ISSN No:-2456-2165

Implementing Security in ATM PIN using hidden key Cryptography Algorithm

Guruaj N. Kulkarni
Assistant Professor A. S. Patil College of Commerce (Autonomous), BCA Department
Vijayapur, Karnataka, India

Vinayakumar S. Chikaraddi
Assistant Professor A. S. Patil College of Commerce (Autonomous), B.Com Department
Vijayapur, Karnataka, India

Abstract:- The primary aim of this project is to style a system which will improve the authentication of shopper's exploitation automatic teller machine. In most of countries using Automatic Teller Machine system to use initial substantiation. The user is sole by four digit pin number that contain distinctive information like password parameters of the ATM card. By getting into a private identification number of the user, the client is echt initial then will access bank account so as to form money dispenses or alternative amenities provided by the bank. Cases of card deception are another hitch once the user's bank card is missing and also the password is purloined, or just snip a customer's card& PIN the illicit can draw all make the most very short time, which is able to being great budgetary losses in customer accounts , this sort of trick has unfold globally. thus to correct this issue we tend to are executing this system exploitation Hidden Key algorithmic program so as to boost confirmation of client using ATM system and assurance within the banking area.

Keywords:- *Hidden Key, ATM, Security PIN.*

I. INTRODUCTION

In the world, nowadays individuals are involved concerning their safety, for his or her valuable things. recent ideas and procedures are becoming changed as per demand of individuals. Now a day's life we did like to search new concept in security system. Therefore we be likely to develop to provide the utmost level of security system to the ATM cash transactions play a crucial role within the Nature of trade. Tremendously developing banking technology has modified the way banking activities are controlled by an ATM system , a consumer is ready to conduct several banking activities like money dispense to particular vendors, paying electricity & postpaid and prepaid bills and cash transfer to one person to another, on the far side official hours and physical interaction with bank employees. An ATM (known by alternative names like an automatic teller banking system, cash point, cash dispenser) may be a system that has its origins entrenched within the accounts and records of a banking establishment. Today, Basic validation of the user used for this purpose, the validation of those transactions are entirely unsecured. Today as we have a tendency to all seen cash dispenser has been utilized in our daily life, as they are used for ease in business activities that was somewhat troublesome in early times wherever users have been long queues in bank for withdrawals and read-through balance of account. ATM system permits a user to form money withdrawals and check account balance while not the necessity for human teller. The current ATM system uses Bank debit and credit cards and with PIN (Personal Identification Number or Unique Identification Number) and also thumb impression that user will modification at any time through ATM system. This secret is fixed sort i.e. once set access are done once exploitation this therefore the probabilities to factotum it a lot of, and if ATM card is lost and password is taken then anyone will simply access that account by creating money losses of users thus there are probabilities of safekeeping pressures in existing system like shoulder surfboarding, knowledge glance at, ATM card trappings.

- This technique doesn't offer any variety for the generation of key. Consistent with this methodology the key value could also be any price larger than or adequate to one. This generation of non-limiting key method is problematic.

II. ALGORITHM DETAILS

A. Encryption Method

- *Firstly, Input the 4 Digit PIN Number A from customer which we have to encrypt.*
- *Calculate sum of 4 digit i.e. B*
- *Find the value of C ie. B/length of key (4).*
- *Add C to PIN Number*
- *Encrypted key e = C + PIN Number*
- *k = Hidden key (UP/ DOWN/ LEFT/ RIGHT/ DEL)*
- *t = Number of times. (1 to 4)*

B. Decryption Method

The coding of the encryption algorithmic program runs in reverse to capture the clear text, referred to as decoding. It takes the cipher text and therefore the secret key that produces the first PIN [4]. The generation of security secret is completely supported the plaintext. The encryption algorithmic rule as it is could use for the coding.

➢ *Decryption*

- *Read Encrypted PIN.*
- *S = Subtract C*
- *Match S and R*
- *Input Hidden Key ik and Times it*
- *Match ik and k*
- *Match it and t*

C. Example

➢ *Encryption*

- *Suppose PIN Number = 1234*
- *Sum of PIN Number =10*
- *Find the value of Q i.e. P/length of key (4).*
- Q = 10/4 = 2
- Add Q to PIN Number.

	1	2	3	4
+	2	2	2	2
=	3	4	5	6

- Encrypted PIN e =3456
- Hidden Key k = UP Arrow
- No of Times t = 2

➢ *Decryption*

- *Encrypted PIN e = 3456*
- *Q = 2*
- *Subtract Q.*

	3	4	5	6
–	2	2	2	2
=	1	2	3	4

- Input Security Key i.e., sk
- Input Number of Times i.e., st
- Match PIN, Security Key, Number of Times

III. CONCLUSION

Review of varied papers we have a affinity to determine that the extension within the electronic transaction in E-Commerce area, it scheme has resulted during a bigger demand for correct user identification and validation of the ATM card. Using Hidden Key algorithmic rule substantiation scheme for bank ATM systems is planned during this article. At the side of hidden key validation for a lot of security measures to take; additionally enclosed during this paper. Finally, our inferences are haggard out once insightful the hidden key algorithmic rule validation theme results.

REFERENCES

[1]. Jain, A.K.; Ross, A.; Prabhakar, S., "An introduction to biometric recognition," Circuits and Systems for Video Technology, IEEE Transactions on, Vol. 14, no. 1, pp. 4,20, Jan. 2004 doi: 10.1109/TCSVT.2003.818349.

[2]. Mr. John Mashurano1, Mr. Wang liqiang2, "ATM Systems Authentication Based On Fingerprint Using ARM Cortex-M3" International Journal of Engineering Research & Technology (IJERT) Vol. 2 Issue 3, March - 2013 ISSN: 2278-0181 1 www.ijert.org IJERTIJERT.

[3]. M. Subha and S. Vanithaasri "A study on authenticated admittance of ATM clients using biometrics based cryptosystem" International Journal of Advances in Engineering & Technology, Sept 2012. ©IJAET ISSN: 2231-1963 Vol. 4, Issue 2, pp. 456-463.