

Secured Data Encryption

by: -

Dhvani Vashist, Tanishi Tyagi, Tushar Mittal, Vishvesh Gupta
E18CSE048, E18CSE186, E18CSE191, E18CSE213



Department of Computer Science Engineering

June 2020

Greater Noida-201310, Uttar Pradesh, India

Abstract—This report is an introduction to the Secure Encryption techniques for ATM Transactions in Python programming. Anybody, who doesn't know even the basics of ATM Transactions in Python, will certainly be able to understand and gain great knowledge from this report. The core theme of the project focuses on the development of Security in ATM Transaction System in Python using Hash and RSA algorithms. The report also contains the strategy used in making ATM Transactions, Comparison with different kinds of algorithm, advantages of Hash algorithm.

----- ✎ -----

1 INTRODUCTION

1.1 What is an ATM?

ATM is short for Automated Teller Machine. It's a dedicated computer that makes it easier for you to manage your money. For instance, withdrawal of money is allowed by all ATMs, and some even allows you to make cash deposits. You can even print a record of your account activity or transactions at some ATMs and check the amount of money in your account at that instance; You can even transfer money from your own account to someone else's account if the option is available.

1.2 Why do we use ATMs?

Money management is very safe and convenient nowadays, thanks to ATMs. You may use an ATM at any time or anywhere, 24/7 hours and 7 days a week. You can even select your own native language or the language you are convenient with, if the option is available at the ATM.

1.3 Vulnerability in online banking.

The digital banking faces many robbery cases which are divided into the following main categories:

1. Attack on the digital infrastructure for accessing information about different funds transfer.
2. Digital Infrastructure attack on ATM management
3. Clients Side attacks while performing e-banking

2 LITERATURE REVIEW

Studies on the topic state that [1] In the modern years the need of security has amplified many folds. It explains that the need to secure data is not new and goes way back to the time of 1st world war and even further back to the time of Julius Caesar. This paper provides a history of the data encryption techniques used in the history and how they have developed from Caesar cipher to DES and from DES to Triple-DES, AES and recent algorithms. This study explained the pros and cons of earlier algorithms and why they aren't used today. The main focus of this paper is initially general data hiding methods and then cryptographic algorithms. A brief study of a paper [2] presented a new Hybrid security algorithm for RSA cryptography named as Hybrid RSA (HRSA). Here the calculation of "public key" (P) plus

"private key" (Q) depends on the value of M, i.e. the product of 4 prime numbers. So difficulty involved in factorizing the M increases. Another appealing feature about this algorithm is the fact that the computation of P and Q involves the calculation of some more midway factors which makes the calculation more complex. This approach eradicates the transfer of variable x and M, where x is the multiplication of 2 prime numbers a and b. Thus the proposed approach gives a safer path for encryption and decryption procedure. To substantiate this statement, the "key generation time", "encryption speed" and "decryption speed" of the proposed algorithm HRSA are compared with conventional RSA and ERSA techniques. Another research was referred because of the use of a wireless medium in the project whose problem statement was [3] ,Security over Vehicular ad hoc network by means of Wi- Fi IEEE 802.11p standard and recognizing accurate attacker vehicle is a main challenge over VANET. Reducing costs of computation, effective expenditure of limited resources and giving uncompromised security was always a challenge over VANET. In this study , RSA algorithm based encryption and decryption techniques and implementation of limit with double RSU has been replicated using MATLAB software. Such background can be used while designing better MAC protocols, transmitting schemes, security features in VANETs. Providing confidentiality, message integrity, detecting and removing nasty and misbehaving nodes, from VANET is the focus of this study.

The literature of behavioral studies on ATMs has mainly focused on adoption and diffusion of technology, impact of technology adoption from customers perspective, suppliers perspective, and bankers perspective [1]. Major Technology Adoption Models as per the study of Norris and Yin (2008), Technology Adoption Research is almost twenty-five years old and there are around eight important theories of adoption. All these eight theories are derived from the foundation of innovation diffusion and Technology acceptance model. The exception among eight models is the Social Cognitive Theory. Technology acceptance model is quite individual focused among eight adoption models. However, other models focus on how diffusion of innovation takes place within the firm. Oliveira and Maria (2011) have explored that there is a dearth of academic literature on reviews of adoption models at firm level used in Information Technology

literature [1]. Author discussed Diffusion of Innovation Theory and Technology, Organization, and Environment (TOE)[7]. For more complex new technology adoption, it is important to integrate more than one theoretical model to achieve a better understanding of the adoption phenomenon. But in many cases, technology adoption research is a replication without substantive theoretical advances. However, there are ample opportunities to make theoretical advances using our current knowledge as the starting point [5]. These are the conclusions of the authors based on their review and comparison of major milestones of technology adoption research, Job Satisfaction research and Theory of Planned behavior. Most of the theories have emphasized on the factor influencing adoption behavior and the process of diffusion of technology. These models also reveal the individual difference and cultural difference in technology adoption. The first developed algorithm for the ATM transactions used to extract features of the bank, for e.g. Cash withdrawal, deposit or balance enquiry. These features were selected in a region form to perform transaction [4]. There was only a simple encryption technique used like for example play fair cipher technique. This method was good but didn't show great results because of less amount of cryptography used. In ATM Transactions we only focus on ATM features and mainly on security. The feature transactions are a topic of deep interest in the Finance domain. The system should be good enough to represent the ATM in feature form. Features of the ATM are in two modules – admin and user. Admin module features include creation of new accounts, pin creation and updating them in the database. Admin module feature category includes taking the input profile information. Today there are a number of methods to extract information from an ATM to the Server. This method uses RSA and Hash function algorithms to implement this feature. This method is often termed as One-way encryption method. Both these methods fall under admin module feature category [2]. Then this data is decrypted to an information set that represents the user's bank information to the server. Encryption is a multistage technique. Encryption uses all the relevant information from the ATM output information that is given by a user that is to be sent to the server. It forms an encrypted text of the account number, pin where the output of others is sent to the server using RSA. User

module features include pin updating, withdrawal, balance enquiry etc. The method used to encrypt this user information is RSA and hash function algorithm. We have implemented this system user friendly and totally secure to protect user information. In ATM transactions, we can also implement SHA (Secure Hash Algorithm), MD5(Message Digest). ATMs are the most important part to maintain a user's financial life.

3 DATA RESOURCES USED:

- For Backend and Linking:
 - ❑ Python 3.x: It is our main programming language. We have used it to develop the backend and frontend.
- For database management:
 - ❑ SQLite 3: It is used for database management. Only the admin can access it. We use it for storing user information after encryption.
- Programming platform: We have used the following platforms for python coding.
 - ❑ Jupyter
 - ❑ Idle
 - ❑ Atoms

4 METHODOLOGY

To implement ATM transactions, we have divided our project into two parts. One module comprises the Administrator and the other one is the ATM. The Admin module is responsible for creation of the database, and handling the customers. Admin module just assigns the card no to the individuals that come to open a new bank account. The bank balance is updated and stored in the database. There is no pre-assigned pin for the users; the user sets his pin on his own when he goes to the ATM for the first time. In the ATM when the user starts his transaction, the ATM sends the data to the server. The server then checks and compares them in the database. If the card number is wrong then it asks to enter the correct card else it asks for the pin. If coming for the first time then it asks for the new pin generation else for his transaction code. The pin is encrypted by the RSA algorithm and sent to the Server, the server firstly decrypts the pin and then hashes the pin. Hashing is used because it is a one-way profile and no MIM attack can take place over it. If a user comes for the first time,

- Update PIN
- Withdrawal and update balance
- PrintAvailablebalance

message authentication code, password databases, fingerprints, manipulation detection, checksums and many more

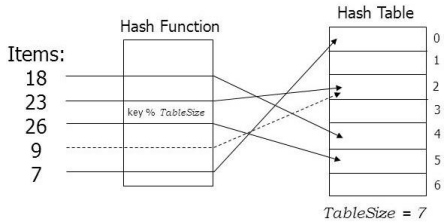


Figure 3

RSA ALGORITHM

Key Generation: -

1. Generate two distinct prime numbers p and q.
2. $n = pq$
3. $m = \Phi(n) = (p-1)(q-1)$
4. Choose a number e, co-prime to m and $GCD(m, e) = 1$ such that $1 < e < \Phi(n)$
5. Find d such that $(de) \bmod \Phi(n) = 1$

- Cipher text = (plain text) e mod n
- Plain text = (Cipher text) d mod n

The ATM sends the pin to the server using RSA encryption. The Server then decrypts that using RSA and uses a hash function for further processing.

6 RESULTS AND EVALUATION:

Following are the screenshots of the working project.

1. A new user is created using the Admin.py file.

```
===== RESTART: C:\Users\HP\AppData\Local\Programs\Python\Python38\admin.py =====
Welcome

1. Create Profile
2. Update Profile
3. Exit
Enter the choice: 1
Enter the Details
Enter the Day of birth: 02
Enter the Month of birth: 02
Enter the Year of birth: 2000
Enter the Name: Tushar
Enter the phone number: 9788778836
Enter the amount deposited: 200000
Card No: 632004
Created

Do you want to continue:
1. Yes 2. No
Enter the Choice: 2
Good Bye
```

Figure 4

2. We add the data of the users to the database and a unique Card number is generated. Initially the pin generated is 0.

Account	Name	Card No	Phone No	Balance	Pin
1 1	Tanishi	632005	6767575763	400000	-8802655181562605797
2 2	Dhvani	632009	3920483234	399999	0
3 3	Vishvesh	632014	2038402334	1000000	0
4 4	Tushar	632004	9788778836	200000	0

Figure 5

3. The user sets his unique transaction pin in the ATM.

```
===== RESTART: C:\Users\HP\AppData\Local\Programs\Python\Python38\ATM
Welcome

1. Withdrawal
2. Check Balance
3. Change Pin
4. Exit
Enter the choice: 3
Enter the Card No.: 632004
Enter the pin: 0000
Create a new Pin: 3456
Pin Created Successfully
```

Figure 6

4. The pin is encrypted and updated on the database.

Account	Name	Card No	Phone No	Balance	Pin
1 1	Tanishi	632005	6767575763	400000	-8802655181562605797
2 2	Dhvani	632009	3920483234	399999	0
3 3	Vishvesh	632014	2038402334	999600	-7057418792655023988
4 4	Tushar	632004	9788778836	200000	-1955858428602731257

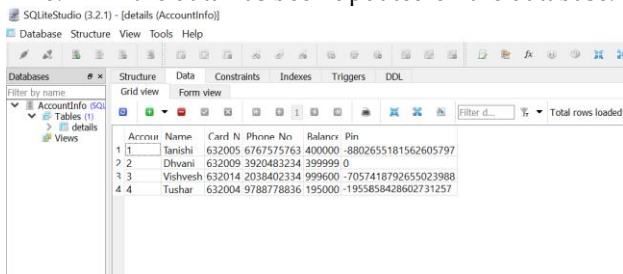
Figure 7

5. Withdrawals using the pin.

```
1. Withdrawal
2. Check Balance
3. Change Pin
4. Exit
Enter the choice: 1
Enter the Card No.: 632004
Enter the pin: 3456
Enter the Amount to be Withdrawn: 5000
Transaction Success
Available Balance 195000
```

Figure 8

6. All the data has been updated on the database.



Account	Name	Card N	Phone No	Balance	Pin
1	Tanishi	632005	6767575763	400000	-8802655181562605797
2	Dhivani	632009	3920483234	399999	0
3	Vishvesh	632014	2038402334	999600	-7057418792655023988
4	Tushar	632004	9788778836	195000	-1955858428602731257

Figure 9

7 CONCLUSIONS

We have made a Secured Data Encryption System using Python language and it is storing details in encrypted form of the user ensuring security to the user. The RSA technique used helps to prevent the third party from knowing the keys of the user. The Hash function prevents the Man in Middle attack. It can be implemented in the real world for personal uses.

8 ACKNOWLEDGMENT

The authors wish to thank Dr. Kuldeep Chaurasia and Dr. Vijay Bohat. They have been a great inspiration and who have provided sufficient background knowledge and understanding of this subject. Their valuable suggestions were of immense help. We would also like to thank our friends and family for their support and encouragement.

9 REFERENCES

- [1] Jyotirnanjan 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] J 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] Identifiers for Digital Identity Management.
- [6] Laplante, P. A. (1977). Real-time systems design and analysis (2nd ed.). Washington, DC: IEEE Press.
- [7] Devinaga, R. (2010). ATM risk management and controls. European journal of economic, finance and administrative sciences. ISSN 1450-2275 issue 21.
- [8] Heather Crawford (2011). Applying Usable Security Principles to Authentication.