as well as 25.6%+20.5%=46.1% of all transactions, which is more than 40,500 transactions, and 35.7%+14.9%=50.6% of all losses, which is more than 2,900 million THB.
- Overall, Bank4 is the third in terms of loss values (13.2%), transactions (12.3%), and number of accounts (14.8%).
- Overall, Bank5 is the fourth place when considering the transactions (11.3%) and the number of accounts (11.9%) but ranked the place fifth when it comes to the number of transactions (10.1%).
- It is surprising that while KKP is placed third in Figure 5(f) based on the volume of transactions (10.5%), it drops to sixth place in Figures 4(f) and 6(f), which take loss values (6.9%) and account volume (7.6%) into account. However, despite Bank6 placing fifth overall in terms of loss value (8.4%) and fraudulent accounts (7.6%) (see Figures 4(f) and 6(f), respectively), it placed sixth when considering the volume of transactions (7.9%), as seen in Figure 5(f).
- Category D (100,001-1,000,000 THB per transaction) and category E (1,000,001-10,000,000 THB per transaction) occupy 49.3%+32.4%=81.7%, or more than four-fifths of the chart, according to Figure 7(a). That indicates that category D has the greatest economic impact.
- Since category B occupies about 39.0% of Figure 7(b) and 38.7% of Figure 7(c), which are linked with transactions and accounts, respectively, one can observe that they are consistent with one another. Additionally, category A and B cover 28.5%+39.0%=67.5% of the transactions in Figure 7(b). If a victim transfers money just once, it might be inferred that categories A and B account for the majority of the victims.
- With more attention paid to categories A and B in Figures 7(b) and (c), it can be seen that there are 1.41 transactions per account, or (25,078+34,304)/(18,124+23,906). This number is not huge, but if banks cut back on the number of accounts used by scammers or money launderers, the volume of transactions and loss amounts will also go down.

- In all, focused on Bank1 in Figures 4(f), 5(f), and 6(f), there were 22,552 total transactions, 14,321 total accounts, and a total loss value of 2,077,239,053 THB. The average is 145.048.46 THB per account or 92.108.86 THB for each transaction. These are large numbers. This implies that financial victimizations are not recorded or complained about.
- Based on the data, the top six banks involved in online scams, Bank1, Bank2, Bank4, Bank5, Bank6, and Bank3, should collaborate closely with BOT, the Thai bank regulator, to develop new measures against money mules and the money laundering process (e.g., do not permit a new bank customer to enable a new online account without money as some banks do). To curtail and halt illicit transactions, cyber frauds, and online scams in general, the government should also think about drafting and passing new legislation.
- It should be mentioned that only the data from ChaladOhn's database from February 2022 to January 2023 were the subject of this study's investigation and analysis. The loss values shown in this article (ranging from 100 to 1,000,000 THB per transaction) cannot be taken to be an accurate representation of all loss values due to online fraud in Thailand. The percentage of money mule accounts in Thailand overall that are scam accounts is likewise unknown.
- The advancement beyond the previous work [13] was investigated, focusing not only on statistics based on numbers of scam bank accounts and loss values by bank, but also on statistics based on transactions.
- The approach in this study might be applied to other countries if they have an available database that is like the ChaladOhn database. Therefore, the findings from that analysis can be utilized for new measures or regulations.

6. CONCLUSION

This study has investigated the ChaladOhn database, examining 89,000 unlawful transactions in Thailand with average losses of less than 10 million THB. It has been determined that from February 2022 to January 2023, internet scam losses totaled more than 3,100 million THB. Furthermore, it was discovered that Bank1 was the most frequently used by scammers, accounting for 28.2%, 25.6%, and 35.7% of all bank accounts, transactions, and total loss value, respectively, while Bank2 came in second place with 16.0%, 20.5%, and 14.9% of all accounts, transactions, and total loss value, respectively. Therefore, the BOT and/or the Thai bankers' association should consider this fact along with other findings in this study, then propose and enforce appropriate regulations and measures to prevent money laundering and reduce illegal transactions as a result of online scamming, especially targeting Bank1 and other financial institutions in the top lists. These measures and regulations should aim to prevent money laundering and reduce online scamming. However, only the data from the ChaladOhn system is considered in this analysis. In the future, data from other trustworthy sources should also be considered, followed by in-depth research and investigation to enable regulators to better understand the behavior of online scams, and finally, the proposal and enforcement of new effective measures against this category of organized crime.

ACKNOWLEDGEMENTS

Thanks to Rajamangala University of Technology Tawan-ok, Rajamangala University of Technology Rattanakosin, and Rajamangala University of Technology Phra Nakhon for their support in this research. Special thanks to the Broadcasting and Telecommunications Research and Development Fund for Public Interest (BTFP) for funding the ChaladOhn project (Contract no. B63-2-(2)-007). Finally, gratitude is extended to Mr. Peter Bint for English editing.

APPENDIX

Table 2. Previous works

Ref.	Findings
[6]	Covid-19 has accelerated e-commerce and digital consumption. The epidemic has increased first-time internet buyers and online merchant visits. Consumer behavior has changed, with certain modifications predicted to remain post-pandemic. Virtual operations seem effective, but consumer culture needs further adjustment. Thus, in reaction to market transformation, managers should create creative digital sales strategies.
[10]	A machine learning model was created to predict phishing simulation success. It was found that users never supplied credentials during anti-phishing training (68.1%), 45.8% of users did not clicked on phishing simulators. It was also found in the study that individual training is more beneficial than group training.
[17]	They suggested a method that can identify phishing phone calls by listening to the discussion between the victim and the fraudster. They conducted an intent analysis of call transcripts using a variety of machine-learning approaches. According to their research, CNN-based models have a peak accuracy of 97.21%.
[18]	This study found that anxiety, stress, and risk-taking are factors that affect the effectiveness of Covid-19 specific themed phishing scams, while educational background has a significant impact on the frequency of these attacks.

Table 2. Previous works (*continued*)

Ref.	Findings
[19]	This study reveals heightened susceptibility to phishing scams when users face time constraints in responding to emails. The increased risk is attributed to real-world issues such as excessive workloads, tight deadlines, and elevated email volume during the Covid-19 pandemic.
[20]	They did a thorough analysis of the numerous frauds that occurred online or through mobile banking applications and services, concentrating on the rise in online fraud instances involving the banking sector. They concluded that education campaigns are required to stop or minimize online fraud.
[21]	They investigated fraud (via the Punjab National Bank case) to pinpoint the contributing reasons. They suggested that all financial institutions watch every employee closely and that the procedures for markers and checkers be enhanced.
[22]	By adopting a more dependable and effective login procedure using a variety of approaches and applications (e.g., third-party apps, IP address, region (location) to log in, API, OTP), they recommended a design change to the current banking system. This is done to lessen the likelihood that customers' sides will experience security breaches.
[23]	Biometric authentication is one of the methods that can be used to increase security, according to Siddiqui. In addition to PIN authentication and verifications, biometric authentication methods like fingerprints, iris scans, palm scans, and even voice recognition can be used to prevent ATM fraud and enhance the security of other financial transactions.
[24]	They suggested locality-based machine learning be used in conjunction with domestic legislation that complies with international norms. This three-layer security method, which combines domestic law, international standards, and machine learning, could address the security and privacy concerns brought on by financial fraud involving social networking sites (SNS) to decrease financial fraud.
[25]	They performed the study and showed how clients of online banking services can suffer as a result of financial companies' violation of precautionary norms. As a result, it's important to safeguard clients from fraud or exploitation by passing the proper legislation and upholding the law.
[26]	To spot master card fraud, they deployed three machine learning algorithms. They indicated that the bank may use their techniques, including Isolation Forest, to identify credit card scams. However, additional steps should be taken.
[27]	They demonstrated how the legislator in the UAE offers decentralized protective implementation across various related laws, which is a significant step toward innovative legislative solutions to offer state-of-the-art protection for UAE consumers during online transactions against false deceptive advertisements.
[28]	They offered an innovative approach that focuses on exploiting the traits of economic and corporate crimes, such as online shopping fraud committed by dishonest customers. Short-term apartment rentals and the use of deferred payment schemes were found to be two important indicators in Japan. They also discovered that scammers frequently purchase products that can be quickly sold for cash.
[29]	They performed an analysis using the information from the ChaladOhn website's database [3]. They discovered that the victims' average age ranged from 20 to 39. Therefore, it is crucial to spread knowledge and provide education about technical literacy to young Thais.
[30]	They employed a method of online surveying about cybercrime and cyber victimization. Identity fraud, cyber harassment, and cyberattacks are the main trends of cyber victimization in the UAE, according to the data. Strong correlations between online behavior, online time, and cyber victimization have been shown by the evidence. The chance of becoming a cyber victim was found to be related to technological guardianship, online behavior and usage, computer skill, time spent online, region of residence, and gender, according to a logistic regression study.
[31]	They carried out research about a system to identify account cloning in online social networks. Twitter Crawler, Attribute Extractor, and Cloning Detector are the three components that make up the framework. As a case study, Twitter was used. The framework has an average accuracy of 80% in identifying whether the posts were phony or real. While decision trees produced the best categorization results, it was discovered.
[32]	They demonstrated the effectiveness of supervised learning in neural network computations, resulting in increased accuracy with a wide scope for misrepresentation and a lower rate of false alarms. Well-trained ANNs show their potential in this area by mimicking the way neurons work in the human brain. Machine learning is used for false detection, utilizing user transaction records to examine e-commerce-related behavior patterns.
[33]	They researched on designing a Twitter threat detection model using semantic networks developed called DetThr, the model was developed to detect threatening and fraudulent tweet messages. it can be used to reduce crime that will occur in the future.
[34]	This study unveils the risks associated with online shopping, emphasizing negative consumer perceptions. Additionally, it raises awareness about cybersecurity issues, offering insights into safeguarding against data breaches and attacks, covering methods such as adware and phishing for both online shoppers and merchants.
[35]	This study utilized structural equation modeling on data from a survey of 11,534 users. The results revealed that low self-control, demonstrated by propensities for risky investments and habitual online activities (e.g., shopping and opening emails from unknown sources), predicted susceptibility to Internet scams. Moreover, falling victim to scams is correlated with greater online privacy concerns, prompting individuals to adopt more privacy protection measures.

REFERENCES

[1] S. A. M. Al-Juboori, F. Hazzaa, Z. S. Jabbar, and S. Salih, “Man-in-the-middle and denial of service attacks detection using machine learning algorithms,” *Bulletin of Electrical Engineering and Informatics (BEEI)*, vol. 12, no. 1, pp. 418-426, 2023, doi: 10.11591/eei. v12i1.4555.

[2] H. I. Nasser and M. A. Hussain, “Provably curb man-in-the-middle attack-based ARP spoofing in a local network,” *Bulletin of Electrical Engineering and Informatics (BEEI)*, vol. 11, no. 4, pp. 2280-2291, 2022, doi: 10.11591/eei. v11i4.3810.

[3] J. R. Alzghoul, E. E. Abdallah, and A.S. Al-Khawaldeh, “Fraud in online classified ads: strategies, risks, and detection methods: a survey,” *Journal of Applied Security Research*, pp. 1-25, 2022, doi: 10.1080/19361610.2022.2124328.

[4] T. Daengsi, P. Pornpongtechavanich, and P. Wuttidittachotti, “cybersecurity awareness enhancement: a study of the effects of age and gender of thai employees associated with phishing attacks,” *Education and Information Technologies*, vol. 27, no. 4, pp. 4729-4752, 2022, doi: 10.1007/s10639-021-10806-7.

[5] Statista, “Total retail e-commerce revenue worldwide in 2023, by region,” Statista Research Department, Feb 8, 2024. [Online]. Available: https://www.statista.com/forecasts/1117851/worldwide-e-commerce-revenue-by-region, (Accessed 8 Aug. 2024).

[6] R. Y. Kim, “The impact of COVID-19 on consumers: preparing for digital sales*,” IEEE Engineering Management Review*, vol. 48, no. 3, pp. 212-218, 2020, doi: 10.1109/EMR.2020.2990115.

[7] N. S. Zaini *et al*., “Phishing detection system using machine learning classifiers,” *The Indonesian Journal of Electrical Engineering and Computer Science (IJEECS),* vol. 17, no. 3, pp. 1165-1171, 2020, doi: 10.11591/ijeecs. v17.i3. pp1165-1171.

[8] M. S. I. Prottasha, M. Z. Rahman, A. K. Hossain, S. F. Mou, M. B. Ahmed, and M. S. Kaiser, “Vote algorithm based probabilistic model for phishing website detection,” *The Indonesian Journal of Electrical Engineering and Computer Science (IJEECS)*, vol. 28, no. 3, pp. 1582-1591, 2022, doi: 10.11591/ijeecs.v28.i3.pp1582-1591.

[9] M. Sánchez-Paniagua, E. Fidalgo, E. Alegre, and R. Alaiz-Rodríguez, “Phishing websites detection using a novel multipurpose dataset and web technologies features,” *Expert Systems with Applications*, vol. 207, pp. 118010-118025, 2022, doi: 10.1016/j.eswa.2022.118010.

[10] T. Sutter, A. S. Bozkir, B. Gehring, and P. Berlich, “Avoiding the hook: influential factors of phishing awareness training on click-rates and a data-driven approach to predict email difficulty perception,” in *IEEE Access*, vol. 10, pp. 100540-100565, 2022, doi: 10.1109/ACCESS.2022.3207272.

[11] M. I. Abdul Rani, S. N. F. Syed Mustapha Nazri, and S. Zolkaflil, “A systematic literature review of money mule: its roles, recruitment and awareness,” *Journal of Financial Crime*, vol. 31, no. 2, pp. 347-361, 2024, doi: 10.1108/JFC-10-2022-0243.

[12] M.I. A. Rani, S. Zolkaflil, and S. N. F. S. M. Nazri, “The trends and challenges of money mule investigation by Malaysian enforcement agency,” *International Journal of Business and Technopreneurship*, vol. 13, no. 1, pp. 37-50, 2023.

[13] T. Daengsi, P. Sirawongphatsara, P. Pornpongtechavanich, and K. Arunruangsirilert, “Analyzing bank account information of nominees and scammers in Thailand: insights from ChaladOhn website data,” *2023 International Conference on Digital Applications, Transformation & Economy (ICDATE),* Miri, Sarawak, Malaysia, 2023, pp. 1-5, doi: 10.1109/ICDATE58146.2023.10248609.

[14] T. Daengsi *et al*., “Chaladohn: website for avoiding of online shopping scams in Thailand,” *2022 IEEE 12th Symposium on Computer Applications & Industrial Electronics (ISCAIE)*, Penang, Malaysia, 2022, pp. 149-152, doi: 10.1109/ISCAIE54458.2022.9794538.

[15] SCB Banking, “Catching online scammers: SMS- LINE–Website-Facebook App,” 2023. [Online]. Availbale: https://www.scb.co.th/en/personal-banking/stories/tips-for-you/fake-sms.html. (Accessed 8 Aug. 2024).

[16] A. Zimba, “A Bayesian attack-network modeling approach to mitigating malware-based banking cyberattacks,” *International Journal of Computer Network and Information Security*, vol. 14, no. 1, pp.25-39, 2022, doi:10.5815/ijcnis.2022.01.03.

[17] N. Kale, S. Kochrekar, R. Mote, and S. Dholay, “Classification of fraud calls by intent analysis of call transcripts,” *2021 12th International Conference on Computing Communication and Networking Technologies (ICCCNT*), Kharagpur, India, 2021, pp. 1-6, doi: 10.1109/ICCCNT51525.2021.9579632.

[18] H. Abroshan, J. Devos, G. Poels, and E. Laermans, “COVID-19 and phishing: effects of human emotions, behavior, and demographics on the success of phishing attempts during the pandemic,” *IEEE Access*, vol. 9, pp. 121916-121929, 2021, doi: 10.1109/ACCESS.2021.3109091.

[19] M. Butavicius, R. Taib, and S. J. Han, “Why people keep falling for phishing scams: The effects of time pressure and deception cues on the detection of phishing emails,” *Computers & Security*, vol. 123, pp. 102937-102946, 2022, doi: 10.1016/j.cose.2022.102937.

[20] P. Datta, S. Tanwar, S. N. Panda, and A. Rana, “Security and issues of m-banking: a technical report,” *2020 8th International Conference on Reliability, Infocom Technologies and Optimization (Trends and Future Directions) (ICRITO)*, Noida, India, 2020, pp. 1115-1118, doi: 10.1109/ICRITO48877.2020.9198032.

[21] G. Singh, S. Srivastav, A. Gupta, and V. Garg, “An analysis of financial fraud through PNB bank scam and its technical implications,” 2020 *International Conference on Computation, Automation and Knowledge Management (ICCAKM)*, Dubai, United Arab Emirates, 2020, pp. 436-442, doi: 10.1109/ICCAKM46823.2020.9051500.

[22] K. Sharma, Y. Goyal, D. Jain, and K. Khanna, “Advanced bank security and management system,” *2022 IEEE 7th International conference for Convergence in Technology (I2CT),* Mumbai, India, 2022, pp. 1-4, doi: 10.1109/I2CT54291.2022.9825468.

[23] A. T. Siddiqui, “Biometrics to control ATM scams: a study,” *2014 International Conference on Circuits, Power and Computing Technologies [ICCPCT-2014],* Nagercoil, India, 2014, pp. 1598-1602, doi: 10.1109/ICCPCT.2014.7054755.

[24] N. Singh, M. A. Alawami, and H. Kim, “When social networks meet payment: a security perspective,” *2023 17th International Conference on Ubiquitous Information Management and Communication (IMCOM)*, Seoul, Korea, Republic of, 2023, pp. 1-6, doi: 10.1109/IMCOM56909.2023.10035613.

[25] C. J. Rawandale, M. M. Deshpande, and V. P. Rajadhyaksha, “Banking on online banking”, *2018 International Conference on Advances in Communication and Computing Technology (ICACCT)*, Sangamner, India, 2018, pp. 240-244, doi: 10.1109/ICACCT.2018.8529572.

[26] P. Roy, P. Rao, J. Gajre, K. Katake, A. Jagtap, and Y. Gajmal, “Comprehensive analysis for fraud detection of credit card through machine learning,” 2021 *International Conference on Emerging Smart Computing and Informatics (ESCI)*, Pune, India, 2021, pp. 765-769, doi: 10.1109/ESCI50559.2021.9397029.

[27] T. A. R. Kameel, M. E. Kandeel, and M. A. Alkrisheh, “Consumer protection from misleading online advertisements an analytical study in UAE Law,” *2022 International Arab Conference on Information Technology (ACIT)*, Abu Dhabi, United Arab Emirates, 2022, pp. 1-8, doi: 10.1109/ACIT57182.2022.9994108.

[28] K. Yoshida, K. Tsuda, S. Kurahashi, and H. Azuma, “Online shopping frauds detecting system and its evaluation,” *2017 IEEE 41st Annual Computer Software and Applications Conference (COMPSAC)*, Turin, Italy, 2017, pp. 649-653, doi: 10.1109/COMPSAC.2017.182.

[29] T. Daengsi, P. Pornpongtechavanich, P. Sirawongphatsara, T. Thimthong, and N. Sukniyom, “a study of online scams associated with age, gender and loss of value in Thailand,” 2022 *International Conference on Data Analytics for Business and Industry (ICDABI),* Sakhir, Bahrain, 2022, pp. 219-222, doi: 10.1109/ICDABI56818.2022.10041456.

[30] A. A. H. Al-Ali and A. Al-Nemrat, “Cyber victimization: UAE as a case study,” *2017 Cybersecurity and Cyberforensics Conference (CCC),* London, UK, 2017, pp. 19-24, doi: 10.1109/CCC.2017.14.

[31] D. Punkamol and R. Marukatat, “Detection of account cloning in online social networks,” *2020 8th International Electrical Engineering Congress (iEECON*), Chiang Mai, Thailand, 2020, pp. 1-4, doi: 10.1109/iEECON48109.2020.229558.

[32] K. Anupriya, R. Gayathri, M. Balaanand, and C. B. Sivaparthipan, “Eshopping scam identification using machine learning,” 2018 *International Conference on Soft-computing and Network Security (ICSNS),* Coimbatore, India, 2018, pp. 1-7, doi: 10.1109/ICSNS.2018.8573687.

[33] F. Fkih and G. Al-Turaif, “Threat modelling and detection using semantic network for improving social media safety,” *International Journal of Computer Network and Information Security*, Vol.15, No.1, pp.39-53, 2023, doi:10.5815/ijcnis.2023.01.04.

[34] A. Aseri, “Security issues for online shoppers,” *International Journal of Scientific & Technology Research*, vol. 10, no. 3, pp. 112-116, 2021.

[35] H. Chen, C. E. Beaudoin, and T. Hong, “Securing online privacy: an empirical test on Internet scam victimization, online privacy concerns, and privacy protection behaviors,” *Computers in Human Behavior*, vol. 70, pp. 291-302, 2017, Doi: 10.1016/j.chb.2017.01.003.

BIOGRAPHIES OF AUTHORS

Patsita Sirawongphatsara is a Lecturer in the Faculty of Science and Technology, Rajamangala University of Technology Tawan-ok (RMUTTO), Chonburi, Thailand. She received B.Sc. in computer science from RMUTTO in 2010 and M.Sc. in information technology at the King Mongkut's University of Technology North Bangkok (KMUTNB) in 2015. Her research interests include VoIP quality measurement, QoS/QoE, mobile networks, cybersecurity, data science, AI, and IoT. She is currently a Ph.D. student in the Faculty of Information Technology and Digital Innovation, KMUTNB. She can be contacted at email: patsita_si@rmutto.ac.th.

Phisit Pornpongtechavanich is an Assistant Professor in the Faculty of Industry and Technology, Rajamangala University of Technology Rattanakosin, Wang Klai Kangwon Campus (RMUTR_KKW). In 2012, he received his bachelor of technology in information technology from RMUTR_KKW. He obtained a scholarship and then received a master of Science in information technology from KMUTNB in 2014 and a Ph.D. in information and communication technology for education in 2023. His research interests include security, deep learning, AI, IoT, VoIP quality measurement, QoE/QoS, mobile networks, and multimedia communications. He can be contacted at email: phisit.kha@rmutr.ac.th.

Pakkasit Sriamorntrakul is now a master student in the Faculty of Engineering, Rajamangala University of Technology Phra Nakhon (RMUTP). He received B.Eng. in computer engineering from Mahidol University in 2005. He obtained the Avaya Certified Expert Certificate and was the Avaya Certified Support Specialist in IP Telephony. He also held other certificates, including Cisco Certified Network Professional, Microsoft Certified Systems Administrator, and VMware Certified Professional 5. He had 18 years of experience in system, network, and telecom businesses. His research interests include high-performance computer systems and networks, VoIP quality measurement, security, mobile network, AI, and IoT. He can be contacted at email: pakkasit-s@rmutp.ac.th.

Therdpong Daengsi is an Assistant Professor in the Faculty of Engineering, RMUTP. He received B.Eng. in electrical engineering from KMUTNB in 1997. He received a Mini-MBA Certificate in Business Management and M.Sc. in information and communication technology from Assumption University in 2006 and 2008 respectively. Finally, he received Ph.D. in information technology from KMUTNB in 2012. He also obtained certificates including Avaya Certified Expert – IP Telephony and ISO27001. With 19 years of experience in the telecom business sector, he also worked as an independent academic for a short period before being a full-time lecturer at present. His research interests include QoS/QoE, mobile networks, multimedia communication, telecommunications, cybersecurity, data science, and AI. He can be contacted at email: therdpong.d@rmutp.ac.th.