ANTI PHONESCAM MOBILE APP

LIN FENG
AMELIA NATASYA ABDUL WAHAB

Fakulti Teknologi & Sains Maklumat, Universiti Kebangsaan Malaysia, 43600 UKM Bangi, Selangor Darul Ehsan, Malaysia

Copyright@FTSM UKM

ABSTRACT

This study aims to develop a mobile application for telephone network fraud in order to enhance users' awareness and ability to prevent telephone network fraud. The problem solved in the study is how to effectively identify and prevent network fraud. To achieve this goal, the study adopted an incremental model development method and used Firebase as a database management tool. It deeply analyzed user needs and system requirements to ensure the practicality and security of the application. The application provides independent reporting of suspicious information, real-time interception of fraudulent calls, query of unknown numbers or links, and receiving the latest fraud news and prevention measures. The results show that the application has a significant effect in identifying and preventing fraud, which helps to enhance users' network security awareness and improve the public's awareness of preventing network fraud.

INTRODUCTION

With the advancement of science and technology, the Internet has become an indispensable part of daily life. People can now perform tasks like shopping, takeout, renting, investing, etc without leaving their homes. However, along these benefits come significant risks. For example, individuals may implant viruses via phone calls or text messages to steal personal information, using stolen identities for illegal purposes.At work, certain individuals solicit investments under the pretense of financial opportunities, offering high returns to investors,while misappropriating funds to repay initial investors.Moreover,there are cases where individuals impersonate authorities like police, or banks over the phone,to device others into fraudulent activities. These threats will not only impact privacy and the economy, but also cause fear in society. Therefore, enhancing people's ability to prevent telecommunications fraud is a top priority. The Anti Phone Scam Mobile App aims to identify the IP sources of incoming calls, alerting users to potential risks, it also provides specific detection whether there are problems with the link. For those who have fallen victim to scams, the app offers an online alarm function to send SMS alert and facilitate online reporting to reduce the economic losses caused by

telecommunications fraud.

In addition, the app regularly updates user on new fraud tactics and prevention methods, fostering public awareness of network security. These efforts aim to create a safe online environment and encourage collective action against telecommunication fraud.

PROBLEM STATEMENT

Nowadays, telecommunication fraud cases occur frequently, causing more and more people to avoid answering phone calls, receiving text messages or even engaging in online interactions. In the long run, this avoidance may lead to them being out of touch in an era of rapid technological development, fostering an instinctive fear when encountering new things. As Xisong Miao (2022) said, modern people may act irrationally when confronted with unfamiliar situations. Only by constantly learning "new tricks" and "new methods" of fraud can we keep a clear mind and keep our eyes open to the Internet.

However, only a very few people will learn how to deal with it. For this reason, the Ministry of Foreign Affairs of the People's Republic of China specially issued a statement (Ministry of Foreign Affairs of the People's Republic of China, 2023), highlighting that various telecommunication fraud criminal activities are currently rampant. Everyone must be vigilant and take precautions.

This also reflects that most young people today have low safety awareness and shallow prevention knowledge, casing them to choose to escape rather than employ correct prevention methods when faced with this kind of problem.

In addition, only a handful of anti phone scam software are currently available, and none of them include manual review, making it impossible to prevent others from maliciously marking phone numbers or URLs. At the same time, due to information blocking, these software often release information on how to prevent fraud only after the problem has occurred. As a result, users are not reminded of important preventives measures in a timely manner.

RESEARCH OBJECTIVE

The project aims to develop a mobile application to prevent online phone scams. This applications can help users to identify potential risks in calls, messages, links, and offering timely reminders,to help users mitigate risks promptly. Moreover,the applications will feature online alarm and reporting functions, to help victims to contact the police when needed. Users will also have access to the latest news and prevention methods to enhance their awareness and proactive prevention capabilities. In order to achieve this goal, several sub-goals are outlined below:

Copyright@FTSM UKM

1.To develop a mobile application that prevents phone fraud by identifying and marking reported links and numbers and providing official prevention methods and news.
2. To conduct user testing to assess the usability of the developed application.

METHODOLOGY

The approach to developing mobile programs to protect against online phone fraud follows the incremental model (Ganney, Pisharody & Claridge, 2020). Figure 1 shows the incremental model used in this project. It was chosen because of its intuitive similarity to the waterfall model. The approach involves multiple iterations of smaller cycles of requirements, design, development, and testing. Each iterations improves or builds upon previous prototypes. The model flexibility allow it to be adapted to various software projects. In the absence of manual processes or existing systems to determine requirements, the prototype helps users plan their use cases and identify their needs. It is also an effective way to demonstrate the feasibility of novel systems,especially where constraints and algorithm development may be uncertain. The following is a brief description of the stages of the incremental model.

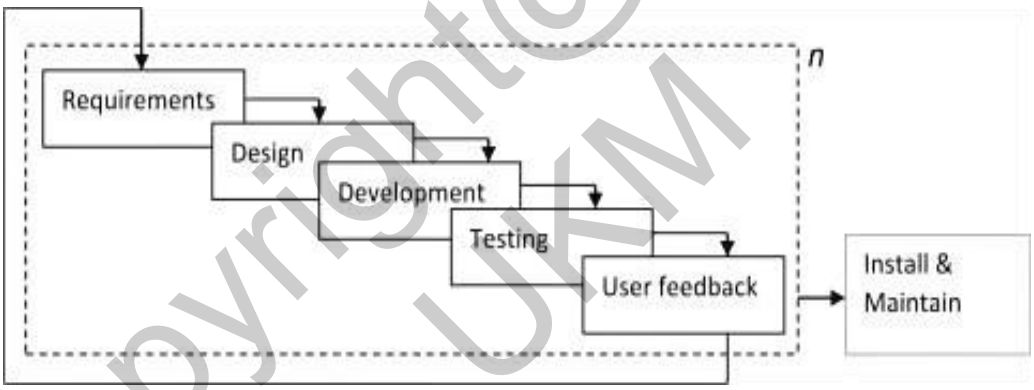

Figure.1 Schematic diagram of the incremental model
Source: Ganney,Pisharody & Claridge, 2020

1.Requirements analysis stage
At the beginning of each iteration, the focus is on understanding and defining the software's requirements. This includes gathering user requirements, market research, and determining the target functionality of the software.

2.Design stage
Based on demand analysis, design and formulate software architecture and design plans. The purpose of this phase is to determine how to implement the functionality described by the requirements.

3.Development stage
At this stage, you start writing code based on the design document. One or

Copyright@FTSM UKM

more modules of the software will be built, gradually forming a software prototype.

4.Testing phase
After each iteration of development is completed, the software prototype undergoes detailed testing. Testing is designed to find and fix bugs and ensure that the quality and performance of the software are as expected.

5.Review and feedback
Once the software prototype is complete, it is shown to users to gather feedback. This feedback will be used to guide the development of the next iteration.

6.Subsequent iterations
Each subsequent iteration improves upon the previous version. The software will be adjusted and optimized based on user feedback and test results.

7.Final delivery
After multiple iterations, when the software reaches predetermined functionality and quality standards, it will be finally delivered to users.

IMPLEMENTATION AND OUTCOME

Users can optionally log in before using the app, so new users can register an account or skip the login screen before logging in. The user's information will be stored in the database so that the application can check whether the user's information exists. Figures 2 and 3 show the registration and login pages respectively.

Copyright@FTSM UKM

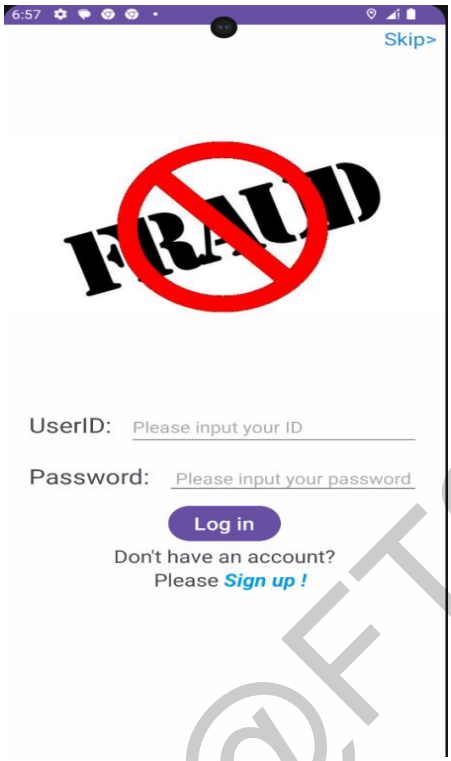

Figure 2 Log in Page

Figure 3 Sign up Page

All important user activities on the app can be accomplished through buttons on the home page. These activities includes activating phone monitoring, reporting, searching, calling the police, contacting customer service, and viewing news. Figure 4 shows the home page of the application.

Copyright@FTSM UKM

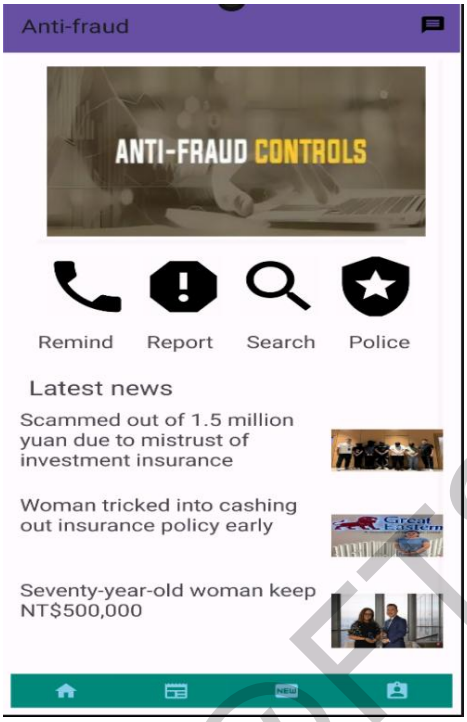

Figure 4 Home Page

The latest news, and prevention knowledge information are stored in the database, accessed through API, and displayed on the "List" page. Figure 5 and Figure 6 show the implementation of news stored in the database and displayed on the list page. Figure 7 shows the detailed information displayed when a selected news item is chosen.

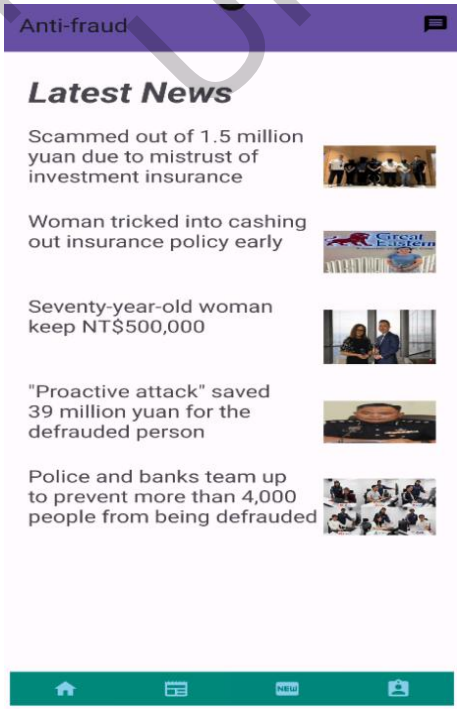

Figure 5 News Page

Copyright@FTSM UKM

Figure 6 Preventive Measures Page

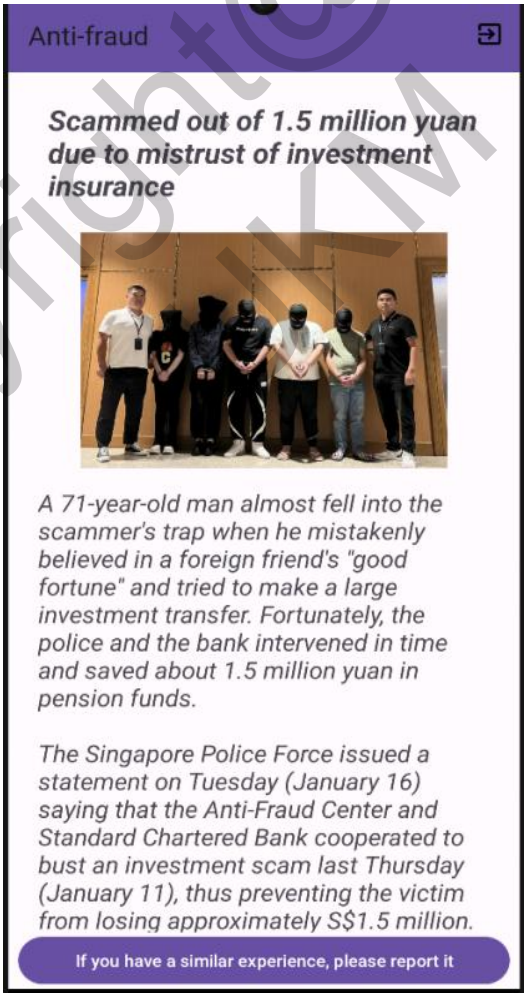

Figure 7 News Details Page

Copyright@FTSM UKM

In order to help users modify account information faster, the administrator interface will allow administrators to directly modify user login passwords.Figure 8 shows the administrator's login interface.Figure 9 shows the administrator's control interface.

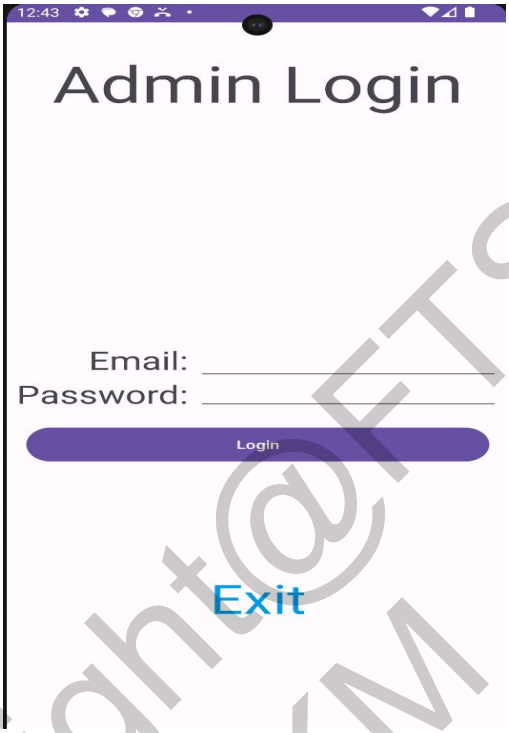

Figure 8 Admin Login Page

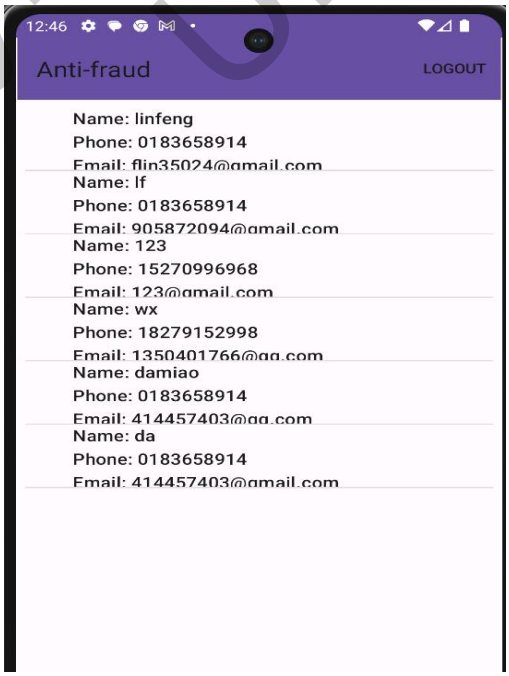

Figure 9 Admin Control Page

Copyright@FTSM UKM

Each time a call is received, the software detects the caller's number and prompts the user with the corresponding risk level. Figure 10 shows pop-up prompt when risky calls are received.

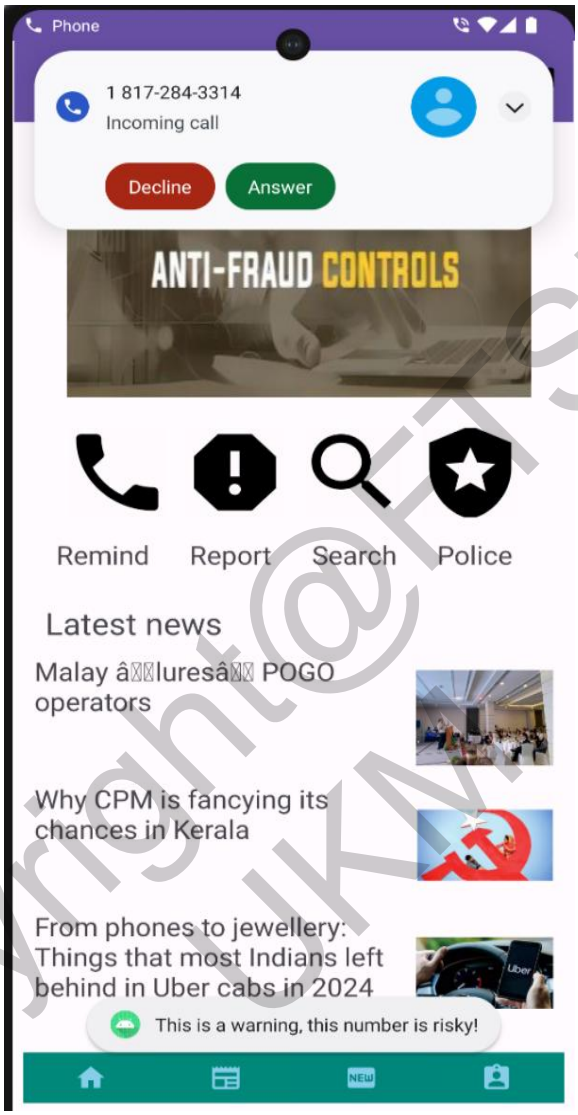

Figure 10 Risk Warning

Users can freely manage the functions they need to enable, and the software will also request corresponding permissions for the corresponding functions.Figure 11 shows the interface for software to request permissions.

Copyright@FTSM UKM

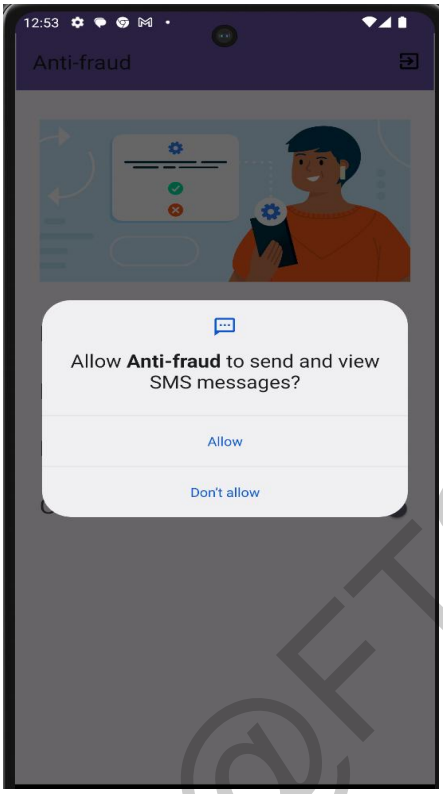

Figure 11 Request Permissions

The software will obtain the user's real-time positioning information and automatically fill in the text information when using the alarm function.Figure 12 shows user's real-time location information.

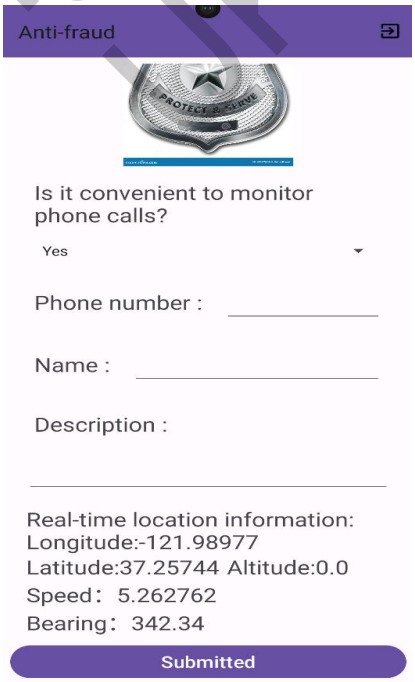

Figure 12 Request Permissions

Copyright@FTSM UKM

The user guide will allow users to select the information they need to know through the list above to complete the study of the software.Figure 13 shows user manual interface.

Figure 13 User GuidLine

The software will allow users to call third-party emails or text messages to contact customer service or make return visits.Figure 14 shows call third-party software interface.

Copyright@FTSM UKM

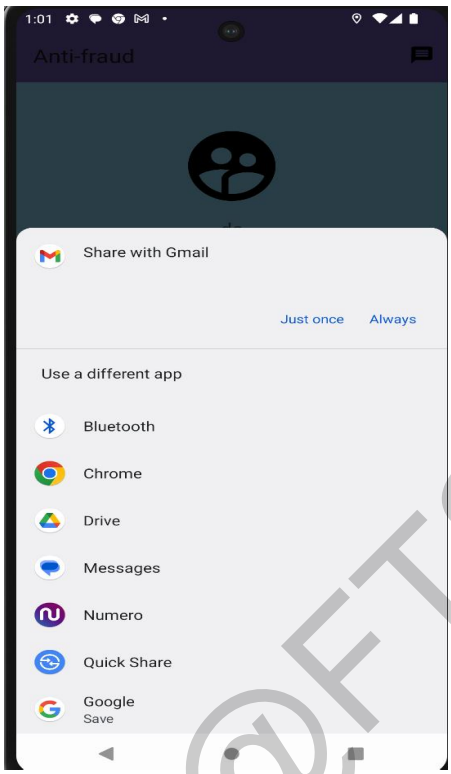

Figure 14 Call Interface

If the device does not have software that meets the requirements, the software will prompt the user.Figure 15 shows the hint.

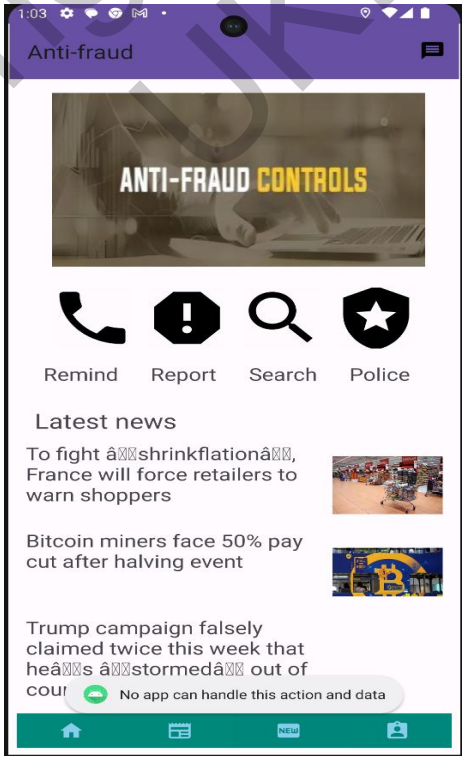

Figure 15 Hint Interface

Copyright@FTSM UKM

CONCLUSION

The project aims to help users safeguard their rights, live healthy lives and learn effectively. At present, this project has completed requirements analysis, system design, framework design and model design. However, the management application does not support currently one-click search of history viewed news. Currently, the app is not complete yet. In the future, we hope that it can support multiple languages besides English and provide more modes for different users to meet the needs of different users.

REFERENCE

Alkhalil, Z., Hewage, C., Nawaf, L., & Khan, I. (2021). Phishing attacks: A recent comprehensive study and a new anatomy. Frontiers in Computer Science, 3, 563060.

Badawi, E., Jourdan, G. V., Bochmann, G., Onut, I. V., & Flood, J. (2019). The "game hack" scam. In Web Engineering: 19th International Conference, ICWE 2019, Daejeon, South Korea, June 11–14, 2019, Proceedings 19 (pp. 280-295). Springer International Publishing.

Bishung, J., et al. (2019). A critical analysis of topics in software architecture and design. Advances in Science, *Technology and Engineering Systems Journal*, 4(2), 211-220.

Chen, H., Hu, S., Hua, R., & Zhao, X. (2021). Improved naive Bayes classification algorithm for traffic risk management. EURASIP Journal on Advances in Signal Processing, 2021(1), 30

Chen, J. (2024). The important role of software engineering technology in database design. *Mechanical and Electronic Control Engineering*, 6(2), 103-105.

Ganney, P. S., Pisharody, S., & Claridge, E. (2020). Software Engineering. In A. Taktak, P. S. Ganney, D. Long, & R. G. Axell (Eds.), Clinical Engineering (Second Edition) (pp. 131-168). *Academic Press.* https://doi.org/10.1016/B978-0-08-102694-6.00009-7

Goel, R. K. (2021). Masquerading the government: Drivers of government impersonation fraud. Public Finance Review, 49(4), 548-572.

Jarzębowicz, A., & Weichbroth, P. (2021). A qualitative study on non-functional requirements in agile software development. *IEEE Access*, 9, 40458-40475.

Kumar, S. (2019). A review on client-server based applications and research opportunity. *International Journal of Recent Scientific Research*, 10(7), 33857-3386.

López-Hernández, D. A., Mezura-Montes, E., Ocharán-Hernández, J. O., & Sánchez-García, A. J. (2021, November). Non-functional requirements classification using artificial neural networks. *In 2021 IEEE International Autumn Meeting on Power, Electronics and Computing (ROPEC) (Vol. 5, pp. 1-6)*. IEEE.

Copyright@FTSM UKM

Miao, X. (2022). Research on Measures of Prevention Against Network Telecommunication Fraud in a University. In Proceedings of the 4th International eminar on Education Research and Social Science (ISERSS 2021) (pp. 317-321). *Atlantis Press*. https://doi.org/10.2991/assehr.k.220107.062

Ministry of Foreign Affairs of the People's Republic of China. (2023, May 11). Chinese Embassy and Consulates in Canada Warn Citizens Against Telecom Fraud. Retrieved May 11, 2023, from https://www.mfa.gov.cn/wjbzwfwpt/kzx/tzgg/202305/t20230511_11074979.html

Pouryousefi, S., & Frooman, J. (2019). The consumer scam: an agency-theoretic approach. Journal of Business Ethics, 154, 1-12.

Rizal, C., Supiyandi, S., Zen, M., & Eka, M. (2022). Perancangan Server Kantor Desa Tomuan Holbung Berbasis Client Server. *Bulletin of Information Technology (BIT),* 3(1), 27-33.

Su, H. (2023). Analysis of factors affecting the effectiveness of online fraud prevention education for college students based on the analytic hierarchy process. *Operations Research and Fuzzy Science,* 13(5), 4904-4912. https://doi.org/10.12677/ORF.2023.135493

LIN FENG (A184539)
Dr. Amelia Natasya Hj. Abdul Wahab
Fakulti Teknologi & Sains Maklumat
Universiti Kebangsaan Malaysia

Copyright@FTSM UKM