

# Customers & E-Customers insight towards the E-Banking

<sup>[1]</sup> Sabia Gupta, <sup>[2]</sup> Er. Kanwal Preet S. Attwal, <sup>[3]</sup> Dr. Gaurav Gupta

<sup>[1]</sup> Research Scholar, <sup>[2][3]</sup> Assistant Professor

<sup>[1][2][3]</sup> Department of Computer Science and Engineering, Punjabi University, Patiala

<sup>[1]</sup> guptasabia@yahoo.com, <sup>[2]</sup> kanwalp78@yahoo.com, <sup>[3]</sup> gaurav.shakti@gmail.com

**Abstract:** - Data Mining is helpful for getting the valuable knowledge from huge sets of data. Data mining techniques mostly have been seen in real-world databases. Many educational organizations like to work on the secure media for e-banking. E-banking provides many services to its clients but still customers are not satisfied. In all the services, security is one of the major issues. In this paper, data mining's cluster technique has been used along with SPSS tool and secured logins have been ensured by providing double security at the login. First is an image along with the username and password and second is a passkey which is sent by the bank server only to the respective user.

**Keywords:** - Data mining-banking, SPSS, Cluster technique, Likert scale.

## 1. INTRODUCTION

Data Mining is a process of finding hidden, unknown, valid and actionable information from previous databases and then using this information to make better results. It comprises many attributes, DM converts huge set of data into the valuable information [13].

### 1.1 Data mining and knowledge discovery databases

DM is additionally known in light of the fact that data decision in database (KDD). Data Mining can be supposed as a basic evaluation of information technology and a joining of various related disciplines and application domains [3]. The KDD represents in (Figure 1) comprises of following phases which narrates how undeveloped data converts into meaningful information.

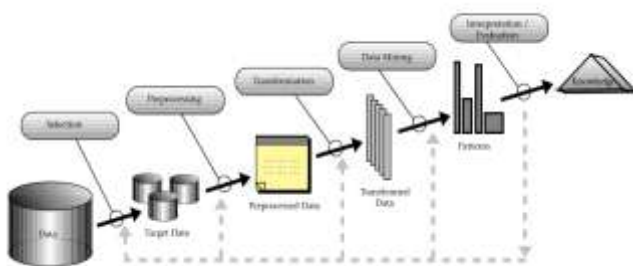


Figure 1: KDD process[3]

KDD handles following phases –

- This association is used for the majority sharing out answer while DM find out as well as find taking place or gone the inhalation data. The entire reorganize might not exceed if the quantify of input attribute is vanished.
- A scope of technique be sold through this period e.g. width diminish confirmation testing, trademark alter in signifying spot choice.
- At this stage, numerous information sources, regularly heterogeneous might be joined in a typical source.
- This period adapt the calculation picked in the before period. It might happen to run the calculation a significant barely any period close adjustment its systematize parameter pending a satisfying impact be gotten.
- Evaluation is the pre-last periods where the unearthing examples are translate in signifying weigh out by vital estimation to the goals.
- Exposed data is capable to live included into an extra association intended for more deed the whole KDD course wind up noticeably effective after the achievement of this stride.

### 1.2 Overview of e-banking security

Electronically managing an account is one of the really far reaching symbols of e-business the world over. Different creators characterize e-banking diversely however the most definition characterizes the importance

## **International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)**

**Vol 6, Issue 9, August 2019**

and highlights of e-Banking as per the following:

- E-Banking is a mix of two, electronic innovation and banking.
- E- Banking is a procedure by which a client performs saving money.
- Exchanges electronically without going to physical organizations.
- E-Banking indicates the arrangement of managing an account and related administration through extensive utilization of data innovation without guide plan of action to the bank by the client [5].

The common e-banking services come under following categories:

- Electronically charge introduction and installment.
- Funds exchange between a client's own checking.
- Bank accounts or to another client's record.
- Investment buy or deal.
- Loan applications and exchanges; for eg- Reimbursements, Bank explanations.
- Financial Institution Organization - Support of numerous clients having changing levels of expert.
- Transaction endorsement process.
- Wire exchange.
- Ticket booking.
- Shopping and so on.

E-Banking signifies the arrangement of saving money and related administration through extensive utilize of data innovation without guide plan of action to the bank by the client. The buyer recognition toward the easiness and eagerness to utilize e-managing an account are distinguished and estimated. Consumer loyalty level towards the E-Banking has been distinguished [9]. The physical approaches or services are only for old age customers & for illiterate people those who don't have the knowledge to operate the e-banking. Sometimes it becomes a big issue to discuss about which technique is reliable for the people.

Customers rapidly switch to e-banking because of time & services. Customers are more satisfied in e-banking services rather than banking [13]. The growth of business increases very fast because of money transfer system is very easy in e-banking. ATM services are best way for withdrawals their money without any interface & interruption from anywhere to any time [3].

The most admired services exposed below e-banking contain:

1. Automated teller machines
2. Credit Cards
3. Debit Cards
4. Smart Cards

5. Electronic Funds Transfer system
6. Mobile banking
7. Internet banking
8. Telephone banking

### **1.3 Internet or E-Banking**

Web managing an account empowers a client to perform keeping money exchanges through the bank's site. This is additionally called virtual managing an account or anyplace managing an account [9]. It resembles conveying the bank to one's PC at one's preferred place and time. The quantity of customers who pick web based keeping money as their saving money normally offers highlights like electronic bill installment.

#### **1.3.1 Security in e-banking**

Data security comprises of three fundamental parts: secrecy, respectability, and accessibility. Every one of the three sections of security might be influenced by absolutely specialized issues. Validation techniques similar to customers id and passwords that recognize clients can come to the objective of secrecy. Other control techniques support confidentiality. For e.g.: constraining each distinguished customer's entrance to the information framework's assets [9].

#### **1.3.2 Attacks on E-Banking**

Hackers have various ways that they can attempt to break into the framework. The issues of the frameworks today are characteristic inside the setup of the interchanges and furthermore inside the PCs itself. The present concentrate of security is on session-layer conventions and the imperfections in end-to-end processing. A safe end-to-end exchange requires a safe convention to convey over entrusted channels, and a trustee code at the two endpoints [11].

There are different sorts of assaults that e-banking can endure. They incorporate:

1. **Social Engineering:** A standout amongst the most widely recognized assaults does not include learning of a PC framework. Misleading purchasers into uncovering touchy data by acting like a framework executive or customer benefit agent is known as social designing [3].
2. **Port Scanners:** Attackers can utilize port scanners to learn section focuses into a framework and utilize different strategies to take data. The fundamental motivation behind a port scanner is to accumulate data identified with equipment and programming that a framework is running with the goal that an

## International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)

Vol 6, Issue 9, August 2019

arrangement assault can be created [11].

3. **Bundle Sniffers:** The association between a client's PC and the web server can be "sniffed" to accumulate a plenitude of information concerning a client including Visa data and passwords. The utilization of a Secure Socket Layer association is the most ideal approach to guarantee that aggressors using bundle sniffers can't take delicate information [11].
4. **Secret word cracking:** Secret word breaking can include diverse kinds of vulnerabilities and unscrambling procedures. Beast constrain splitting exploits frameworks that don't require solid passwords, hence clients will frequently utilize regular names and exercises making it straightforward for a secret word wafer to access a framework [11].
5. **Trojans:** Trojans can be utilized to channel information from a wide range of customers, servers, and database frameworks. Trojans can be introduced to screen messages, texts, database interchanges, and a large number of different administrations [9].
6. **Server Bugs:** Server bugs are regularly found and fixed in a fortunate manner that does not enable an attacker to use the danger against an e-commerce site. In any case, framework directors are frequently ease back to actualize the most up to date refresh [13].
7. **Password Cracking:** Password Cracking breaking can include diverse sorts of vulnerabilities and decrypting techniques;. Brute force secret key assaults are utilized to split a person's username and password for a particular site. Other password breaking techniques utilizing hash tables to unscramble password records that may disclose a whole frameworks client name also, password list
8. **Intrusion detection and audits of security logs:** Security strategy is to prevent attacks and to detect Potential attackers. This helps understand the nature of the system's traffic, or as a starting point for legal action against the attackers. Suppose that you have implemented a password policy: If a consumer makes 6 failed logon Attempts, then his account is locked out. In this scenario, the company sends an email to the customer, informing them that his account is locked. This incident should also be logged in the system, either by sending an email to the administrator, writing the event to a security log or both.
9. **Identity theft:** Fraud is a wrongdoing in which a phone gets key bits of individual data, for example, date of birth, bank subtle elements in order to copy another person. The individual data is utilized wrongfully to apply for credit, buy goods and administrations, or access financial balances.

**10. Keystroke catching/logging:** Keystroke logging is frequently utilized by fraudsters to catch individual elements including passwords. The danger of experiencing keystroke logging is more noteworthy on PCs shared by various clients.

### 1.3.3 Present security systems for e- banking

To get to web based managing an account offices, a client need to enroll him with an exceptional id and secret key for client check. The new User id must be 6 to 19 characters and the secret key must be 8 to 17 characters and should contain no less than 2 alpha and 2 numeric characters. Client can set security information to email address, Security Queries, Authentication Pass Phrase and Computer Registration. Presently, client can access and take full advantages of internet saving money administrations.

- **OTP:** (One Time Password) Client can utilize this OTP for better security on the web exchange by downloading unique secret word age programming to their cell phone. Client can perform verification by entering an OTP showed by the cell phone application notwithstanding their typical ID and secret word.
- **QRP:** (Quick Response Protocol) is a safe verification framework that uses a two factor confirmation by consolidating a secret word and a camera prepared cell phone, where cell phone is going about as a confirmation token.
- **Security Question:** A client was exhibited the principal security challenge question and had two chances to answer appropriately. In the event that the client didn't give the right reaction, the second security challenge question was exhibited and the client again had two chances to give the right answer.
- **SMS keeping money:** SMS Banking is an administration that gives clients to get to their record data by means of portable handset. SMS keeping money offices are worked utilizing similarly push and draw messages. Push messages are those that the bank chooses to convey to a client's handset, without the customer starting a demand for the data. Draw messages are those that are presented by the client, for acquiring data, utilizing a cell phone.

## 2. METHODOLOGY

### 2.1 Introduction

A questionnaire has been intended to gather the information from the respondents. The study is embraced in Urban communities specifically as these urban areas are

## International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)

Vol 6, Issue 9, August 2019

immature and less investigations have been directed there for comprehend the capability of e-banking money. Advantageous inspecting configuration has been utilized. T-test and rate strategies have been utilized to dissect the information.

The examination is worried about the customer attention towards e-banking. The information is gathered through pretested, Weighted Average score will figured from the five point likert scale. Weights will give in view of the positions. The most elevated weight is given to first rank and the least weight is given to most reduced rank.

Following steps taken through research:-

- Comprehend the different administrations gave under the shades of e-banking.
- Proposing ways for assembly e-banking.
- Interrelate with customers, e-customers & bankers.
- Investigate the collected response by using various statically test, data mining tools & techniques.

### 2.2 Pre requisite

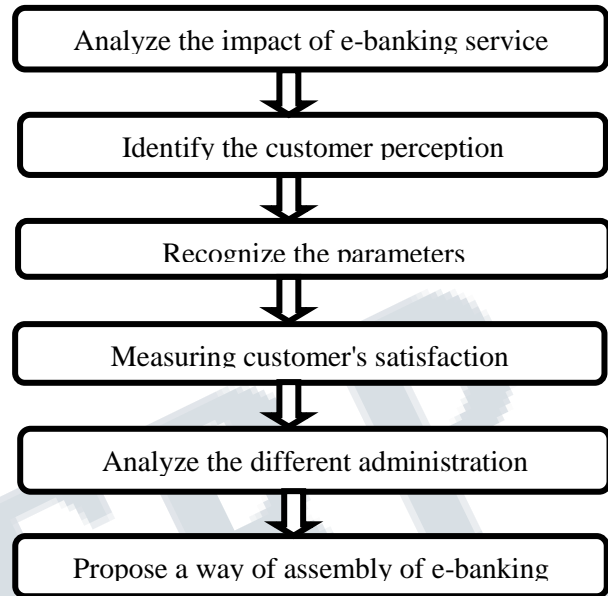
The information gathering was completely based on survey done by means of inside and out individual meetings.

- Testing design-stratified and irregular examining for investors, e-customers and bank customers.
- Data Collection
  - **Primary Data:** Structured Questionnaire.
  - **Secondary Data:** Online Database, Journals, Survey
  - **Sampling:** The study's objective was accomplished through the collection and analysis of primary data obtained from a purposive sampling technique. Likert scale questionnaire was used to measure the perception of customers about e-banking. Members of the population are chosen based on their relative ease of access. To sample relatives, friends, co-workers, businessman, govt. employees, are all examples of convenience sampling.
- Test Size
- Data mining apparatuses
- For information gathering MS-Excel, Text records and so on.
- SPSS tool

### 2.3 Algorithm for present work

- Analyze the impact of e-banking service
- Identify the customer perception
- Recognize the parameters
- Measuring customer's satisfaction

- Analyze the different administration
- Propose a way of assembly of e-banking



*Fig 2: functionality of e-banking*

The first step in the basic algorithm followed during this research work was the analysis of the impression of e-banking services over the customers. The second step was to find out what the customers perceived. The third step included the recognition of the various parameters. The fourth step was to measure the contentment of the customers. The next step was analyzing different administration. The last step was to propose a way of assembly of e-banking.

## 3. RESULTS AND DISCUSSION

The main aspect of this research is to design a scenario which helpful for e-banking security. Various responses from customers and e-customers had been collected according to the questionnaire framed. The response collected is analyzed and classified using classification technique as presented below

### 3.1 Demographic Profile

The distribution of respondents according to various socio-economic characteristics is described below:-

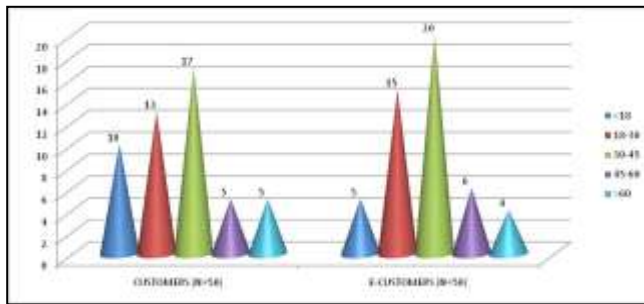
#### 3.1.1 Age

A Table 6.2.1 shows that highest proportion of customers belongs to age group of 30-45 years, followed by 18-30 years. The lowest proportion was of age greater

than 60 years. Similar trend has been observed in e-customers as the highest proportion belongs to age group of 30-45 years, followed by 18-30 years. The lowest proportion was of age greater than 60 years. It is predicted that old aged people do not like banking or e-banking. It is also shown in fig 6.2.1

Demographic Profile	Customers (N=50)	e-Customers (N=50)
Age (years)	Frequency	Frequency
<18	10	5
18-30	13	15
30-45	17	20
45-60	5	6
>60	5	4

**Table 6.2.1: Age demographic profile**



**Fig6.2.1 : Age demographic profile**

**3.1.2 Gender**

As shown below, majority of the customers as well as e-customers are males in contrast to females. It may be due to the fact males are more encouraging in visiting bank and availing e-banking services.

Demographic Profile	Customers (N=50)	e-Customers (N=50)
Gender	Frequency	Frequency
Male	30	37
Female	20	13

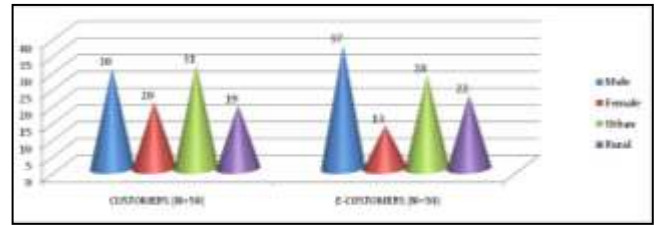
**Table 6.2.2: Gender demographic profile**

**3.1.3 Locality**

As shown below, majority of customers and e-customers are living in urban areas according to the response.

Demographic Profile	Customers (N=50)	e-Customers (N=50)
locality	Frequency	Frequency
Urban	31	28
Rural	19	22

**Table 6.2.3: Locality demographic profile**



**Fig 6.2.2 Gender and locality demographic profile**

**3.1.4 Occupation**

Occupation table shows that majority of customers and e-customers are either in some service or business. Only few are unemployed or retired.

Demographic Profile	Customers (N=50)	e-Customers (N=50)
Occupation	Frequency	Frequency
Service/Business	20	28
Agriculturist	15	2
Unemployed	2	3
Retired	5	5
Any Other	8	12

**Table 6.2.4: Occupation demographic profile**

**3.2 Perception of Customers and e-Customers**

Parameters such as “Don’t trust internet services when it comes to managing money”, “Unexpected system failure & framework”, “Security provides (Cyber security, information uprightness, assurance of client’s classified data and wholesale fraud)”, “Not being able to maintain security” has been found highly significant as indicated by “\*\*\*” in t-values. These all parameters reflect that respondents are aware of e-banking security issues. They still do not have trust on e-banking system and afraid to use netbanking in order to lose their money.

Parameters such as “Threats from Hackers through encryption of login”, “E-banking not being able to maintain security”, “E-banking security always updated to protect any theft or fraudulent”, “Timeliness of data through web keep money “, “Bank quickly resolves problems when customer encounters with own online transactions”, “Increased comfort and time-saving” have been found to be significant as indicated by “\*” in their t-values. All these parameters also reflect the securities issues. Other factors have been found to be a part

**International Journal of Engineering Research in Computer Science and Engineering  
(IJERCSE)**

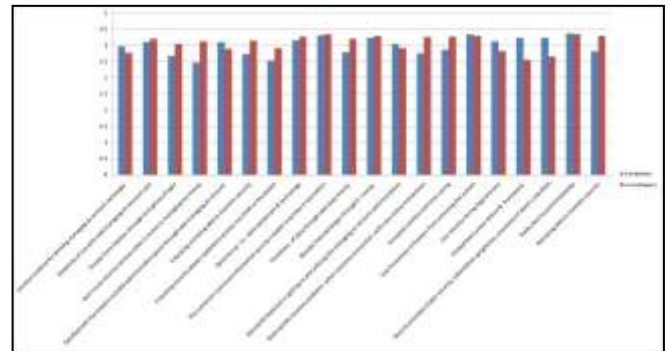
**Vol 6, Issue 9, August 2019**

PARAMETERS	Customers	e-Customers	T-Test
Comfort method for working managing an account exchanges	3.97	3.77	1.087
Simplicity of use with web managing an account cash	4.11	4.21	0.638
Threats from Hackers through encryption of login	3.68	4.05	2.106*
Don't trust internet services when it comes to managing money	3.47	4.13	3.511**
Satisfied with the esteem included administrations given through web managing an account	4.11	3.89	1.292
E-banking not being able to maintain security	3.74	4.15	2.597*
E-banking security always updated to protect any theft or fraudulent	3.53	3.92	2.478*
Bank has up - to - date equipment & technology	4.16	4.27	0.702
The customer's personal information security is better now than it was before	4.32	4.35	0.32
Timeliness of data through web keep money	3.79	4.21	2.552*
Blunder free exchanges through E- money	4.24	4.29	0.345
Decreased expenses in getting to and utilizing the managing an	4.05	3.92	0.823

account administrations			
Bank quickly resolves problems when customer encounters with own online transactions	3.76	4.26	2.68*
Increased comfort and time-saving	3.87	4.27	2.637*
Low Prevention of hackers from accessing the system	4.34	4.29	0.354
Less security during login process	4.13	3.82	1.865
Unexpected system failure & framework	4.24	3.56	3.655**
Security provides (Cyber security, information uprightness, assurance of client's classified data and wholesale fraud).	4.24	3.66	3.548**
Thefts Not Found Immediately	4.37	4.35	0.091
Not being able to maintain security	3.83	4.29	2.731**

**Table 3.3.1: Perception of respondents**

All the values have been represented in column chart as:



**Fig 3.2.1: Chart representation of respondents**

The fig 3.2.1 depicts a chart where blue bars represent the customers and red bars represent the e-customers. This

## International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)

Vol 6, Issue 9, August 2019

chart shows the response of customers and e-customers towards various factors plotted on the chart.

### 3.3 Summary

In this research work, views of the customers have been taken. The parameters on the different demographic profiles are graphically represented in the form of tables and charts. The comparison respondents of different datasets are shown in tabular form.

### 4. CONCLUSION AND FUTURE SCOPE

The present verification strategy for on the web installment framework isn't exceptionally secure to shield client from data fraud, therefore any assailant can pick up the entrance on the secret data of client like Visa number or record password and make unlawful exchange of information. It is demonstrated from our experience that solitary factor validation builds dangers postured by phishing, data fraud, misrepresentation and loss of client classified data.

This paper is based on research work being done towards secured logins to ensure that no hackers can hack your account because of the two more securities applied on the login, first one is image along with the username & password and second is passkey which is only accessible to you and is sent by the bank server through e-mail.

To know what the future of online banking looks like, it's probably worth looking at the present – online banking isn't new. In this regard, those destined to utilize the web are in the upper pay gathering, proficient. The connection amongst proficiency and view of Customers can likewise be done to best judge the execution of the banks. A vast example of Customers and E- Customers might be overviewed to have profound view of e-saving money benefit per exchange expenses of the banks working in India. More images can be added to confuse the hacker. Equation can be more difficult. The e-mails can be converted into the messages. In demographic profiles, factors can be added more. Parameters can be increased by future need for analyzing, security images can be including more in the choice of selection for customers. The passkey can be made more difficult which can have more than 6 characters with symbols.

### REFERENCES

- [1] A. Kshirsagar, L. Dole (2014), "A review on data mining methods for identity crime detection", *International Journal of Electrical, Economics and computer systems* 2(1), pp. 51-55.
- [2] Amutha (2016), "A study of consumer awareness towards E-Banking", *International Journal of Economics & Management Sciences*, 5(4), pp. 350-353.
- [3] B. M. Ramageri (2014), "Data mining techniques and applications", *Indian Journal of Computer Science and Engineering*, 1(4), pp. 301-305.
- [4] D. N. V. K. Reddy, M. S. Reddy (2015), "A study on customer's perception and satisfaction towards electronic banking in Khammam district", *IOSR Journal of Business and Management*, 17(12), pp.20-27.
- [5] D. Stojanovic, M. Krstic (2017), "Modern approaches and challenges of risk management in electronic banking", 10th International Scientific Conference "Science and Higher Education in Function of Sustainable Development", 2(7), pp. 41-48.
- [6] E. A. Shanab, S. Matalqa (2015), "Security and fraud issues of E-Banking", *International Journal of Computer Networks and Applications*, 2(4), pp. 179-187.
- [7] E. M. K. Ahmad, H. A. Zubi (2011), "E-banking functionality and outcomes of customer satisfaction: An empirical investigation", *International Journal of Marketing Studies*, 3(1), pp. 50-65.
- [8] E. R. Nwogu (2014), "Improving the security of the internet banking system using three-level security implementation", *International Journal of Computer Science and Information Technology & Security*, 4(6), pp. 167-176.
- [9] Fozia (2013), "A comparative study of customer perception towards e-banking services provided by selected private & public sector bank in India", *International Journal of Scientific and Research Publication*, 3(9), pp. 283-292.
- [10] F. S. Roozbahani, S. N. Hojjati, R. Azad (2015), "The role of e-payment tools and e-banking in customer satisfaction", *International Journal of Advanced Networking and Applications*, 7(2), pp. 2640-2649.
- [11] L. Ali, F. Ali, P. Surendran, B. Thomas (2016), "The effects of cyber threat on customer's behavior in e-banking services", *International Journal of E-Education, E-Management and E-Learning*, 7(1), pp. 70-78.
- [12] M. Rani (2012), "A study on the customer perception towards e-banking in Ferozpur district", *International Journal of Multidisciplinary Research*, 2(1), pp. 108-118.
- [13] N. Devadiga, H. Kothari, H. Jain (2017), "E-banking

**International Journal of Engineering Research in Computer Science and Engineering  
(IJERCSE)****Vol 6, Issue 9, August 2019**

---

- security using cryptography, steganography and data mining ”, International Journal of Computer Applications”, 164(9), pp. 26-30.
- [14] N. Jain, V. Srivastava (2013), “Data mining techniques: A survey paper”, International Journal of Research in Engineering and Technology, 2(11), pp. 116-119.
- [15] S. Pakojwar, N. J. Uke (2014), “Security in online banking services-A comparative study”, International Journal of Innovative Research in Science, Engineering and Technology, 3(10), pp. 16850-16857.
- [16] U.S. Rajput (2015), “Customer perception on e-banking service”, Pacific Business Review International, 8(4), pp. 85-94.
- [17] V. Jayasree, V. S. Balan (2013), “A review on data mining in banking sector”, American Journal of Applied Sciences, 10(10), pp. 1160-1165
- [18] V. Jham (2016), “Customer satisfaction with internet banking: Exploring the mediating role of trust”, Journal of Emerging Trends in economics and Management Sciences, 7(2), pp.75-87.
- [19] Z. B. Omariba, N. B. Masese, G. Wanyembi (2012), “Security and privacy of electronic banking”, International Journal of Computer Science Issues, 9(4), pp.432-446

