ISSN 2348-1196 (print)
International Journal of Computer Science and Information Technology Research ISSN 2348-120X (online)
Vol. 3, Issue 4, pp: (340-344), Month: October - December 2015, Available at: www.researchpublish.com

# Security Enhanced Cost Effective Online Transaction

[1]Shailesh Hule, [2]Komal Mohite, [3]Priyanka Pawar, [4]Yash Patil

[1,2,3,4] Department of Computer Engineering, PCCOE Pune, India

***Abstract:*** **This paper improves the security of the credit/debit card in the fields of E-commerce, E-banking, and ATM's. Our paper protects the credit card by using Fingerprint authentication system. The minutiae-based matching algorithm is used in fingerprint recognition Systems of RASPBERRY PIE which is cost efficeint and minimized size of the processing system. This will increase the security level in the society against the fraudsters. The system will be protected using Fingerprint Authentication system, Credit card/Debit Card, and Fingerprint Biometrics. Fingerprint Authentication system feature combines One Time Password and Fingerprint authentic-cation. To safeguard the user authentication the user needs to provide his biometrics Fingerprint feature. The biometrics Fingerprint recognition will be done using the users Secugen Biometric Solutions. This software will provide Unique image processing algorithm extracts fingerprint minutiae very accurately, Encryption function to protect user privacy, Fast overall process of extraction, matching and verification**

***Keywords:*** **control system, raspberry pi, fingerprint monitoring sensors and monitoring system.**

## I. INTRODUCTION

As credit card is becoming popular mode for online financial transactions, at the same time fraud associated with it are also rising. Credit card frauds are increasing day by day regardless of the various techniques developed for its detection. Fingerprint Authentication system continues to lead the industry in safeguarding the future and integrity of the self-service channel through investing in new technologies,services and initiatives to stay ahead of the criminal. Our Project aims to improve the security level using Fingerprint authentication system. The main objective of this project is to detect the fraudulent and to give successful transaction to the authenticator. Our approach is to enhance information security in the field of E-commerce, E-banking & ATM.

## II. RELATED WORK

Many individual data mining and non-data mining techniques have been designed implemented and evaluated in fraud detection. There are non-data mining layers of defence to protect against credit application fraud which also has certain limitations. The first existing defence is created up of scorecards and business rules. In Australia, one business rule is the hundred-point physical identity check testwhich requires the applicant to provide sufficient point-weighted identity documents face-to-face. They must add up to at least 100 points, where a passport is worth 70 points. Another business rule is to contact (or investigate) the applicant over the Internet or telephone. The above two business rules are highly effective, however human resource intensive. To rely less on human resources, a business rule is to match an application‟s identity number, phone number, or address against external databases. This is convenient; however the public telephone and address directories, credit history data and semipublic voters‟ register, can have data quality issues of completeness, accuracy and timeliness. In addition, scorecards for credit grading can catch a small percentage of fraud which does not look creditworthy; but it also removes outlier applications which have a higher probability of being fraudulent. The second existing defence is called fraud matching. Here, better known frauds are complete applications which were confirmed to have the intent to defraud and usually periodically recorded into a blacklist. Moreover, the

current applications are matched against the blacklist. This has the profit and clarity of hindsight because patterns often repeat themselves. Additionally, there are two main problems in using known frauds. Firstly, they are untimely due to long time delays, in days or months, for fraud to expose it, and be reported and recorded. This provides a window of opportunity for fraudsters. Secondly, recording of frauds is highly manual. This implies known frauds can be incorrect, expensive, difficult to obtain and have the potential of breaching privacy. In many data mining techniques much of work in credit application fraud detection remains proprietary and exact performance figures unpublished so it is not necessary to compare the new techniques with leading ones. For example,[3] has Detect which provides four categories of policy rules to signal fraud, one of which is checking a new credit application against historical application data for consistency. In another example,[10] has ID Score-Risk which gives a combine view of each credit application‟s characteristics and their similarity to other industry-provided or Web identity‟s characteristics. Statistical tools are based on comparing the observed data with expected values, but expected values can be derived depending upon the content. [9], has Statistical fraud detection methods which may be „supervised‟ or „unsupervised‟.In supervised, samples of both fraudulent and non fraudulent records are used to construct models which allow one to assign new observations into one of the two classes. Unsupervised methods simply seek those accounts or customers which are most dissimilar from the norm. Case-based reasoning is used in screening of Credit Applications. [3] uses threshold nearest neighbour matching. Diagnosis utilizes multiple selection criteria and resolution strategies to analyse the retrieved cases. Peer group Analysis [2] compares the cumulative mean weekly amount between a target account and other similar accounts at subsequent time points. On credit card accounts, the time window to calculate a peer group is 13 weeks and the future time window is 4 weeks. Bayesian networks [5] uncover simulated anthrax attacks from real emergency department data. Break Point Analysis [2] monitors intraaccount behaviour over time. It detects rapid spending or sharp increases in weekly spending within a single account.

## III. EXISTING SYSYEM

This section is divided into five sections which systematically explain the modules and its purposes [1].

### A. Credit Card Application Form & Initial White List Creation:

Bank Database is created. Credit card Application for with ten attributes is created. The attributes include Applicant name Address, Date of Birth, mobile Number, email id, occupation, Driving License ID, Passport ID, Social Security Number (SSN) etc. The SSN, Passport ID, Driving License ID are known as Unique IDs of a person. Customers request the bank to obtain Credit Card. Now the Bank provides application forms to the customers. The customers fill the application form and submit it to the Bank. The applications are compared to each other and will be assigned a link type. The link type is nothing but a binary string (eg.01011111) in which „1‟ represents matched fields and „0‟ represents unmatched fields. Finally, initial white list is created. The White list has list of verified applications, link type, number of applications corresponding to a particular link type and weight. transaction. If the credit transaction amount is higher than the threshold, the fraudster or legal user is asked to challenge the security question. If the challenge is success i.e. in case of legal user the transaction is authenticated otherwise it is declined in case of fraudster. Hence the secure transaction is performed.

### B. CD Suspicious Score:

Here a new application form submitted by a user and applications in the whitelist are taken as input to the Communal Detection (CD) layer. New Application is compared with windows of applications in the whitelist. CD layer is used to find communal relationships between the applications. If four or more fields are matched in the new application against application in the whitelist, then CD assigns less suspicious score. Otherwise the new application form is added into the whitelist and the list is updated. Since CD accounts for legal relationship it assigns less suspicious scores to new application form and gives as input to the SD layer. Fig. 1 Fraud in Credit Applications Fig 1 shows the detailed ups and downs in the credit applications for two months.

### C. SD Suspicious Score:

Here the application form i.e. the output of the CD layer is taken into account. Spike Detection (SD) layer verifies the matched fields for their priority. The unique ID fields are given higher priority. If unique IDs are matched then the suspicious score gets increased and the application form is declared as fraud and hence finally rejected. If none of the unique IDs are matched then the application form is added into the whitelist and the list is updated. Since the SD accounts for fraud behaviour detection, the fraud application is rejected.

ISSN 2348-1196 (print)
International Journal of Computer Science and Information Technology Research ISSN 2348-120X (online)
Vol. 3, Issue 4, pp: (340-344), Month: October - December 2015, Available at: www.researchpublish.com

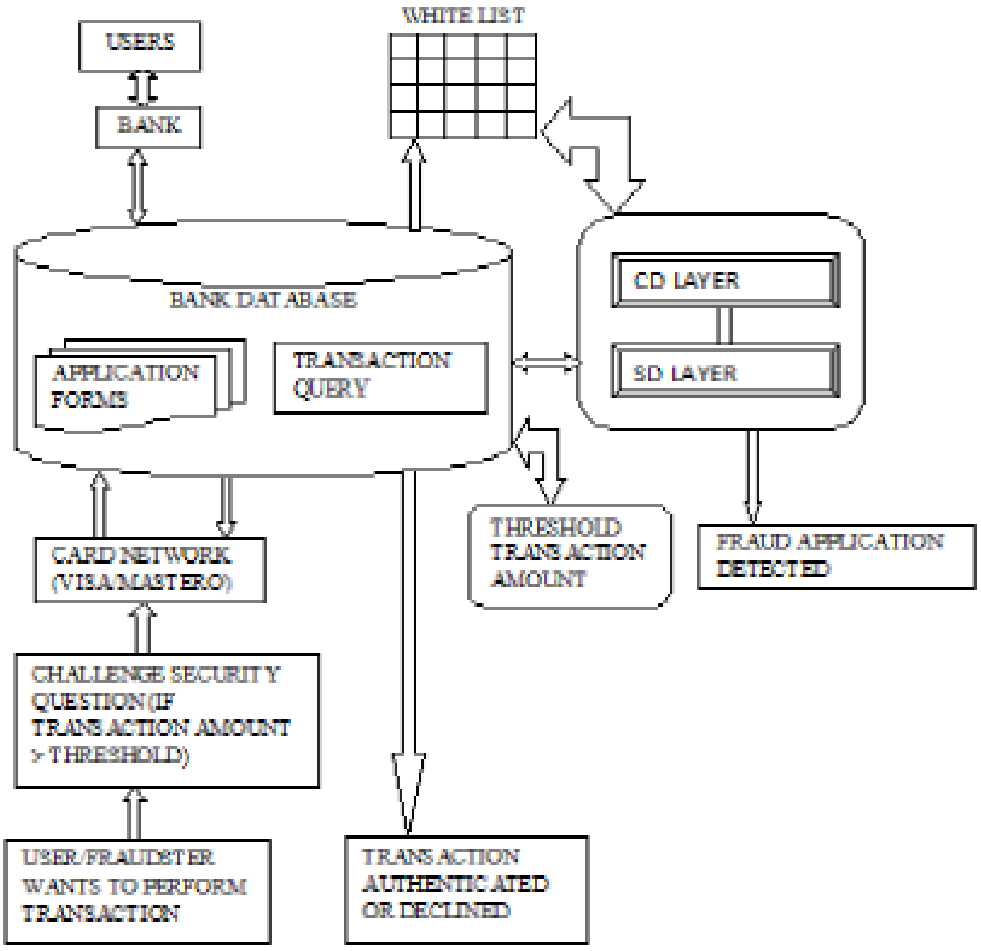


**Fig. 1. Existing system**

### D. Threshold Transaction Amount Calculation:

The Bank monitors the transaction history of legal user or the credit card holder. Based on the previous transactions made by the user the bank calculates a threshold value of the transaction amount. The threshold value is nothing but average of all the previous transactions.

### E. Secure Transaction:

The case assumed here is that the card holder unfortunately missed his card there by a fraud gets the card. Now the fraudster or the legal user performs credit transaction. If the credit transaction amount is higher than the threshold, the fraudster or legal user is asked to challenge the security question. If the challenge is success i.e. in case of legal user the transaction is authenticated otherwise it is declined in case of fraudster. Hence the secure transaction is performed.

## IV. PROPOSED SYSTEM

### A. *Complete system:*

Humans also need DECISION MAKING COMPUTER to reduce human efforts as well as to increase accuracy. Not only decision making but even the efficient and secure bank transaction with the security monitoring is important as well, which is possible by a various technologies available today like biometric, sensors, control systems, etc. Every transaction to be done secure manner and function to the human friendly manner to do it accurately on their own, for this computers

ISSN 2348-1196 (print)
International Journal of Computer Science and Information Technology Research ISSN 2348-120X (online)
Vol. 3, Issue 4, pp: (340-344), Month: October - December 2015, Available at: www.researchpublish.com

are needed to manage them all. For the sole reason of securing the human finance and booming the transaction security a system with its own mind and high control over a vast field is needed. This will not only save us the resources but will give a good efficiency and reliability. So the concept is about introducing higher level of authentication with the help of computers and biometric along with big sensor networks.

***B. Concept:***

Server programs are supposed to serve multiple requests simultaneously on various TCP/IP connections. Client loads vary and so do requests per client. Taking that into consideration, the performance parameters of web servers include the following: number and type of requests per second; latency time, measuring in milliseconds how long it takes to complete each new connection or request; throughput or the amount of data transmitted in response to a request measured in bytes per second. This depends on, among other things, file size and available network bandwidth. Performance is also determined by concurrency levels or the ability for the server to provide access to specific files, in this case, those that make up web pages, to multiple users simultaneously. Finally, the server model, whether client-side or server-side, used to execute web server programs establishes scalability. Scalability is a system property that refers to a system or network's ability to manage increasing workloads well and the ability to expand gracefully

***C. Raspberry Pie:***

This system is basically included for the compares of the fingerprint authenticated by the user consisting the transaction function over the web site for the shopping the added advantage of this function is that it is cost effective and very **simplified function over the system server.**

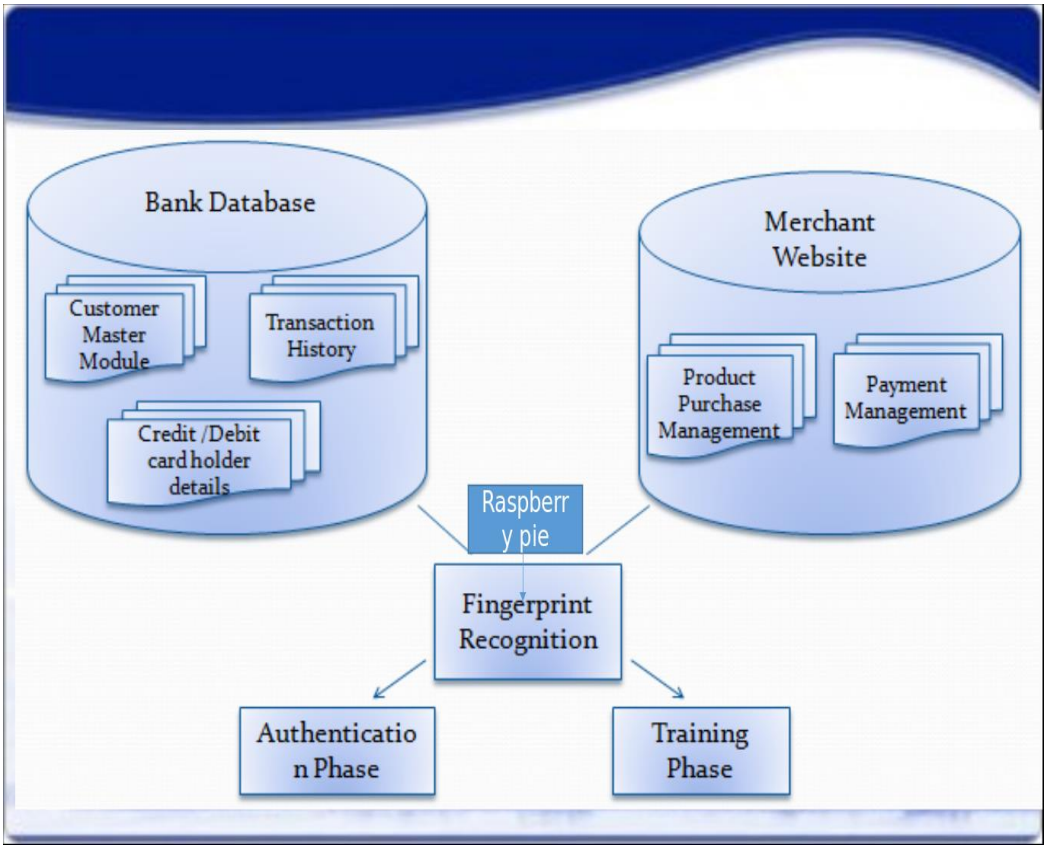


**Fig.2. Architecture of proposed system**

## V. CONCLUSIONS

The paper proposes on the detection of fraudsters in credit/debit card applications and by presenting a novel mechanism which will help in performing secure transaction.. To grasp the optimal condition, The minutiae matching algorithm will extract the accurate features of fingerprint for authentication purpose. through the feasibility test.

**ACKNOWLEDGMENT**

The authors thanks to Project Guide Prof. **Sailesh Hule** for his encouragement and support. The authors also like to thank to Project Co-coordinator **Ms. Sonali Tidke** for his assistance, genuine support and guidance from early stages of the project. The author would like to thank **Prof Dr. K. Rajeswari**, Head of Computer Engineering Department for her unwavering support during the entire course of this project work.

**REFERENCES**

[1] ALKA HERENJ,SUSHMITA MISHRA, Secure Mechanism for credit card transaction fraud detection system issue 2,February 2013

[2] R. Boltan and D. Hand, "Unsupervised Profiling Methods for Fraud Detection", Statistical Science, vol. 17, no. 3, pp.235-255, 2001.

[3] .I. Witten and E. Frank, "Data Mining: Practical Machine Learning Tools and Techniques with Java", Morgan Kauffman, 2000.

[4] Chris Jay Hoofnagle, Identity Theft: Making the Known Unknowns Known, Harvard Journal of Law and Technology, Vol. 21 no.1, pp.98-122, 2007.

[5] P. Brockett, R. Derrig, L. Golden, A. Levine and M. Alpert, Fraud Classification Using Principal Component Analysis of

[6] RIDITs", The J.Risk and Insurance, vol.69, no. 3, pp.341-371, 2002.

[7] Clifton Phua, Kate Smith-Miles, Vincent Cheng-Siong Lee and Ross Gayler,"Resilient Identity Crime Detection", IEEE Transactions on Knowledge and Data Engineering, vol.2, no. 3,pp.533-546, 2012.

[8] KOICHI ITO, AYOMI MORITA, TAKAFUMI AOKI, HIROSHI NAKAJIMA, A Fingerprint Recognition Algorithm Combining Phase-Based Image Matching and Feature-Based Matching-2012.IEEE Paper IJET-IJENS Vol:09 No:09

[9] Linda Delamaire, Hussein Abdou and John Pointon, "Credit Card Fraud and Detection Techniques", bank and bank systems,vol.4,no.2,pp.57-68, 2009.

[10] Richard J.Boltan and David J.Hand, "Statistical Fraud Detection", pp.1-54, 2002.

[11] ID Analytics, "ID Score-Risk: Gain Greater Visibility into Individual Identity Risk, "Unpublished, 2008.

[12] W. Wong, A. Moore, G. Cooper and M. Wagner, "Bayesian Network Anomaly Pattern Detection for Detecting Disease Outbreaks", Proc.20 th Int"l Conf. Machine Learning, pp.808- 815, 2003.

[13] Clifton Phua, Kate Smith-Miles, Vincent Cheng-Siong Lee and Ross Gayler, "Resilient Identity Crime Detection", IEEE Transactions on Knowledge and Data Engineering, vol.2, no. 3,pp.533-546, 2012.

[14] LUKASZ WIECLAW A Minutiae-Based Matching Algorithms in Fingerprint Recognition Systems vol 13/2009

[15] Experian Detect: Application Fraud Prevention System, Whitepaper, http://www.experian.com/products/pdf/experian_detect.pdf, 2008.

[16] https://en.wikipedia.org/wiki/Main_Page.

[17] http://www.ieee.org/.