



International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirccce.com

Vol. 5, Issue 2, February 2017

Multi Bank Smart Card with User Behavior Monitoring Using HMM & Formula Verification

Jayapradha. V¹, Keshika. S², Vanitha.D³, Kapila Vani.R.K⁴,

B. E, Student, Department of Computer Science and Engineering, Prince Shri Venkateshwara Padmavathy Engineering
College, Chennai, India^{1,2}

M.E, Assistant Professor, Department of Computer Science and Engineering, Prince Shri Venkateshwara Padmavathy
Engineering College, Chennai, India³

M. E, Assistant Professor, Department of Computer Science and Engineering, Prince Dr.k.Vasudevan College of
Engineering and Technology, Chennai, India⁴

ABSTRACT: Big data is a trending topic that captures considerable attention of many researchers. It is really opportunity based environment where many data scientists were created. Big data analytics would definitely lead to valuable knowledge for many organizations. Integration of Big Data, Business analytical and RFID like technology is supposed to be recent trends in IT. In this paper we propose an idea for a banking sector particularly for a Debit/ATM card transaction in which multiple user accounts were integrated into a single smart card with unique PIN numbers accordingly. The user behaviour is monitored through HMM model and this smart card is also tracked using RFID technology. From our perception we can assure this idea will improve the existing bank management system.

KEYWORDS: Big Data, RFID, Business analytics, HMM (Hidden Markov Model), Formula Verification.

I. INTRODUCTION

BIGDATA the latest buzz in technology industry which is an emerging topic and it plays vital role in many business oriented activities. In this digital world enormous amount of data is being generated day by day. Nowadays, collecting and processing those large amounts of data is an easier process. That being said extracting and validating huge necessary information from dynamic database is far from easy [2]. The role of Bigdata in Business Intelligence leads to improvement in business management such as replanning and rescheduling. In this paper we concentrate on Bigdata and banking system in which an idea is proposed for an efficient banking system. Current banking system has several issues related with debit/credit card fraudulence. Recently, 3.2 million Indian debit cards were hacked due to improper maintenance of banks as well as the third party service providers. The reason behind these hacks is improper maintenance and there is no user behaviour monitoring and analysis. Thus, in this paper we propose an idea in which three major technologies like Bigdata, Business Intelligence and RFID technology were integrated. That being said, big data analytics for business operations and risk management will enhance business operations in which following three sections were discussed, 1) BI and data mining; 2) Industrial systems reliability and security; 3) Business operation risk management (ORM); [5]. In another study, advances of business intelligence method (BI) [2] brought huge improvement to business operations. The main idea of this paper is integration of multiple banks and multiple user accounts into a single smart card with unique pin numbers accordingly in which user behaviour is monitored through Hidden Markov Model (HMM). Li and Meeker [6] gave introduction to the basic ideas of using Bayesian methods for a reliable data analysis. The HMM is a statistical model which uses Bayesian methods for effective analysis of data. For an efficient security purpose formula based authentication is introduced. The formula based authentication avoid various security breaches such as credit/debit card hacking. The RFID technology is the most exciting and fastest



International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirccce.com

Vol. 5, Issue 2, February 2017

growing technology in terms of scope of application in next generation BI [3]. On the other hand, RFID technology is a good channel for coordination in industrial systems at item level [4]. Here the RFID technology enable tracking the card as well as the customer. To the best of our knowledge, this is the first paper where big data analytics can be employed for banking systems in order to reduce system risk and to enhance efficiency in banking operations.

II. BACKGROUND AND RELATED WORK

Big data is really opportunity based environment. Big data analytics would definitely lead to valuable knowledge for many organizations. There is no standard application by integrating three major emerging technologies like Big data, Business Intelligence and RFID technologies. In the present banking sector there are many security breaches. In this paper, we review various credit/debit card fraudulent activities and statistics related to credit/debit card hacks.

A. VARIOUS SECURITY THREATS TO CREDIT/DEBIT CARDS:

The current banking system has several drawbacks which lead to increase in security threats to its transactions. The privacy of customer transaction details in those banks is at risk. Hence it is necessary to discuss those security threats.

a) **Hacking:**

Hackers can use key logging software to capture whatever the user types including the PIN number and the name of the user. This happens when the card holder uses his/her card in the WIFI network.

b) **Phishing:**

Phishing attacks were originated around 1995 [7] but only after ten years from that the common people came to know about phishing. It is an attack where emails can look like they are from legitimate sources but actually be from scammers. If the embedded link is accessed by the user then the personal information data can straight to criminals.

c) **Skimming:**

Identity thieves can retrieve account data from the credit/debit cards magnetic strip using a device called a skimmer. They can use that data to produce counterfeit cards.

d) **Spying:**

The criminals simply look over the shoulder of the user while entering the PIN or the criminal can plant camera near the ATM's to capture the PIN which entered by the card holder.

e) **Application Fraud:**

It happens when the criminal has entire personal detail about the user. In application fraud, the criminal or the hacker may know the card holder well.

f) **CNP (Card Not Present) Fraud:**

It happens when the criminal knows the expiry date and account number of the debit/credit card. The fraudster can also have the card number too. Additionally, there are only 999 possible combinations for the verification code. So the fraudster can easily hack the card.

g) **Mail Non-Receipt card fraud:**

This type of fraud is also known as intercept fraud. In this case while the user expecting new card or replacement one and a criminal is able to intercept these. Then the criminal will register the card and the criminal will use that card to make purchases and more.

h) **Doctored or Fake cards:**

A doctored card is a card whereby a strong magnet has erased its metallic stripe and managed to change the details of the card itself so that they match those of valid cards.



International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 2, February 2017

B. VARIOUS SECURITY THREAT STATISTICS:

The various threats which are happened previously are listed. This table clearly states data breaches and number of affected people is also mentioned. The largest credit/debit card data breaches in 2005 are represented in the following table.

COMPANY	YEAR	NUMBER OF ACCOUNTS AFFECTED
Card Systems Solutions.	2005	40 million
TJX Companies, Inc.	2006	94 million
U.S. Veterans Affairs.	2006	17.5 million
Certegy.	2007	8.5 million
Fidelity National Information Service.	2007	3.2 million
Heartland payment system.	2008	134 million
Sony.	2011	12 million
Global Payments.	2012	1 million

Table 1.1: Data breaches occurred in previous years.

Recently, there is another security breach in India, where a virus or malware infection at Hitachi Payments Services led to over 32 lakhs of debit cards being compromised.

III. PROPOSED SYSTEM

A. MULTI BANK:

A single user may have multiple bank accounts in different banks. Our implementation is to integrate multiple bank accounts and multiple users account in a single card. The need for this implementation is if the specific ATM card has no cash in it then the user can able to withdraw cash from other bank accounts by registering all his different bank accounts information in the single card by specifying their unique PIN numbers. The pros of this implementation are,

- a) User doesn't need to carry all ATM cards.
- b) Since every user account is integrated in a single card it's easy to track his all over transaction because of this we can avoid black money.
- c) To open a new bank account user need not buy a detail in his existing card. As the result of this the user can save his ATM card productivity.

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirccce.com

Vol. 5, Issue 2, February 2017

B. MULTI USER:

Users can also include their family members account details like father, mother and wife with their knowledge by adding their PIN number and the user can able to do his transaction. Likewise the user family members can also include the user details and integrate accounts in their card. In another case, the user itself may have multiple accounts in different banks all these accounts also been integrated into single smart card.

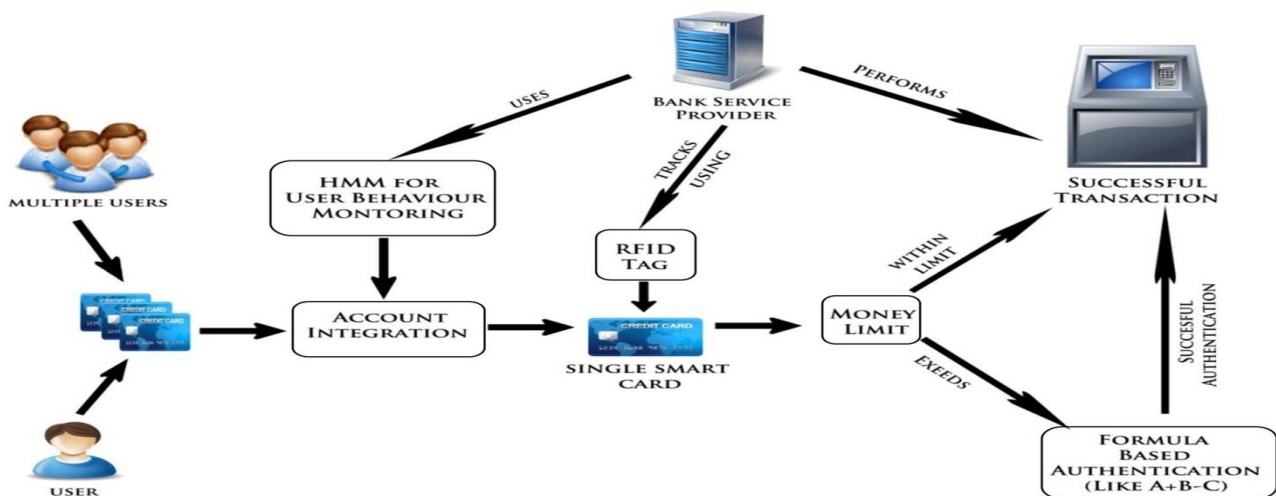


Figure1.1: Architecture of Multi Bank Smart Card.

C. PROHIBITION OF SECURITY THREATS:

Since integrating multiple accounts into a single card to hack the card account information using shoulder surfing attack or through tracking the server is also possible. To avoid this user behaviour is monitored using HMM (Hidden Markov Model).

a) Hidden Markov Model (HMM):

The HMM is based on the Markov model. The Markov Model is a finite automata model which is used to find out what will be the next state depending on the current state. Hence to predict the future, you do not have to look at the past history of states of the model. HMM will look for the user behaviour change by looking into their probabilities of usage of ATM card and amount of cash they withdraw. It depends on two main factors. First, how frequently user is using his ATM card? Second, how much amount he is withdrawing? If any deviation occurs in either of the above, the HMM will detects for the user behaviour in order to check whether he is the valid user or not. If the user tries to withdraw the cash more than his limit an email alert will be sent to the user to intimate the user.

b) Formula based authentication:

While creating the account itself the user has to register a formula which consists of 3 characters and 2 operators (+,-). Any deviation occurs in user behavior then the user has to undergo the formula based verification. A panel will be displayed which consists of (a-z) alphabets and (0-9) numbers the user has to compute the formula which is registered by the user during registration process and has to give only the computed answer as input, and also the number displayed under the alphabets will change for every time because of this we can provide maximum security and flexibility than the existing system.

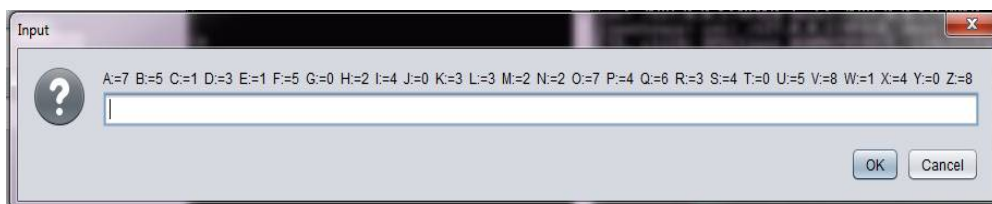


Figure1.2: Formula based authentication panel (Entering computed answer).

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirccce.com

Vol. 5, Issue 2, February 2017

c) **RFID Tag:**

Radio-Frequency Identification (RFID) this refers to small electronic devices that consist of a small chip and an antenna. The chip can able to carry up to 2,000 bytes of data or less. The RFID device serves the same purpose as a magnetic strip on the back of a credit/debit card. It provides a unique identifier for that object and the magnetic strip must be scanned to get the information. Similarly the RFID device must also be scanned to retrieve the identifying information. The RFID used in the ATM card automatically scans the customer information when they enter the bank and the customer information system sends the alert to the back staff that the customer needs service. Also it is easy to track and monitor the card with the RFID when the card is hacked or lost.

IV. ALGORITHM METHODOLOGY

In this section, first we discussed about multiple account integration then the Hidden Markov Model and describe how it is used for behaviour monitoring.

A. **MULTIPLE ACCOUNTS INTEGRATION:**

The integration of multiple accounts has been done by the user by registering the account details which are to be integrated into the single smart card in the bank service provider application. The details of the integrated account details can be maintained by the bank using hadoop like technology. After, giving the account details to the bank service provider the user can able to access all the accounts which are integrated within his/her account by providing unique pin numbers. All these actions are done only by the bank service provider to enhance current banking scenario. Since, the technology is growing day by day introducing this concept like this will improve Business to consumer relationship.



Figure 1.2: Bank Service Provider Application

B. **MULTI ACCOUNT TRANSACTION:**

In this application the transaction is done by entering unique PIN numbers of multiple accounts. For each and every transaction the user has to enter unique PIN number of corresponding account. There are three cases in this transaction. First case is, if the user is a valid user then the transaction is successful otherwise, the transaction fails. The

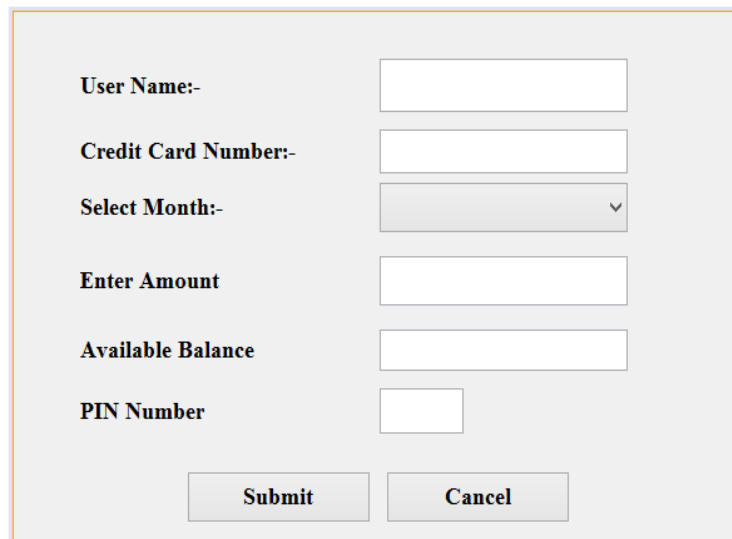
International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 2, February 2017

second case is, if the money taken by the user exceeds the limit then an OTP and alert will be sent to user. The third case is, after OTP and alert formula based authentication occurs. Now, the user has to enter the value of the computed formula then only the transaction is performed.



The image shows a transaction panel with the following fields and buttons:

- User Name:-
- Credit Card Number:-
- Select Month:-
- Enter Amount
- Available Balance
- PIN Number
- Submit
- Cancel

Figure1.3: Transaction Panel

C. HIDDEN MARKOV MODEL:

One of the most intriguing problems in managing a banking system is multiuser applications analysis. As the first step to user-behavior analysis, we wish to classify user behavior analysis into two groups based on the flow of money and the time frequency.

- Frequency of money taken
- Frequency of time that the amount taken

The solution to this analysis is, assume that a system has N hidden states and K possible outputs. By HMM, all hidden states are connected with a zero-memory Markov chain. When a system is in certain state, there is a probability of generating every possible system output. Each output is dependent only on the current system-state and not on previous states outputs. HMM definition includes also the initial probabilities of starting the system in each of the hidden states. Similarly, in this paper for effective user behaviour analysis hadoop architecture is used for analysis.

Here, email alert is used to verify that the user is a valid user and formula based authentication is used to avoid several security breaches like shoulder surfing etc.

V. FUTURE ENHANCEMENTS

Bigdata and RFID like technologies play a major role in Business intelligence. In this paper, the RFID technology provides Near Field Communication (NFC) between the smart RFID card and the RFID reader. Since, Chip technology has been already introduced in banking for debit cards as EMV (Europe Master Visa) smart card but not widely used. The EMV smart cards are very expensive compared to magnetic strip cards and which leads to several security breaches. Hence, Introducing RFID like technology will be a future advancement in several business intelligence systems such as bank management system.



International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirccce.com

Vol. 5, Issue 2, February 2017

VI. CONCLUSION

In this paper we had established the integration of multi bank accounts and multi user in a single card using emerging technologies like business analytics , Big data and RFID .Since our approach uses HMM (Hidden Markov Model) and formula based authentication we ensures maximum security and flexibility for the card holders to withdraw the cash. And it is difficult for the hackers to track the card because of the usage of RFID, and for the successful withdrawal for the cash the user has to cross the security mechanism. User can withdraw cash from their accounts after successful authentication of the corresponding PIN numbers

REFERENCES

1. S. Negash, "Business intelligence," *Commun. Assoc. Inf. Syst.*, vol. 2, no.1, pp. 177-195, Oct, 2004.
2. D.Kumar et al., "A hybrid approach to clustering in big data," *IEEE Trans. Cybern.*, to be published.
3. E. W. T. Ngai, K. K. L. Moon, F. J. Riggins, and C. Y. Yi, "RFID research: An academic literature review (1995-2005) and future research directions," *Int. J. Prod.Econ.*, vol. 112, no. 2, pp.510-520, 2008.
4. G. M. Gaukler, "Item-level RFID in a retail supply chain with stock-out-based substitution," *IEEE Trans. Ind. Informat.*, vol. 7, no. 2, pp. 362-370, May 2011.
5. Tsan-Ming Choi, Hing Kai Chan, and Xiaohang Yue, "Recent development in bigdata analytics for business operations and risk management," *IEEE Trans. Cybern.* vol. 47, NO.1, January 2017.
6. M. Li and W. Q. Meeker, "Application of Bayesian methods in reliability data analysis," *J. Qual. Technol.*, vol. 46, no. 1, pp. 1-23, 2014.
7. "phishing," http://www.phishing.org/history_of_phishing.
8. N. Manwani and P. S. Sastry, "Noise tolerance under risk minimization," *IEEE Trans. Cybern.*, vol. 43, no. 3, pp. 1146-1151, Jun. 2013.
9. H. K. Chan and F. T. S. Chan, "Early order completion contract approach to minimize the impact of demand uncertainty on supply chains," *IEEE Trans. Ind. Informat.*, vol. 2, no. 1, pp. 48-58, Feb. 2006.
10. G. M. Gaukler, "Item-level RFID in a retail supply chain with stockout-based substitution," *IEEE Trans. Ind. Informat.*, vol. 7, no. 2, pp. 362-370, May 2011.

BIOGRAPHY

- ❖ **Jayapradha V** is a student doing B.E degree in computer science and engineering in Prince Shri Venkateshwara Padmavathy Engineering College, Chennai. Her research interest includes Hacking, Network security, and cyber security.
- ❖ **Keshika S** is a student doing B.E degree in computer science and engineering in Prince Shri Venkateshwara Padmavathy Engineering College, Chennai. Her research interest includes cryptography, information security.
- ❖ **Vanitha. D** is an Assistant Professor in department of Computer Science and Engineering at Prince Shri Venkateshwara Padmavathy Engineering College, Chennai. She is a M.E graduate. Her research interest includes computer graphics, internet programming, and mobile computing.
- ❖ **Kapila Vani. R. K.** as Assistant Professor in department of Computer Science and Engineering at Prince Dr.K.Vasudevan College of Engineering and Technology, Chennai. She is a M.E graduate. Her research interest includes compiler design, Theory of computation and Software project management.