International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 09 Issue: 09 | Sep 2022 www.irjet.net p-ISSN: 2395-0072

SECURE DATA ENCRYPTION FOR ATM TRANSACTIONS

BOYAPATI SRI SAI GANESH, NAGELLA YATHEESH, PRATAPA DEEPAK BALAJI

Students, Dept. of Computer Science and Engineering (SCOPE), VIT University, Tamil Nadu, India

---

Abstract - This report is a prologue to the Protected Encryption procedures for ATM Exchanges in Python programming. Anyone, who doesn't know even the nuts and bolts of ATM Exchanges in Python, can unquestionably comprehend furthermore, gain extraordinary information from this report. The center subject of the undertaking centers around the improvement of Safety in ATM Exchange Framework in Python utilizing Hash and RSA calculations. The report additionally contains the methodology utilized in making ATM Exchanges, Correlation with various types of calculation, benefits of Hash calculation.

***Key Words*: ATM , RSA , HASH , ATTACKS**

1. INTRODUCTION

ATM represents Computerized Teller Machine. A particular PC makes it helpful to deal with your cash. For instance, practically all ATMs permit you to pull out cash, and many permit you to put aside installments. At certain ATMs, you can print an assertion (a record of your record movement or exchanges); check your record adjusts (how much cash in your records at the present time);Since finger vein confirmation frameworks are related with the Web during exchange from ATM, security dangers issues emerges. In this paper a finger vein distinguishing proof framework is made by Picture procurement gadget (worked in house) and is used in ATM with higher exactness rate. After that the obtained finger vein picture is shipped off the ATM server. For safely moving this picture through web to the focal server for characterization, a more gotten strategy is utilized which uses joined approach of light-weight cryptography and steganography [proposed variable most huge piece least critical piece methods. In focal server first and foremost the caught picture is gone through thresholding for removing the district of interest, and afterward contrast restricted versatile histogram adjustment (CLAHE) is utilized for the strengthening of the caught picture. A while later, it is changed to high contrast picture and edge, surface and element extraction is finished by Gabor channel, fractal aspect and Lacunae. At last the learning and grouping is finished by help vector machine. move cash between your records; and even buy stamps. You can ordinarily get to the most administrations at an ATM that is worked by your own bank.

1.1 Why use ATMs?

ATMs are a protected and helpful method for dealing with your cash. There are a large number of ATMs overall and you can utilize numerous ATMs 24 hours every day, 7 days per week. Some permit you to choose the language you need to utilize.

1.2 Is there a fee for using an ATM?

Check with your bank to check whether they charge any ATM expenses to clients. Practically all banks really do charge an expense to non-clients who utilize their ATMs. Remember that despite the fact that utilizing ATMs might cost you cash, it's significantly less costly than utilizing a check changing out help.

2. OBJECTIVE

The sole goal is to construct a program that commitments secure exchanges of ATM utilizing the ideas of cryptography fundamentals. i.e , it ought to give Classification like as it were approved ones just approach, for example, for our situation the profile creation and updation are confined to all with the exception of administrator who works for ATM or bank that is the reason we utilized separate module to deal with it. It should likewise give appropriate confirmation like for our situation we use card no and stick to distinguish regardless of whether the client is substantial. Trustworthiness should likewise be there as the Accessible equilibrium of client's shouldn't change without going through an exchange, for this in the event that the exchange is bombed there should be a rollback component to accomplish respectability. MIM assault should be eliminated, this should be possible by RSA plan and hash capabilities by producing keys for ATM and Server preceding ATM establishment i.e the critical sets of ATM and server ought to be concluded by individual banks and they ought to be kept classified.

3. PROPOSED METHODOLOGY

To carry out ATM exchanges we have partitioned our undertaking into two sections. One module involves the Executive and the other one is the ATM.

The Administrator module is answerable for production of the information base, and taking care of the clients. Administrator module simply doles out the card no to the people that come to open another financial balance. The bank balance is refreshed and put away in the data set. There is no pre-relegated pin for the clients; the client sets his pin all alone when He goes to the ATM interestingly.

In the ATM when the client begins his exchange, the ATM sends the information to the server. The server then, at that point, checks and thinks about them in the data set. On the off chance that the card number is off-base, it requests to enter the right card else it requests the pin. On the off chance that approaching interestingly, it requests the new pin age else for his exchange code. The pin is scrambled by the RSA calculation and shipped off the Server, the server unscrambles the pin and afterward hashes the pin, first and foremost.

Hashing is utilized in light of the fact that it is a one-way profile and no MIM assault can happen over it. On the off chance that a client comes for the first time, a hashed pin is put away in the data set. Else the hashed pin is then contrasted with the put away hashed pin. On the off chance that the pin matches, it executes the sum and the equivalent is refreshed in the database. If the pin doesn't match it requests the right pin and cuts short the exchange.

4. DATASET USED

The dataset we utilized in this undertaking is independent without help from anyone else.

5. ALGORITHMS USED

RSA encryption and decryption and SHA1

6. EXPECTED RESULTS

[1] How the ATM stores the subtleties of the client in scrambled structure in this manner guaranteeing security to the client.

[2]How RSA procedure assists with keeping outsiders from knowing keys of the client..

[3]How the HASH function prevents the Man in Middle Attack.

7. TOOLS, HARDWARE AND SOFTWARE REQUIREMENTS

Python 2.7 and sqlite3 module and hashlib module , SQLiteStudio (3.2.1)

8. MODULE COMPONENTS

In this, we will be using two modules

8.1 Admin

8.2 ATM user

8.1 ADMIN

On the off chance that there comes another client, he really wants to make another record/profile where the account number will be given sequential astute and the client needs to enter his/her own details. The given subtleties by the client are put away in scrambled structure in the data set. In the wake of making another record, the new client is given the card number for utilizing ATM administration.

In the wake of making and giving his/her details to the server, in the event that he/she really wants to refresh his/her subtleties, he/she ought to enter a card number to login and to actually take a look at validity. He/she enters the refreshed subtleties and similar subtleties are refreshed in the data set.

8.2 ATM USER

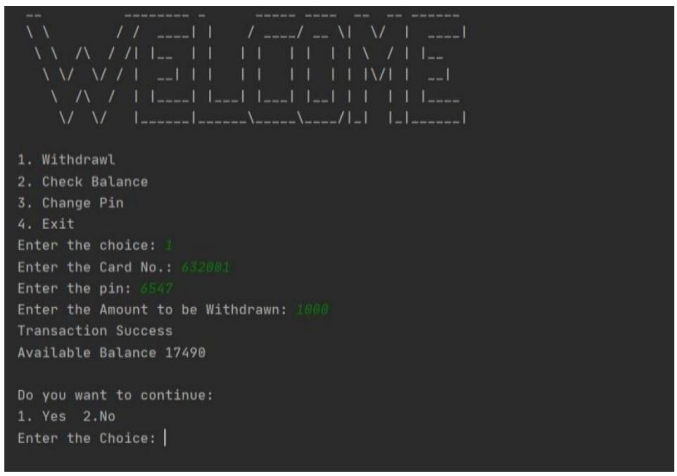
ATM Services:

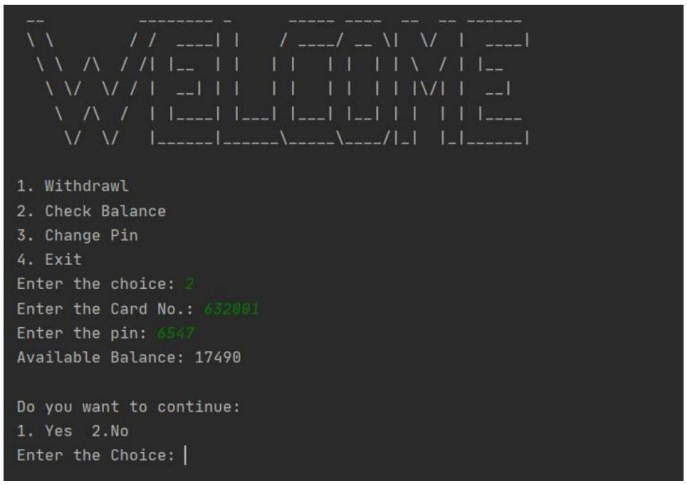
8.2.1 Update PIN

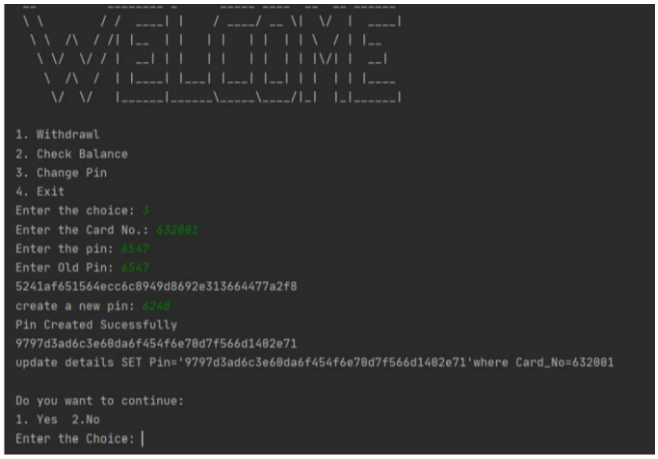
8.2.2 Withdrawal and update balance

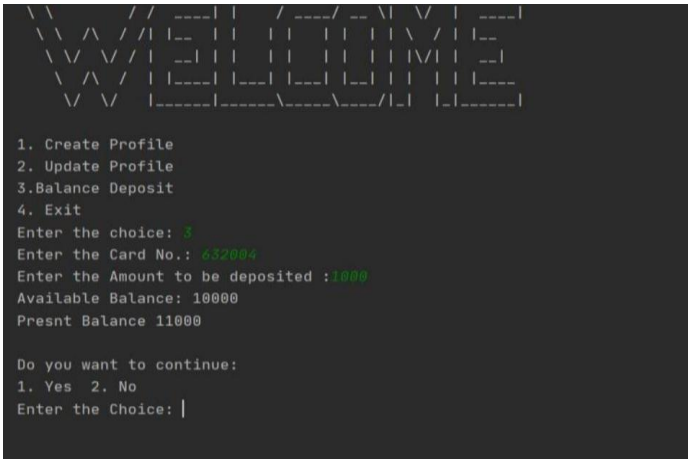
8.2.3 Print Available balance

9. RESULT OVERVIEW

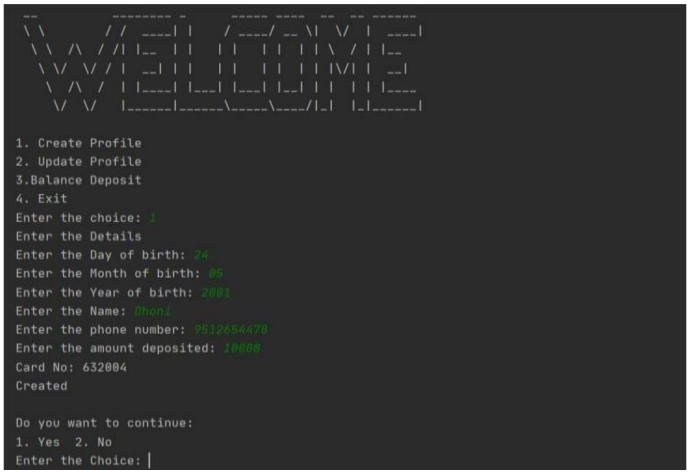


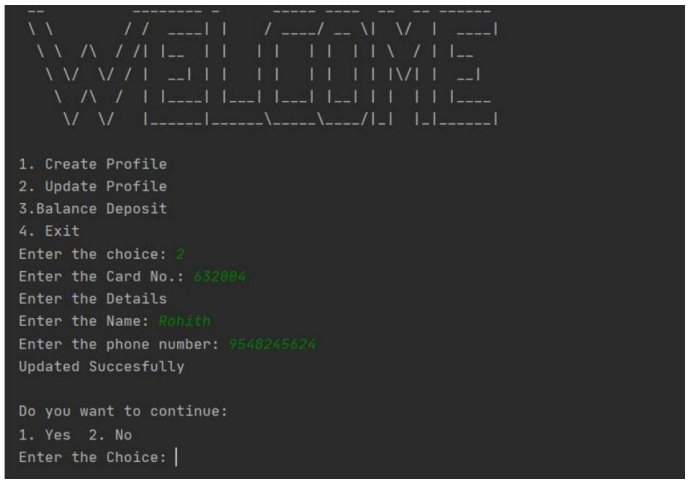


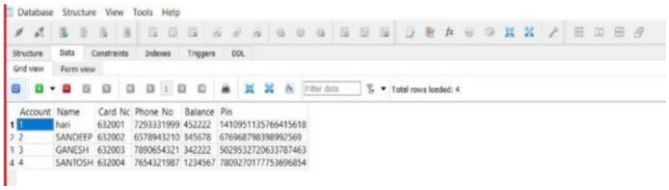




9.1 ADMIN SIDE







10. CONCLUSION

We have made a Gotten Information Encryption Framework utilizing Python language and it is putting away subtleties in scrambled type of the client guaranteeing security to the client. The RSA procedure utilized assists with keeping the outsider from knowing the keys of the client. The Hash capability forestalls the Man in middle attack. It tends to be carried out in reality for individual purposes.

REFERENCES

[1] Jyotiranjan Hota, "Automated Teller Machines in India", Proceedings of GLOGIFT 13, Dec-2013.

[2] Oliveira, T. and Martins, M, F. (2011) Literature Review of Information Technology Adoption Models at Firm Level, The Electronic Journal Information Systems Evaluation, 14(1): 110-121.

[3] Hota, J.R. (2013) Growth of ATM Industry in India, CSI Communications, 36(11): 23-25.

[4] Agarwal, R. and Prasad, J. (1998) A Conceptual and Operational Definition of Personal Innovativeness in the Domain of Information Technology, Information Systems Research, 9(2): 204-215.

[5] Chang, C. C., & Hwang, M. S. (1996). Parallel computation of the generatingkeys for RSA cryptosystems. Electronics Letters, 32(15), 1365- 1366.

[6] Huang, X., & Wang, W. (2015). A novel and efficient design for an RSA cryptosystemwith a very large key size. IEEE Transactions on Circuits and Systems II: Express Briefs, 62(10), 972-976.

[7] Yang, C. C., Chang, T. S., & Jen, C. W. (1998). A new RSA cryptosystem hardwaredesign based on Montgomery's algorithm. IEEE Transactions on Circuits and Systems II: Analog and Digital Signal Processing, 45(7), 908-913.

[8] Identifiers for Digital Identity Management.

[9] Venkat Prasad K., & Magesh S. (2015).a survey on encryption algo using modern techniques. International Journal of Pure and Applied Mathematics

[10] Laplante, P. A. (1977). Real-time systems design and analysis (2nd ed.). Washington, DC: IEEE Press.

[11] Devinaga, R. (2010). ATM risk management and controls. European journal of economic, finance and administrative sciences. ISSN 1450- 2275 issue 21.

[12] Heather Crawford (2011). Applying Usable Security Principles to Authentication.