"3-TIER SECURITY AUHENTICATION SYSTEM"

Dept. of Computer, Sir Visvesvaraya Institute of Technology
A/P: Chincholi, Tal: Sinner, Dist.: Nashik, Maharashtra, India-422102.

Prof. Rajendra P. Sabale
rpsabale1971@gmail.com
Department of Computer Engineering

Mr. Rohit S. Kute
rohitkute214@gmail.com
Department of Computer Engineering

Miss. Rutuja J. Adhav
rutujaadhav276@gmail.com
Department of Computer Engineering

Miss. Chetana M. Pakhale
chetanapakhale@gmail.com
Department of Computer Engineering

Miss. Mrunal L. Chaudhari
mrunalchaudhari2002@gmail.com
Department of Computer Engineering

Abstract

Online information systems currently heavily rely on the username and password traditional method for protecting information and controlling access. With the advancement in digital technology and popularity of fields like AI and Machine Learning, face recognition security is becoming increasingly popular because of the usability advantage. This system reports how machine learning based three step authentication such as QR scanner, face recognition and time-based OTP can be integrated into a web-based system as a method of authentication to reap the benefits of improved usability. The resulting classifier is integrated into the web-based system and used for authenticating users.

Key Words: *python, face recognition, secure system.*

INTRODUCTION :

User authentication is the main building block for any secure cooperative computing system. Security concerns are on the rise in all areas of industry such as banks, healthcare institutions, industry, etc. Due to the proliferation of mobile devices and the heightened interaction between mobile applications and web services, the authentication of users is more frequent for mobile devices than for desktop users [1]. In many instances of multi-factor authentication, both a mobile device and a desktop are necessary and go hand in hand for adequate authentication. One of the drawbacks of multifactor authentication is that user ID's and passwords are abundant, with many users stating that they have more user IDs and passwords than they can remember.

PURPOSE SYSTEM

This cost of convenience makes the proposed implementation of higher security measures and added authentication factors worrisome to many users and providers. To better understand the factors in play with authentication, it is first necessary to understand what authentication is. Authentication and the

various measures of authentication are used to verify that a specific user or process is who they say they are. It is that simple. There are four standard ways that users are authenticated. This is the most basic form of authentication with which most users are familiar. This standard is usually presented as a username or password which is known only to the user. This form of authentication is represented by the user having possession of a physical entity or device. This can be represented as a physical token such as the user's smartphone or other media device generating a temporary and sometimes single use authentication code. This form of authentication is represented such as a QR Scanner, facial recognition and one time OTP.

EXISTING SYSTEM

Authentication technology is always changing. Businesses have to move beyond passwords and think of authentication as a means of enhancing user experience. Authentication methods like biometrics eliminate the need to remember long and complex

passwords. As a result of enhanced authentication methods and technologies, attackers will not be able to exploit passwords, and a data breach will be prevented.

DRAWBACKS OF EXISTING SYSTEM

• **Less User Friendly:** The current framework isn't easy to use in light of the fact that the recovery of everyday exercises information/records is exceptionally lethargic and records are not kept up with productively and successfully.
• **Complex for producing the report:** We require more estimations and endeavors to create the report so it is produced toward the finish of the meeting. What's more the understudy doesn't get an opportunity to work on their participation.
• **Extended time:** Every work is done physically so we can't produce report in the meeting or according to the necessity since it is extremely tedious

LITERATURE SURVEY:

As a fast web framework is being created and individuals are informationized, even the budgetary undertakings are occupied with web field. In PC organizing, hacking is any specialized exertion to control the ordinary conduct of system associations and associated frameworks. The current web banking framework was presented to the threat of hacking and its result which couldn't be overlooked. As of late, the individual data has been spilled by a high-degree technique, for example, Phishing or Pharming past grabbing a client's ID and Password. Along these lines, a protected client affirmation framework gets considerably more fundamental and significant. Right now, propose another Online Banking Authentication framework. This confirmation framework utilized Mobile OTP with the mix of QR-code which is a variation of the 2D standardized identification.

Inside the proposed plan, the client can without such an inconceivable system a stretch and essentially login into the methodology. We look at the interest and solace of the proposed plan and uncover the check of the proposed plan to the hacking of login limits, shoulder surveying and accidental login. The shoulder riding attack may moreover be performed by the adversary to add up to the buyer's unprecedented explanation by truly zeroing in on the client's shoulder as he enters his mystery key. Since we have made a safeguarded system plans with a ton of levels of safety from shoulder watching out for were proposed. Quick Response (QR) codes can set this. QR Code is the brand name for the two-layered standardized conspicuous truly explore structure. The incredibly isolating square is on everything from upgrades to stock. In E-Authentication utilizing QR Code" we are giving secure login by the QR code and email confirmations. It very well may be executes the best security for clients login. As a fast web structure is being made and people are informationized, even the cash related tries are busy with web field. In PC sorting out, hacking is a particular work to control the normal lead of framework affiliations and related structures. The predictable web banking structure had a lot of contribution in the bet of hacking and its outcome which couldn't be pardoned. Of late, the single information has been spilled by a serious level framework, for instance, Phishing or Pharming past getting a client's ID and Password. Therefore, a remained mindful of client support structure gets totally more key and major. At this moment, propose another Online Banking Authentication structure. This deals structure used Mobile OTP with the blend of QR-code which is a method of the 2D normalized clear check.

The use of QR code-based technologies and applications has become prevalent in recent years where QR codes are accepted to be a practical and intriguing data representation / processing mechanism amongst worldwide users. The aim of this study is to design and implement an alternative two-factor identity authentication system by using QR codes and to make the relevant mechanism and process that could be more user-friendly and practical than one-time password mechanisms used with similar purposes today. The proposed model in this project has been designed in order to enable the verification and validation steps with several security and networking options during the logon process. The model has been implemented by developing a two-factor identity verification system where the second factor is the user's smart / mobile phone device and a pseudo-randomly generated alphanumerical QR code which is used as the one-time password token sent to the user via e-mail or MMS. The proposed model has been developed using C, asp.net and jQuery languages with symmetrical and asymmetrical cryptography standards for database encryption / hashing and network infrastructure and it has been tested as a prototype

User authentication and the verification of online transactions that are performed on an untrusted computer or device is an important and challenging problem. This paper presents an approach to authentication and transaction verification using a trusted mobile de-vice, equipped with a camera, in conjunction with QR codes. The mobile device does not require an active connection (e.g., Internet or cellular network), as the required information is obtained by the mobile device through its camera, i.e. solely via the visual channel. The proposed approach consists of an initial user authentication phase, which is followed by a transaction verification phase. The transaction verification phase provides a mechanism whereby important transactions have to be verified by both the user and the server. We describe the adversarial model to capture the possible attacks to the system. In addition, this paper analyzes the security of the propose scheme, and discusses the practical issues and mechanisms by which the scheme is able to circumvent a variety of security threats including password stealing, man-in-the-middle and man-in-the-browser attacks. We note that our technique is applicable to many practical applications ranging from standard user authentication implementations to protecting online banking transaction

PROPOSED SYSTEM

- Fully secure system.
- The system also can be implemented at a low costr.
- This system uses AES algorithm to encrypt the (IMEI number combined with Random digit) string hidden behind the QR code.
- To obtain good pattern recognition results, and therefore a successful private message extraction.

.

SYSTEM ARCHITECTURE

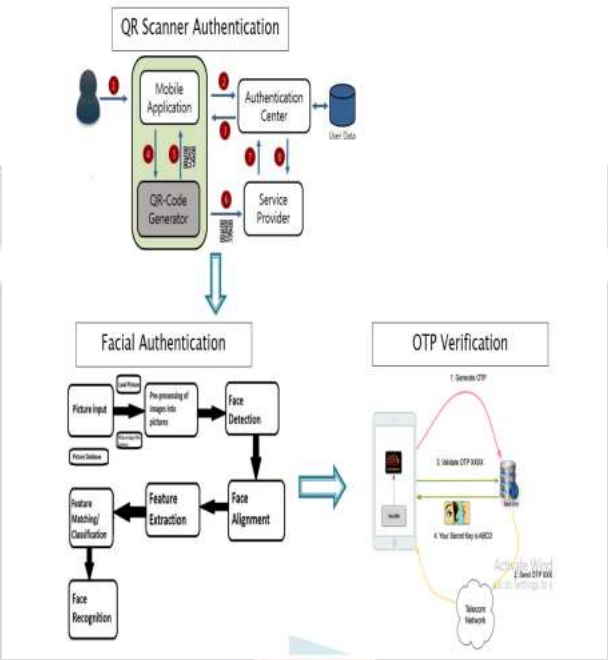


Fig -1: System Architecture Diagram

Mathematical Model:

System Description:
S = (I,O,F)
Where,
S: System.
I = { UF, TOTP, S} are set of Inputs
Where,
S : Scan QR code
TOTP: Time based OTP
UF: User Face
F = {A, FM, DP} are set of Function
Where,
A : Authentication
DP: Data Processing.
DP: Data Processing
O = {S} are set of Output
Where,
S: Security
Success Conditions:

Proper database, Face Picture
Failure Conditions:
No database, Internet connection

ADVANTAGES:

1. Innovative.
2. Centralised Database.
3. Easy to use.
4. Efficient cost.

SDLC MODELS:

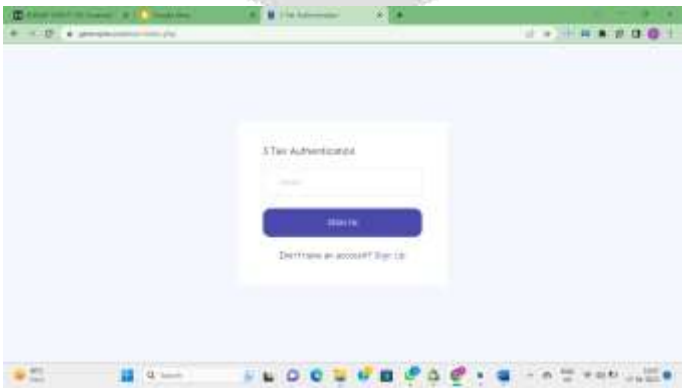
Arranging: This is the first stage in quite a while advancement process. It recognizes whether or not there is the requirement for another framework to accomplish a business' essential goals. This is a primer arrangement (or a practicality study) for an organization's business drive to secure the assets to expand on a foundation to adjust or work on an assistance. The organization may be attempting to meet or surpass assumptions for their representatives, clients and partners as well. The reason for this progression is to discover the extent of the issue and decide arrangements. Assets, costs, time, benefits and different things ought to be considered at this stage.

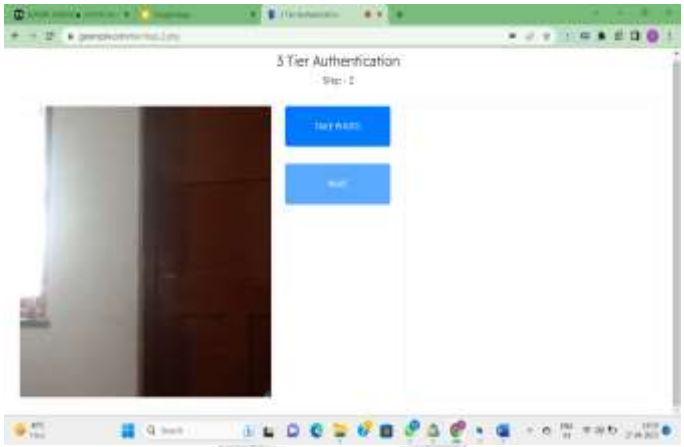
Frameworks Analysis and Requirements: - The subsequent stage is the place where organizations will chip away at the wellspring of their concern or the requirement for a change. In case of an issue, potential arrangements are submitted and investigated to distinguish the best fit for a definitive goal(s) of the undertaking. This is the place where groups think about the practical prerequisites of the venture or arrangement. It is likewise where framework investigation happens—or dissecting the necessities of the end clients to guarantee the new framework can live up to their desires. Frameworks examination is indispensable in figuring out what a business's needs are, also as how they can be met, who will be answerable for individual bits of the task, and what kind of timetable ought not out of the ordinary.

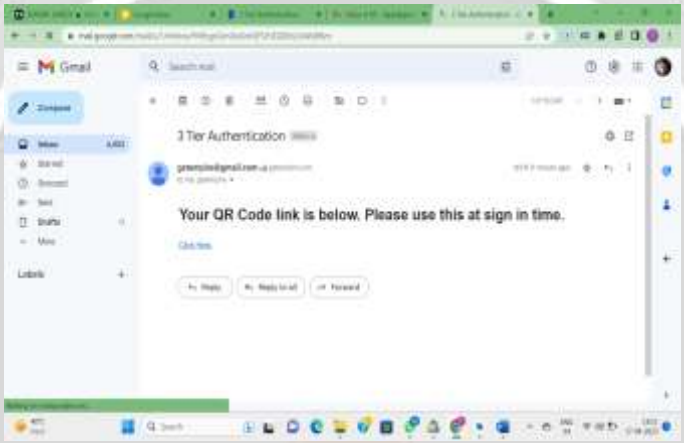
Advancement: The fourth stage is the point at which the genuine work starts—specifically, when a software engineer, network engineer or potentially data set designer are welcomed on to accomplish the significant work on the venture. This work incorporates utilizing a stream outline to guarantee that the course of the framework is appropriately coordinated. The improvement stage denotes the finish of the underlying segment of the cycle. Moreover, this stage connotes the beginning of creation. The improvement stage is additionally portrayed by instillation and change. Zeroing in on preparing can be an immense advantage during this stage.

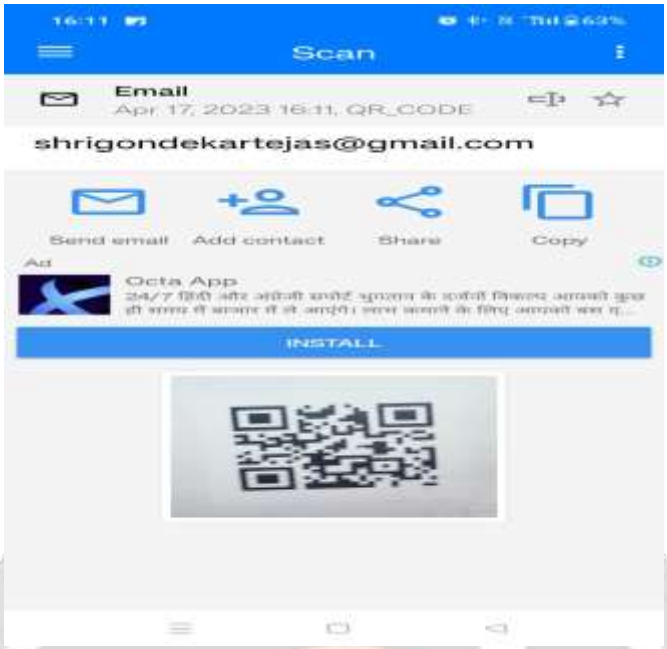
Combination and testing:- The fifth stage includes frameworks mix and framework testing (of projects and strategies)—typically did by a Quality Assurance (QA) proficient—to decide whether the proposed configuration meets the underlying arrangement of business objectives. Testing might be rehashed, explicitly to check for mistakes, bugs and interoperability. This testing will be performed until the end client thinks that it is OK. One more piece of this stage is confirmation and approval, the two of which will assist with guaranteeing the program's effective fruition.

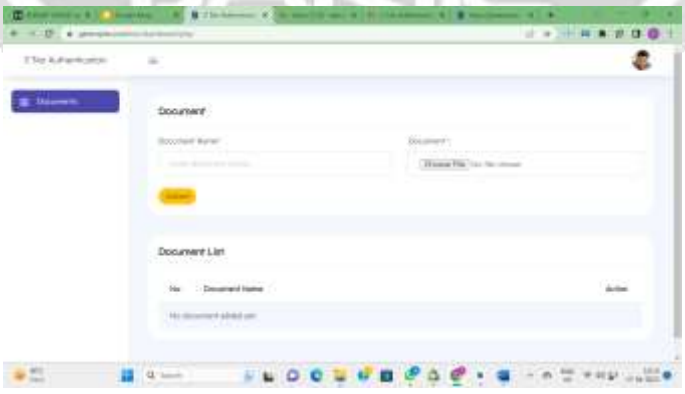
RESULTS




3 Tier Authentication


Gmail
3 Tier Authentication
Your QR Code link is below. Please use this at sign in time.





CONCLUSION

Thus our proposed private verification process or for authentication scenarios provide better security.

Our system provides goods delivery process in an efficient manner. This system uses AES algorithm to encrypt the (IMEI number combined with Random digit) string hidden behind the QR code. The algorithm is light weight and used by industry standards for

application software to protect the information of the users which is of utmost concern in the net-banking era. Hence, to improve the security of authentication process by adding an additional layer such as facial recognition and time limit OTP authentication.

REFERENCES

[1] Web opedia, "Authentication," 2016. [Online]. Available: http://www.webopedia.com/TERM/A/authentication.html. [Accessed 1 Oct 2016].

[2] H. Abie, "semantic scholar," 12 12 2006. [Online]. Available: https://pdfs.semanticscholar.org/3733/2607f7a7ac8284c514845957fd00583e5614.pdf. [Accessed 1 October 2016]

[3] Wikipedia, "Social engineering (security)," [Online]. Available: https://en.wikipedia.org/wiki/Social engineering (security). [Accessed 1 October 2016].

[4] M. Farik, "Algorithm to Ensure and enforce Brutce force attack resilient password in routers," Algorithm to Ensure and enforce Brutce force attack resilient password in routers, vol. 4, no. 10, p. 5, 2015.

[5] wikipedia, "Multi-factor authentication," 2005. [Online]. Available: https://en.wikipedia.org/wiki/Multi-factor authentication. [Accessed 1 October 2016].

[6] B. Schneier, "Schneier on Security," 2010. [Online]. Available: https://www.schneier.com/blog/archives/2010/02/man-in-the-midd 1.html. [Accessed 1 October 2016]

[7] M. McDowell, "US-CERT," 22 October 2009. [Online]. Available: https://www.us-cert.gov/ncas/tips/ST04-014. [Accessed 3 October 2016].

[8] bioelectronix, "Biometric Security," [Online]. Available: http://www.bioelectronix.com/whatisbiometrics.html.[Accessed1October2016].

[9] "3-TIER SECURITY AUTHENTICATION", International Journal of Science & Engineering Development Research (www.ijsdr.org), ISSN:2455-2631, Vol.7, Issue 11, page no.1077 - 1080, November-2022, http://www.ijsdr.org/papers/IJSDR2211161.pdf