Online Bank using Three-factor Authentication

Ankesh Singh,[a] Nevin Mathews Kuruvilla,[b] Peter, Allen Thomas,[c] Zihan Azad[d]

[a] *Student 19BCE2502, Dubai, United Arab Emirates* [b] *Student 19BCE2507, Salmiya, Kuwait* [c] *Student 19BCE2463, Salmiya, Kuwait* [d] *Student 19BCE2442, Jeddah, Saudi Arabia*

Abstract:

In this paper we propose an online banking system, which is user-friendly and secure. The main aspect of the paper for us is to provide basic functionality of a bank in a secure manner, we propose using a Three-factor authentication system. Many online systems use two-factor authentication systems and there have been many cases and studies done where the two-factor systems were able to be bypassed, so we intended to add another level of security, so as to further secure our banking system and provide users with peace of mind when performing online transactions and while dealing with their personal accounts and information.

Keywords*:* Online banking; Three-factor authentication; multi factor authentication; OTP; Bcrypt; Knowledge based image recognition; TOTP.

1. Introduction:

In the current state of the world, physically going to a bank outlet has become increasingly difficult as well as dangerous, this has given rise to a large increase in online banking systems around the world.

An Online banking system is a simple User Interface aiming to provide essential banking features, we aim to design a system that is simple and comprehensible to any customer.

A user will be able to login as either an admin or customer, both having different privileges and permission within the system.

The main goal for us is to be able to perform crucial tasks such as money transfers and taking deposits, through online transactions, all of which will be done using a secure system.

We are implementing a three-factor authentication system for all users.
A customer is validated using
(1) Customer's password
(2) A One-time password which is sent to the Users Email and
(3) By selecting three images that was decided upon by the customer at the time of registration

2. Literature review:

Citation	**Objective**	**Advantage**	**Disadvantage**
Multi-Factor Authentication to Systems Login Bandar Omar AlSaleem, Abdullah I. Alshoshan Year -2021	This paper proposes a multi-factor authentication system that combines ease of use and lowcost factors. The system does not need any special settings or infrastructure. It relies on graphical passwords, so the user, in registration phase, chooses three images that he/she considered during the registration process in a specific order. When the user registers for the first time, he fills the fields of the registration form and selects 3 pictures. After that, the system hashing the password field, get the selected photos IDs, merging them and hashing them with SHA256 and stores this data into the user's table. The next stage is to login with the username and password, as usual, and then a screen appears to the user with 9 randomly selected images including 3 correct ones	Low cost and easy to implement Uses recognitionbased system Anti-key-logger: key-loggers cannot detect what is being typed in keyboard	More than 60% of the users liked the image authentication method used in the survey, however, 26% of them mentioned that it might be difficult for a user to memorize images Registration takes longer than normal login Users not familiar with this method

2)Robust login authentication using time-based OTP through secure tunnel Navpreet Kaur, Mandeep Devgan, Shash Bhushan Year - 2016	The aim of this paper is to design a secure authentication system that uses existing cryptographic algorithms, the proposed authentication system uses the Android mobile phones to provide a stronger authentication using seed exchange, and occurs through the verification of onetime passwords on the server side and the one-time password generated seed value of the android phone	The OTP is generated on the device itself, thus doesn't rely on the network and can avoid time-based constraint that could occur if the user's network is slow Seed value is transferred through secure tunnel and is AES Encrypted Prevents the use of same account credentials on multiple devices, as the users IMEI Number is stored on the server side along with the unique id, username and password	Initial implementation of this proposed system is very complex Since each account is associated with the IMEI number, if the mobile device is lost or stolen, the users account can be easily accessed
3)A Multi-Factor Security Protocol for Wireless Payment - Secure Web Authentication using Mobile Devices Ayu Tiwari, Sudip Sanyal, Ajith Abraham, Svein Johan Knapskog, Sugata Sanyal Year - 2011	This paper proposes a multifactor authentication technique based on multifactor authentication technique based on Transaction Identification Code (TICs) and SMS Confirmation The TIC code verifies the transaction has been initiated by the right person and that the user is trying to access their account. The TIC codes are issued by the Customers Bank and maybe a complicated digital sequence or a combination of numeric and alphanumeric characters The financial institution stores the users cell phone number, the valid user receives an SMS from the authentication server which should be validated by the user and once the authentication server receives a 'Yes' the user is approved for the transition	The authentication system can be applied with limited resources of a Java MIDP device without modification to underlying protocols The data is always encrypted while using untrusted networks to prevent from man in the middle attacks. The TICs are also encrypted before being stored on the users device Both parties are authenticated in this system	The method of receiving the Transaction identification code for the server is not efficient The installation of the TIC code on the user's device is not user friendly

4)Multi-factor Authentication Framework for Cloud Computing R.K. Banyal, P. Jain, V.K Jain. Year - 2013	This paper proposes to create a Cloud Access Management system which will authenticate the user using multiple factors, it also uses secret splitting and encrypted value for arithmetic captcha in the cloud computing environment. All the cloud computing services are divided into three levels based on their security requirements. The first level uses secret key factor and arithmetic captcha expression, the second level is the same as the first and add extra factor a one-time password, the highest level uses three factors, first is arithmetic captcha, second is an OTP and third is the IMEI number of the users mobile phone	The system takes advantage of the fact that smartphones have become ubiquitous. It allows for secure change of credentials of any users like change of password, mobile phone and IMEI Number Uses a high entropy OTP and the secret key to the arithmetic captcha is never transmitted through public channels Even if an attacker were able to login into a user's system, they would be unable to use the cloud services, as they would require a secret key, OTP and IMEI Number.	If there is an issue with the Cloud Access Management server it will affect the access control of all users Maintenance and cost of a the server would be expensive and would require constant overview of the cloud administrator

5) Enhanced Ecommerce application security using three-factor authentication Binitha Ann Scaria, Dr. Rajesh Kannan Megalingam Year - 2018	This paper talks about how the use of e-commerce websites like online banking is increasing day by day and due to technological advancement, it is easier for hackers to gain access to user's accounts. It talks about different attacks and how it is carried out. To tackle this issue a 3-factor authentication system is introduced which are username password, OTP and biometric such as fingerprints	This paper proposes a strong methodology which has little to no risk. The use of OTP which is generated by a cryptography concept of elliptic curve and fingerprint biometric is a strong security feature which banking portals must implement	The use of biometrics for login can only be done when a user has a device which is capable of scanning fingerprints. Due to this the cost of the product increases and not many users can take advantage of hte 3-level security

6)Two Factor Authentications for Secured Login in support of effective Information Preservation and Network Security S. Vaithya subramanian, A. Christy D. Saravanan Year - 2015	This paper focuses on the implementation of a two-factor authentication method which is done by user-friendly traditional Alphanumeric Password and Graphical Password as a gateway for authentication The first gateway is an Alphanumeric password which was defined by the user during registration and gets verified by the admin, then the user provides a second password to get into the second gateway which is an image/pass faces. Both passwords are maintained by the service provider	Both passwords are given by the user during registration The passwords are maintained by the service provider and not a password management system Easy to implement	User has to remember both passwords and will not be able to get access without them The system is configured to assist the second gateway and takes additional time High space complexity
7)Robust Multi-Factor Authentication for Fragile Communications Xinyi Huang,	This paper has two proposals, the first is a generic multifactor authentication protocol to speed up authentication on large scale systems which tend to be slow, it provides a three-factor authentication protocol using	The added computation and storage of the Stand-alone authentication is independent of the number of users	If a user is revoked and there is a communication failure, device will not receive latest revocation list and user will have

Yang Xiang, E.Bertino, Jianying Zhou, Li Xu Year - 2014	smart-card based passwords and fuzzy factor with improved efficiency the second objective is to provide a stand-alone authentication system which can authenticate users when the connection to the central server is down, it uses existing multi-factor authentication protocols without introducing any additional computational burden on the users' side	It is applicable on in a dynamic environment	successful standalone authentication The stand-alone authentication is vulnerable to online dictionary attacks
8)Internet Banking Login with MultiFactor Authentication Sirapat Boonkrong Year - 2017	This paper puts an emphasis on a security mechanism that provides the first protection to internet banking It aims to design and implement an authentication mechanism that can reduce the risk of an attack on the login process on internet banking, with the focus on the service provided via the web	The method only requires three messages between the bank's server and the client to complete the authentication process. In each of the three messages various authentication factors are applied The factors of auth entication to be generated and used include a username, a password, number of iterations, a public key, a private key, a symmetric key, a digital signature and an IP address. All of these are unique to each user.	The threat of password r euse has not been addressed nor mitig ated. If the user's password is guessed or known by an adversary, the system will become more vulnerable. This is because the password is one component that is used to generate the user's symmetric key, whi ch in turn can unlo ck his or her privat e key.

9)Multi-Factor Authentication: A Survey Aleksandr Ometov, Sergey Bezzateev, Niko Makitalo, Sergey Andreev, Tommi Mikkonen, Yevgeni Koucheryavy Year - 2018	The main ideas of this paper are: • To provide a detailed analysis of factors that are presently utilized for MFA with their corresponding operational requirements. • To showcase the challenges related to MFA adoption from both the user experience and the technological perspectives • It proposes the framework based on the reversed Lagrange polynomial to allow for utilizing MFA in cases where some of the factors are missing	MFA becomes a system that promises the security and ease of use needed for modern users while acquiring access to sensitive data. Utilizing neural networks for the next-generation biometrics is the most likely way to proceed due to presently high levels of the analysis complexity Biometric technology is a prominent direction driven by the mobile device market..	User acceptance is a critical aspect for the adoption of strong identity and multifactor authentication. An extremely important problem of MFA usability roots in the fact that “not all users can use any given biometric system”, for eg: . People who have lost their limb due to an accident may not be able to

10)A Method of Risk Assessment for Multi-Factor Authentication Jae-Jung Kim, Seng-Phil Hong Year - 2011	This paper analyzes user authentication methods being used in various online environments to identify the characteristics and issues of such authentication methods in order to present a user authentication level system model suitable for different online services	Improved the UALS (user authentication level system) model into a 5 level user authentication system Highly secure user authentication schemes using PKI and biometric This scheme can be used for high-risk financial transactions Providers of online products and services can provide the customer with safe and reliable authentication measures by carrying out regular risk assessments	As many diverse user authentication methods are provided by different services, a s tandard definition of levels in user authenticatio n has come to be req uire.

11)Multi factor authentication using mobile phones Fadi Aloul, Syed Zahidi, Wasim El-Hajj Year - 2009	This paper describes a method of implementing two factor authentication using mobile phones. The proposed method guarantees that authenticating to services, such as online banking or ATM machines, is done in a very secure manner.	The proposed system is secure and consists of three parts: software installed on the client's mobile phone, server software, and a GSM modem connected to the server. Both methods have been successfully implemented and tested, and shown to be robust and secure	The GUI is not user friendly Proposed system does not work on android phones without an os

12)Secure Online Transaction Algorithm: Securing Online Transaction Using Two-Factor Authentication Joseph Gualdoni, Andrew Kurtz, Ilva Myzyri, Megan Wheeler, Syed Rizvi Year - 2017	This paper presents a new algorithm of mitigating risk, the Secure Online Transaction Algorithm (SOTA) The proposed SOTA seeks to use 2FA with random codes The proposed SOTA uses mobile devices to log into card accounts via an application to view the randomly generated code. This is then inputted on an online retailer's website when prompted in order to authenticate the individual making the purchase.	This minimizes the possibility that an illegitimate user can use someone else's information to make fraudulent purchases This protects both the consumer and the credit card companies, which could be harmed financially	Credit card companies, users, and providers would need to be utilizing the scheme to so that the scheme to work properly. The model itself would cost credit card companies some money in order to implement it.

13)Universal Multi-Factor Authentication Using Graphical Passwords Alireza Pirayesh Sabzevar, Angelos Stavrou Year - 2008	This paper proposes a variety of methods to authenticate a user with a graphical password It employs the users handheld device as the password decoder and the second factor of authentication In our methods, a service provider challenges the user with an image password. To determine the appropriate click points and their order, the user needs some hint information transmitted only to her handheld device.	This method can overcome threats such as keyloggers, weak password, and shoulder, surfing. The approach can be leveraged by many organizations without forcing the user to memorize different password s or carrying around different tokens. Renders attacks inc luding dictionary attacks and keybo ard sniffers compu tationally hard increasing our abil ity to defend agai nst brute-force attacks	If the click points are explicitly marked, then anybody who has access to the handheld can authenticate as th e real owner of the handheld

14)Trusted framework for online banking in public cloud using multifactor authentication and privacy protection gateway Sabout Nagaraju, Latha Parthiban Year-2015	This paper proposes a systematic Multi-factor biometric, fingerprint Authentication approach to provide a highly-secure identity verification process for validating the legitimacy of remote users. It also investigates the framework to develop a privacy protection gateway for obscuring and desensitizing the customers' account details using tokenization and data anonymization techniques.	The original format of data fields is retained at various levels of the database management systems and makes the data worthless to others except the owner In this approach the authentication credentials of the users are not revealed to the bank and cloud authentication servers	Banking governance, compliance and audit management are very complex

15)Enhanced Authentication In Online Banking Gregory D. Williamson Year-2006	This study simplifies and provides a resource for understanding the many options available when implementing enhanced authentication in the online banking environment. It provides a detailed analysis on the number of authentication solutions that are available, it also lays out guidelines on how to select and implement an authentication system	It conducts an online survey, analyzing the demographics of users and their typical usage patterns and also asks what were the login procedures of banking accounts.	The paper does not provide an authentication solution Survey that was conducted only included one hundred and nineteen users ignoring a large user base
16) A Feasible and Cost Effective Two-Factor Authentication for Online Transactions Jing-Chiou Liou, Sujith Bhashyam Year-2010	This paper proposes a technique for two-factor authentication, called SofToken, If a user requests an account for online transaction from a service provider, the server delivers a client software to the user's computer which installs two components onto user's computer. A logon application that is responsible to set up a direct communication between the server and user's computer without going through a webbased logon screen and a pseudorandom number generator which stores the server generated encrypted key on to the users computer	The provides strong online security while having a simple deployment process This method is cost effective and feasible for many online services	The security provided is not as much as those provided my one time password based multi- factor systems

17)A Survey on Multi-Factor Authentication for Online Banking in the Wild Federico Sinigaglia, Roberto Carbone, Gabriele Costa, Nicola Zannone Year - 2020	This paper presents a latitudinal study on the adoption of MFA and the design choices made by banks operating in different countries In particular it evaluates the MFA solutions currently adopted in the banking sector in terms of (1)compliance with laws and best practices, (2)robustness against attacks and (3)complexity They also investigate possible correlations between these criteria	Banks usually provide their clients with a variety of MFA protocols All banks employ a min of 2 and a max of 9 authenticators EU banks on average, comply with half of the considered requirements The majority of the banks can easily become compliant with these requirements just by offering a subset of the MFA protocols they currently support	The paper only considered 3 banks per country, which cannot fully support statements on national trends The approach for analyzing the robustness and complexity of MFA protocols is independent from the specific application domain, therefore the approach can be applied to analyze MFA protocols in general
18) A Survey of Authentication and Communications Security in Online Banking Kilijan S, Simoens K, Cock D.D., Eekelen M.C.J.D. van, Vranken H.P.E Year - 2017	The paper provides a new state of the art, based on a longer observation period between 2013 and 2015, and with a larger number of banks from differents part of the world The scope of the paper is authentication and communications security between banks and customers, using information sources from the websites of banks and publicly available documentation	Multiple factors provide protection against long-term credential stealing attacks 75% of the banks offer an authentication method that relies on multiple factors for home banking	If an attacker can observe network traffic and manipulate a victim's browser to submit requests to a target site, it is possible to retrieve data from the TLS stream when DEFLATE compression is used An attacker can steal session cookies with CRIME, which makes it possible to hijack a session

19)Evaluation of transaction authentication methods for online banking Kilijan S, Vranken H, Eekelen M.C.J.D van Year - 2018	This paper proposes feasibility as an additional dimension which quantifies aspects related to the secure usability of transaction authentication methods Four implemented and eight proposed authentication methods for online banking were evaluated by seven experts. The results indicate that the mechanism can be applied on a wide range of authentication methods, since it is able to evaluate methods based on different information schemes	Can be applied on a wide range of authentication methods. Expanded Renaud's quantifying mechanism to accommodate aspects related to transaction authentication in online banking in a user-centric context	Care must be taken that evaluations are performed by multiple experts, due to the amount of subjectivity inherent in the mechanism and in difference of the raters

20)On app-bases Matrix Code Authentication in Online Banking Vincent Haupert, Tilo Muller Year - 2016	This paper emphasizes the risks that single-device mobile banking poses They show a transaction manipulation attack on the appbased authentication schemes of Deutsche Bank, Commerzbank and Norisbank Furthermore, they evaluate whether the matrix code authentication method that these banks and Comdirect implement - wisely known as photoTan - is compliant with the upcoming Revises Payment Service Directive (P2D2) of the European Banking Authority (EBA)	The chipTAN is an established procedure used in online banking. It uses the customer's personal bank card and a dedicated reader device to securely authenticate a transaction The photoTAN method is adopted by a lot of german and swiss banks	App-based authentication schemes provide less security than other methods because they run on a smartphone Running the banking and the photoTAN app on the same device cannot be regarded as secure

21)Databases using multifactor authentication Rajyashree R, Vaishnavi Moorthy, Nedunchelian R Year - 2017	This paper proposes a new multifactor authentication framework for cloud computing. The proposed framework provides a feasible and a most effective mechanism which can closely integrate with the traditional authentication system to ensure data confidentiality by encrypting the files before they are uploaded into the cloud drive. Random function generated unique key that does contains any data corresponding to the actual file data attributes used for decrypt the metadata and acquire information	Storage devices with inbuilt encryption techniques are available which are resilient to unauthorized access Multi-factor authentication with client owned master key provide privacy services to intended customer. Key generated does not include any file attributes without any algorithm for reconstruction of the key and hence it is more secure.	The main issue with data-at-rest in the cloud is loss of control, even a nonauthorized user/party may have access to the data

22)Case study: Online banking security Kjell J Hole, Vebjørn Moen, Thomas Tjøstheim Year - 2006	This paper studied customer authentication methods in several Norwegian Internet banks from 2003 through 2004 Their investigation shows that authentication was often weak, offering simple but powerful attack possibilities They discuss the authentication methods and the attacks they made possible	A well designed system should be invulnerable to brute forcing They list out all the simple attacks possible which can be easily avoided	The attacks discussed use wellknown brute-force and DDoS techniques and require no high-level expertise to perform Application layer DDoS attacks are still a serious problem

23)Multilevel Security and Dual OTP System for Online Transaction Against Attacks Muneeswari, G. Puthussery, Antony Year - 2019	This paper proposes a secured online transaction system for banking using multilevel encryption of blowfish and AES algorithms incorporated with dual OTP technique The performance of the proposed methodology is analyzed with respect to a number of bytes encrypted per unit time and they conclude that the multilevel encryption provides better security system with faster encryption standards than the ones that are currently in use	Multilevel encryption provides better security system with faster encryption standards than the ones that are currently in use. Blowfish algorithm has been incorporated which is found to be a less time consuming process . Dual OTP scheme is also one of the identified high security over one time OTP system.	Even though tough encryption standards are provided against network atta cks, it is prone to be broken. With this method, all the banking customers are supposed to have two mobile numbers
24)Information systems continuance intention of web-based applications customers: The case of online banking Banphot Vatanasombut, Magid Igbaria , Antonis C. Stylianou,	This paper extended Commitment–Trust theory, an expectation–confirmation model, and technology acceptance theory to develop a model of IS continuance intention of customers of web-based applications Relationship commitment and trust were found to be central to IS continuance intention. Also, perceived empowerment influenced relationship commitment, while perceived security influenced trust.	Customers who receive high benefits from a relationship with their online bank are likely to commit themselves to that relationship. Empowered customers are likely to commit themselves to their relationship with an online bank	The drive for differentiation and speed-to-market has led in a large number of comparable alternative sites and users find it easy to switch between them. Customers who are committed to their relationship with their online bank are likely to continue

Waymond Rodgers Year - 2008	Their findings thus supported traditional intention factors, highlighting the role of trust as a stronger predictor of intention than commitment but, contradicting findings from marketing research, trust was found to be a stronger predictor of retention in the e-commerce context	Customers who perceive that their online bank's services are secure are likely to trust that bank.	using the services offered by that bank. The high costs of collecting real data on customer activity in maintaining or terminating their banking relationships and the unpredictable temporal pattern of customers leaving the bank prevented the use of real IS continuance intention data.
25)On the Security of Today's On-line Electronic Banking Systems Joris Claessens, Valentin Dem, Danny De Cock, Bart Preneel, Joos Vandewalle	This paper discusses the security of today's electronic banking systems. They focus on Internet and mobile banking and present an overview and evaluation of the techniques that are used in the current systems The best practice is indicated, together with improvements for the future. The issues discussed in this paper are generally applicable in other electronic services such as e-commerce and e-government.	On-line electronic banking systems give everybody the opportunity for easy access to their banking activities. Almost all today's electronic banking systems rely on the SSL/TLS/WTLS protocols. The use of other hardware tokens, such as a Digipass that generates responses to unpredictable challenges of the bank and that is able to calculate MACs, or such as a smart card that is already used in other (related) applications	Main security issue consists of the establishment of a secure channel to provide data confidentiality and data integrity of communications between a client and an authenticated bank. The fact that a client platform is not secure is often just due to the lack of Security knowledge of the end-use

3. Proposed work:

Our Online banking interface has three layers of authentication: signup using password, Time based OTP via Email and image recognition. We use protected routes to ensure that users cannot access bank features via url once they have signed out.
If a user tries to access the '/transaction' feature via url if they're not signed in, the application will redirect them to the sign in page.

a. First Layer of Authentication

The first layer of authentication is a sign up page that contains two fields: username and password. If the incoming user is a new user, they can register themselves and their details will be stored in the database. The passwords of the users are hashed using bcrypt which uses blowfish cypher and hashes the users passwords with a random salt value generated by the backend.

b. Second Layer of Authentication

The second layer of authentication is a One Time Password. The otp is generated by the backend. Each time a user enters the system, a new token is generated which is hashed using SHA-256 algorithm and stored in the database. If a new user uses the application a new token is inserted into the database. If an existing user uses the application, the token gets updated. Using the user's token we generate a TOTP (Time based One Time Password) which has a lifetime of 30 seconds and a window of 1. This window of 1 specifies that the previous OTP sent by the backend is still valid if the user runs out of time. This OTP is sent to the user via mail. The user then retrieves the OTP and pastes it in the field. This OTP is validated against the backend and if it is the right OTP, then the user gets redirected to the third layer of authentication.

c. Third Layer of authentication

The third layer of authentication is knowledge-based image recognition The user will be prompted to choose 3 different images from 3 different categories, the first category will be a color and the user can choose their favorite color, the hex code of the color will be hashed and stored in the database, the user can choose any shade or tint of the color.
For instance, if they choose a shade of yellow, any shade or tint of yellow is valid. The second category will be an object like cars or items.
The third category will be a celebrity. The user is expected to remember all these three values for their banking authentication, an email will be sent to the user after they've selected these images during the registration phase, which will contain the images they've selected and this will be sent only once during the
registration phase

3.4. Functional Requirements:

3.4.1. Login/Register new user

The users should be able to sign in as an existing user or register as a new user. The details of the user must be stored securely in the database and sensitive details such as passwords must be hashed and non-retrievable by any other third-party members.

3.4.2. Account Details

The dashboard of the user must display the account details of the user such as balance amount, account number and so on. The system must allow the user to edit his account details or add a new account. If the user wants to add a new account, it must be permitted by the administrator.

3.4.3. Money Transfer

The users must be able to transfer money from one account to another via account numbers. The balance must be updated based on the transfer.

3.4.4. Credit Card/Debit Card

The system must be able to generate a credit card and debit card for each user. The user also must be able to request for a card depending on the type. Payments using

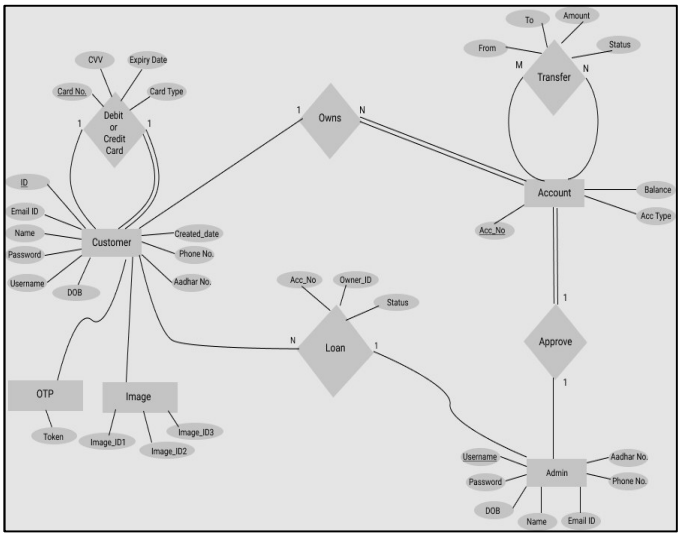
3.4.5. History of Transactions

The user must be able to view the history of transactions conducted by the user in that specific account. The list of transactions along with source, recipient and time should be displayed to the user.

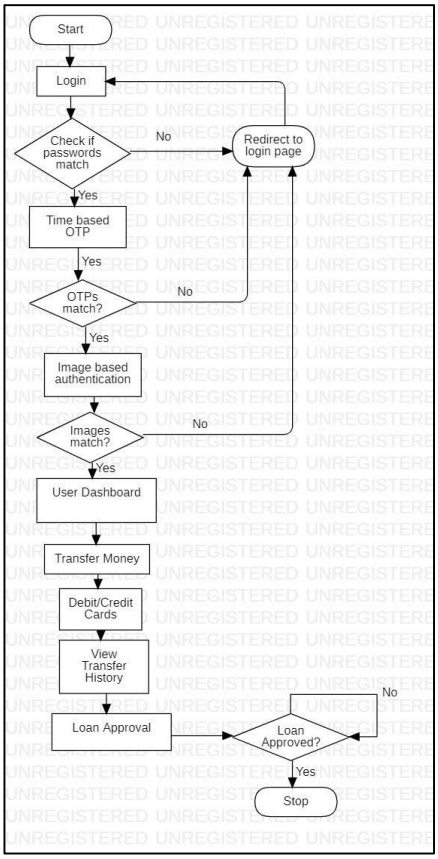
Add Details — Explanation

3.5. Architectures/Diagrams:

3.5.1. Entity Relationship Diagram



3.5.2. Flow Diagram



4. Result Analysis

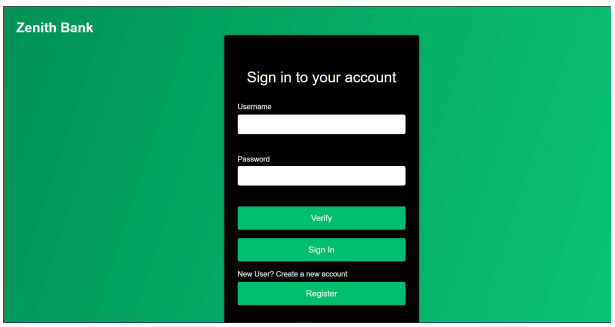


Fig 1: Sign in Form

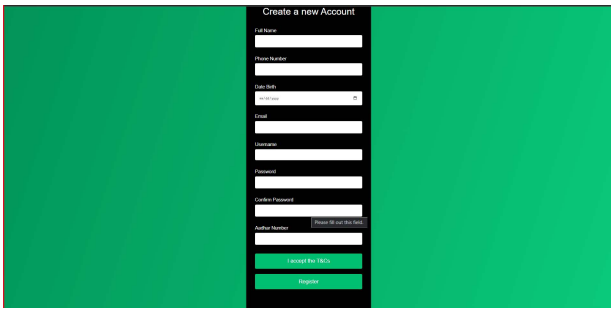


Fig 2: Register Form

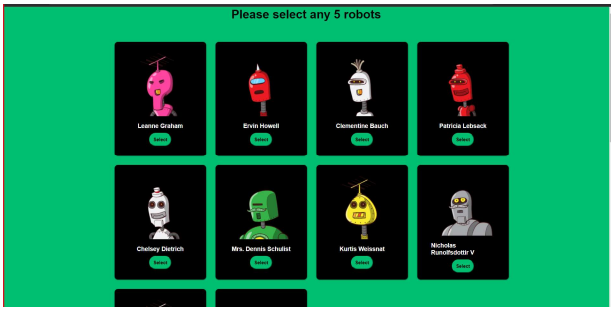


Fig3: Robot Selection after Registration

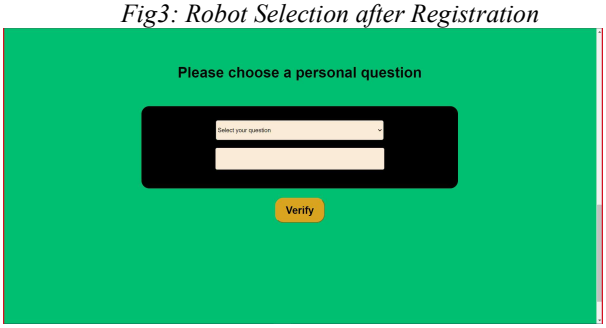


Fig4: Personal Question Selection after Registration

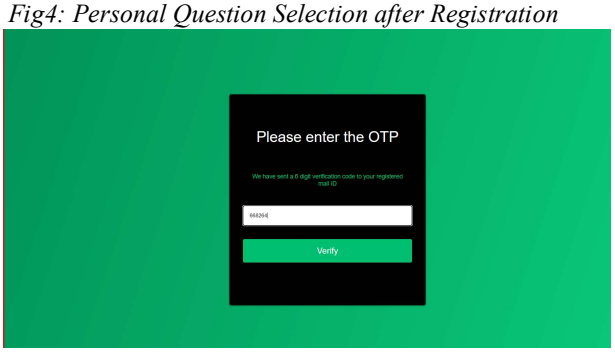


Fig 5: OTP as Second Layer of Authentication

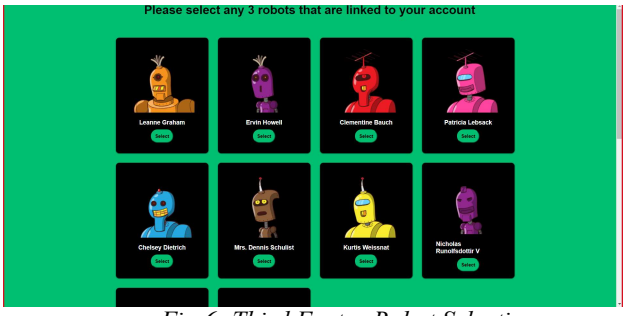


Fig 6: Third Factor Robot Selection after OTP

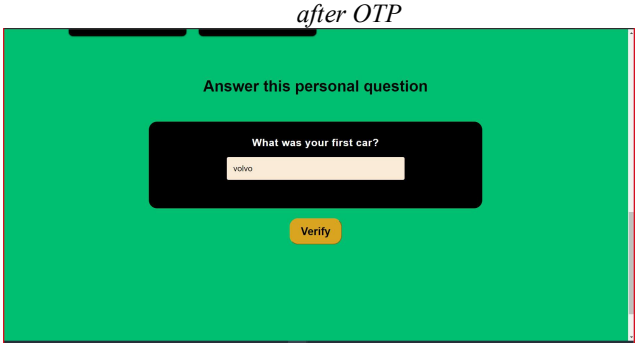


Fig 7: Third Factor Personal Question

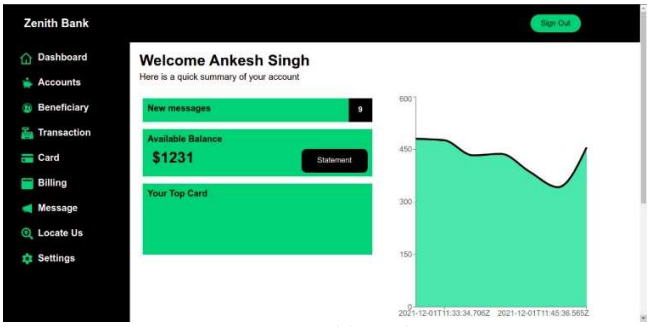


Fig 8: User Dashboard

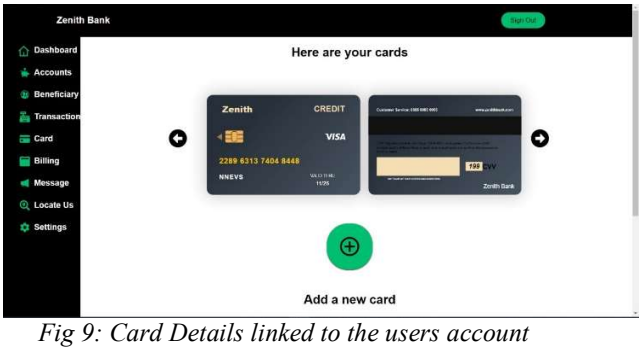


Fig 9: Card Details linked to the users account

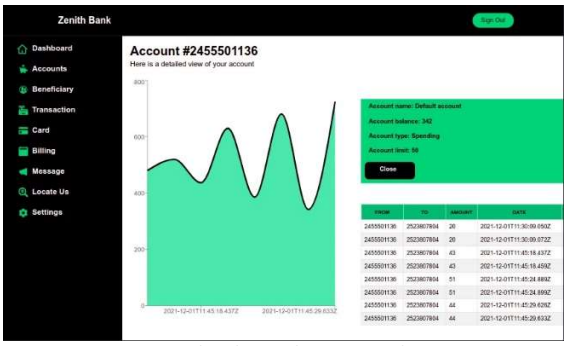


Fig 10: Details about the particular account

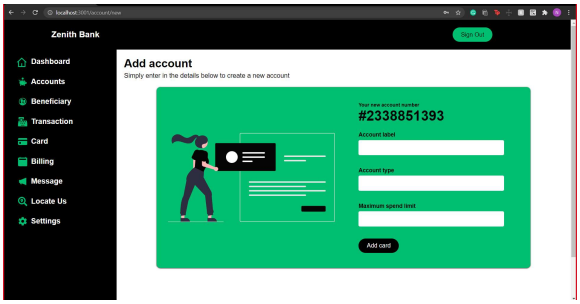


Fig 11: Add a new account

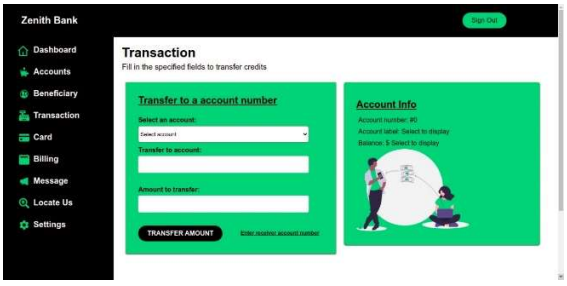


Fig 12: Transaction Page

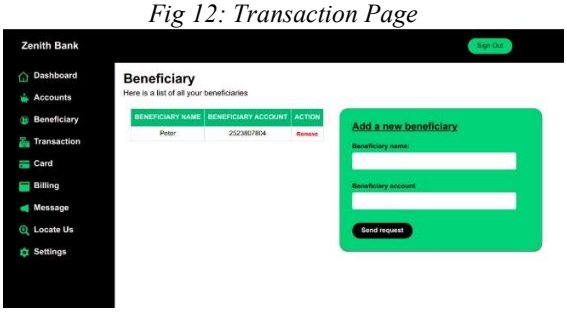


Fig 13: Beneficiary Page

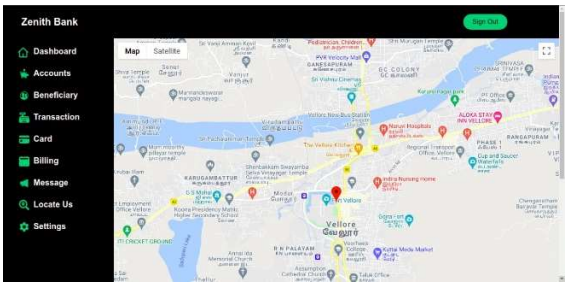


Fig 14: Google Maps

The user can is first directed to the launch page. From there the user can either sign in or register as a new user. If the user chose register, then they will have to enter the details and then they will be redirected to the third factor selection page as show in the results. The user gets a mail regarding his registration details.

If the user selected sign in, they have to enter their username and password. On successful authentication, they will be redirected to the OTP page which is a TOTP (Time Based OTP) with a duration of 30s and a window of 1. The user will receive the OTP in his mail. On successful, authentication, the user gets redirected to the third factor, where they have to choose three of the five robots that they have registered with and answer a personal question that they have selected.

All sensitive information regarding the user such as password, robot Ids have been hashed and stored in the database. The hash used the bcrypt hash with a salt round of ten rounds. The user's secret key for the generation of OTP is created each time the user enters the website and is discarded after they sign out. The third factor robots have been generated with the help of the user's phone number which is unique to each user.

5. Risk Analysis

If a user's email is compromised an attackers will be able to intercept the OTP and negate the first factor of the authentication system

The sample size of the images that can be selected in relatively small so an attacker could run a brute force attack and identify the images that the user had chosen

6. Future work

In Real-time deployment of a three-factor authentication system, it could suffer from security risks due to bad design or underestimating the severity of client-side attacks.

Advances to the system that could be addressed in future works on the topic of multi factor authentication is the use of Out-Of-Band channels. Which will allow a user to be authenticated by being able to communicate with the authentication servers through the OOB Channel.

The use of public packages could lead to the loss of information as security is not guaranteed

If an attacker as adequate information of a user they will be able to brute force the personal question section of the 3rd factor of the system

A survey could be conducted to analyze if users are satisfied with the

3-factor system whether it is able to accommodate for the tradeoff between usability and security. Increasing the image sample size to help prevent against brute force attacks.

Emails are sent to users using public packages, a standalone SMTP server could be used instead where it would have encryption methods to prevent loss of information

7. References

[1] ALSaleem, B. O. and Alshoshan, A. I. (2021) 'Multi-Factor Authentication to Systems Login', *2021 National Computing Colleges Conference (NCCC), National Computing Colleges Conference (NCCC), 2021*, pp. 1–4. doi: 10.1109/NCCC49330.2021.9428806. https://ieeexplore.ieee.org/abstract/document/9428806

[2] Kaur, N., Devgan, M. and Bhushan, S. (2016) 'Robust login authentication using time-based OTP through secure tunnel', 2016 3rd International Conference on Computing for Sustainable Global Development (INDIACom), Computing for Sustainable Global Development (INDIACom), 2016 3rd International Conference on, pp. 3222–3226. Available at: https://search.ebscohost.com/login.aspx?direct=true&db=edseee&AN=edseee.7724860&site=eds-live

[3] Tiwari, A., Sanyal, S., Abraham, A., Knapskog, S.J. and Sanyal, S., 2011. A multi-factor security protocol for wireless payment-secure web authentication using mobile devices. arXiv preprint arXiv:1111.3010. *https://arxiv.org/abs/1111.3010*

[4] Banyal, R. K., Jain, P. and Jain, V. K. (2013) 'Multi-factor

Authentication Framework for Cloud Computing', 2013 Fifth International Conference on Computational Intelligence, Modelling and Simulation, Computational Intelligence, Modelling and Simulation (CIMSim), 2013 Fifth International Conference on, Computational Intelligence, Modelling and Simulation, International Conference on, pp. 105–110. doi: 10.1109/CIMSim.2013.25. https://ieeexplore.ieee.org/abstract/document/6663171

[5] Scaria, B. A. and Karman Megalingam, R. (2018) 'Enhanced E-Commerce Application Security Using Three-Factor Authentication', 2018 Second International Conference on Intelligent Computing and Control Systems (ICICCS), Intelligent Computing and Control Systems (ICICCS), 2018 Second International Conference on, pp. 1588–1591. doi: 10.1109/ICCONS.2018.8662831. https://ieeexplore.ieee.org/abstract/document/8662831

[6] Vaithyasubramanian, S., Christy, A. and Saravanan, D., 2015. Two factor authentications for secured login in support of effective information preservation and network security. India: ARPN Journal of Engineering and Applied Sciences, 10(5). https://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.1039.9625&rep=rep1&type=pdf

[7] Huang, X., Xiang, Y., Bertino, E., Zhou, J. and Xu, L., 2014. Robust multi-factor authentication for fragile communications. IEEE Transactions on Dependable and Secure Computing, 11(6), pp.568-581. https://ieeexplore.ieee.org/abstract/document/6701152

[8] Boonkrong, S., 2017. Internet banking login with multi-factor authentication. KSII Transactions on Internet and Information Systems (TIIS), 11(1), pp.511-535. https://www.koreascience.or.kr/article/JAKO201711656707177.page

[9] Ometov, A., Bezzateev, S., Mäkitalo, N., Andreev, S., Mikkonen, T. and Koucheryavy, Y., 2018. Multi-factor authentication: A survey. Cryptography, 2(1), p.1. https://www.mdpi.com/2410-387X/2/1/1

[10] Kim, J.J. and Hong, S.P., 2011. A method of risk assessment for multi-factor authentication. Journal of Information Processing Systems, 7(1), pp.187-198. https://www.koreascience.or.kr/article/JAKO201113753748218.page

[11] Aloul, F., Zahidi, S. and El-Hajj, W., 2009. Multi factor authentication using mobile phones. International Journal of Mathematics and Computer Science, 4(2), pp.65-80. https://www.researchgate.net/profile/Fadi-Aloul/publication/228972704_Multi_Factor_Authentication_Using_Mobile_Phones/links/02e7e5259692e45bbe000000/Multi-Factor-Authentication-Using-Mobile-Phones.pdf

[12] Gualdoni, J., Kurtz, A., Myzyri, I., Wheeler, M. and Rizvi, S., 2017. Secure online transaction algorithm: securing online transaction using two-factor authentication. Procedia computer science, 114, pp.93-99. https://www.sciencedirect.com/science/article/pii/S1877050917318100

[13] Sabzevar, A.P. and Stavrou, A., 2008, November. Universal multi-factor authentication using graphical passwords. In 2008 IEEE international conference on signal image technology and internet-based systems (pp. 625-632). IEEE. https://ieeexplore.ieee.org/abstract/document/4725863

[14] Nagaraju, S. and Parthiban, L., 2015. Trusted framework for online banking in public cloud using multi-factor authentication and privacy protection gateway. Journal of Cloud Computing, 4(1), pp.1-23. https://journalofcloudcomputing.springeropen.com/articles/10.1186/s13677-015-0046-4

[15] Williamson, G.D. and Money–America's, G.E., 2006. Enhanced authentication in online banking (Doctoral dissertation, Utica College). http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.594.5225&rep=rep1&type=pdf