

# **Information Security**

# Semester Project Report

## **Name:** Manahil Faisal (i200683), Saba Karim (i200813), Muhammad Hamza Iqbal (i200856)

## 

## **Section:** C

## 

## **Submitted to:** Ma’am Urooj Ghani

## 

## **Date:** 4th December, 2023

**Academic Integrity Declaration**

We hereby confirm that the present Project work

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**\_Multi Factor Authentication**\_\_\_\_\_\_\_\_\_\_\_

Title is the result of my own independent scholarly work, and that in all cases material from the work of others (in books, articles, essays, dissertations, and on the internet) is acknowledged, and quotations and paraphrases are clearly indicated. No material other than that listed has been used. I have read and understood the Institute’s regulations and procedures concerning plagiarism.

Name: \_\_\_\_Manahil Faisal, Saba Karim, M.Hamza Iqbal \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Date: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_December 4, 2023\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Signature : \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

(Blank Page)

# Table of Contents

[**Introduction 6**](#_h4rdr4wgs6so)

[**Literature Review 6**](#_8kmhqfg7b8gd)

[Research Papers 7](#_14mj6698uk77)

["Security Engineering: A Guide to Building Dependable Distributed Systems" (Ross Anderson) 7](#_6ntbhs2gvnsn)

["A Comparative Usability Evaluation of Traditional Authentication and Client Certificates" (Forget, Chiasson, van Oorschot) 7](#_hoidlef14cg4)

["The Quest to Replace Passwords: A Framework for Comparative Evaluation of Web Authentication Schemes" (Bonneau, Herley, van Oorschot, Stajano) 7](#_uobnqywjy902)

["A Survey of Biometric Recognition Methods" (Jain, Ross, Prabhakar) 8](#_z5ppod27kzx)

["Multi-Factor Authentication: A User-Centric Evaluation of Three Commercial Systems" (Mannan, van Oorschot) 8](#_t32b9pcqjod8)

["A Survey of Two-Factor Authentication in Banking Applications" (Mannan, van Oorschot) 8](#_ue1srkqmorj4)

["Security and Usability: The Gap in Realizing Trusted Biometric Identity Systems" (Patrick, Busch) 8](#_u8s0p0qp58uj)

["Password Managers: A Comparative Study and Password Usability" (Vance, Eargle, Becker) 9](#_yud9jsp20eo)

[**Technical Proficiency in Prototype/POC Development 9**](#_ycjtad8lfsas)

[A) SDLC Methodologies 9](#_mxl187fxxnte)

[1. Planning and Requirement Analysis 9](#_1gvdcfp0qr1s)

[2. Design 10](#_kh1se5ftnpz)

[3. Implementation 10](#_osfcm2kh5tyh)

[4. Testing 10](#_s2jqtiige5rb)

[5. Deployment 11](#_vc0iqhwaf5z7)

[6. Maintenance 11](#_y9frl7tzqwui)

[B) Requirement Gathering 11](#_1axw7ftpr27t)

[1. Stakeholder Meetings 11](#_sh1nb7lalj40)

[2. Market Research 11](#_m1eezx32rr42)

[3. Security Assessment 12](#_iehoec9t7qcb)

[C) Explanation of Technology Used and its Significance 12](#_d7vel3euyuin)

[1. Front-end Development 12](#_u0a52nclm0rl)

[2. Back-end Development 12](#_bmuuv9a8y8b2)

[3. Email Code Authentication 12](#_efcve2pkw8q)

[4. Security Questions 13](#_71d87dvql739)

[D) Use of Test Cases 14](#_c0bd0pw5hijh)

[E) Troubleshooting and Issues Addressing Using Various Methodologies 14](#_eol2ei61wrvn)

[F) Stress Testing 14](#_c30y663r3hz7)

[1. Simulating High Traffic 15](#_s624bah1vpyb)

[2. Identifying Breaking Points 15](#_8aojz97uvt3s)

[G) Proper Demonstration with Test Scenarios 15](#_h6jqmh2pjmda)

[H) Drawbacks 16](#_k35nxucj1mba)

[1. Dependency on Email Delivery 16](#_122x9daeryrw)

[2. Memory-Dependent Security Questions 16](#_6qvkj7d9iwcp)

[**Application GUI Interface 16**](#_pv6qj0py34i9)

[A) Login Screen: 16](#_2hqeqo3bv0hi)

[B) Mysql Database: 17](#_en5nfo80vw8a)

[C) One Time MFA Code Generation Screen: 17](#_425mfhp7iqd2)

[D) MFA Code Sent to User’s Email: 18](#_fj7d7jd9gyb9)

[E) Security Question Screen: 18](#_ky5v2up3qu7p)

[F) Failed Authentication Due to Incorrect Answer : 19](#_h0ud8l9e5cx5)

[G) Audit Trail: 20](#_u07g651pdf3u)

[**Conclusion 20**](#_raue8kr5ffpp)

[**References 21**](#_f3162l4ickb1)

[Appendix A: Definitions 21](#_za2zv7mfhluz)

[Appendix B: Acronyms and Abbreviations 21](#_qf0zfg4ibzvq)

[Citations: 22](#_ors8hxdwxrvf)

Title: Multi Factor Authentication System (MFA)

# Introduction

The MFA system project represents a significant advancement in digital security. With the increasing prevalence of cyber threats, the need for robust authentication methods has never been greater. This project addresses this need by implementing a multi-layered authentication framework, using a combination of front-end and back-end technologies. The front-end is developed using React, providing a responsive and interactive user interface. The back-end, built with Express and SQL ensures efficient data handling and server-side logic implementation.

# Literature Review

Strong authentication techniques are desperately needed in order to combat the growing threat of cyberattacks, especially in the banking and Internet of Things (IoT) industries. In order to create a Multi-Factor Authentication (MFA) system with excellent security and user experience, the first study introduces a secure adaptive Five-Factor Authentication (5FA) scheme for online banking. This scheme incorporates modalities such as username, password, PIN, OTP, registered devices, fingerprints, and time-based location. In order to strengthen user authentication and thwart phishing attacks, the second research article tackles the spread of cloud and Internet of Things platforms. It suggests a risk assessment coupled with Multi-Factor Authentication (MFA), which advances the developing concept of Adaptive Authentication as a Service. In order to improve identity verification and combat potentially hostile behaviors in cloud services, the third article, which focuses on cloud security, presents an adaptive multi-factor multi-layer authentication architecture with access control, intrusion detection, and encryption algorithms. The fourth study, which switches to decentralized authentication, presents an adaptive multi-factor strategy blockchain-based authentication scheme that uses a consensus model based on Raft to reduce the risks associated with centralized authentication and shows superior efficacy against cyberattacks in dynamic environments. Finally, the fifth study addresses the security issues with online banking by implementing an improved Multi-factor authentication scheme that includes multiple modalities and a track-and-trace feature. When compared to existing schemes, the results show promise in terms of security, resource usage, and response time. Taken as a whole, these research offer insightful information on improving authentication techniques in a variety of online domains.

## Research Papers

### **"Security Engineering: A Guide to Building Dependable Distributed Systems" (Ross Anderson)**

* **Overview:** This seminal work covers various aspects of security engineering, including authentication methods and the design of dependable distributed systems.
* **Contribution:** Anderson provides insights into principles and practices for building secure systems, offering a foundation for understanding security challenges and solutions.

### **"A Comparative Usability Evaluation of Traditional Authentication and Client Certificates" (Forget, Chiasson, van Oorschot)**

* **Overview:** The paper explores the usability aspects of authentication methods, comparing traditional methods with client certificates.
* **Contribution:** The authors assess user experiences and challenges associated with different authentication mechanisms, providing valuable insights for designing user-friendly authentication systems.

### **"The Quest to Replace Passwords: A Framework for Comparative Evaluation of Web Authentication Schemes" (Bonneau, Herley, van Oorschot, Stajano)**

* **Overview:** This research paper addresses the challenges of replacing passwords and offers a framework for evaluating web authentication schemes.
* **Contribution:** The paper contributes to the ongoing discourse on secure and usable alternatives to passwords, providing a framework for comparing various authentication approaches.

### **"A Survey of Biometric Recognition Methods" (Jain, Ross, Prabhakar)**

* **Overview:** The survey paper covers a broad range of biometric recognition methods, discussing the principles and applications of biometrics.
* **Contribution:** The authors provide a comprehensive overview of biometric technologies, aiding researchers and practitioners in understanding the landscape of biometric recognition.

### **"Multi-Factor Authentication: A User-Centric Evaluation of Three Commercial Systems" (Mannan, van Oorschot)**

* **Overview:** The paper evaluates the user-centric aspects of three commercial MFA systems.
* **Contribution:** The authors assess user experiences and perceptions of MFA systems, contributing insights into the usability and acceptance of multi-factor authentication.

### **"A Survey of Two-Factor Authentication in Banking Applications" (Mannan, van Oorschot)**

* **Overview:** This survey explores the implementation and security aspects of two-factor authentication in banking applications.
* **Contribution:** The authors provide an overview of the state of two-factor authentication in the banking sector, offering insights into security practices and challenges.

### **"Security and Usability: The Gap in Realizing Trusted Biometric Identity Systems" (Patrick, Busch)**

* **Overview:** The paper discusses the gap between the security and usability of biometric identity systems.
* **Contribution:** The authors highlight challenges and considerations in the implementation of biometric identity systems, emphasizing the need for balancing security and usability.

### **"Password Managers: A Comparative Study and Password Usability" (Vance, Eargle, Becker)**

* **Overview:** The study focuses on password managers, evaluating their usability and user behaviors.
* **Contribution:** The authors provide insights into the usability of password managers and user practices, contributing to the understanding of password-related security challenges.

# Technical Proficiency in Prototype/POC Development

## SDLC Methodologies

### **Planning and Requirement Analysis**

This initial phase was crucial for setting a strong foundation for the project. Here’s how it was approached:

* **Identifying the Need for an MFA System:** The team conducted an analysis of current cybersecurity challenges and identified the growing need for more robust authentication methods in the face of increasing digital threats.
* **Defining the Scope:** The project's scope included the creation of a secure, scalable, and user-friendly MFA system. This involved defining the technical requirements, user interface specifications, and security protocols to be implemented.
* **Risk Assessment:** A comprehensive risk assessment was conducted to understand potential vulnerabilities and incorporate necessary safeguards from the outset.

### **Design**

The design phase focused on creating a blueprint for the MFA system:

* **Security-Centric Architecture:** The system was architected with a primary focus on security, ensuring that all components, from the frontend to the backend, adhere to the highest security standards.
* **Performance Optimization:** Special attention was given to the system’s performance, ensuring quick response times and efficient handling of requests.
* **Scalability Planning:** The design accounted for future expansion, both in terms of user base and functionality, to ensure the system could grow without compromising on performance or security.

### **Implementation**

During the implementation phase, the designs and plans were brought to life:

* **Frontend Development:** The React-based frontend was developed with an emphasis on user experience, ensuring a seamless and intuitive interface.
* **Backend Development:** The Express and SQL backend was built to handle requests efficiently, manage data securely, and integrate seamlessly with the frontend.
* **Security Integration:** Implementing robust security measures, including encryption and secure communication protocols, to protect against various cyber threats.

### **Testing**

Testing was a rigorous and multi-faceted process:

* **Functional Testing:** Ensuring that all features work as intended and meet the requirements set during the planning phase.
* **Security Testing:** Specialized tests were conducted to identify any vulnerabilities and assess the effectiveness of security measures.
* **User Acceptance Testing (UAT):** Selected users tested the system in a controlled environment to validate the usability and functionality.

### **Deployment**

The deployment phase marked the system’s transition into a live environment:

* **Staged Rollout:** The system was initially rolled out to a limited user base to monitor performance and gather feedback.
* **Monitoring and Optimization:** Continuous monitoring was implemented to ensure smooth operation and to quickly identify and resolve any issues.

### **Maintenance**

Ongoing maintenance is essential for the system’s longevity:

* **Regular Updates:** The system is regularly updated to incorporate new security patches, feature improvements, and performance enhancements.
* **Performance Monitoring:** Continuous monitoring of the system’s performance to ensure it meets the expected standards.
* **User Feedback Incorporation:** Regularly collecting and analyzing user feedback to refine and improve the system.

## Requirement Gathering

A thorough requirement gathering process was undertaken:

### **Stakeholder Meetings**

* **Diverse Participation:** Meetings included a range of stakeholders, such as potential users, IT staff, and security experts.
* **Feedback Integration:** The feedback from these meetings was directly incorporated into the system’s design and functionality.

### **Market Research**

* **Competitive Analysis:** A detailed analysis of existing MFA solutions was conducted to understand the market landscape and identify best practices.
* **Trend Identification:** Research focused on identifying emerging trends in MFA technology and cybersecurity to ensure the system remains relevant and effective.

### **Security Assessment**

* **Threat Analysis:** A thorough analysis of current and potential future threats was conducted to ensure the system’s defenses are robust and comprehensive.
* **Compliance Check:** Ensuring the system adheres to relevant laws and regulations related to data protection and cybersecurity.

## Explanation of Technology Used and its Significance

### **Front-end Development**

* Framework used: ***React***

Chosen for its efficiency in creating dynamic and responsive user interfaces for front-end development.

### **Back-end Development**

* Framework Used: ***Express and SQL***

These technologies offer a robust platform for backend development, with Express facilitating rapid development and SQL providing reliable data management.

### **Email Code Authentication**

* **Implementation:**

This feature involves sending a time-sensitive, randomly generated code to the user's registered email address as part of the login process. Once the user receives this code, they enter it on the login screen to gain access.

* **Justification:**
* **Layered Security:** By adding this step, the system ensures that even if a password is compromised, unauthorized access is still prevented unless the attacker also has access to the user's email.
* **Time-Sensitivity:** The time limit on the code adds urgency and reduces the window of opportunity for attackers.
* **Randomization:** Generating a new code for each login attempt makes it nearly impossible for attackers to guess the correct code.
* **User Familiarity:** Email is a common communication tool, making this method user-friendly as most people are familiar with receiving and handling emails.
* **Security Enhancements:**
* **Two-Channel Verification:** Since the email is sent to a separate device or account, it provides two-channel verification, significantly enhancing security.
* **Audit Trail:** The use of email allows for an audit trail, enabling the tracking and recording of login attempts and authentications.

### **Security Questions**

* **Implementation:**

Users are required to set up security questions during the registration process. These questions are personal and the answers are known only to the user. During authentication, in addition to the standard password, users may be prompted to answer one of their security questions.

* **Justification:**
* **Personalization:** The personal nature of the questions makes it difficult for outsiders to guess the answers, adding a layer of personalized security.
* **Versatility:** Security questions can be used not only for additional login security but also for account recovery processes.
* **User Control:** Users have control over their security questions, allowing them to choose questions they are comfortable with and answers they will remember.

* **Security Enhancements:**
* **Psychological Barrier:** The requirement to answer something personal adds a psychological barrier to unauthorized users.
* **Redundancy:** In a situation where other authentication methods (like email codes) might fail or be inaccessible, security questions provide an alternate method of verifying identity.
* **Flexibility in Usage:** They can be utilized in various scenarios, such as when logging in from a new device or location, adding an additional layer of verification.
* **Best Practices for Implementation:**
* **Choice of Questions:** Offering a wide range of questions for users to choose from, ensuring they can select ones that have memorable yet secure answers.
* **Encryption of Answers:** Storing the answers in an encrypted format in the database to prevent unauthorized access or leaks.

## Use of Test Cases

Extensive test cases were developed and executed, covering:

* **Functionality Testing:** Ensuring each feature works as intended.
* **Security Testing:** Testing the system's resilience against various cyber threats.
* **User Experience Testing:** Making sure the system is intuitive and user-friendly.

## Troubleshooting and Issues Addressing Using Various Methodologies

A systematic approach was adopted for troubleshooting:

* **Debugging:** Identifying and fixing bugs in the code.
* **Code Reviews:** Peer-to-peer review sessions to ensure code quality and security.
* **Iterative Testing:** Repeated testing to refine and improve the system.

## Stress Testing

Stress testing was a critical part of the project, designed to test the system's limits by:

### **Simulating High Traffic**

* **Objective:** To assess how the system performs under extreme load conditions. This simulation involves artificially creating conditions where a large number of users attempt to access or use the system simultaneously.
* **Methodology:** Tools and scripts were employed to mimic a surge in user traffic, pushing the system beyond its normal operational capacity.
* **Outcome:** This test helped in identifying how the system's performance varied under stress, such as slowdowns, response time delays, or failures in handling requests. The insights gained were crucial for optimizing and scaling the system to handle high traffic efficiently.

### **Identifying Breaking Points**

* **Objective:** To determine the maximum load the system can handle before it becomes unresponsive or breaks down. This involves gradually increasing the load until the system reaches its threshold.
* **Methodology:** Incremental load increases were applied, closely monitoring system resources like CPU, memory, and network bandwidth. The focus was on identifying at what point the system fails or its performance degrades significantly.
* **Outcome:** This exercise provided valuable information about the system's capacity limits. It was instrumental in establishing benchmarks for system performance and in identifying areas where enhancements were needed to improve resilience and stability.

## Proper Demonstration with Test Scenarios

The demonstration of the MFA system effectively showcased its functionality through a variety of real-world scenarios, with a particular focus on the standard authentication flows. These demonstrations were designed to illustrate the typical user experience during the login process. Attendees observed firsthand how users would interact with the system, from entering their credentials to navigating the multi-factor authentication steps, including email code verification and security question responses. This practical display provided a clear and tangible understanding of how the system operates under normal usage conditions, highlighting its user-friendliness, security robustness, and the overall smoothness of the authentication process. Such demonstrations were key in validating the system's design and effectiveness, offering a comprehensive view of the user's journey from start to finish in the authentication cycle.

## Drawbacks

While the MFA system is robust and well-designed, it does have certain limitations that are worth noting:

### **Dependency on Email Delivery**

The system's reliance on email code authentication introduces a dependency on external email services. This can be a potential issue as the timely delivery of authentication codes is crucial for a smooth login process. Delays in email delivery, which can be caused by factors like server downtimes, network issues, or spam filters, might lead to user frustration and hinder immediate access to the system. This reliance on a third-party service adds an external variable that can impact the overall efficiency and reliability of the authentication process.

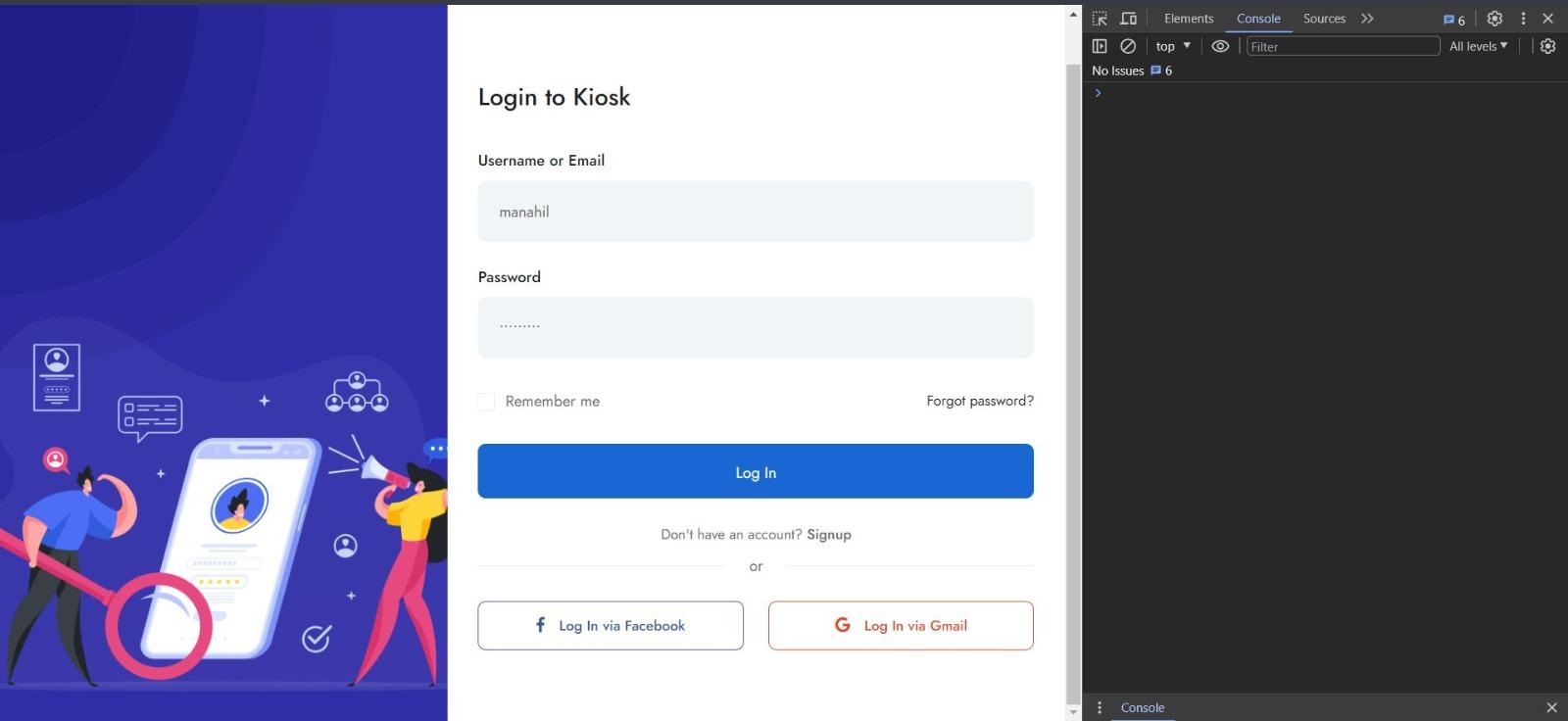
### **Memory-Dependent Security Questions**

The use of security questions as an authentication factor, while adding a layer of personalized security, also introduces a challenge. These questions are memory-dependent, meaning the user's ability to recall their answers is crucial. Over time, users might forget the answers they provided, especially if they don't log in frequently or if the questions were set up a long time ago. This can lead to access issues, locking users out of their accounts and necessitating a potentially cumbersome account recovery process. It also adds an additional burden on the support system to assist users in regaining access to their accounts.

# Application GUI Interface

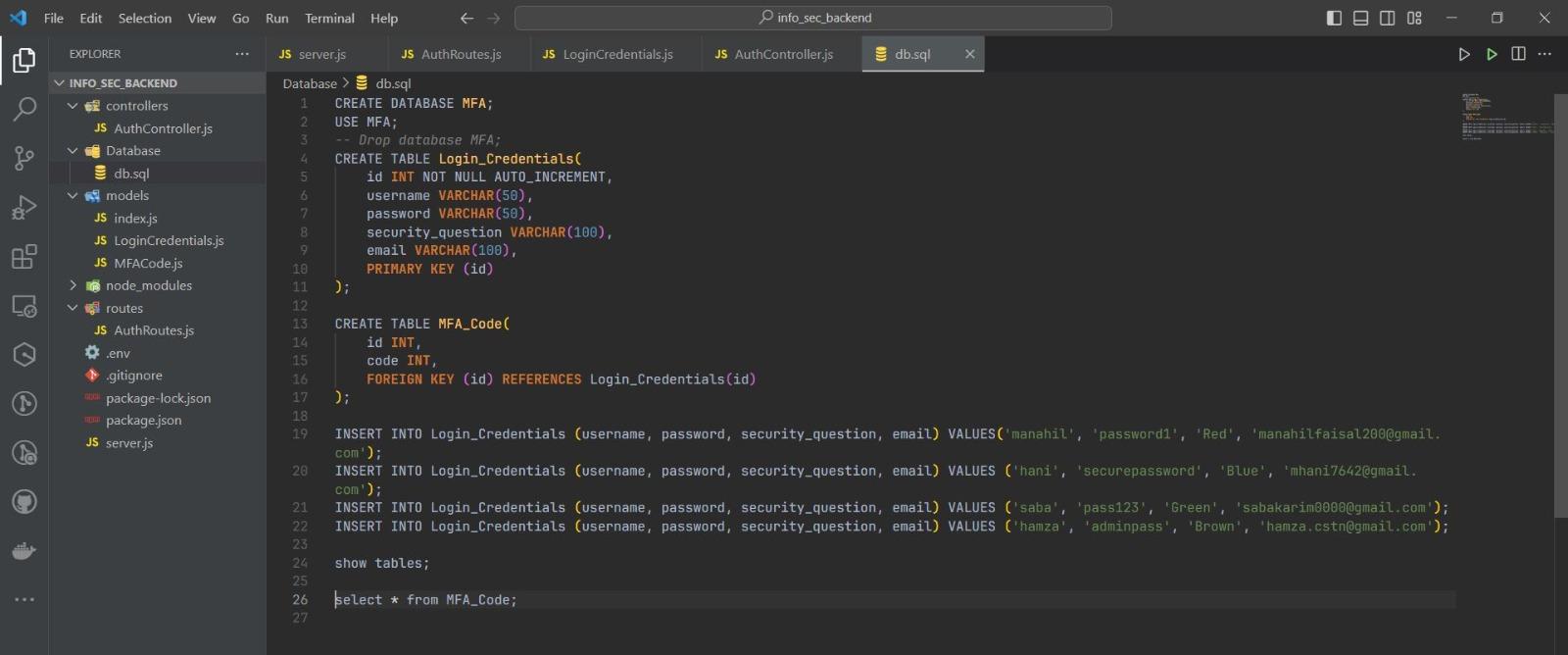
## Login Screen:

The user is prompted to login using their registered username and password. The data of the registered users is maintained in a Mysql database (as shown in *Figure 1)*  from which the login credentials are verified and authenticated.



*Figure 1: Login Screen*

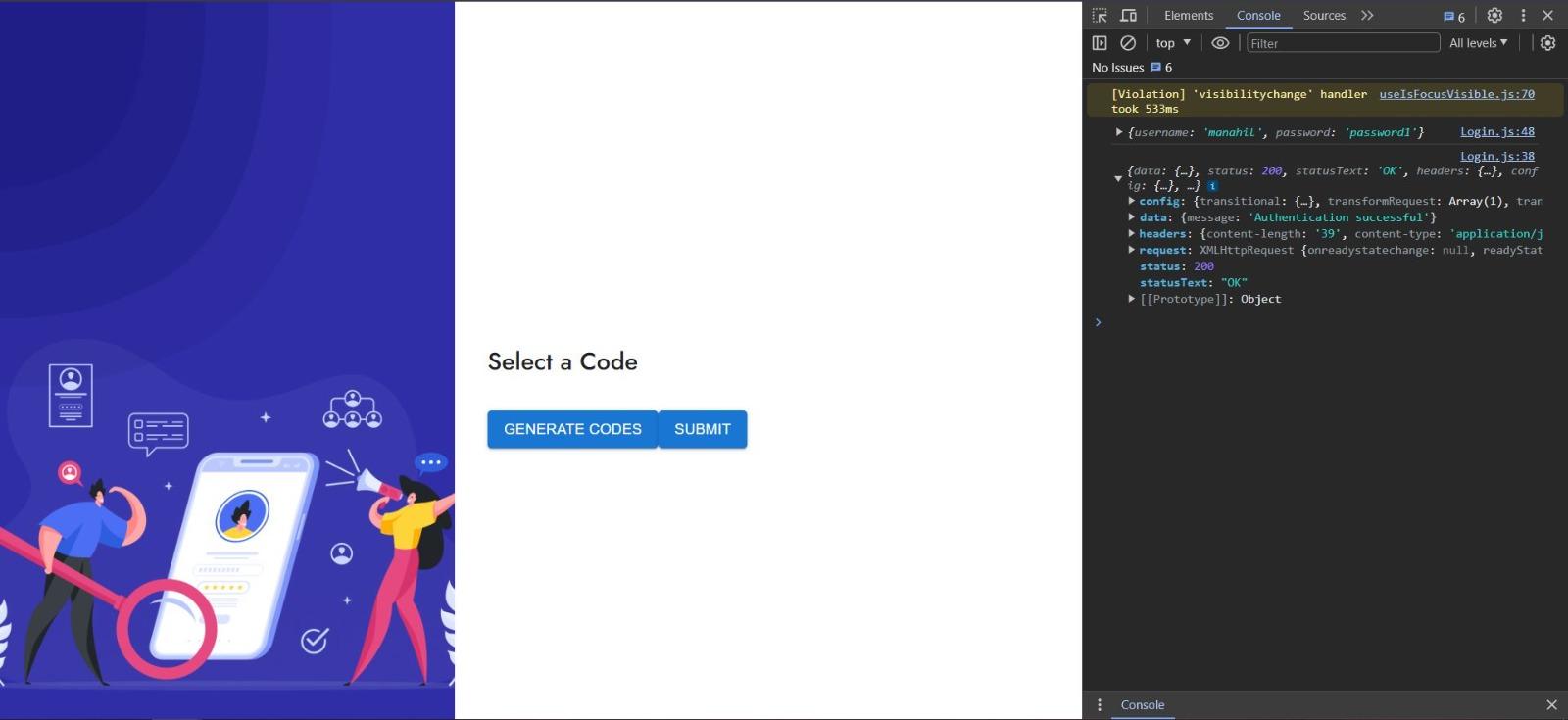
## Mysql Database:



*Figure 2: Database*

## One Time MFA Code Generation Screen:

The user selects the option to generate code which instantly sends an email to the user's registered email containing a unique code (as shown in *Figure 4*) which expires within one minute. A new code has to be generated if the one minute timer is exceeded. This is done to prevent brute force attacks and other security vulnerabilities.



*Figure 3: MFA Code Generation Screen*

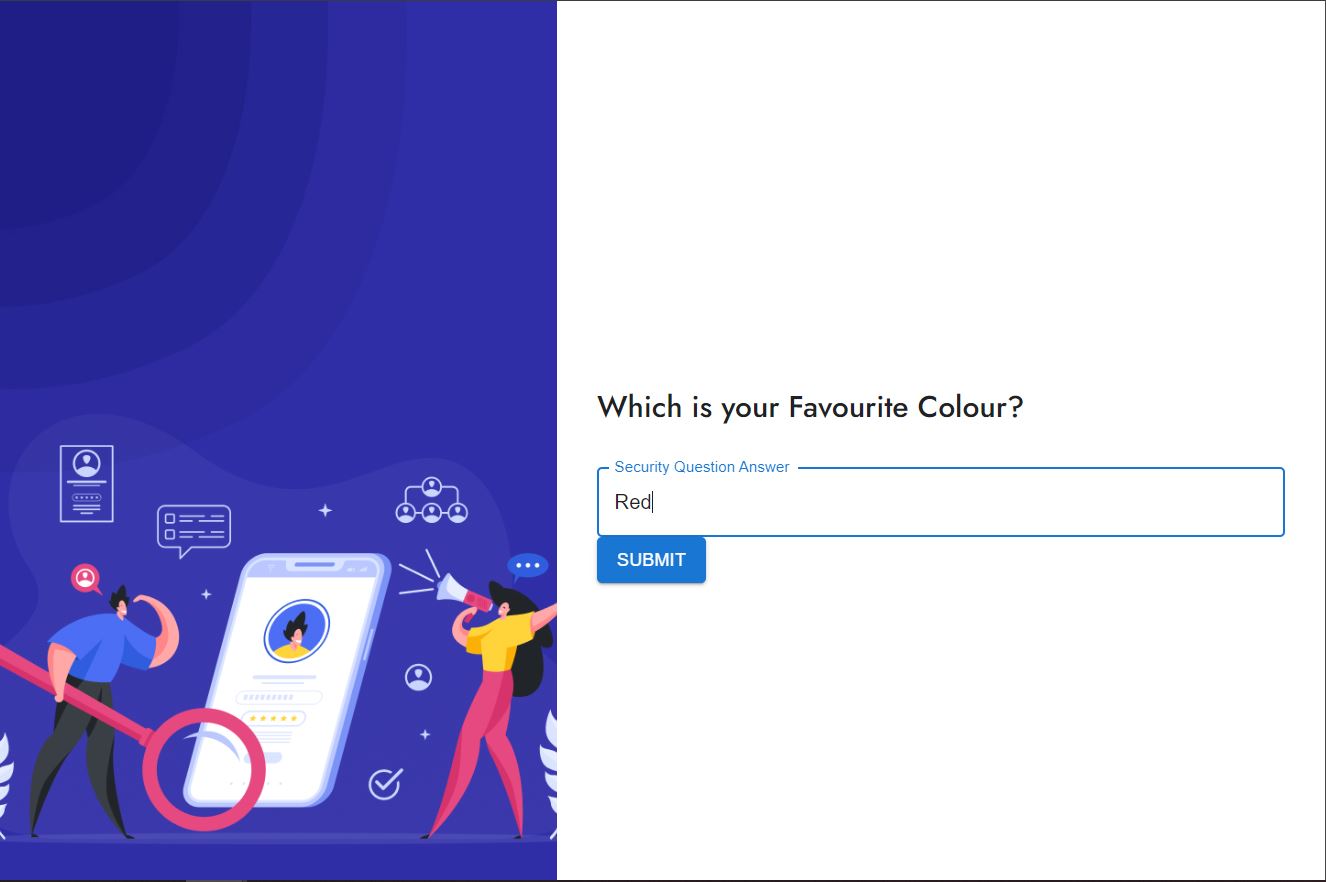
## MFA Code Sent to User’s Email:



*Figure 4: MFA Email Screen*

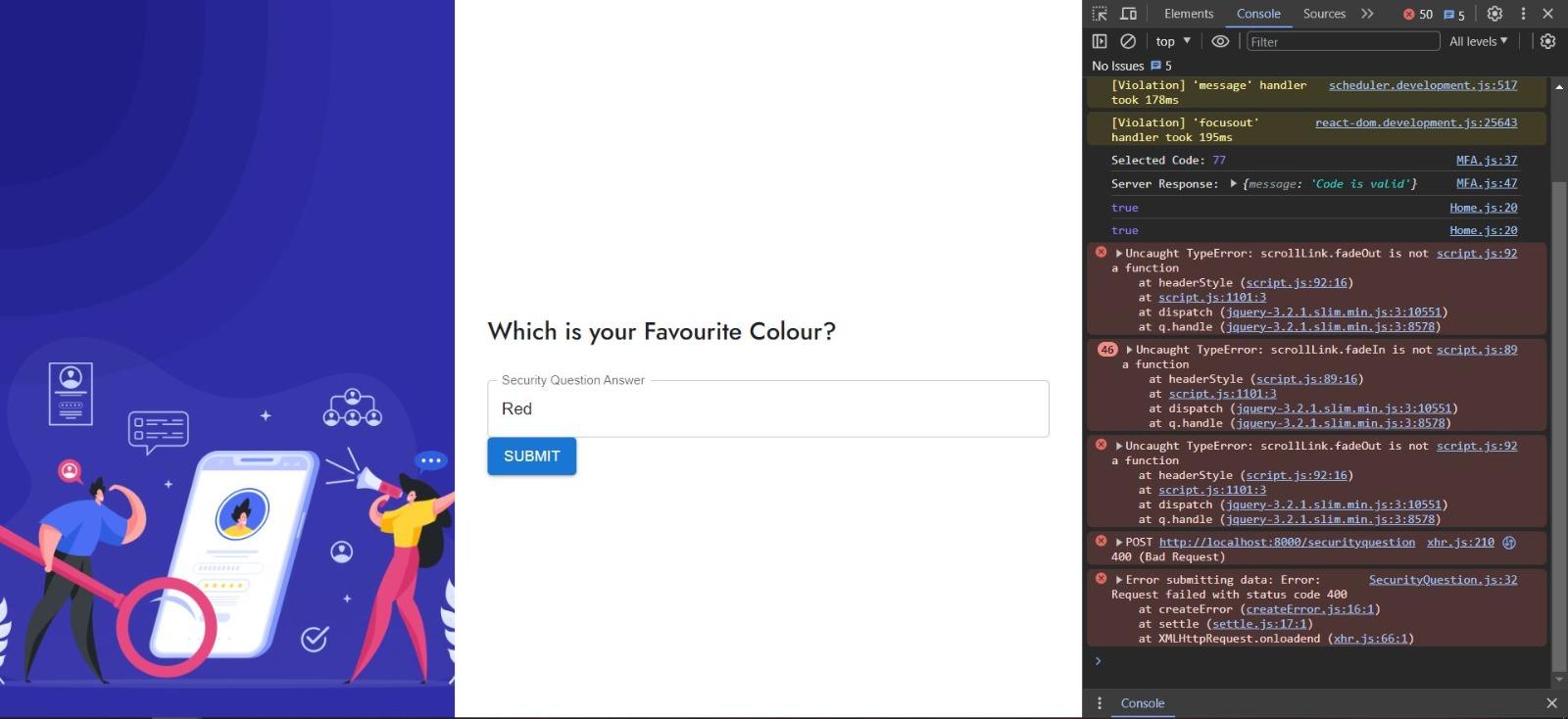
## Security Question Screen:

The user is prompted to enter their answer to the security question as the final authentication step. If the user answers incorrectly, their authentication is failed and an error message is displayed as can be seen in *Figure 6* attached below.



*Figure 5: Security Question Screen*

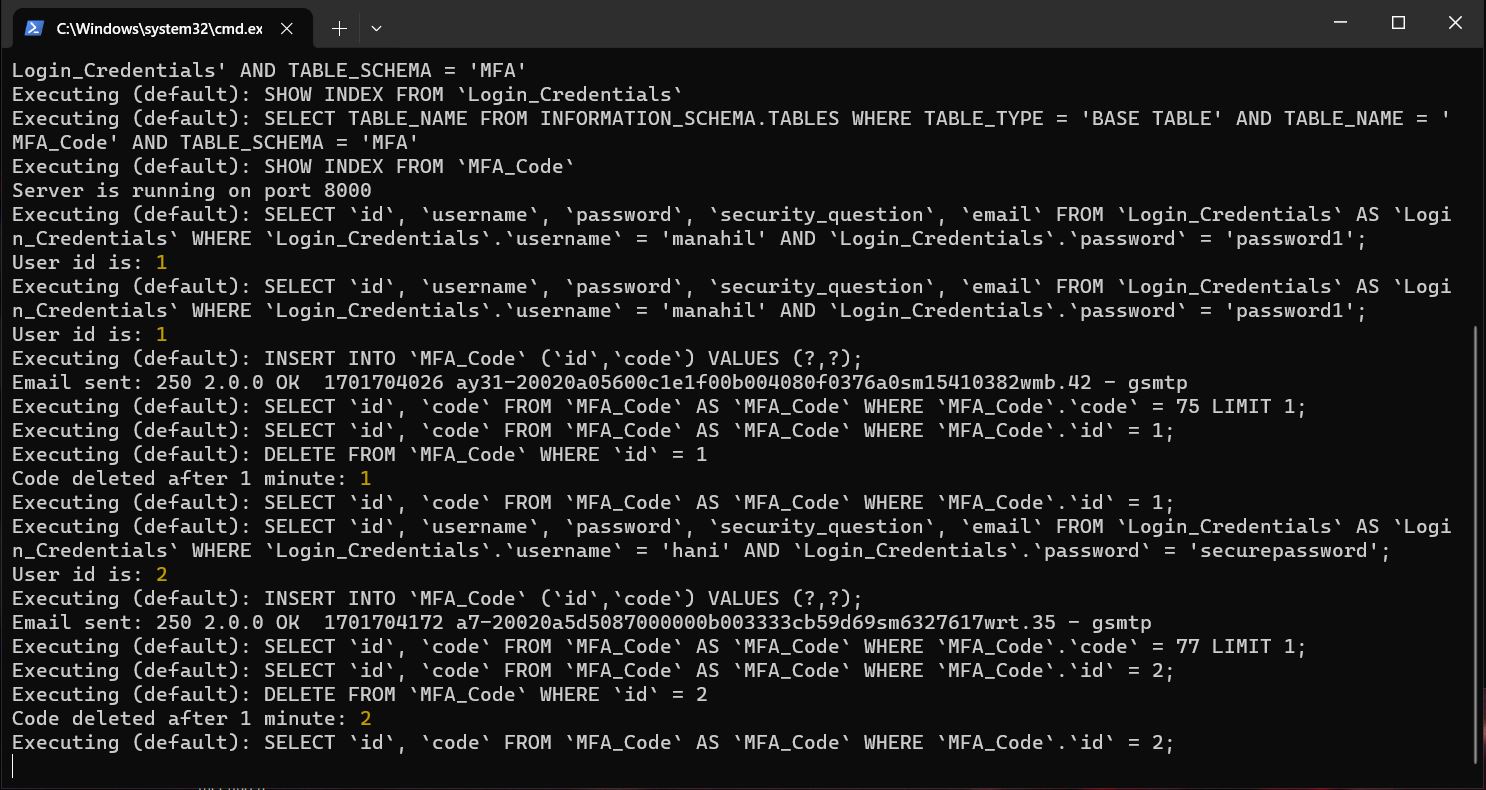
## Failed Authentication Due to Incorrect Answer :



*Figure 6: Incorrect Answer to Security Question Screen*

## Audit Trail:

The following figure shows the audit trail which helps maintain logs of the users and their login attempts



*Figure 7: Audit Trail*

# Conclusion

In conclusion, the MFA system represents a significant step forward in securing digital identities and transactions. Through the thoughtful application of modern technologies and adherence to best security practices, the system provides a robust defense against a variety of cyber threats. While it excels in many areas, like any system, it has room for improvements, particularly in user dependency elements. Future enhancements could focus on alternative authentication methods and even more user-friendly recovery options, ensuring that security is always balanced with ease of use.

# References

## Appendix A: Definitions

|  |  |
| --- | --- |
| **Term** | **Definition** |
| Multi-factor authentication | Multi-factor authentication is an electronic authentication method in which a user is granted access to a website or application only after successfully presenting two or more pieces of evidence to an authentication mechanism. |
| Brute Force Attack | A brute force attack is a hacking method that uses trial and error to crack passwords, login credentials, and encryption keys. |
| Key Logging | The practice of covertly recording input signals into a computer from a keyboard so that the computer user is not aware. |
| Stakeholder | A person, group or organization with a vested interest, or stake, in the decision-making and activities of a business, organization or project. |
| Authentication | The process or action of verifying the identity of a user or process. |

## Appendix B: Acronyms and Abbreviations

|  |  |
| --- | --- |
| **Acronym/Abbreviation** | **Meaning** |
| MFA | Multi-Factor Authentication. |
| Key logging | Keystroke logging. |
| UAT | User Acceptance Testing. |
| IT | Information Technology. |

## Citations:

1. Implementation of an Adaptive Five-Factor Authentication Scheme for Online Banking Services in South Africa | IEEE Conference Publication | IEEE Xplore. (n.d.). Ieeexplore.ieee.org. Retrieved December 4, 2023, from https://ieeexplore.ieee.org/abstract/document/10293332
2. ‌Moepi, G.L.; Mathonsi, T.E. Implementation of an Enhanced Multi-Factor Authentication Scheme with a Track and Trace Capability for Online Banking Platforms. Preprints 2023, 2023110950. <https://doi.org/10.20944/preprints202311.0950.v1>
3. Ayman Mohamed Mostafa, Ezz, M., Elbashir, M. K., Meshrif Alruily, Hamouda, E., Alsarhani, M., & Said, W. (2023). Strengthening Cloud Security: An Innovative Multi-Factor Multi-Layer Authentication Framework for Cloud User Authentication. Applied Sciences, 13(19), 10871–10871. https://doi.org/10.3390/app131910871

‌