RFID Authentication System Integrated with the Enhancement of the Security of OTP using Cryptography

J. Sivapriya [1], P. Vamsi Mohan [2], V. Surya Teja [3], N.V. Harsha Vardhan Gupta [4]
[1] Assistant Professor, Department of Computer Science Engineering, SRM Institute of Science and Technology, Ramapuram, Chennai, India.
[2, 3, 4] Department of Computer Science Engineering, SRM Institute of Science and Technology, Ramapuram, Chennai, India.

Abstract – The technology of RFID has been evolving in various aspects of implementation in every industry. We believe that RFID microchip is been erupting as a new technology which can be implanted in the body of a human being for entry into more secured locations and to protect the data which is most important. The main approach for the RFID environment is for the safety purpose of the data which can be achieved in a highly secured manner .In this paper, we purposed a system for E-commerce websites to avoid fraud and ensure safe bank transaction to the customer, we provided RFID login authentication which is connected to database and the OTP is encrypted for the safety of the customer's bank transaction using Cryptography.

Index Terms – RFID, Microchip, Cryptography.

1. INTRODUCTION

At present, E-commerce websites has been evolving more and more same as the population. The security of the E-commerce website is also needed for the effective running of the site .Many online frauds is being taken place and the safety of the customer's details stored in the server of the website is needed. This can be achieved by using RFID technology by in building the data in the tags and read by the readers in the range.

This can also be done in a different way by using Cryptography techniques which will be very useful for the user.With the help of cryptography,we can control the attacks of eavesdropping, replying, counterfeiting, tracking etc., RFID technology can be used for various purposes like to buy something, attendance, entering into restricting places etc.,RFID tags come in different shapes like circular, rectangular, microchip, keychain.

In this paper,we propose a system in which the user will be given with a RFID tag with which he/she can access their account through a user connected to database.When they are going to do a transaction then the OTP will be send in a secured way using cryptography techniques like advanced encryption standard ,elliptic curve cryptography, data encryption standard which helps the customer from being attacked by third parties.

2. KEY TECHNOLOGIES

2.1 Advanced Encryption Standard (AES):

An AES involves symmetric key algorithm ciphers a given text block of 128 bits which is one the most trusted way of important information to be stored.The processs involved in transforming the given string is,at first, the values will be substituted with different values,second,the shifting of rows takes place ,third ,now the shifting of column occurs finally the XOR operation is applied on columns using a key then the obtained value will be cipher text.It provides a good security strength and there by the cost for implementation is affordable.

2.2 OTP Authentication:

When the OTP is requested by user then it is generated in the bank transaction server there by will be encrypted and send to user through the SMS which is already registered by the website and sored in the database ,there by he/she is prompted to enter the encrypted OTP to decrypt it using a secret key will be verified . The OTP verification is absolutely necessary to know whether the transaction is valid or not.But with the help of AES we prevent the OTP from being attacked by the third parties.

3. PROPOSED MODELLING

The proposed system can be divided into two parts.There are hardware design and software design.The detailed structure of the design is given below.

3.1 Hardware design:

The design of the hardware consists of a voltage regulator(12V) of model IC7809, Arduino UNO, RFID tags and reader.An adapter of input AC 100-240V is given can be converted to 12V DC.Voltage regulater is used for providing two sets of 12V ,one for RFID reader and another for Arduino UNO.The power used for RFID reader to read the data present in the tag as the tag is passive in nature and for Arduino UNO to retrieve the

values from the RFID reader.The process of the system goes in the following way:

1.The RFID tag is kept on the RFID reader.

2.RFID reader reads the data present in the RFID tag.

3.The data which is read by the RFID reader is retrieved by the Arduino UNO.

4.The data is transferred to the dersired location of the website through the USB cable.

Figure-1:Hardware Kit

3.2 Software Design:

At first ,the application starts registering the details of the users and provides them with a unique identification number through RFID tag .The RFID reader is also given to user will be attached to the user's PC once is registration with user is done .The software is designed with the help of java for coding and MySQL for database .The process involved is divided into two phases.They are login authentication using RFID and OTP verification which is used for the flow of the system.

3.2.1 RFID login authentication phase:

The data required for the login into the account of the user is through RFID which the only possible way.The data is stored in the RFID tag which is given by the management authority of the application which the details for login. When the RFID tag and reader is given to the user then he/she access the account by placing the RFID tag on the RFID reader which reads the data present in the RFID tag by energizing it with power supplied by the voltage regulator.If the RFID tag data is valid which is read by reader then the the user can access the account.

3.2.2 OTP Verification phase:

In this phase ,when the user requests the OTP then a random number will be generated and will encrypted using symmetric key algorithm of Advanced Encryption Standard and send to registered mobile number of the user over a communication channel.When the encrypted OTP reaches to the mobile number of the user then the website prompts the user to enter the encrypted OTP and the decryption process starts only when the appropriate secret key is matched and finally the OTP verification takes place.

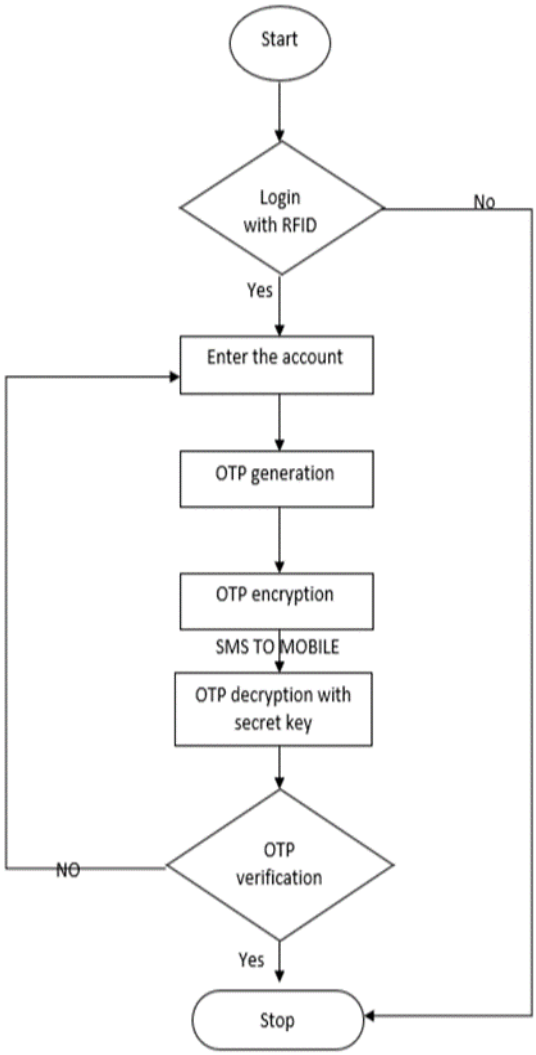

Figure-2:Flow chart of the system

Figure-3:OTP verification phase

4. RESULTS AND DISCUSSION

The system which is proposed shows the results in a best way by avoiding the attacks of the third parties and by providing confidentiality, mutual authentication, forward security ,prevent decimal attack and reliable. The account with a RFID login and OTP security plays an important role in the safe transaction between the customer and the seller. With the help of RFID and Advanced Encryption Standard we can protect the attacks of intruders.

5. CONCLUSION

In summary, the system shows how an account in a website can protected from different kinds of attacks is shown.The use of RFID is for the individual entry and no other can intrude and the OTP is secured with the help of symmertric key algorithm of AES can be trustworthy.Now-a-days every body is onto the computer creating accounts in whichever they want then this helps them from being attacked.

REFERENCES

[1] Chunling CHEN, yang WANG, Han YU and Xiao-Hui Qiang The RFID Mutual Authentication scheme Based on ECC and OTP Authentication : 2016 IEEE International Conference on Ubiquitous Wireless Broadband (ICUWB) ,2016,PP 1-4.

[2] D.Eastlake, 3rd, RFC 3174:"US Secure Hash Algorithm 1 (SHA1)", September 2001 .

[3] D.M'Raihi, RFC 4226:"HOTP: An HMAC-Based OneTime Password Algorithm",December 2005 .

[4] D.M'Raihi, RFC 6238:"TOTP: Time-Based One-Time Password Algorithm",May 2011