NEW GENERATION SMART CARD

Jeet Thakar[1]; Rishabh Jain[2]; Prof. Manjunath CR[3]

[1]Department of CSE, School of Engineering and Technology-Jain University, Bangalore, India
[2]Department of CSE, School of Engineering and Technology-Jain University, Bangalore, India
[3]Department of CSE, School of Engineering and Technology-Jain University, Bangalore, India
[1] jeetthakar60@gmail.com, [2] rishabhsmjain@gmail.com, [3] manjucr123@gmail.com

Abstract- In recent times, there has been a constant increase in usage of plastic cards, used for identification, banking and other such purposes. This technology has bolstered due to its easiness and transparency. It is based on the concept of Internet of Things (IoT). Every card has its specific details and identification factor with the help of which it is recognised. The other processes happen at the backend and the user is unaware of it. Earlier, a magnetic strip was used on each card, now it is being replaced by a micro chip embedded on the card. During financial transactions, security of the user's credentials is a crucial thing. If it is tampered with, results can be fatal.
Keywords - Banking, Micro chip, Security, Internet of Things, Magnetic Strip.

I.   INTRODUCTION

Internet of Things, a term which is alluded to a system of gadgets, is rising at an exponential rate since it came without stalling. IoT can be amalgamated with various disciplines, for example, Artificial Intelligence and Machine Learning to make new gadgets/items for particular as well as general use. It can likewise be incorporated with installed frameworks, for example, a miniaturised scale controller to make superior frameworks. IoT is an interesting branch which can be utilized to perform local tasks just as those which has a high effect and the exactness ought to be on the pinnacle. The cardinal property for IoT is the dimension of similarity that it offers. IoT mixes in with practically every one of the areas. It plays an essential job in different divisions, for example, communication, networking, research and also domestic use. Henceforth, utilising it in the wellbeing segment can have a gigantic effect in technological revolution.

Fig.1 Smart card (Source: www.indiamart.com)

A smart card consists of an embedded integrated chip that works as a micro-controller or as a source of memory storage. The card communicates with either a wireless contactless frequency (e.g online payments) or by physical contact (e.g swiping machine). Every card can store a certain amount of data that includes the credentials of user that are used for authentication purpose. This technology has its own international standards such as ISO/IEC 7816 and ISO/IEC 14443. Smart cards includes banking cards, SIM cards used in phone and also other USB based cards.

Fig. 2 Micro chip embedded card [3]

As banking is associated with this, security becomes an integral part of the system. Certain security checks are to be done to ensure its maximum protection. Various security protocols are designed just for this purpose. Heavy encryption is used to achieve the same. In the proposed system, we are introducing a new type of card that is used for more than one purpose. Currently, there are multipurpose cards but discrete from our idea. While introducing this new variety of card, the security and effectiveness of its use is taken into consideration.

II.   LITERATURE SURVEY

There has been a flow of ideas and systems in this field, each upgrading the previously used methods, protocols and technology. In the system proposed in [1], the usual encryption methods such as DSA, RSA, Elgamal in public key cryptography were replaced by Authenticated Encryption (AE). This resulted in lesser transaction time with minimal computational effort. AE is a simple cryptography technique. It uses three types of combination of techniques to fulfil algorithm. These combinations are Encrypt then MAC (EtM), Encrypt and MAC, MAC then Encrypt (MtE). But this can only support banking transactions and not for other use.
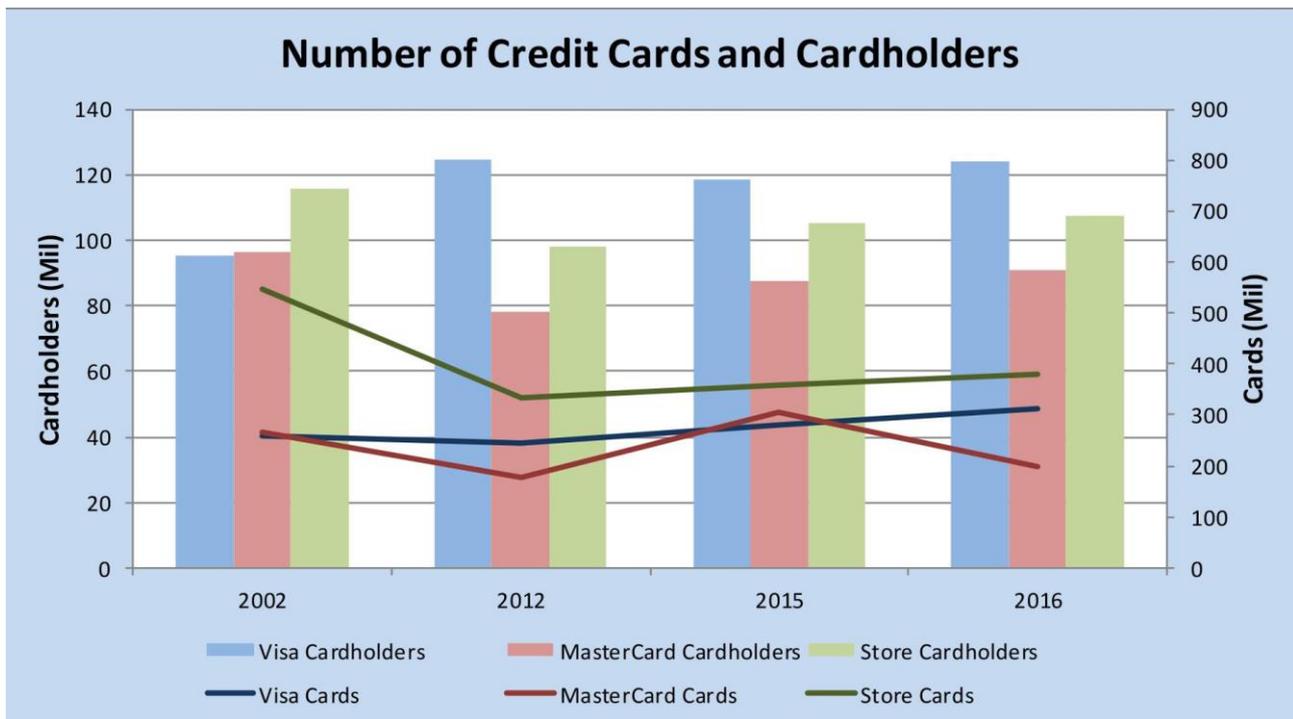
Fig. 3 Graph displaying number of credit cards and card holders

A similar system is proposed in [2] but in a more secured way. Unlike the general OTP method, this uses two level authentication. First is the user's PIN and second is OTP. Also, it uses SHA-256 to generate OTP. Furthermore, it also states why SHA-256 is used for OTP generation. This is justified with the help of various Hash algorithms. But similar to the system proposed in [1], this card is used only for banking.

In the system proposed in [3], it has introduced a very unique way of inducing Card Management System (CMS) and Application Management System (AMS). For data security, Public Key Infrastructure (PKI) is implemented in the system. Both the methods are driven through one database, which is praise worthy. Later, in [4], a smart card is introduced for the students of higher education. They have presented a single card that is used throughout the campus in places like library and canteen. Every card has a unique barcode that is used to identify the user and the data is processed accordingly.

In [5], various case studies are taken into consideration and the usage and effect of smart cards on each scenario has been explained. Certain points like how it has changed the previously used methods are discussed and how this process is made more efficient using this technology. They have covered domains such as IT Network and Security Identification, Public health, Banking and Finance, Cashless Gaming.

Thus, from the former work, we can say that a smart card containing all the essential features is still required that covers the drawbacks of the currently existing system and provides a better user experience as well as ease of managing the database at the backend. So, we aim to propose a system that can work as a Debit card, Credit card, one that also supports UPI transactions.

III. METHODOLOGY

With this card, banking transactions can be either online or physically by swiping or by tapping on the machine. Along with these features, a printed QR code will be printed on the card that can be used to receive UPI payments. Each of the features has different method of working. Let's see each of them in detail.
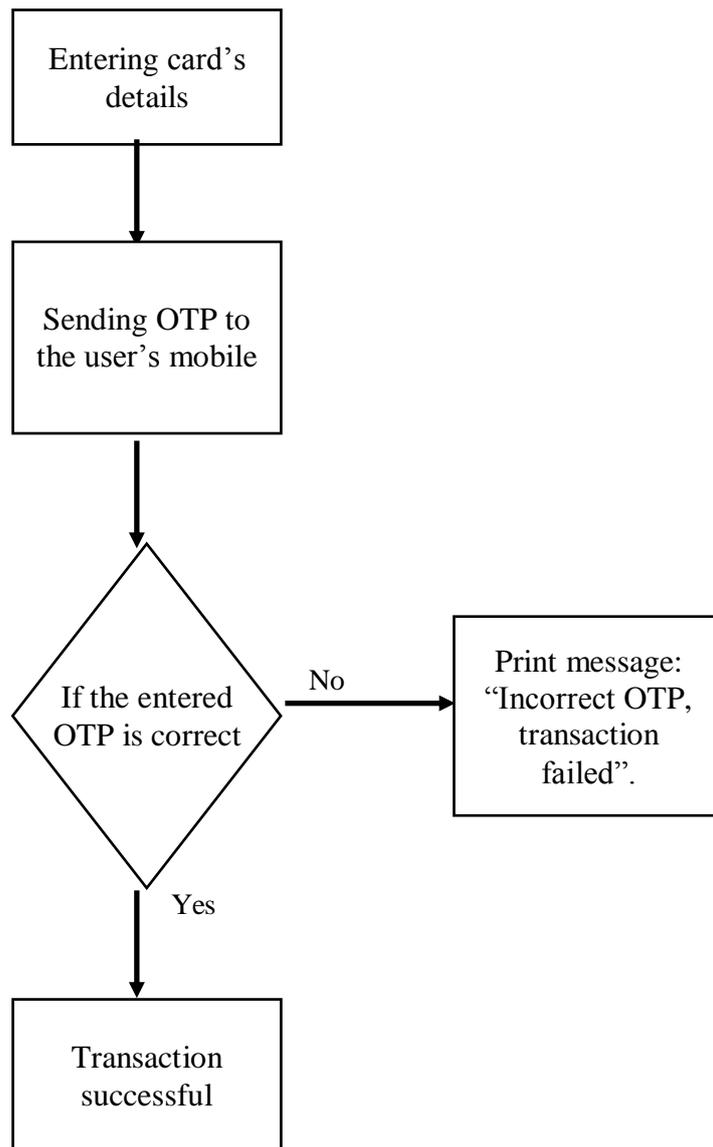
```
┌─────────────────┐
│ Entering card's │
│     details     │
└─────────────────┘
         │
         ▼
┌─────────────────┐
│ Sending OTP to  │
│ the user's mobile│
└─────────────────┘
         │
         ▼
      ◇ If the entered ◇ ──No──→ ┌──────────────┐
      ◇ OTP is correct ◇         │Print message:│
                                 │"Incorrect OTP,│
         │Yes                    │  transaction │
         ▼                       │   failed".   │
┌─────────────────┐              └──────────────┘
│   Transaction   │
│    successful   │
└─────────────────┘
```

Fig. 4 Flowchart of banking transaction

A) Banking Transactions

As the card is embedded with two circuit chips, it can be used as a credit and a debit card. If the person is using it physically, the machine will ask for its 4 digit password. If it is used for online payment then the user will redirected to the banking portal and will be asked to enter the card details, later an OTP will be sent to the user's registered mobile number. After entering the correct OTP, the transaction will be completed. If OTP is incorrect, system will ask the user to enter correct OTP, if it is still incorrect, the portal will get terminated. There will be an option to resend the OTP in case if the previously sent OTP was not received.

If the EDC machine is a recent one then it also supports the transaction by tapping the card on it. For instance, the shopkeeper will enter the amount in the machine and the user just has to tap his/her card to initiate the payment.

B) QR code

On every card, a unique QR code will be printed, different for each user, that will be used as a UPI gateway. If the user wants to receive payment from anyone then the sender just has to scan that QR code and the money will directly get credited in the user's bank account.
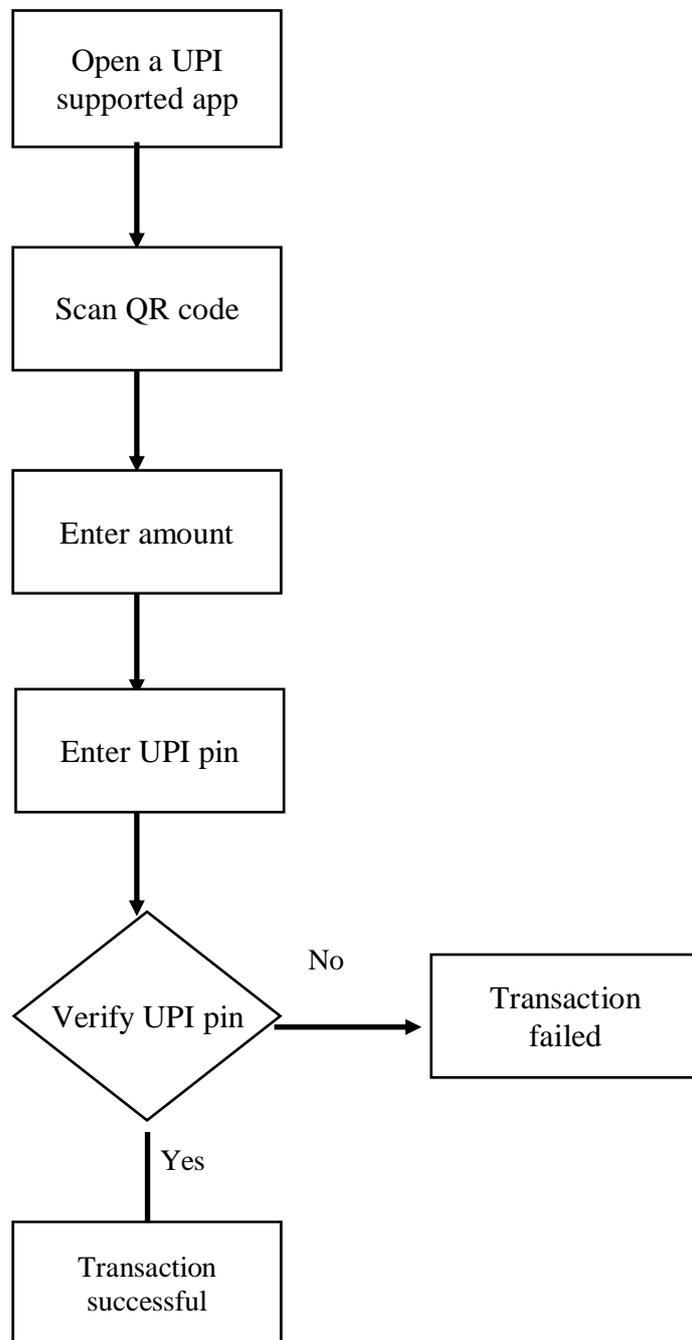
```
┌─────────────────┐
│  Open a UPI     │
│  supported app  │
└─────────────────┘
         │
         ▼
┌─────────────────┐
│  Scan QR code   │
└─────────────────┘
         │
         ▼
┌─────────────────┐
│  Enter amount   │
└─────────────────┘
         │
         ▼
┌─────────────────┐
│  Enter UPI pin  │
└─────────────────┘
         │
         ▼
    ◇─────────◇           No    ┌──────────────┐
    │ Verify  │ ──────────────→ │ Transaction  │
    │ UPI pin │                 │ failed       │
    ◇─────────◇                 └──────────────┘
         │
        Yes
         │
         ▼
┌─────────────────┐
│  Transaction    │
│  successful     │
└─────────────────┘
```

Fig. 5 Flowchart of UPI transaction

IV. SYSTEM IMPLEMENTATION

The prototype of the smart card proposed in this paper consists of four exclusive features. For every feature, certain characteristics as well as protocols are followed. The transaction protocol for the banking transactions of credit as well as debit card is Secure Electronic Transaction (SET). It is not just a payment system, but a group of security protocols and formats that allows these transactions to flow in a smooth transition. Along with SET, another protocol 3-D secure is used. It is an XML based procedure that provides an additional layer of security to ensure safer transactions.

153

Also, for UPI transactions, each user will be given their unique QR code. If someone has to pay them, then they can directly scan the QR code using any UPI supported banking apps and can send money directly from one bank account to another.
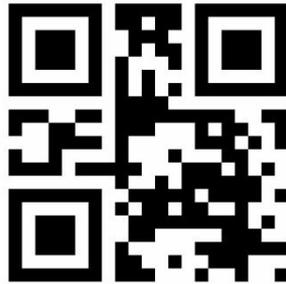

Fig. 6 QR Code (Source: www.qr-code-generator.com)

To store the user's activities and their credentials, a backend database will be created that will be managed by their respective banks. They can also opt for various messaging services that will notify them whenever a transaction has occurred. A common database is used for all the entities and their data can be retrieved through basic queries.

V.   CONCLUSION

In this paper, a multipurpose smart card is proposed. It is equipped with four major features that makes this card more appealing. All these components allows this smart card to be efficient, user friendly and secure. The idea of embedding a QR code has never been implemented before. We have tried to overcome almost all the drawbacks from the previously proposed smart cards. The protocols used in this device are reliable and up to the mark making this new generation smart card one of its kind.

REFERENCES

[1] Yoso Adi Setyoko and I.G.B. Baskara Nugraha, "Multipurpose Smart Card System" in Institute of Electrical and Electronics Engineers, 2014.
[2] S. Nivetha, N. Edna Elizabeth, T. Prasanya Padmasha, I. Gohulalakshmi, "Secure Authentication Process In Smart Cards" in Institute of Electrical and Electronics Engineers, 2016.
[3] Mohamed Mohandes, "A Smart Card Management and Application System" in Institute of Electrical and Electronics Engineers, 2010.
[4] Abhishek Singh, Ashish Chopra, Mohammad Imran, Rahul Singh, "Designing and Implementation of Smart Card Technology for the Students of Higher Education" in International Journal of Computer Science and Mobile Computing, 2017.
[5] Michael **R.** Carr, "Smart Card Technology With Case Studies", in Institute of Electrical and Electronics Engineers, 2002.