International Journal on Recent and Innovation Trends in Computing and Communication ISSN: 2321-8169
Volume: 7 Issue: 1 35-42

Classification of Bank Employees in Using Biometric System

Gaurav Gupta
Department of Computer Science and Engineering
Punjabi University, Patiala (Pb), India
gaurav.shakti@gmail.com
ORCID - 0000-0002-9273-6511

Abstract **-** Today's century is driven majorly by the IT scenario which has proved to be a great boon for the society but as every coin has two sides, hence the advancement in IT has urged the need to secure one's private database from the hackers. Therefore, today banks are scrolling for the techniques to provide quicker, easier and secured banking transactions to the authenticated users. Security is one major factor that holds the power to strengthen or disrupt the customer's trust in the banks. Implementation of an effective authentication method, that allows the access only to the authorized users, can contribute a great deal of help to the banks in providing safe and secured services to their customers. Thus, Biometric authentication method is one pioneer way that can be utilized in the banks in order to offer a relatively higher degree of security, which is implemented in numerous banks around the globe. One primary issue that arises while dealing with the application of the biometric authentication system at the banks is the consent of the employees and their willingness and flexibility to accept the change in the banking process. Therefore, the current paper discusses about the employees' conceptions with respect to the introduction and implementation of the secure biometric authentication system amongst the Indian public and private sector banks and the issue has been inspected vividly in the thesis.

Keywords: Data Mining, Classification, Biometric system, t-test, Frequency

*****

1. INTRODUCTION

One significant factor that contributes to the growth and upliftment of an enterprise or organization is 'trust'. Hence, it is very vital for an organization to maintain a level of trust amongst its customers so as to maintain a healthy bond of client-customer relationship. Therefore, it becomes even more crucial for the financial institutions and banks to maintain a trustworthy bond as they hold a pivotal role in contributing towards the economic development of the countries. It is the primary objective of the banks specifically, to ensure that the customer's investments are in safe hands and are subject to no sort of danger. A bank can readily win the customer's reliance by maintaining pace, easiness and security in the services offered by the banks but there are other factors too which add to the process which compel the banks to take sufficient care of the customer's interests and hence leave no space for carelessness that may lead to security disaster. Being a part of this advanced IT world, the banks must take a step forward to adopt a security method which is both reliable and easy to use. Therefore, based on the analysis of the customers, the authentication process at the banks can be distributed into three broad categories:

Information that user knows (For instance- passphrase, PIN (Personal Identification Number))

Information that user owns (For instance- identification card, passport, swipe card, USB tokens and keys)

Information related to what user is (Biometric) (Wu, 1998).

2. BIOMETRIC SYSTEM

A biometric authentication system is designed to verify one's identity by measuring one or more physical or behavioral characteristics so as to provide access to the protected information only to the authorized users. Biometrics serve to be a secure and convenient authentication method since biometric traits are inherent to an individual, hence it offers complete protection as it is practically neither possible for the intruders to manipulate the biometric features nor for the users to share or forget their biometric characteristics (Jain et al, 2011). Some of the widely known techniques employed for biometric authentication include- hand scan, iris or retina scan, fingerprints, heart beat etc.

Biometric Technology has numerous applications in various aspects of daily life for instance- law enforcement, forensic applications, passport enquiry process, financial sector, industry employee registration, healthcare applications and many more to contribute to the list (Drygajlo, 2006). Thus, one is not wrong in saying that biometric technology offers a great deal of help in maintaining and uplifting the level of security for allowing authorized access only to the authenticated users. Specific major tasks that are involved in a banking system process include- branch banking, ATM banking, internet banking, telephone banking and POS

banking. Therefore, the implementation of biometric protection system in these operations can bring a great advancement in the level of security. In addition to the benefits that the biometric protection technology showers on the bank organizations there are certain issues that require to be addressed with regard to the implementation of the biometric authentication system which includes- training of the employees, creating customer awareness, considering economical problems etc which are equally crucial and vital in the implementation process of a strong reliable protection system. The preliminary step that is required to be taken by the bank before initiating the process of implementation is to evaluate and jot down the total cost that would be involved in the whole process of implementation of the biometric authentication system. Not to ignore that a robust reliable protection structure like Biometrics can prove to be advantageous if that banks are supported by knowledgeable employees who are quite familiar with the working of such a system and hence can contribute to the implementation process. The following sections throw some light on the advantages of the biometric authentication system.

3. LITERATURE REVIEW

In today's scenario where internet has touched almost every aspect of life, it becomes very crucial to secure the information traversing through the web. Therefore, in order to promote internet banking amongst the customers it is very vital to ensure that the security measures undertaken do not compromise with the privacy rights of the customers, Peterson (2003). According to the study conducted by Lee (2006), a new scenario came into picture which revealed that the acceptance rate of the facility of online banking is influenced majorly by demographic factors, it was further revealed that the section of population which utilizes this facility the most points towards the youth, who use this facility for numerous online transactions permitted by the banks (like online shopping of various products e.g. clothes, food etc).

As per the views of David (2006), the success of an e-banking facility relies to a great extent on the financial products and the quality of service offered to listen to and satisfy to the needs of the customers. Further, David (2006) also discussed that certain factors like convenience and easiness in using the banking system, assurance of secure transactions and the pace of the network are some of the characteristic features which effect the utilization of online banking concept amongst the customers.

The decision of the customer to prefer online banking depends on the single most vital factor which includes the vivid research on the customer relationship management, David (2008).

Boukhonine et al., (2005), the fundamental objective of a bank is to offer a sound environment of protection to its customers in internet banking transactions. The factors that hold a great potential role in the process of framing a reliable security policy include accountability, integrity, confidentiality, availability and non-repudiation concerns. Thus, the banks employ a robust security policy by keeping in focus the above discussed potential concerns by utilizing various physical devices like support access cards, and automated monitoring system that holds the right to accept or reject the deployment or usage of any particular information or object into the system.

Madu and Madu (2002) were of the view that security of the private information of the customers is the major cause of dissatisfaction among them as they are not sure about the reliability of the authentication system being used by the banks.

Ihejiahi (2009) expressed his concern about the issue of increasing cases of ATM frauds in the market and the banks failing to address the soaring issue with sincerity. He was of the view that the banks which are supposed to be the most reliable and trustworthy organization for the customers must deploy such a protection method which envelops a strong firewall against such online theft cases.

Obiano (2009) was of the view that the task involving distribution of ATM cards among the customers was done without creating proper awareness and knowledge about the utilization of the card, due to which the customers generally exhibit careless attitude in maintaining the crucial card details like PIN number properly and also get easily deceived by the various fake websites and text messages demanding the card details of the customers.

Omankhanleu (2009) has put forth an opinion that the soaring situations of ATM (Automated Teller Machine) fraud cases are piling up to the issue of customer dissatisfaction which requires great attention and thought from the banks' perspectives of the nation so as to keep up to the expectations of the customers and allow them a safer sound journey in pursuing online transactions.

Adeloye (2008) observed that the major factors which contributed to the ATM fraud cases in Nigeria were security and power suspension. Further, Brunner et al. (2004) concluded in their study that one vital factor responsible for ATM thefts is possibly the location of the ATM point. The facts fetched from the research showed that about 75% of the ATM swindle cases, as asked by respondents, were due to the deserted locations of the ATM points. Thus, an ATM point located at a nearby spot to the banks is supposed to have relatively more security in comparison to the one located in a secluded place, hence a place of crowd like malls, market place etc can serve to be the most suitable locations for the ATM points where chances of thefts are negligible.

Diebold (2002) stated that a major proportion of ATM fraud cases occurred as PIN theft i.e. stealing away of the PIN

number of an ATM holder. It was reported that majority of the customers were struck by PIN thefts, which occurs mainly by shoulder surfing, keypad recording equipment, skimming etc. On further research it came out that PIN thefts occur majorly due to congestion at the ATM points, an issue to be addressed and sorted. Certain other forms of ATM fraud cases that came on bench from the respondents included card theft, force withdrawal etc at the ATM point. Thus, it came out that the protection at ATM points, say by appointing a guard was essential.

Cynthia (2000) presented a view that providing ATM service round the clock is like two sides of a coin situation, which has both the bright and the dark side.

Roli Bansal et al (2011) addressed that keeping in consideration all the fingerprint features, the minutia point characteristics clubbed with relative orientation maps are quite exclusive to distinguish amongst the fingerprints effectively. It was further stated that the minutiae feature presentation contributes a lot in reducing the intricate fingerprint pattern recognition to a point pattern matching query.

It is quite clear from the above discussed and portrayed literature review that numerous studies have organized and observed with regard to Bio-Metric Protection System specifically with respect to banks keeping in view their security perspectives. However, it was observed that rarely any sort of research was conducted to illustrate the urgency of awareness creation to the bank customers and employees.

4. OBJECTIVES OF STUDY

Thus, on the basis of the above discussion, the following study was proposed. Following comprise the definitive objectives of the current study,

- To appraise the rate of effectuation of the Bio-Metric Systems in the Banks
- To appraise the performance and the efficacy of the Bio Metric Systems implemented in the Banks
- To appraise the views and aspects of the Bank employees' perspective with regard to the Bio Metric System
- To seek ideas or suggestions for the efficient deployment of the advanced Bio Metric Authentication System in the Banks.

5. RESULTS AND DISCUSSION

Demographic Profile

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

Gender

As listed in the Table 5-1 below, majority of employees are males as compared to females. This may be due that they are still not allowed to do job frequently as compared to males. It is also is shown in Figure 5-1 below.

Table 5-1 Gender Demographic Profile

Demographic Profile	Employees (N=200)
Gender	**Frequency**
Male	113
Female	87

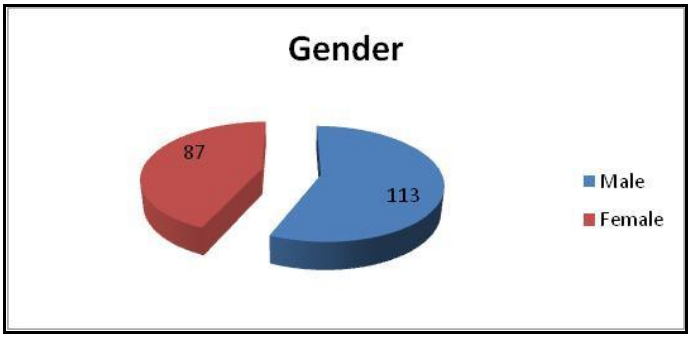


Figure 5-1 Gender Demographic Profile

Age

A perusal of Table 5-2 below shows that highest proportion of employees belongs to age group of 25-50 years, followed by >50 years. The lowest proportion was of age <25 years. The mean age in case of males and females comes out to be 39 and 35 years respectively. This shows that maximum employees belong to age group of 25-50 years. It is also is shown in Figure 5-2 below.

Table 5-2 Age Demographic Profile

Demographic Profile	Employees (N=200)	
Age (years)	**Male**	**Female**
<25	21	19
25-50	67	44
>50	25	18
Mean	**39.02**	**35.46**

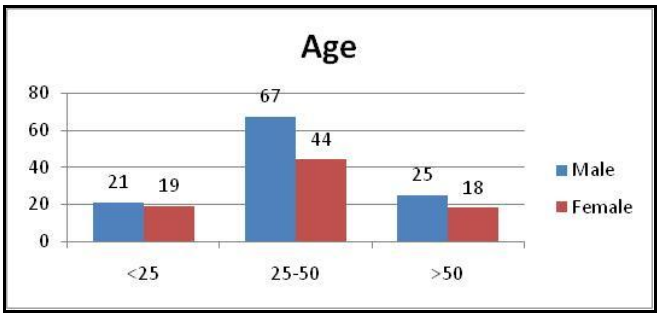


Figure 5-2 Age Demographic Profile

Marital Status

As illustrated in the Table 5-3 below, majority of employees belongs to the married class. This is due to the fact as the average age of employees is over 35years. It is also is shown in Figure 5-3 below.

Table 5-3 Marital Status Demographic Profile

Demographic Profile	Employees (N=200)
Marital Status	**Frequency**
Single	78
Married	122

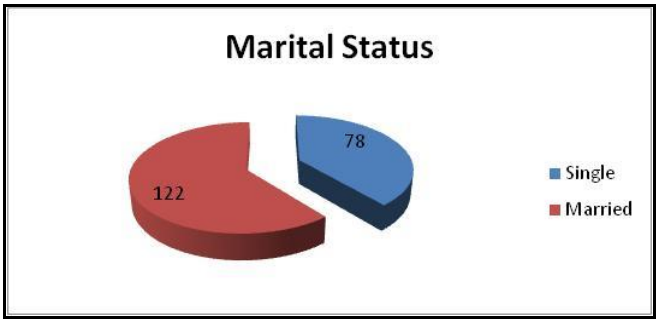


Figure 5-3 Marital Status Demographic Profile

Area

As illustrated in the Table **5-4** below, majority of employees belongs to the urban area. This is due to the fact as the average age of employees is over 35years and has to settle their family and kids. It is also is shown in Figure 5-4 below.

Table 5-4 Marital Status Demographic Profile

Demographic Profile	Employees (N=200)
	Frequency
Rural	72
Urban	128

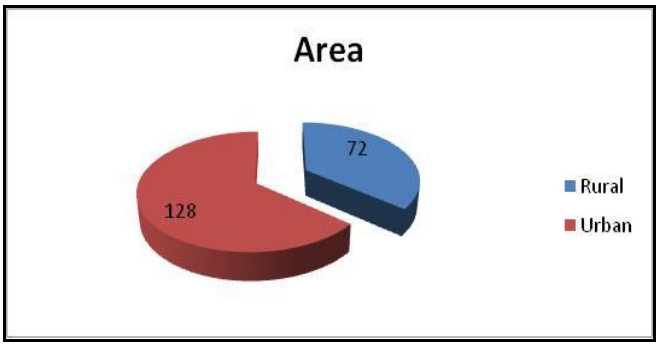


Figure 5-4 Marital Status Demographic Profile

Annual Income

As depicted in the Table 5-5 below, the highest proportion of employees belongs to group 3-5 lacs, followed by 5-7 lacs group then by 1-3 lacs whereas lowest is <7 lacs followed by >7 lac. The same proportion is followed among males and females. It is also is shown in Figure 5-5 below.

Table 5-5 Annual Income Demographic Profile

Demographic Profile	Employees (N=200)	
Annual Income	**Males**	**Females**
<1 lac	3	2
1-3 lacs	18	15
3-5 lacs	44	33
5-7 lacs	31	22
>7 lacs	17	15

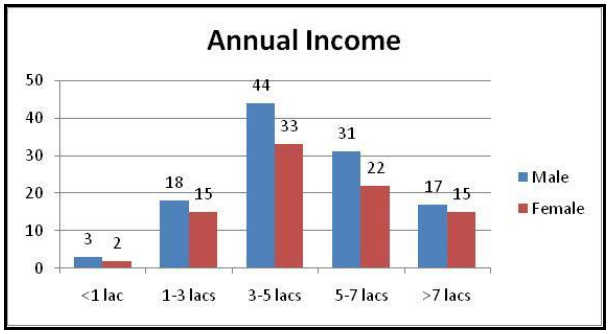


Figure 5-5 Annual Income Demographic Profile

Education

As illustrated in the Table 5-6 below, the highest proportion of employee belongs to graduate group, followed by post graduate group and any other whereas lowest proportion belongs to illiterate followed by higher education group. The same proportion is followed among males and females. It is also is shown in Figure 5-6 below.

Table 5-6 Education Demographic Profile

Demographic Profile	Employees (N=200)	
Education	**Males**	**Females**
Illiterate	0	0
Higher Secondary	3	4
Graduation	72	46
Post Graduation	30	28
Any Other	8	9

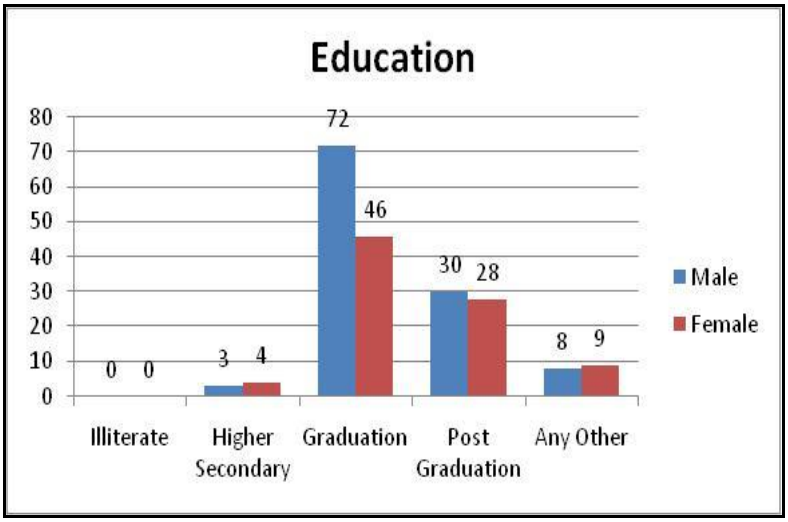


Figure 5-6 Education Demographic Profile

Perception Male and Female Employees

It is clear from below

Table 5-7 that there is a significant difference among males and females.

Table 5-7 Perception of Employees

PARAMETERS	EMPLOYEES		
	FEMALE	MALE	T-TEST
Online banking with biometric system helps in satisfying the banking needs of the client.	3.97	3.77	1.087
Money can be managed intelligently and efficiently through online banking & biometric system	4.11	4.21	0.638
The main challenge that the system faces is to safeguard the privacy and security of its customer's information	3.68	4.05	2.106*
Developing newer security technologies, is of paramount importance to keep the system safe and secure	3.47	4.13	3.511**
A biometric authenticating system in banking ensures Privacy and Security	4.11	3.89	1.292
In Internet Banking, biometric authentication satisfies the crucial need of providing security.	3.74	4.15	2.597*
Biometric Technology can now replace the need for passwords and pins, as it offers more security and convenience.	3.53	3.92	2.478*
A 100% true identification can be gauged with the help of the Biometric Technology	4.16	4.27	0.702
Malpractices in online banking can be controlled through biometric technology to a greater degree.	4.32	4.35	0.32
Biometric technology can easily fit into the existing network	3.79	4.21	2.552*
It can safely and easily access the inbuilt features in modern Laptops and PC's like recognizing face and fingerprints.	4.24	4.29	0.345
With the advent of Biometric Technology several ID proofs will become redundant.	4.05	3.92	0.823
Customers are unaware about how safe net banking is.	3.76	4.26	2.68*

An online banker's perception suggests they see a lot of loopholes in the security of net banking.	3.87	4.27	2.637*
Indian banking culture doesn't support the use of the biometric technology	4.34	4.29	0.354
People's attitude towards this technology influences the Indian banks decision of adopting it	4.13	3.82	1.865
Biometric technology is still in its initial phase to be fully accepted by the Indian banks	4.24	3.56	3.655**
Difficulties and complications faced while managing this technology also hinders its acceptance, by the banks.	4.24	3.66	3.548**
Acceptance of this technology also becomes difficult due to default rates and high administration expenses.	4.37	4.35	0.091
Customers online are anxious to protect their identity, and fear someone stealing it	3.83	4.29	2.731**
Customers should be informed about the safety measure that they can adopt in fraudulent situations	3.77	3.37	2.212*
Biometric technology has a bright future in Indian banking	4.45	4.47	0.153
Passwords will now give way to a biometric authentication system.	3.47	4.19	3.99**
Customers in the Indian financial markets are more receptive to this technology that other age old markets.	3.97	3.92	0.304
Biometric technology is 100% safe when it comes to online security.	3.58	3.89	1.953

According to males parameters such as "Developing newer security technologies, is of paramount importance to keep the system safe and secure", "Biometric technology is still in its initial phase to be fully accepted by the Indian banks", "Difficulties and complications faced while managing this technology also hinders its acceptance, by the banks", "Customers online are anxious to protect their identity, and fear someone stealing it" and "Passwords will now give way to a biometric authentication system" are highly significant in contrast to males as indicated by "**".

Other parameters such as "The main challenge that the system faces is to safeguard the privacy and security of its customer's information", "In Internet Banking, biometric authentication satisfies the crucial need of providing security", "Biometric Technology can now replace the need for passwords and pins, as it offers more security and convenience", "Biometric technology can easily fit into the existing network", "Customers are unaware about how safe net banking is", "An online banker's perception suggests they see a lot of loopholes in the security of net banking" and "Customers should be informed about the safety measure that they can adopt in fraudulent situations" were found to be significant as indicated by "*". This indicates that male perception is more in these parameters as compared to females with biometric system.

Other factors were found at par both for males and females.

All the significant values have been represented in Figure 5-7. The values that were non-significant have been removed from the figure. It gives the clear picture of the perception of teachers.

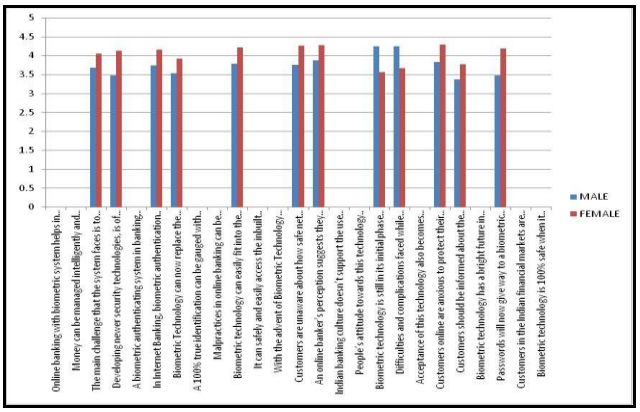


Figure 5-7 Perception of Employees

Data Mining

Data mining or knowledge discovery is the computer-assisted process of digging through and analyzing enormous sets of data and then extracting the meaning of the data. Data mining tools predict behaviors and future trends, allowing businesses to make proactive, knowledge-driven decisions. Data mining tools can answer business questions that traditionally were too time-consuming to resolve. They scour databases for hidden patterns, finding predictive

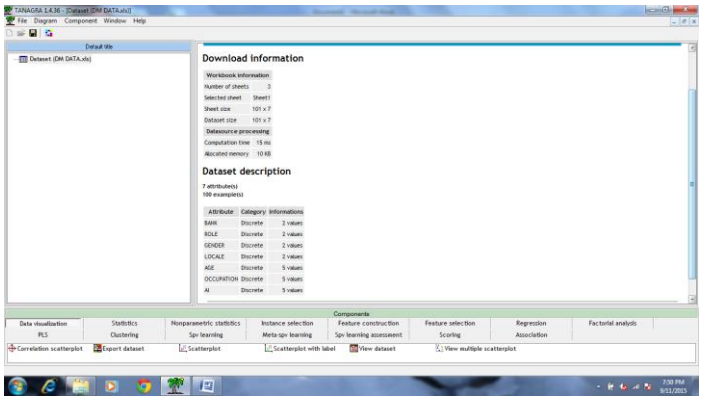
information that experts may miss because it lies outside their expectations.

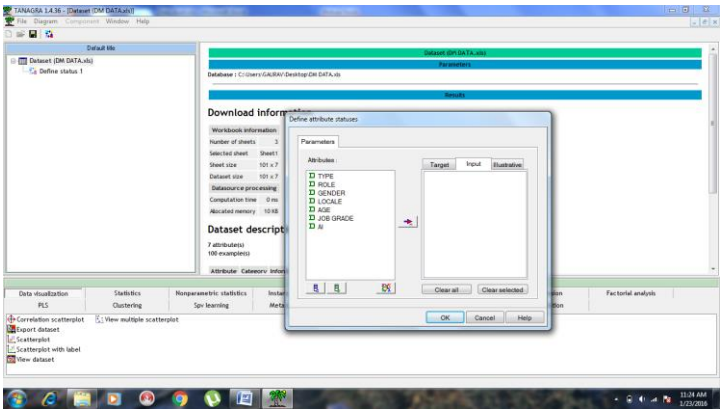
Data mining derives its name from the similarities between searching for valuable information in a large database and mining a mountain for a vein of valuable ore. Both processes require either sifting through an immense amount of material, or intelligently probing it to find where the value resides.

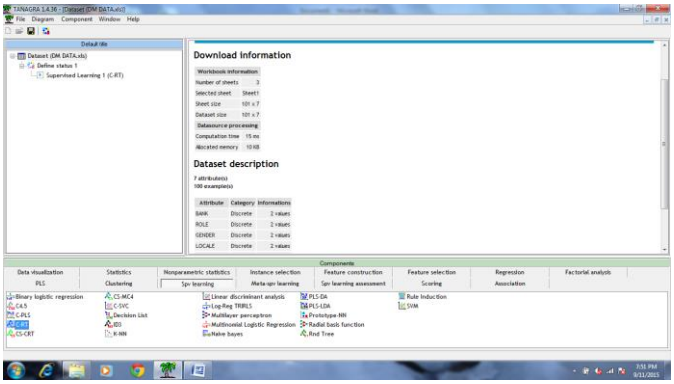
Classification

Classification consists of predicting a certain outcome based on a given input. In order to predict the outcome, the algorithm processes a training set containing a set of attributes and the respective outcome, usually called goal or prediction attribute. The algorithm tries to discover relationships between the attributes that would make it possible to predict the outcome. Next the algorithm is given a data set not seen before, called prediction set, which contains the same set of attributes, except for the prediction attribute – not yet known. The algorithm analyses the input and produces a prediction. The prediction accuracy defines how "good" the algorithm is. For example, in a medical database the training set would have relevant patient information recorded previously, where the prediction attribute is whether or not the patient had a heart problem.

The following are the figures illustrate the results produced from classification.



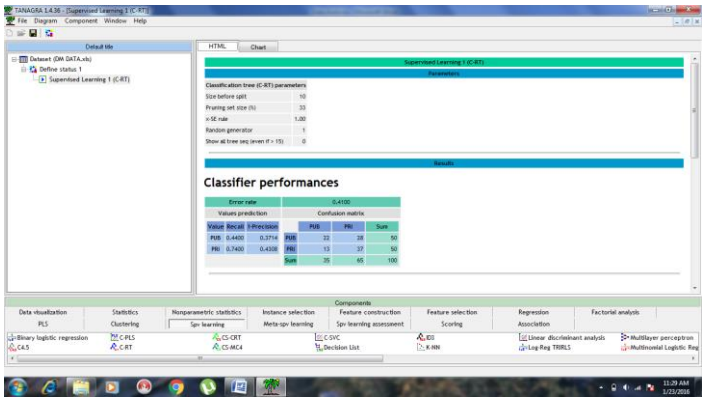




MIN SIZE OF NODE TO SPLIT means the minimum number of instances needed for performing a splitting of a node. For our dataset, we do not perform a split if there are less than 10 instances.

PRUNING SET SIZE means the part of the learning set used for the post pruning process. The default value is 33% i.e. 67% of the learning set is used for the growing phase (67% of 300 = 201 instances), 33% for the pruning phase (33% of 300 = 99 instances).

We have the sequences of trees table, with the number of leaves, the error rate calculated on the growing set and pruning set. The error rate computed on the growing set decreases as the number of leaves increases. We cannot use this information to select the right model. We use the pruning sample to select the "best" model. The tree which minimizes the error rate on the pruning set is highlighted in green.



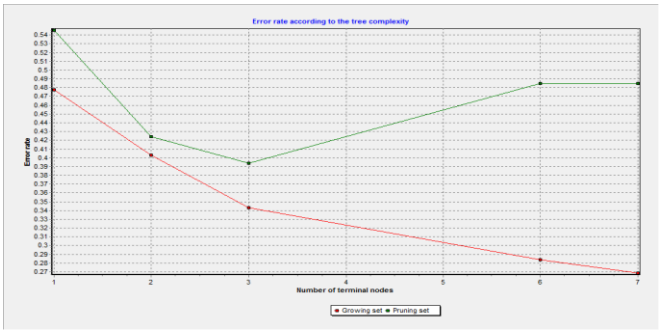


Figure 5-8 Classification

6. CONCLUSION

- Classification predicts which class of employees is in favour of biometric system.
- Each employee is classified into particular group.
- According to the data collection, it is predicted that there are more males employees in contrast to females.
- The maximum age group is 25-50 years which depicts that employees are generally experiences.
- The employees generally belong to urban area and it may be due to the fact that they are settled with their family in urban cities for their future.
- Mainly the employees are graduate or post graduate which implies that the banks used to have qualified staff.
- The income of employees is good as predicted by their annual income which predicts the banks are paying good handsome salary.

REFERENCE

[1] Adeloye LA 2008. E-banking as new frontiers for banks. Sunday Punch, September 14, P. 25.

[2] Brunner, A., Decressin, J. and Kudela, B. (2004): Germany's Three-Pillar Banking System – Cross Country Perspectives in Europe, Occasional Paper, International Monetary Fund, Washington DC.

[3] Diebold I. (2002). ATM fraud and security: White Paper, New York.

[4] Drygajlo, A., 2006. Information and communication security: Biometrics. Accessed 2014. Available at: http://scgwww.epfl.ch/courses/Biometrics-Lectures-2006-2007/01-Biometrics- Lecture-Part2-2006-10-23.pdf

[5] Ihejiahi R 2009. How to fight ATM fraud online. Nigeria Daily News, June 21, P. 18.

[6] Jain, A., Arun A. Ross, A. and Karthik N. ,2011. Introduction to Biometrics. New York: Springer.

[7] Jain, A., Ross, A., Prabhakar, S., 2004. An introduction to biometric technology. Circuits and Systems for Video Technology, IEEE Transactions. Vol. 14, Issue 1. pp: 4-20.

[8] Lee (2006) How to Measure Survey Reliability and Validity. London: Sage.

[9] Litan, A. , 2004. Phishing Attack Victims Likely Targets for Identity Theft. Gartner Reasearch.

[10] Madu, C.N., & Madu, A.A. (2002). Dimensions of e-quality. International Journal of Quality & Reliability Management, 19(3), 246-58.

[11] O'Gorman, L. Comparing Passwords, Tokens, and Biometrics for User authentication, Proc. IEEE, Vol. 91, No. 12, 2003, pp: 2021-2040

[12] Obiano W 2009. How to fight ATM fraud. online Nigeria Daily News, June 21, P. 18

[13] Omankhanlen Odidison (2009).ATM fraud rises: Nigerians groan in Nigeria. Daily News,Sunday, June 21, pp. 8-10.

[14] Roli, B., Priti S. and Punam B. (2011): Minutiae Extraction from Fingerprint Images. International Journal of Computer Science Issues, vol.8, Issue 5, No3. ISSN(online):1694-0814 www.IJCSI.org

[15] Wu, Th., 1998. The secure remote password protocol. In proceeding of the Internet Society Network and Distributed System Security Symposium, pp 97-111.