# E-Authentication System with QR Code

Sagar[1], Raju Ranjan[2]
[1]*Author, Dept. Of Computer Science and Engineering, Galgotias UniversityGreater Noida,India*
[2]*Mentor, Dept. Of Computer Science and Engineering, Galgotias University Greater Noida,India*

***Abstract*** **- Even budgetary ventures are obsessed with the online area since a quick web framework is being established and people are becoming more informed. Hacking is the process of gaining access to personal or business information by exploiting security flaws in a computer system or network. Present online banking structure was vulnerable to hacking, that too with disastrous consequences. Personal Information of clients has recently been leaked by hackers using hacking methods, such as Phishing or social engineering, by which they can acquire a client's ID and password.**

**We need to implement a new authentication framework for internet Banking right now. A new authentication framework combined with One Time Password and a QR-code, that is a type of 2-factor standardized identification. The technique of building trust in user identities submitted to an informationsystem electronically is known as electronic authentication.**

**When we refer to authentication it simply means a process that can confirms or certify a person's claim of their identity and works, the terms digital authentication and e-authentication are interchangeable. When used in combination with an electronic signature, it can show if datareceived has been altered with after it was signed by its original sender. By confirming the identity of a person and confirm that they are in fact who they say they are when conducting transactions online, electronic authentication can lessen the risk of fraud and identity theft.**

## I. INTRODUCTION

Online-based banking, often known as web banking, is basically a type of electronic payment system which allows the clients of a specific bank orsome other kind of banking establishment to easily do a variety of banking transactions through their website.

A few banks operate as a "instant bank" or “quick bank”(also known as a"virtual bank"), rely only on web banking .

Individual and corporate financial administrations are provided using web banking programming, which includes features such as viewing account changes, obtaining proclamations, checking ongoing exchange, and making secure installments. The most common/basic method of accessing is through a well-protected gateway with a user defined Unique ID and security key/code, and many financial establishments also offer 2FA authentication with a phone number.

The security of a client's financial data is critical, as internet banking would not be possible without it. Furthermore, there are huge reputation risks for institutions. Different security methods have been implemented by financial institutions to reduce the risk of anyone trying to access to a client's online records unapproved, but there is no uniformity across the other various methodologies that are used.

Despite of the dangers that single factor authentication possess it is still being used by the population, it is not even considered safe enough by the authorities for web-based banking or transactions in certain countries. For web- based banking, there are mostly two main security mechanisms in use.

The PIN/TAN system, in which the PINrefers to a secret key that is used only for login and if we talk about TANs it refer to OTP used to complete most of the transactions. TANs are distributed in a variety of ways.
Its a common technique to deliver a list of TANs to the client through post, and another method is to construct TANs on demand using a secure Codes. These are based on time

Many Hi-tech TAN generators incorporate the exchange information in TAN age processes immediately afterthey display them on the screens, allowing the client to detect if there is a man-in- the-middle attack carried out by worms or viruses trying to control transaction info behind the PC's back.

One more way to provide TANs to a online financial customer is to
send the current bank exchange's TAN by SMS to the client's (GSM) cell phone. The exchange sum and nuances are normally stated in the SMS message, while the TAN is only valid for a limited time. This "SMS TAN"

administration has been received by several banks, in many countries.

## II. RELATED WORK

### A. QR CODE

The Japanese organist Denso Wave devised the QR Code. All the Information can be encoded in both vertical and horizontal directions, allowing it to contain a lot more info than a traditional code. The data thatis obtained by scanning or taking a picture of the code/image with a camera (as an example, one camera integrated within a smart phone) and then processing the QR with a QR code reader.

Product monitoring, identification of an item ,tracking of time, management of documents,and general marketing are some of the basic applications.

Despite the fact that this technology has been present for us for more than a decade, it has become an easy way for advertisers to reach modern smart phone clients. QR Codes, or Quick Response Codes, are nothing new. Tobe honest, they've been employed as a kind of promotion and stock control in Japan and Europe for the previous ten years. One-dimensional (1D) bar-codes have a lower level of securitythan two-dimensional (2D) barcodes.

Filtering the lines and spaces in 1D barcodes makes them very easy to read. In any case, human eyes have a hard time reading 2D barcodes in a pictorial design. Single-dimensional barcodes always give their response in single direction in order to be relevant. The data would not be accurately reviewed if the objective of a scan line did not fit within a range.

Regardless, 2D barcodes have a broad Spectrum of scanning possibilities. The main them is the amount of data they store and share. QR codes are two-dimensional (2D) grid barcodes can carry 7,089 numeric , 4,296 alphabetic, and 1,817 kanji characters of information easily. They are appropriate for autonomousgroups because of the capability to contain more data and easy access.

Security of QR CODES

For managing Codes, there are two distinct threat models to consider. Atfirst, aggressor has the option of reversing any module, converting it from dark to white or vice versa.

Furthermore, a limited attacker can only switch from white to dark modules, not the other way around.

Multicoloured : A sticker consisting of a Quick Response Code with altered Quick Response Code in same form to the original QR Code. Obviously, this would necessitate some preparation or the use of a printer and planning software for a smart-phone.

When assaulting a large area against a single target, the time necessary for preparation should not be considered a real constraint.

Single Color: In this case, we limit ourselves to changing only one colourat a time. The basis for this restriction can be found in the scenario of an attacker attempting to change a singleitem .

Example of QR code:-

### B. One Time Password (OTP)

One Time Password is a constructed secure code and can only be used only once. It can be a number or a string made of alphanumeric characters that are generated automatically and they validate the client for any particular transaction oreven a login session.

Depending on how the token is built, this secret code can basically changesevery minute and many can even change in 30-40 seconds.

The customer is given a device that generates an One Time Password using a cartographic key and an algorithm. And server consist of a confirmation server with a similar method and key-scan verify the secretkey's legitimacy.

In One Time Pass-code based validation approaches, customer's OTP app and the server always tend to rely on the insider information that is shared between them. The Hashed Message Authentication Code( “HMAC” in short) are used to create one-time password qualities (HOTP). For further security, the OTP values carry moment or second time stamps. A client can get the one-time secret phrase via a variety of methods, including an SMS,MMS, or a dedicated app on the end terminals.

The one-time secret code/key keeps IT chairmen and security directors safe from common traps when it comes

to secret key security. They don't ever have to worry about all those structural rules, like bad or the weak passwords, users sharing their credentials, or the reuse of a similar secret password across multiple records and systems. One plus point of OTP is that they expire every few minutes, preventing the attackers or unauthorized users from obtaining and reusing the secret codes.

## III. PROPOSED SYSTEM

One very important component of authentication system's is security protocols. Recognizable proof througha safe process in which only genuine customers must be able to get assistance after getting authorization from server by using the produced information from the customers' smart-phone.

Furthermore, comfort is important, as is the safety, because system's burden has made it possible use the system. As a result, rather than using the bank's security card and using the mobile OTP, a key mechanism suggested here it is being used to create a Quick Response-code. Theinstitute generates the Quick Response -code using the client's transfer data,

Finally, have the customer have to enter the generated OTP code on thedevice to complete their transfer. We anticipate secure communication between service organizations and the service organizations certification authority in our proposed scheme.

## IV. SECURITY ANALYSIS

We do expect a secure communicationchannel between the client (PC) and the certification authority (CA) via an SSL/TLS tunnel, as well as specialty co-ops (Bank). As a result, a malicious customer will not be able to decipher the contents of Information since the suggested system uses the camera of a smart-phone to recognize QR-codes and never splits information between the client's PC and Smart-phones.

Similarly, in the underlying enrolment stage, the consumer and certification authority (CA) can share the sequence number (SN) of the customer's smart-phone through a secure mechanism.

OTP value is changed if a fraudulentor altered PIN is entered. In the suggested structure, the consumer can avoid Phishing attacks by recognize the random number (RN) before checking transaction info when the QR changes. After consulting a genuine expert service, transaction data is changed over.

The age of OTP can be interrupted byclient awareness in the case that the random number (RN) and transaction data are faked or altered. In the meantime, our suggested approach necessitates an important contribution of transaction info by QR and allowed validation by a PC in order to generate OTP. Authentic clients are identified as a result of this approach, and the threat to the clients is prevented.

## V. CONCLUSION

The importance of security and comfort in electronic monetary administrations is similar to two sides of a coin. It is impossible to ponder about something that appears on one side. As a result, we should be on the lookout for health-related gadgets that meet all of the convenience and security requirements of electronic money-related administrations. The term authentication refers to an electronic technique that permits a natural or legal person to be electronically identified. Authentication can also be used to verify the origin and integrity of data in electronic form, such as the issue of a digital certificate to verify a website's validity. The overall goal of authentication is to limit the risk of fraud, particularly when someone intentionally misrepresents their identity or uses another person'scredentials without permission.

The phrases digital authentication and electronic authentication (e- authentication) are interchangeable terminology for the act of establishing trust in user identities and presenting them to an information system electronically.

The use of electronic banking services is gradually becoming more prevalent in everyday life, and existing internet banking required the use of a security card from each bank, which does not correspond to today's mobile environment because we have no idea when and where internet banking will be used. In the case of a financial emergency, internet banking is impossible without a security card. To overcome the security card's unease, a internet based financial authentication structure based on 2D barcodes or OTP.

## REFERENCES

[1] http://ajast.net/data/uploads/4ajast-9.pdf
[2] http://academicscience.co.in/admin/re sources/project/paper/f201405051399 309076.pdf
[3] https://searchsecurity.techtarget.co m/definition/one-time-password- OTP
[4] https://en.wikipedia.org/wiki/One-time_password
[5] https://en.wikipedia.org/wiki/Barcode
[6] https://www.the-qrcode-generator.com
[7] https://ieeexplore.ieee.org/document/5711134