Cyber Romance Scam Victimization Analysis using Routine Activity Theory Versus Apriori Algorithm

Mohd Ezri Saad[1]
Commercial Crime Investigation Department
Royal Malaysia Police, Bukit Aman
Kuala Lumpur, Malaysia

Siti Norul Huda Sheikh Abdullah[2], Mohd Zamri Murah[3]
Center for Cyber Security Faculty of Information
Science and Technology Bangi,
Selangor, Malaysia

***Abstract*—The advance new digital era nowadays has led to the increasing cases of cyber romance scam in Malaysia. These technologies have offered both opportunities and challenge, depending on the purpose of the user. To face this challenge, the key factors that influence the susceptibility to cyber romance scam need to be identified. Therefore, this study proposed cyber romance scam models using statistical method and Apriori techniques to explore the key factors of cyber romance scam victimization based on the real police report lodged by the victims. The relationship between demographic variables such as age, education level, marital status, monthly income and independent variables such as level of computer skills and the level of cyber-fraud awareness has been investigated. Then, the result of this study was compared with Routine Activity Theory (RAT). This study found that those between the ages of 25 and 45 years were likely to be the victims of cyber romance scams in Malaysia. The majority of the victims are educated and having a Diploma. In addition, this research shows that married people are more likely to be the victims of cyber romance scams. Study shows that non-income individuals are also vulnerable to being the victims because the study shows that 17 percent of respondents who are the victims are from this group. As expected, those who work and have monthly income between RM2001 and above are more likely to be targeted and become a victim of cyber romance scams. The study also shows that those who lack computer skills and less levels of cyber-fraud awareness are more likely to be victims of cyber romance scams.**

***Keywords*—Cybercrime; love-scam; routine activity theory**

I. INTRODUCTION

In the era of globalization information, users should be wiser in sharing their information especially personal information. Users negligence will give advantage to the cyber scammers [1], [2]. These scammers usually targeting people who looking for romantic partners as a victim, often via dating websites, apps or social media by pretending to be prospective companions. Scammers typically create fake online profiles designed to lure victims in [3]. They will start by profess strong feeling for the victim and ask to chat with them privately. As soon as the scammer has gained the trust from the victim, they begin requesting money by pretending to need money for some sort of personal emergency. Among other possibilities, the scammer may request photos or personal information that could eventually be used to blackmail the victim and extort more money [4].

Sponsored by Ministry of Higher Education using grant AP2017-005/2

These cyber romance scams has fraud Australians out of millions every years [1], [5]. No exception to Malaysia that has been the top 6 countries that recorded highest number of cybercrime cases, with total loses reaching RM1 billion (Source: Bernama Report in 2014). Other countries like Taiwan, China, Thailand, Indonesia and Hong Kong also were listed together. While, Sophos Threat Report in 2014 stated that cybercrime attacks have been increased in the first quarter of 2014 and 81% of them happened in Malaysia. This phenomenon was in line with the rapid growth of Malaysia's digital economy [6].

Furthermore, Business Insider reports that Malaysia has become a center of cybercrime mastermind by Nigerian. They have been successfully tricked hundreds American woman into cyber criminals with the average loses is USD250 thousand [5]. Their operation is same by start hacking the internet infrastructure, then broke into Malaysian banking system. This repeating cases have been shows that Malaysia is lacked of resources and expertise to handle these cybercrimes [6], [7]. This situation has been drop Malaysian image and credibleness in combating cybercrime. Despite the fact that cybersecurity in Malaysia has been improved in term of the national policy formulation and the management mechanism of national cyber crisis. However, it can be seen that this strategy are still unsuccessful and need to be enhanced [7], [8]. If this situation continued, it will give a serious impact on political, economic and social sectors in Malaysia.

This cyber romance scams happen on a global scale and there is no international statistical center that stores the victim's data and the exact amount of loss [9]. In contrast, Malaysian have been recorded those important information by the Commercial Crime Investigation Department (CCID), Royal Malaysian Police (PDRM). Based on the statistics recorded by CCID, the increasing in cybercrime cases in Malaysia have gone up at an alarming rate and this situation has inadvertently urge agencies and authorities in Malaysia to analyze cyber romance scam in Malaysia as a whole to seek a preventive measure in reducing cybercrime rate.

However, [9] emphasized that the authorities only received a portion of the report because there are some victims is shame to appear after recognizing themselves being deceived by this syndicated, or some of the victims still do not realize they have been deceived. Nevertheless, cybercrime statistics obtained from the CCID still can be used. Users who like to find a romantic partner or soul mate online is the main target

of this syndicate. Therefore, in-depth studies need to be conducted to find out more details and pattern about these cybercriminal [8].

On the other hand, [10] have been introduced a theory to understand the crime victimization that called Routine Activity Theory (RAT). This theory suggests three key factors to identify the crime victimization: (i) the presence of a motivated criminal, at the same time and place, (ii) the existence of an opportunity to meet the appropriate target, (iii) the target or the victim has no adequate care. This theory has been successfully applied for a tendency crime prediction such as robbery, theft, vandalism, rape, assault and fraud [11]. In recent years, RAT theory has been tested in cyber criminology and they found very significant correlation between individual tendencies to receive virus in cyberspace and the tendency to become cybercrime victim [11]. While [12] found a correlation between online shopping behavior and the tendency to become a cybercrime victim of financial fraud. Hence, these findings clearly show that RAT theory also can be used as a framework of study involving fraud or crime in cyberspace. Therefore, this study will compared the findings of cyber romance scam victimization analysis using RAT theory and Apriori algorithm. Then proposed a cyber romance scam model.

II. METHOD

Quantitative method such as questionnaire survey was used in this study to investigate cyber romance scam victimization tendency factors. Furthermore, to identify the reliability of instruments used, a pioneer test was carried out before the actual studies were conducted. There are three methods used in this study which is (i) participants, (ii) materials, and (iii) pioneer test. The highlighted method is explained as below:

A. Participants

The participant of this study is cyber romance scam victims based on the sample survey in Selangor, Malaysia. The total samples are 280 surveys that represent 2508 of target populations. The participants included 42 men and 238 women. Aged below 25 years old is 17, aged between 25-35 is 92, aged between 36-45 is 87, and aged above 46 is 84. The education level of participants included 92 bachelor degree holder, diplomas holder is 104, and STPM holder is 17. For marital status, 84 is single, 28 divorced, and 168 married. Working status included 224 is working, 8 retired, and 48 unemployed. While, monthly salary included 48 participants has no income, 22 participants got salary between RM1-RM2000, 92 participants got salary between RM2001-RM4000, 73 participants got salary between RM4001-RM6000, and 42 participants got salary from RM6001 and above.

B. Materials

The materials used in this study is based on questionnaire. The questionnaire consists of three section and all section is required to be answered by the participant. The first section explains the objective of research and the background information regarding to this study to ensure that the respondent understands the purpose of the study. The contact information such as phone numbers and e-mail address also stated in this section to allow the respondents contacting the researchers if they need any clarification regarding the survey. Then, this section is followed by the respondents' demographics related-questions such as gender, age, education level, marital status, employment status and monthly income. The dichotomous question types in used to able respondents selecting only one answer based on several given answers.

Whereas for second section is consist of question that is used as an instrument in measuring relationship between levels of cybercrime awareness and the tendency to become a victim of cyber romance crime. There are six items used to measure the level of cyber-fraud awareness as shown in table 1. The questions in this section are adapted from [1], which the study is investigating a tendency to become a victim of online scam.

The last section is consisting of question that is used as an instrument in measuring relationship between the level of computer-based skills and the tendency to be a victim of cyber romance crime. There are three items used to measure the level of computer skills such as: (i) Period of using computer (years), (ii) Period of using computer (hours) and (iii) Taking IT courses. The questions in this section are also adapted from the study conducted by [1]. To gather the information, both section which is section two and three is using dichotomous and Likert scale of questionnaires types in range between 1 to 6. The dichotomous method is a straight question and answer type which allows respondents to select only one simple answer. While Likert scare are used to select the degree to which respondents agree to a specific statement.

C. Pioneer Test

Reliability is the level of suitability and the accuracy of the instrument to measure the variable studies. Therefore, reliability analysis is carried out using pioneer test before the actual survey was distributed to ensure that the research findings are consistently based on the selected data collection method.

These tests were conducted in early December 2017 and distributed randomly to the victims who has been lodge a police report regarding cyber romance crime. This pioneer test has been used to ensure the usability and validity of the instrument's content used. Then the reliability of this instrument is measured by the Cronbach Alpha Coefficient.

For the purpose of this pioneer test, survey questions are built online using Google Forms services and links to the questionnaire are sent using WhatsApp application. Within two weeks, 350 surveys were distributed to the victims of cyber romance scams. However, only 300 surveys were answered. 20 of the 300 surveys should not be used. This is due to some of unanswered survey questions by the respondents, so it cannot be applied to this study. Therefore, the number of surveys used in this study is 280 and respondents' response rate is 80 percent. All respondents find that the question in the instrument are easy to understand and the contents were clearly explained. The average time to answer the questionnaire is about 10 minutes.

Then, the Cronbach Alpha Coefficient is computed using SPSS software. All used variables shows the result between 0.83 - 0.92. Where the level of cyber-fraud awareness got a higher Cronbach Alpha values (0.92) against computer skill level (0.83). This result has been confirmed that the instruments used in assessing the level of computer-based skills and the level of cyber-fraud awareness is reliable and consistent.

III. Results and Discussion

A. Preliminary Analysis

In preliminary analysis, normality test was conducted to ensure that the normality of the data recorded in this study is approaching a normal distribution. Normality is the assumption used that involving two or more variables. There are two types of variables in this study namely demographic variables and manipulated variables including the level of computer skills and the level of cyber-fraud awareness. While the responding variable is a tendency to become a victim of cyber romance scams. As shown in table 1, there are six questions used to study the level of cyber-fraud awareness. The mean values for these questions are between 1.157 - 1.891. While three questions are used to study the level of computer skills and the mean or average values for these questions are between 1.231 - 2.752. It can be conclude that the recorded survey data in this study is approaching a normal distribution.

TABLE I. Descriptive Analysis of Variables

Variables: Levels of cyber-fraud awareness	**Min (Average)**
Knowledge level about cyber romance scam	1.157
Awareness levels about cyber romance scam	1.591
Knowing about 419 scam / Nigeria scam 419 / parcel scam	1.825
Awareness levels about 419 scam / Nigeria scam 419 / parcel scam	1.386
Knowing about phishing scams	1.891
Awareness levels about phishing scam	1.758
Variables: Levels of computer skills	**Min (Average)**
Period of using computer (years)	2.752
Period of using computer (hours)	2.517
Taking IT courses	1.231

TABLE II. Pearson Correlation Analysis

Variables	**Tendency to become a victim of cyber romance crime**	**Levels of cyber-fraud awareness**	**Levels of computer skills**
Tendency to become a victim of cyber romance crime	1	-	-
Levels of cyber-fraud awareness	0.626	1	-
Levels of computer skills	0.306	0.403	1

Then, Pearson correlation coefficients is used to evaluate the degree of linear relationship between all variables in this studies. Based on the result in table 2, the correlation between the level of cyber-fraud awareness and the tendency to become a victim of cyber romance scam is 0.626 ($r = 0.626$, $p < 0.01$). This value indicates a positive relationship between these two variables. On the other hand, a weak positive relationship can be seen among computer skills and the tendency to be a victim of cyber romance scam with coefficient value of 0.306 ($r = 0.306$, $p < 0.01$).

After that, in order to identify cases (or respondents) that are above or below standard deviation units, the Casewise Diagnostics analysis need to be implemented. Three unusual cases have been identified as shown in Table 3. However, this unusual cases are not affect the analysis result since the number of cases identified is 1% of the total cases and Cook's coefficient value is less than 1. Therefore, this unusual cases will not be removed.

TABLE III. Casewise Diagnostics and Analysis of Cook Distance

Total cases	**Levels of cyber-fraud awareness**	**Expected value**	**Cook coefficient**
91	4.23	1.3001	
110	3.50	1.8972	
			0.446

Lastly, regression analysis was applied. Unlike correlation analysis, regression analysis can assess the strength of causal relationships between manipulated variables and responding variables. Multiple regression coefficients are used to determine the strength of relationships between respondents' variables (the tendency to become a victim of cyber romance crime and manipulated variables (levels of cyber-fraud awareness and computer skills). Multiple regression coefficients, R2 measures the variation of respondents' variables that are likely to become a victims of cyber romance scams that can be statistically explained by manipulated variables i.e. level of cyber-fraud awareness and computer skill level.

TABLE IV. Multiple Regression Coefficients Analysis

Variables	**R2**	**F-values**	**Beta coefficient**	**t**	**P-values**
Tendency to become a victim of cyber romance crime	0.669	31.275			0.000
Levels of cybercrime awareness			0.626	8.730	0.000
Levels of computer skills			0.306	3.493	0.001

Based on table 4, the R2 value which is 0.669 indicates that 66.9 percent of the variance in "Tendency to become a victim of cyber romance crime" can be explained by a regression model. The value of F is 31.276 with a value of p 0.000. This is means that the probability of this decision happens by chance is less than 0.0005. Hence, significant

relationships have been shown among the level of cyber- fraud awareness is 8.730 and the t value for computer skill level is 3.493. Again, the probable probability of the result is less than 0.05.

Therefore, based on the results obtained and the interpretations made from the statistical analysis, it can be concluded that four hypotheses have been supported (H1, H2, H5 and H6). The hypothesis summary of their relevant research questions is shown in table 5. Next, the studies were continued to examine how far the demographic variables influencing the tendency to become a victim of cyber romance crime using Apriori based association rules technique.

TABLE V. HYPOTHESIS SUMMARY BASED ON INTERPRETATION OF STATISTICAL ANALYSIS

No	Research Question	Hypothesis	Results
H1	Is age influencing the tendency to become a victim of cyber romance crime?	Older individuals are more likely to be a victims of cyber romance scams.	Supported
H2	Is education level influencing the tendency to become a victim of cyber romance crime?	Uneducated individuals are more likely to be a victims of cyber romance scams.	Supported
H3	Is marital status influencing the tendency to become a victim of cyber romance crime?	Single individuals are more likely to be a victims of cyber romance scams.	Unsupported
H4	Is monthly income influencing the tendency to become a victim of cyber romance crime?	High-income individuals are more likely to be a victims of cyber romance scams.	Unsupported
H5	Is levels of computer skills influencing the tendency to become a victim of cyber romance crime?	Individuals with low computer skills are more likely to be a victims of cyber romance scams.	Supported
H6	Is levels of cybercrime awareness influencing the tendency to become a victim of cyber romance crime?	Individuals who lack of cyber-crime awareness are more likely to be a victims of cyber romance scams.	Supported

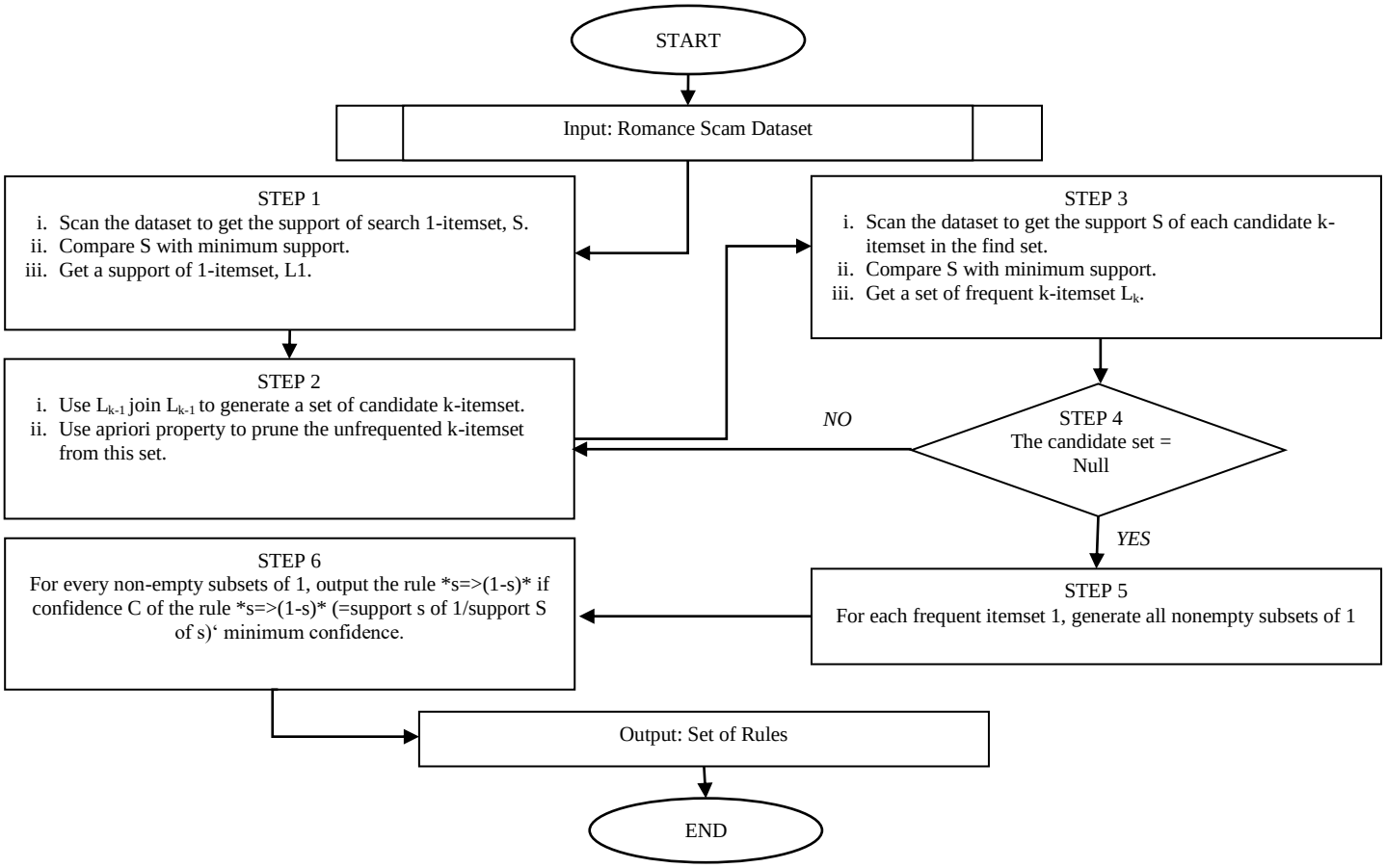

Fig. 1. The Steps of Generating Association Rules using Apriori Algorithms on Romance Scam Dataset.

B. Cyber Love Fraud Pattern Recognition in Malaysia using Apriori based Association Rules Technique

This study will use the Apriori based Association Rules algorithm to get a meaningful information from the data. This algorithm works by generating frequent item set and then generating a set of rules. Association rule learning is a prominent and a well-explored method for determining relations among variables in large databases compared to other methods. In addition, this method is still popular and been used recently to solve the problem in various domain [13]–[15]. Association rules are usually required to satisfy a user-specified minimum support and a user-specified minimum confidence at the same time [16].

Association rule generation is usually split up into two separate steps which is a minimum support threshold is applied to find all frequent item sets in a database; and a minimum confidence constraint is applied to these frequent item sets in order to form rules. The first step needs more attention, while the second step is straightforward [17]. Figure 1 shows the steps of generating association rules using Apriori algorithms that have been used in this study

These experiments were conducted by involving the relationship between seven main attributes/variables namely Races, Gender, Marital Status, Age, Occupation, Type of fraud and Total losses. The data set used is an original record of cyber romance fraud victims in Selangor that representing 2274 cases in 2017. The data set is recorded by the CCID in Bukit Aman. Strong, interesting and authentic association between attributes is generated as a set of rules for the pattern recognition of cyber romance fraud in Malaysia. This experiment was conducted using the Waikato Environment for Knowledge Analysis (WEKA) software.

TABLE VI. RULES SUMMARY FOR ALL SELECTED ATTRIBUTES

Min. Support 0.1			
No.	**Rules**	**Min. Confidence**	**Frequency**
1	**IF** TypeOfFraud=ParcelScam **AND** Occupation=UnEmployed **AND** MaritalStatus=Married **THEN** Gender=Female	0.95	257
2	**IF** TypeOfFraud=ParcelScam **AND** Age=36-45 **AND** MaritalStatus=Married **THEN** Gender=Female	0.86	320
3	**IF** Races=Chinese **AND** TypeOfFraud=ParcelScam **AND** Occupation=PrivateSector **THEN** Gender=Female	0.86	382
4	**IF** TypeOfFraud=ParcelScam **AND** Age=25-30 **AND** MaritalStatus=Single **THEN** Gender=Female	0.85	249
5	**IF** TypeOfFraud=ParcelScam **AND** Occupation=PrivateSector **AND** Age=25-30 **THEN** Gender=Female	0.85	337
6	**IF** TypeOfFraud=ParcelScam **AND** Age=25-30 **AND** MaritalStatus=Married **THEN** Gender=Female	0.85	230
7	**IF** TypeOfFraud=ParcelScam **AND** Occupation=PrivateSector **AND** MaritalStatus=Single **THEN** Gender=Female	0.83	288
8	**IF** Races=Chinese **AND** Occupation=PrivateSector **AND** MaritalStatus=Married **THEN** Gender=Female	0.82	256
9	**IF** TypeOfFraud=ParcelScam **AND** Occupation=PrivateSector **AND** Age=36-45 **THEN** Gender=Female	0.81	228
10	**IF** Races=Malay **AND** TypeOfFraud=ParcelScam **AND** MaritalStatus=Married **THEN** Gender=Female	0.80	412
11	**IF** Races=Malay **AND** TypeOfFraud=ParcelScam **AND** Age=46< **THEN** Gender=Female	0.80	231
12	**IF** Races=Malay **AND** TypeOfFraud=ParcelScam **AND** Occupation=PrivateSector **THEN** Gender=Female	0.77	282
13	**IF** TypeOfFraud=ParcelScam **AND** Occupation=PrivateSector **AND** MaritalStatus=Married **THEN** Gender=Female	0.76	431
14	**IF** TypeOfFraud=ParcelScam **AND** Age=46< **AND** MaritalStatus=Married **THEN** Gender=Female	0.75	305
15	**IF** Races=Chinese **AND** Gender=Female **AND** TypeOfFraud=ParcelScam **THEN** Occupation=PrivateSector	0.7	382
16	**IF** Gender=Female **AND** TypeOfFraud=ParcelScam **AND** Occupation=UnEmployed **THEN** MaritalStatus=Married	0.76	257
17	**IF** Gender=Female **AND** TypeOfFraud=ParcelScam **AND Age=36-45 THEN** MaritalStatus=Married	0.74	320
18	**IF** Gender=Female **AND** TypeOfFraud=ParcelScam **AND** Age=46< **THEN** MaritalStatus=Married	0.72	305
19	**IF** Gender=Female **AND** MaritalStatus=Single **AND** Age=25-30 **THEN** TypeOfFraud=ParcelScam	0.88	249
20	**IF** Gender=Female **AND** Age=25-30 **AND** Occupation=PrivateSector **THEN** TypeOfFraud=ParcelScam	0.88	337
21	**IF** Gender=Female **AND** MaritalStatus=Married **AND** Age=25-30 **THEN** TypeOfFraud=ParcelScam	0.88	230
22	**IF** Gender=Female **AND** MaritalStatus=Single **AND** Occupation=PrivateSector **THEN** TypeOfFraud=ParcelScam	0.86	288
23	**IF** Gender=Female **AND** MaritalStatus=Married **AND** Occupation=UnEmployed **THEN** TypeOfFraud=ParcelScam	0.84	257
24	**IF** Races=Malay **AND** Gender=Female **AND** MaritalStatus=Married **THEN** TypeOfFraud=ParcelScam	0.83	412
25	**IF** Races=Malay **AND** Gender=Female **AND** Occupation=PrivateSector **THEN** TypeOfFraud=ParcelScam	0.82	282
26	**IF** Races=Malay **AND** Gender=Female **AND** Age=46< **THEN** TypeOfFraud=ParcelScam	0.81	231
27	**IF** Races=Chinese **AND** Gender=Female **AND** Occupation=PrivateSector **THEN** TypeOfFraud=ParcelScam	0.81	382
28	**IF** Gender=Female **AND** MaritalStatus=Married **AND** Age=36-45 **THEN** TypeOfFraud=ParcelScam	0.81	320
29	**IF** Gender=Female **AND** MaritalStatus=Married **AND** Occupation=PrivateSector **THEN** TypeOfFraud=ParcelScam	0.81	431
30	**IF** Gender=Female **AND** Age=36-45 **AND** Occupation=PrivateSector **THEN** TypeOfFraud=ParcelScam	0.78	228
31	**IF** Gender=Female **AND** MaritalStatus=Married **AND** Age=46< **THEN** TypeOfFraud=ParcelScam	0.77	305
32	**IF** Races=Chinese **AND** Gender=Female **AND** MaritalStatus=Married **THEN** TypeOfFraud=ParcelScam	0.77	294
33	**IF** Races=Chinese **AND** MaritalStatus=Married **AND** Occupation=PrivateSector **THEN** TypeOfFraud=ParcelScam	0.76	292

In this study, rule generation is controlled by parameter setting, such as minimum support level and minimum confidence level. Determining the value of support and minimum confidence levels is a complex task as it affects the quality of the generated rules. Normally, rules were generated with high confidence value and it is a top priority for rules selection because they are considered strong, but this method does not provide an opportunity for odd cases.

Therefore, this study sets the parameter of confidence value from 0.3 to 1.0 and the minimum support value is set as 0.1. This is to ensure that the rules with frequent and meaningful attributes at low confidence and support values can be generated and discovered. In this section, the results of the study were broken down into seven experiments where each attribute was given the opportunity to become a class attribute on the data record. Then, meaningful rules will be selected through two criteria:

- Confidence and support values are greater than other.
- High support value and low confidence value, but rules are generated earlier that the other rules.

Through the study, Apriori's based Association Rules algorithm has been selected based on its effectiveness in producing interesting rules. The choice of meaningful rules is obtained through the process of repeated analysis. Table 6 shows the selected rules which minimum confidence is above 0.7 and minimum support is 0.1.

Overall, experimental results have shown the uniform pattern for the association between all selected attributes despite different attributes class. This shows that the data used is able to produce interesting and stable pattern. Therefore, based on the rules obtained and the interpretations made from several analyses, it can be concluded that Chinese and Malay women were likely easier to become a victim. This may be due to the large ratio of Chinese and Malay population in Malaysia. Those between the ages of 25 and 45 years were likely to be the victims of cyber romance scams. In addition, this research shows that married people are more likely to become a victim of cyber romance scams. This is contrary to the study's hypothesis that single individuals are more likely to become a victim. Unemployed person also can be a victim of cyber romance scam probably because they have a lot of time to go online. Lastly, the scammer usually will ask the money from the victim around RM3025 until RM5490. The model of cyber romance scam based on extracted rules can be illustrated as figure 2.

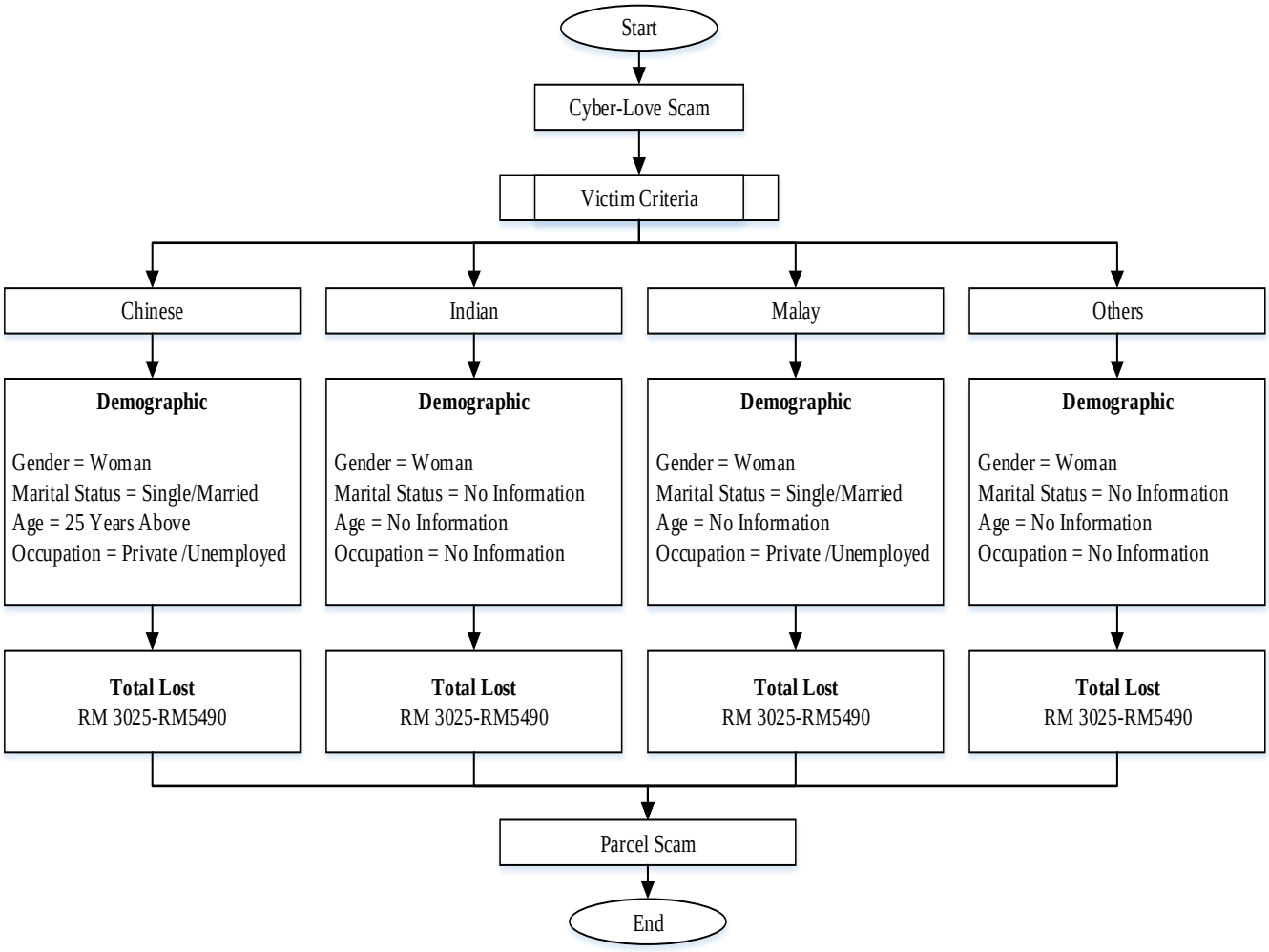

Fig. 2. Cyber Romance Scam Models using Apriori Techniques.

IV. CONCLUSION

The main objective of this study is to analyze the factors that influence the susceptibility to become a cyber romance scam victim in Malaysia using the information from the individuals who have been victims of cyber romance scams and lodged the police reports in the state of Selangor, Malaysia. The lack of research in this area as well as the growing case of cyber romance scam in Malaysia yearly has been a driving force in publishing this research. RAT Theory is used as a theoretical basis and this study will help to improve understanding of this theory in the context of cyber crime because this theory is more synonym and often used in the context of ordinary street crime. The framework of this study examines demographic variables such as Age, Education Level, Marital Status, Monthly Income, and manipulated variables such as level of computer skills and the level of cyber crime awareness. Both of these manipulated variables are hypothesized to have a relationship with the tendency to become a victim of cyber romance scam in Malaysia.

Overall, the study found that those between the ages of 25 and 45 years were likely to be victims of cyber romance scams in Malaysia. The majority of the victims are educated and having a Diploma, the remaining have a degree, STPM and SPM / SPMV. In addition, this research shows that both single and married people can become victims of cyber romance scams. Furthermore, studies show that individuals who are not earning are also vulnerable to being a victims because the study shows that 17 percent of respondents who are victims are from this group. However, as expected, those who work and have monthly income between RM2001 and above are more likely to be targeted and victims of cyber romance scams. The study also shows that those who lack computer skills and less awareness of cyber-fraud are more likely to be victims of cyber romance scams. The findings of this study are useful for policy makers and enforcement agencies to protect Internet users in Malaysia. Based on the analysis, it can be concluded that this research has found strong characteristics of cyber romance scam victimization in Malaysia.

Furthermore, this study is based on RAT theory, so this study confirms the fundamental principle of this theory and the usability of the theory in cyberspace environment. This theory is not limited to ordinary street crime but is relevant for application in cyber-crime. Indirectly, this study contributes to an increased understanding of RAT Theory and its usability in different contexts.

For future work, the researchers should investigate the extent of financial loss suffered by the victim and take the environment, motives or major motivation of the cyber criminals in choosing their target into account. Overall, the findings of this study may useful for policy makers in creating internet-related policies to protect the Internet users in Malaysia.

ACKNOWLEDGMENT

This research was funded by Ministry of Higher Education using grant AP2017-005/2.

REFERENCES

[1] E. V. Garrett, “Exploring internet users’ vulnerability to online dating fraud: Analysis of routine activities theory factors,” 2014.

[2] A. Salman, S. Saad, and M. N. Shahizan Ali, “Dealing with ethical issues among internet users: Do we need legal enforcement?,” Asian Soc. Sci., 2013.

[3] C. Kopp, R. Layton, J. Sillitoe, and I. Gondal, “The role of love stories in Romance Scams: A qualitative analysis of fraudulent profiles,” Int. J. Cyber Criminol., 2016.

[4] N. A. Manap, A. A. Rahim, and H. Taji, “Cyberspace Identity Theft: The Conceptual Framework,” Mediterr. J. Soc. Sci. , 2015.

[5] M. T. Whitty, “Anatomy of the online dating romance scam,” Secur. J., vol. 28, no. 4, pp. 443–455, 2015.

[6] James Lyne, “Cybersecurity in 2015,” sophos, 2015.

[7] M. Riek, R. Böhme, and T. Moore, “Measuring the Influence of Perceived Cybercrime Risk on Online Service Avoidance,” IEEE Trans. Dependable Secur. Comput., 2016.

[8] M. A. Bin Pitchan, W. A. W. Mahmud, S. N. Sannusi, and A. Salman, “Control and freedom of the Internet: Challenges faced by the government,” J. Asian Pacific Commun., vol. 25, no. 2, pp. 243–252, 2015.

[9] C. Barclay, “Using Frugal Innovations to Support Cybercrime Legislations in Small Developing States: Introducing the Cyber-Legislation Development and Implementation Process Model (CyberLeg-DPM),” Inf. Technol. Dev., 2014.

[10] L. E. Cohen and M. Felson, “Social Change and Crime Rate Trends: A Routine Activity Approach,” Am. Sociol. Rev., 1979.

[11] F. Ngo and R. Paternoster, “Cybercrime Victimization: An examination of Individual and Situational level factors.,” Int. J. Cyber, 2011.

[12] J. van Wilsem, “Worlds tied together? online and non-domestic routine activities and their impact on digital and traditional threat victimization,” Eur. J. Criminol., 2011.

[13] P. Yuan, D. Chen, T. Wang, S. Cao, Y. Cai, and L. Xue, “A compensation method based on extreme learning machine to enhance absolute position accuracy for aviation drilling robot,” Adv. Mech. Eng., vol. 10, no. 3, p. 1687814018763411, 2018.

[14] P. Pravallika and K. Narendra, “Analysis on Medical Data sets using Apriori Algorithm Based on Association Rules,” 2018.

[15] R. Wadhawan, “Prediction of Coronary Heart Disease Using Apriori algorithm with Data Mining Classification,” Int. J. Res. Sci. Technol., vol. 3, no. 1, pp. 1–15, 2018.

[16] R. A. A. Rashid, P. N. E. Nohuddin, and Z. Zainol, “Association Rule Mining Using Time Series Data for Malaysia Climate Variability Prediction,” in International Visual Informatics Conference, 2017, pp. 120–130.

[17] Z. A. Othman, N. Ismail, and M. T. Latif, “Association pattern of NO 2 and NMHC towards high ozone concentration in klang,” in Electrical Engineering and Informatics (ICEEI), 2017 6th International Conference on, 2017, pp. 1–6.