Advances in Computer Science and its Applications (ACSA)
Vol. 2, No. 2, 2012, ISSN 2166-2924

www.worldsciencepublisher.org

Security and privacy issues of modern banking services in Iranian banks

[1]Ali Aghaeirad, [2]Behrouz Fathi-Vajargah, [3]Mehdi Afzali

[1]Islamic Azad University of Zanjan, Iran
[2]Department of Statistics, University of Guilan, Iran
[3]Department of IT Engineering, Zanjan Branch, Islamic Azad University, Zanjan, Iran

Email: aliagrad@gmail.com,
[2]fathi@guilan.ac.ir,
[3]afzali@hacettepe.edu.tr

Abstract – In this paper, presentation of the current Methods of Modern Baking Services such as, on line banking services, services through the ATM and selling by the POS machines, in Iranian banks will be considered and the impediments in presenting of such modern services will also be checked. Mainly, security and privacy domains in inter and intra banking transactions will be examined, and security issues which the new banking systems are facing with them will also be described. Moreover, it will be shown, through simulation, how much of the personal information might be accessible by unauthorized companies and people in the current system. Finally, for solving the mentioned problems, a banking system based on the collaboration between the banks is offered, and it will be proved that this approach can eliminate many of the problems facing the current system. In proposed methods, the technical and hardware limitations of current banking system such as lacking PKI infrastructure is considered and it is tried to present a solution which would be compatible with the currently available hardware such as POS and ATM. Here, the proposed solution is based on the short time passwords. which from the author's point of view, is one of the best technology available, also it is tried to design a system in a way to be intrinsically secure and the security of system does not depends on the users behavior regarding security issues consideration as much as possible.

Keywords – e-banking, privacy, inference, Collaborative banking

1. Introduction

Banking services are an integral part of everyday life of people in today's world. At any time of day, people can withdraw cash from ATM machines or transfer funds to other accounts. They can buy in most stores and even supermarkets, without carrying cash. They can also manage their accounts or transfer money from anywhere in the world via the Internet. New strategies for managing accounts using mobile phones as SMS - Banking and Mobile Banking have also recently been launched. And in Iran, these services are being launched by some banks. The modern banking services have become a vital part of people's lives and businesses.

Traditionally, the financial information relating to financial institutions and credit transfer between institutions and their clients, have been very important. And since through these data, Lot of information about customers' personal issues such as the way of doing business and even their interests and hobbies is achievable, many banks are trying to keep this information safe.

In the modern banking privacy is of special importance. Part of privacy, the problem of unauthorized access to account information is being reviewed in another article [1]. Another problem that can arise in privacy is the inference of private information, from information that alone is not classified as confidential. Similar to the inference problem, that may occur in multilevel databases [2]. In this paper, it will be shown through simulation that in the present state the banking system is vulnerable in this aspect. And it will be explained, how the proposed solution will solve the problem.

Currently, most Iranian banks that offer ATM services use fixed password for authentication of clients. The user can use the ATM card and a fixed password to purchase from POS devices. He can transfer money from ATM machines, or choose to withdraw cash. Users can also use

the specifications listed on the card and a password to do online shopping.

While this method is only able to provide security, provided that, Appropriate length and non-guessable passwords used, The password is modified regularly, And authentication data does not saved on devices that are completely unsafe, such as personal computers [3]. Bank customers rarely consider all these cases.

In the traditional banking system, the financial information of each user was only available in the bank that has opened the account (we call it reference bank). But with the advent of modern banking systems and formation of SHETAB network, it is possible for other financial institutions to have access to some parts of the customer's account information. And thus, by putting together the little information that is available, it is possible for these financial institutions to infer higher level private information about another bank's customers.

In this paper, using agent-based modeling a small model of a country banking system is simulated. And it has been shown, how little information that comes from the interaction with the ATM machines, POS devices and Internet payments, can be used to deduced considerable information about the bank's customers. In the second part of this article, we review the history of privacy in banking. In the third section, the banking network modeling and simulation method are discussed. The fourth section presents the results of simulation, In the fifth section presented solutions to solve the problem is explained, and finally, in sixth Section, conclusions are done.

2. Literature review

With the expansion of the Internet and web, bank transactions have entered a new space of technology in which organizations are able to cooperate in financial calculations and transactions within a common space. Always between these transactions, an amount of private banking information is also transferred. Numerous studies have been carried out on protecting private information of individuals during financial transactions. Based on the protocol presented in [4], required data for data analysis are transmitted between partner organizations in form of encrypted data to ensure transmission security. In this method, each organization is divided into a number of virtual divisions and the encrypted data are distributed between these divisions. A Modifier Token is assigned to each virtual division. Then, these tokens are transmitted and alongside encrypted data combined with fake data. Received data are processed by computational functions, and in this way, the possibility of data theft is reduced to zero. Reference [5] firstly attempts to examine the millionaire's problem, which aims to find the wealthiest millionaire without knowing anything about their wealth, and further, introduces a few conclusive methods for this problem. The problem of forecasting and approximating data from statistics of similar organizations is introduced in [6] for the purpose of reaching cooperative benchmarking, and states that no organization tends to share its information with others. For this, the idea of determining private benchmarking is introduced, which initiates contribution in a way that prevents compromise of members' information. Methods including linear regression and time series techniques (e.g. Exponential Smoothing) are used in the presented protocol. The main difference between this method and other secure multiparty computation methods is use of floating point calculations. Reference [7] attempts to examine the prerequisites of a central authentication system in which each individual, by having an IDC identity card, can carry out payments and financial operations with maintained privacy. Anonymity and pseudo-anonymity techniques in transactions carried out with intelligent credit cards are examined in [8]. In recent years, a new definition of privacy namely k-anonymity has been introduced, which in a set possessing this feature, a record cannot be recognized from at least k-1 other records considering some predetermined recognition features. In [9], firstly, by introducing two types of attacks, the problem of lack of privacy protection in a set with k-anonymity conditions is shown, and then, it is specified that k-anonymity is incapable of protecting privacy against attackers with previous information about the set. Then, a method namely l-diversity is presented, which is capable of protecting the set data against such attacks. Another article examined the effect of security and privacy protection on individual tendency in using electronic banking systems, and utilized an extended version of the Technology Acceptance Model for testing this hypothesis.

3. Modeling and simulation

In this study, a set of banks providing banking services via ATM, POS, and the Internet, and their customers, which can be enterprises and or individuals, are modeled as intelligent agents. This set will work for a specific period under a series of regulations, which will be described in the following, and all financial transactions will be registered. Then, assuming that information related to the transactions of two of the banks are at the disposal of a third party, we will investigate to what extent private information of customers from other banks will be compromised, and we will show how much of the information which was not available at the initial stage, will be accessible through superposition.

A two-dimensional grid is considered for the completely modeled set, and banks, enterprises, and individuals are located in an arbitrary geographical location in the grid. In each instance of the simulation, individuals will have a random movement in the 2D environment; however, the location of the banks and enterprises is assumed fixed. During the simulation, individuals attempt to carry out their financial transactions base on their need, from the closest bank in their vicinity. In this model, it is assumed that banks and enterprises have only one branch; and it is assumed that each enterprise and or individual has only one bank account with any of the participating banks.

Moreover, it is assumed that the ATM device of each bank modeled in the 2D grid, resides only at the bank location, and each enterprise possesses a POS system of its related bank. In addition, all banks offer internet-banking services.

All businesses are modeled as enterprise type agents. Enterprises include three separate sets of commercial, industrial, and services enterprises; and the ratio and type of expenses vary for each set of modeled enterprises. Agents with low and medium level of income are modeled in each one of the three enterprises. Expenses related to each one of the three enterprises are given in Table 1, Table 2 and Table 3. In these tables, the "Value" column represents the ratio of each expense for different enterprise activities, and the "Schedule" column specifies the time tone for each activity. The "Payment/Year" column represents the annual frequency of each activity. As can be seen in the "Payment/Year" column of the expenses ratio, each expense item is spent in different frequencies throughout the year. The probability of related transactions occurrence is computed for each activity in a way that collectively at the end of the year, each enterprise has made transactions amounting to the specified number for each activity in the table.

Table 1: *Commercial enterprise*

Item	Value	Payment/Year	Schedule
Sales (Income)	100.00%	30	Random
Purchase (Cost)	65.00%	4	Random
Share Holder (Cost)	25.00%	4	Random
Employee (Cost)	3.00%	12	each month
Office (Cost)	2.50%	12	each month
Financial (Cost)	2.50%	12	each month
Tax (Cost)	2.00%	12	each month

***Table** 2: Industrial enterprise*

Item	Value	Payment/Year	Schedule
Sales (Income)	100.00%	30	Random
Purchase (Cost)	50.00%	50	Random
Share Holder (Cost)	15.00%	10	Random
Employee (Cost)	25.00%	4	Random
Office (Cost)	3.00%	12	each month
Financial (Cost)	2.50%	12	each month
Tax (Cost)	2.50%	12	each month

***Table** 3: Service Enterprise*

Item	Value	Payment/Year	Schedule
Sales (Income)	100.00%	200	Random
Purchase (Cost)	25.00%	4	Random
Share Holder (Cost)	65.00%	12	each month
Employee (Cost)	4.00%	12	each month
Office (Cost)	3.00%	12	each month
Financial (Cost)	3.00%	12	each month
Tax (Cost)	3.00%	12	each month

Individuals in the modeled society are categorized into two general sets, people that are employees of an enterprise, and stockholders. Stockholders based on the annual income of the enterprise, may constitute one or many individuals. As specified in the expenses ratio table, parts of the enterprise income will be assigned to stockholders. During the year, stockholder income is deposited to their accounts on a random basis. Moreover, one of the expenses of an enterprise is employee salaries. Employee salary for individuals working in each enterprise will be deposited to their account at the end of each month. In terms of income spending, individuals are categorized into sets of students, employees, senior employees, stockholders, and major stockholders, each of them having a different consumption pattern. Table 4 shows the income range for each simulated occupation set. Income of each individual based on the set it belongs to is randomly selected from the designated range in the table.

***Table 4**: Income ranges for each job (Toman)*

	Min Income	Max Income
Employee 1	400000	600000
Employee 2	400000	1000000
Employee 3	1000000	5000000
Share Holder 4	1000000	10000000
Share Holder 5	5000000	20000000

Individual expenses in a few general sets comprise basic living expenses, personal care expenses, leisure and entertainment expenses, educational and training expenses, and tax and savings. Table 5 shows the consumption pattern for each of the five considered individual sets accompanied by the proportion of each expense item.

***Table 5:** The proportion of each expense item to total revenue*

	Employee 1	Employee 2	Employee 3	Share Holder 4	Share Holder 5
Primary	0.600	0.500	0.300	0.200	0.150
Auto	0.000	0.100	0.100	0.100	0.100
Entertainment	0.100	0.100	0.150	0.200	0.200
Education	0.250	0.150	0.100	0.050	0.050
Tax & Insurance	0.050	0.250	0.250	0.250	0.250
Saving	0.000	0.000	0.100	0.200	0.25

The number of carried out transactions related to each expense is specified for each month. The probability of occurrence for each transaction is set in a way that overall, a specific amount of transaction are carried out within a month. As previously mentioned, individuals move randomly in the simulated grid during the simulation. Based on the mentioned expense pattern, they engage in financial transactions to fulfill their needs. If a physical purchase is made, the closest enterprise to the individual's location is chosen, and the transaction is made via POS. If it is an online purchase, the enterprise is chosen randomly, and an internet transaction will be made.

In this article, we assume that two banks are assigned to one advertising enterprise, and we want to know, apart from the information of the customers of the two banks, what other information from other banks' customers is accessible to the enterprise? The enterprise in question is interested in information such as individuals' social-economic class, monthly income level, method of individual spending, and their favorite leisure activities; and our objective in analyzing the transactions made by these two banks is to see whether this information can be obtained merely from some of the individual transactions randomly made through these banks?

4. Simulated results

An agent-based code is written in C++ language, and agents are simulated as described above.

In this section the results of the simulation are described. And It is shown that, upon disclosure of the data, much information will be accessible by unauthorized firms simply through people transaction history. The simulation is carried out in a specific time and all transactions are recorded separately for each bank. Then, two banks will be selected randomly, and it is assumed that, their information is provided to a third firm (For example, an ad agency). We want to know that, Except for the clients of two selected banks, what other information will be available to commercial firms by the customers of the other banks.

Using transaction data on the record for two selected banks, and based on the maximum level of account balance, that has been seen over a month in their account; people are divided into 5 categories. Account balance of each category is shown in Table 6. And in Figure 1 percent of those who belong to each of these five categories are indicated.

Table 6: *Classification based on the maximum account balance*

	Max Deposit
Level 1	0.4~0.6
Level 2	0.6~1.0
Level 3	1~5
Level 4	5~10
Level 5	10~20

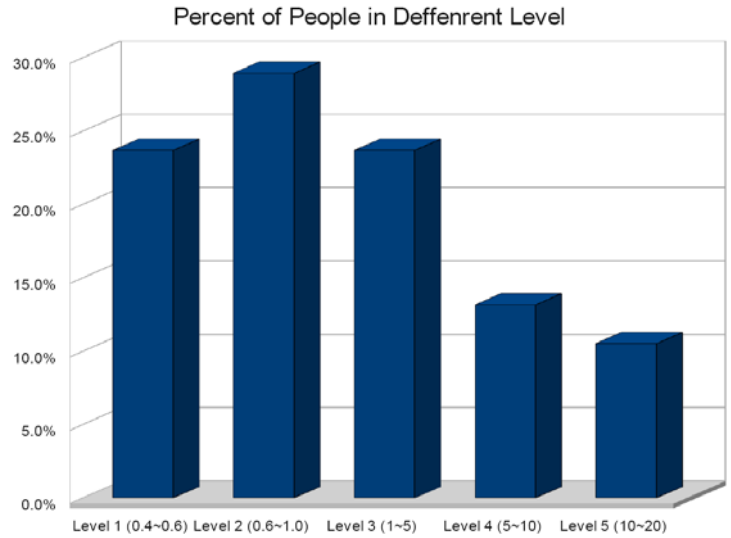

Figure 1: Classification based on the maximum account balance

Although these five categories of people do not necessarily shows the same categories that were created at the beginning of the simulation. But the average account balance that is repeated in several months is a good measure of the income level of individuals, and consequently their social or economic category.

In Figure 2 the average account balance of each of the categories is specified. Straight line perpendicular to the mean identifies minimum and maximum account balance for each category of individuals. So, advertsising agency has been able to use this data in determining the approximate level of income for these people.

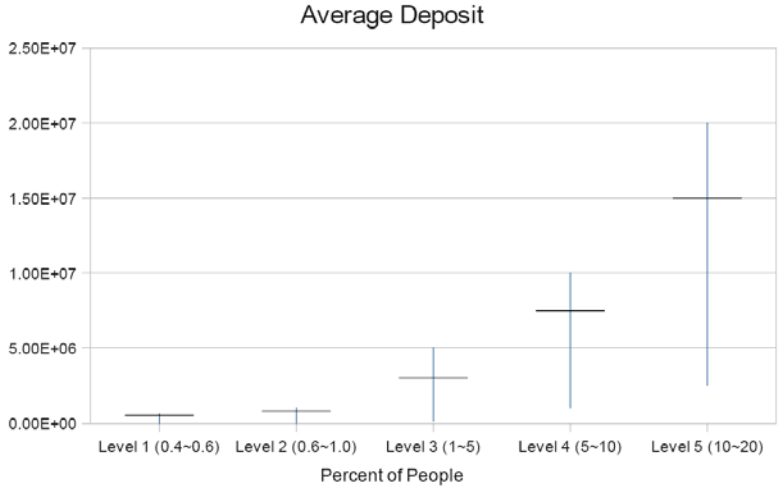

Figure 2. Approximate account balance of each category

With a closer look, people are classified, In terms of how to spend their income. As we shall see, Information in the cost of basic necessities (Primary Expense) maintenance costs of car (Auto Expense) and costs related to entertainment (Entertainment Expense) is to the extent, that we have been able to classify and to extract useful information. But In the other main items of costs, because there was little information, we've not been able to gather useful results.

In Figure 3, The subjects were divided into four groups. Based on the amount of money that has been spent for basic necessities of life (Primary Expense). The average cost is shown in figure, And the percentage of each group are shown below each column.

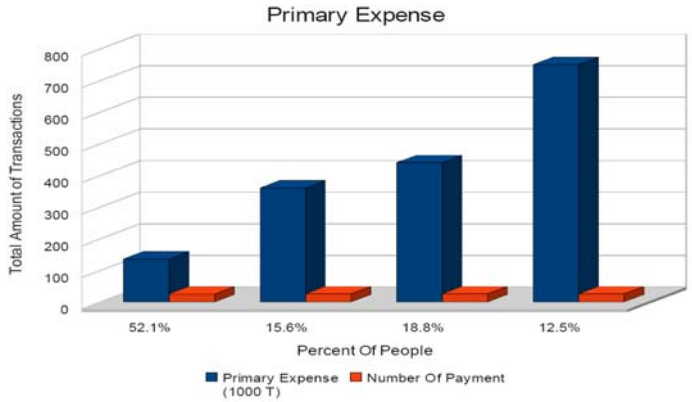

Figure 3: Average of Primary Expense for each group

In Figure 4, they are divided into 5 categories, Based on the amount of money they have spent for maintenance of personal car (Auto Expense). In Figure 5, based on the amount of money that people have spent for recreation (Entertainment Expense), they have been divided into four categories.

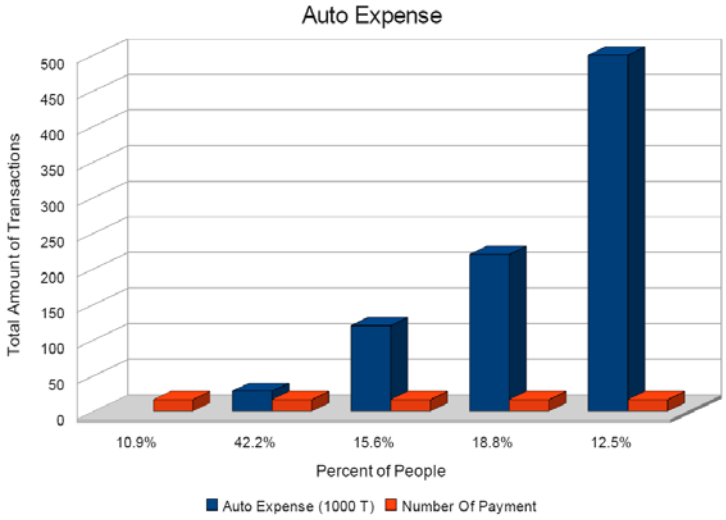

Figure 4: *Average of personal car expenses*

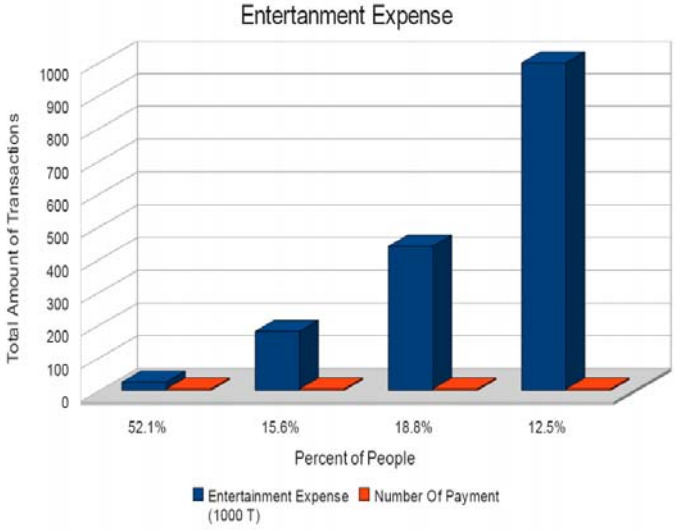

Figure 5: *Average of entertainment expenses*

The advertising agency has been able to classify people into groups, based on the average balance of the people's bank account, and how they spend their income. And so, based on these results, Advertising agency will be able to introduce products and services appropriate to each category.

It is clear that small and seemingly worthless information that comes in every transaction. How much could be valuable to another firm, and of course, how much privacy-threatening. Using the information gained here with the purpose of promoting the goods and services, may not seem so threatening. But surely with the amount of information gained here, there are many potential abuse, Which, unlike the example presented here, does not limit just to the ads! And may severely limit the scope of the individual's privacy

5. Proposed Solution

In this section, the solution to upgrade the banking system in Iran is proposed, to remove security and privacy problems in the current system as far as possible. Because many ATMs and POS Machines are working across the country, the new system is designed so that there is no need to change existing hardware. Also, in the design of new system, simplicity of use are taken intoconsideration. And application of hardware has changed very little, so that users are not confused.

Based on the above, and conditions in the country, most notably the lack of a PKI infrastructure, the proposed system is as follows.

1- Actual client profile information (client identity) is kept in the Central Bank, And Central Bank assigns a unique identification number (Bank-ID) to each Dual pair (bank - client).

2- Central Bank gives to every client a onetime password token (OTP). And by receiving the password generated by the token, And identification number (Bank-ID) of the Dual pair (bank-client) from the Bank, confirms the identity of the client. Central Bank approves an identification number (Bank-ID) only for the bank, which is part of the Dual pair (bank-client).

3- In every bank, a client has a unique account number, for each account. Thus, a bank client can have separate accounts with a single Bank-ID. Only through Internet website and ATMs of the reference bank it is possible to get account report or account balance.

Thus, except the central bank and the reference bank, a customer's true identity assigned to a Bank-ID is not revealed to other banks or agents. And if a customer has two bank accounts in different banks, one bank will not be able to identify the client's identity through the Bank-ID in another bank.

Client to perform banking operations via ports of the bank gives password generated by the token along his account number to the bank. Bank sends Bank-ID associated to client's Account-Number along the password received from the client, to the central bank. And finally, after receiving the customer authentication from Central Bank, Will allow the client to perform banking operations.

For banking through ATM, POS Machines and Internet portals of other banks, Intermediary bank receives account number and password from the user and sends it to the reference bank. Then reference Bank announces the result of the authentication process to the intermediary bank.

Tokens can be equipped with a USB port, so when the required hardware is present (e.g. online banking), Users do not need to type the generated password. A PIN code will be placed on the token, so, if the token is lost, it is not abuse.

6. Conclusion

In the first parts of this paper, it was shown that how the modern banking system in Iran may Lead to the disclosure of private information. Then, an alternative for this matter has been introduced for preservation of the privacy with maximum usage of current hardware and minimum change in software User Interface. As a result of using short term and onetime passwords, the methods is robust considering numerous offline data thefts. Furthermore, in comparison to current vulnerable state of banking transaction security, this method can provide highly improved security in banking services.

In Terms of privacy, because each bank identifies a customer with unique number and this identification number varies in different banks. Banks can never know the true identity of another bank customer, and on the other hand, given that account report and account balance through the banks are no longer available. Only transaction information will be provided to other banks. But since, bank cannot link the information to a natural or legal person. This information does not jeopardize the privacy of customers. Of course, if you need to track and review all transactions relating to an individual or firm in all banks. Assuming there is a court order, the central bank can discloses identification numbers assigned to a true identity in different banks, for the authorities.

Method proposed in this article would be very easy for bank customers, and they do not need to remember passwords for their various accounts or separate passwords for Internet banking. Also, users do not need to carry ATM cards and tokens of various banks. If they know their account numbers, they will need only a one-time password token, to access their accounts at different banks from the nearest port.

References

[1] A. Rad, “Security , simplicity and acceptability , issues of modern banking services in Iranian banking sector.”

[2] M. Morgenstern, *Security and inference in multilevel database and knowledge-based systems*, vol. 16, no. 3. ACM, 1987.

[3] A. HILTGEN, T. KRAMP, and T. WEIGOLD, “Secure Internet Banking Authentication,” *IEEE SECURITY & PRIVACY*, 2005.

[4] R. Pathak, S. Joshi, and D. Mishra, “A Novel Protocol for Privacy Preserving Banking Computations using Arithmetic Cryptography,” pp. 1–6.

[5] A. C. Yao, “Protocols for secure computations,” in *Proceedings of the 23rd Annual Symposium on Foundations of Computer Science*, 1982, pp. 160–164.

[6] M. Bykova, J. Li, K. Frikken, M. Topkara, M. Atallah, M. Bykova, J. Li, K. Frikken, and M. Topkara, "Private collaborative forecasting and benchmarking," in *Proceedings of the 2004 ACM workshop on Privacy in the electronic society*, 2004, pp. 103–114.

[7] E. Androulaki, B. D. Vo, and S. M. Bellovin, "Cybersecurity through an Identity Management System," 2009.

[8] R. Clarke, "Identification, anonymity and pseudonymity in consumer transactions: A vital systems design and public policy issue," *Proceedings of Smart Cards: The Issues, Sydney*, 1996.

[9] A. Machanavajjhala, D. Kifer, J. Gehrke, and M. Venkitasubramaniam, "L -diversity," *ACM Transactions on Knowledge Discovery from Data*, vol. 1, no. 1, p. 3–es, Mar. 2007.

[10] M. Lallmahamood, "An Examination of Individual ' s Perceived Security and Privacy of the Internet in Malaysia and the Influence of This on Their Intention to Use E-Commerce : Using An Extension of the Technology Acceptance Model," vol. 12, no. 3, 2007.