A

Synopsis/Project Report

On

USER AUTHENTICATION

Submitted in partial fulfillment of the requirement for the VI semester

Bachelor of Technology

By

Harshit Pathak

1961060

Under the Guidance of

Dr. Sandeep K. Budhani

Deptt. of CSE

DEPARTMENT OF COMPUTER SCIENCE & ENGINEERING

GRAPHIC ERA HILL UNIVERSITY, BHIMTAL CAMPUSE

SATTAL ROAD, P.O. BHOWALI,

DISTRICT- NAINITAL-263132

2021 - 2022

STUDENT'S DECLARATION

I,Harshit Pathak here by declare the work, which is being presented in the project, entitled "User Authentication" in partial fulfillment of the requirement for the award of the degree **B-Tech** in the session **2021-2022**, is an authentic record of my own work carried out under the supervision of Dr. Sandeep K. Budhani, Graphic Era Hill University, Bhimtal.

The matter embodied in this project has not been submitted by me for the award of any other degree.

Date: 15-09-21 …….

(Full signature of student)

CERTIFICATE

The project report entitled "User Authentication" being submitted by Harshit Pathak enrollment no PV-B1961060 Roll no 1961060 to Graphic Era Hill University Bhimtal Campus for the award of bonafide work carried out by him. He has worked under my guidance and supervision and fulfilled the requirement for the submission of report.

(Dr. Sandeep K. Budhani) **(……)**

Project Guide **(HOD, CSE Dept.)**

ACKNOWLEDGEMENT

I take immense pleasure in thanking Honorable **"Dr. Sandeep K. Budhani"** to permit me and carry out this project work with his excellent and optimistic supervision. This has all been possible due to his novel inspiration, able guidance and useful suggestions that helped me to develop as a creative researcher and complete the research work, in time.

Words are inadequate in offering my thanks to GOD for providing me everything that I need. I again want to extend thanks to our President **"Prof. (Dr.) Kamal Ghanshala"** for providing us all infrastructure and facilities to work in need without which this work could not be possible.

Many thanks to Professor **"Dr. Ankur Singh Bist"** (HOD-CS&E, GEHU), and other faculties for their insightful comments, constructive suggestions, valuable advice, and time in reviewing this thesis.

Finally, yet importantly, I would like to express my heartiest thanks to my beloved parent for their moral support, affection and blessings. I would also like to pay my sincere thanks to all my friends and well-wishers for their help and wishes for the successful completion of this research.

(HARSHIT PATHAK)
hpathak1238@gmail.com

TABLE OF CONTENTS

Declaration ..... **I**
Certificate ..... **II**
Acknowledgement ..... **III**
Abstract ..... **IV**

CHAPTER1 INTRODUCTION **1**

1.1 Problem Statement 1

1.2 Objectives and Research Methodology 2

1.3 Background and Motivation 2

CHAPTER 2: Literature Review **3**

2.1 Existing proposed Solution Overview 3

2.2 Two Factor Authentication 4

2.3 Hash Fuction 5

2.4 Comparison Between Proposed Solution 6

CHAPTER 3: Proposed METHOD/APPROACH **7**

3.1 Design Specification 7

3.2 System Requirement 8

3.3 Software Requirement 8

3.4 Implementation Issue and Challenges 8

CHAPTER 4: Discussion **9**

4.1 Security issue of Current Login System 9

4.2 Reason For Selection tool 10

4.2.1 Reason of choosing MONGODB 10

4.2.2 Reason of choosing VS CODE 11

2.2.3 Reason of choosing NODE JS 12

USER AUTHENTICATION

Chapter 1 :

INTRODUCTION

1.1 PROBLEM STATEMENT

Authentication is an activity to authenticate the person credential that wishes to perform the activity. In the process of authentication, the password enter by the user will be transmitted along the traffic to the authentication server in order to allow the server to grant access to the authorized user. When the password is transmitted, the attackers will try to sniff into the network to obtain data that include the user's password. Currently, there is rainbow table which able to trace the password with the hash algorithm to obtain the user's password. Once the password is succeeded to be decrypted, the attackers can use the user credential to do something illegal such as fraud others which will cause the user lost in credit. According to Pagliery(2014), there is 47% of the American adults account been hacked in that year. Their personal information is exposed by the hackers. Due to the problem exists, there are more people no longer trust that password will be able to protect their online account. According to Sulleyman(2017), some of the attackers will sell the email account that is been hacked to others to gain profit. It is important to protect our own account because our credit is priceless. It is hard to trace the attackers in the cyber world. The secure login system is needed to ensure the cybersafety. Therefore, this project would like to provide alternative ways to log in to a system because current login system is not secure enough.

1.2 PROJECT OBJECTIVES

The 2 main objectives for this project:

1. The main objective is to implement a secure login authentication system with utilizing with two-factor authentications. By using the concept two-factor authentication could help to increase the strength of the login system. The attacker will need to pass through the next barrier of defence to success to log in. This system will help to enhance the login authentication system.
2. Next objective is to ensure login password will not be transmitted over the network. As compared to the previous solution, the password is just encrypted, but the attackers might succeed to decode the data and retrieve the password. So in order to prevent this happens, the password with the random key will need to be hash before the sender sends the password to the server. It is important to secure the password of the user.

1.3 BACKGROUND AND MOTIVATION

Authentication is an activity to authenticate the person credential that wishes to perform the activity. If the credential is matched, the process is completed and the user will be granted for the access. Generally, the user will need to provide their password to begin using a service of the system. According to Rouse (2014), user authentication authorizes human-to-machine interactions in operating systems and applications as well as both wired and wireless networks to enable access to networked and Internetconnected systems, applications and resources. In their investigation of password evolution, Bonneau (2015) state that: The password is added to the sharing operating system in 1960s. However, the problem arose very quick due to the leakage of the unencrypted password master file. When reaching 1970s, the password started to be stored in the hashed form. In 1979, the hashed password was improved with the salting. With the mid-1990s introduce of the World Wide Web, the password is secure using the public-key cryptography via secure sockets layer (SSL) client certificates. The password is then started to link to the email and two-factor authentication is introduced. In the early of 2010s, the smartphone starts to be widely used. The reason for the implementation is also because of the free smartphone applications to act as a second factor based on the emerging time-based-onetime-pad (TOTP) standard. TOTP is an algorithm that computes a one-time password from a shared secret key and the current time. There are also services provided by sending codes via short message service (SMS) as a backup authentication mechanism.

Chapter 2 :

LITERATURE REVIEW

2.1 EXISTING PROPOSED SOLUTIONS OVERVIEW

Authentication is a process to access to login account and accessing the service provided by the system or server using the password. It also has an alternative way to authenticate the user which is using biometric authentication by using fingerprint or iris recognition. However, human has the tendency to create easily remember password which it will lead to a problem. By definition, authentication is the use of one or more mechanisms to confirm that you are the authenticated user. Once the identity of the human or machine is validated, access is granted. There are existing acknowledged three authentication factors are things the user know, things the user have and biometric authentication. Biometric-based authentication is a good way to authenticate the user but it is expensive and raises some privacy concern.

Two-factor authentication solution equips customers with a cost effective means of providing flexible and strong authentication to very large scale. The goal of computer security to maintain the integrity, availability and privacy of the information entrusted to the system can be obtained by adopting this authentication technique. There is also company uses the hashing algorithm to store their password. In the transmission of the password, the password has already been hashed and become unreadable.

Lastly, most of the password is now encrypted when it is sent from the sender to the receiver. The password is encrypted so that the attackers will not easily obtaining the correct password since they will need another step to decrypt the data (Mathur, A. ,2012).

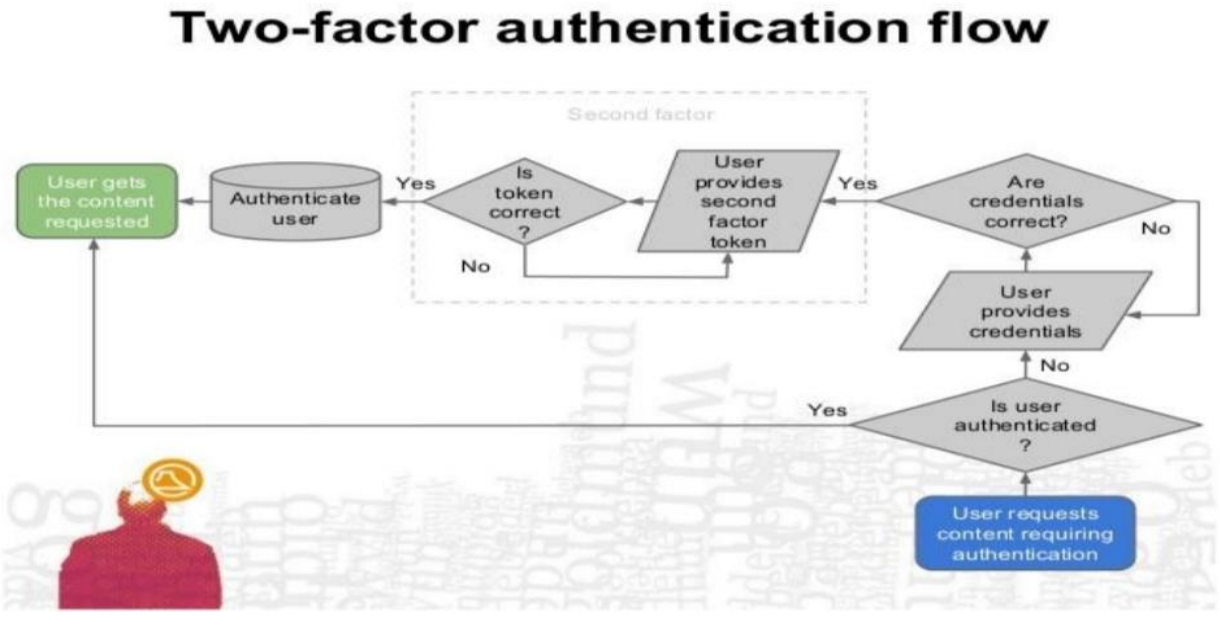
2.2 TWO FACTOR AUTHENTICATION

Two-factor authentication has been introduced long time ago. It is also known as the two-step verification. The organization will implement this method because it is easy the implement it. They can save the cost from replacing the existing system and increase security level by adding a layer of security that protects the existing authentication system.

The reason for the two-factor authentication is been started to use by many organizations is because of the ease of implementation of the method. They do not require to replace the existing system but just increase security level by adding a layer of security that protects the existing authentication system. The process will require 2 reliable authentication factors which is something the users knows such as alphanumeric password, something user has such as the phone and something the user is such as biological unique features (eg. Fingerprint).

Two-factor authentication is an evolvement from single-factor authentication which only requires the password of the user. However, single-factor authentication is no longer secure due to user tends to have the weak password which is common. Users also tend to have the same password for multiple accounts. This provides a chance for the hacker to succeed in password exploitation.

The two-factor authentication helps to provide an additional layer of security. In two factor authentication, the user provides dual means of identification, one of which is typically a physical token, such as a card and the other of which is typically something memorized, such as security code. The aim of the multifactor is to create a more difficult step for attackers/ unauthorized people to access a target. This mechanism still able to be secure if there is still existing a barrier to breach before accessing the target.



2.3 HASH FUNCTION

Hashing is a step that will use a hash algorithm such as the MD5 to turn a password into a long random string which consists of letters and numbers. The hashes are the opposite of encryption which is not reversible to be the original text. There is no algorithm exist to reverse back the hashes. However, the attackers can try the different combination of the password in order to match the user password. The combination password hashes are then collected to store into the rainbow table. This method will be very time exhausting.

Encryption is a process that converts the message into unreadable using some algorithm. It is one of the processes that applying the cryptography. Encryption is a step that transforms or convert the data into a random and meaningless message. In another word, it can be said as is a process to convert plaintext into the ciphertext. **Decryption** is the vice versa of the encryption which will convert the data into the meaning form. It is a process to transform ciphertext into plain text.

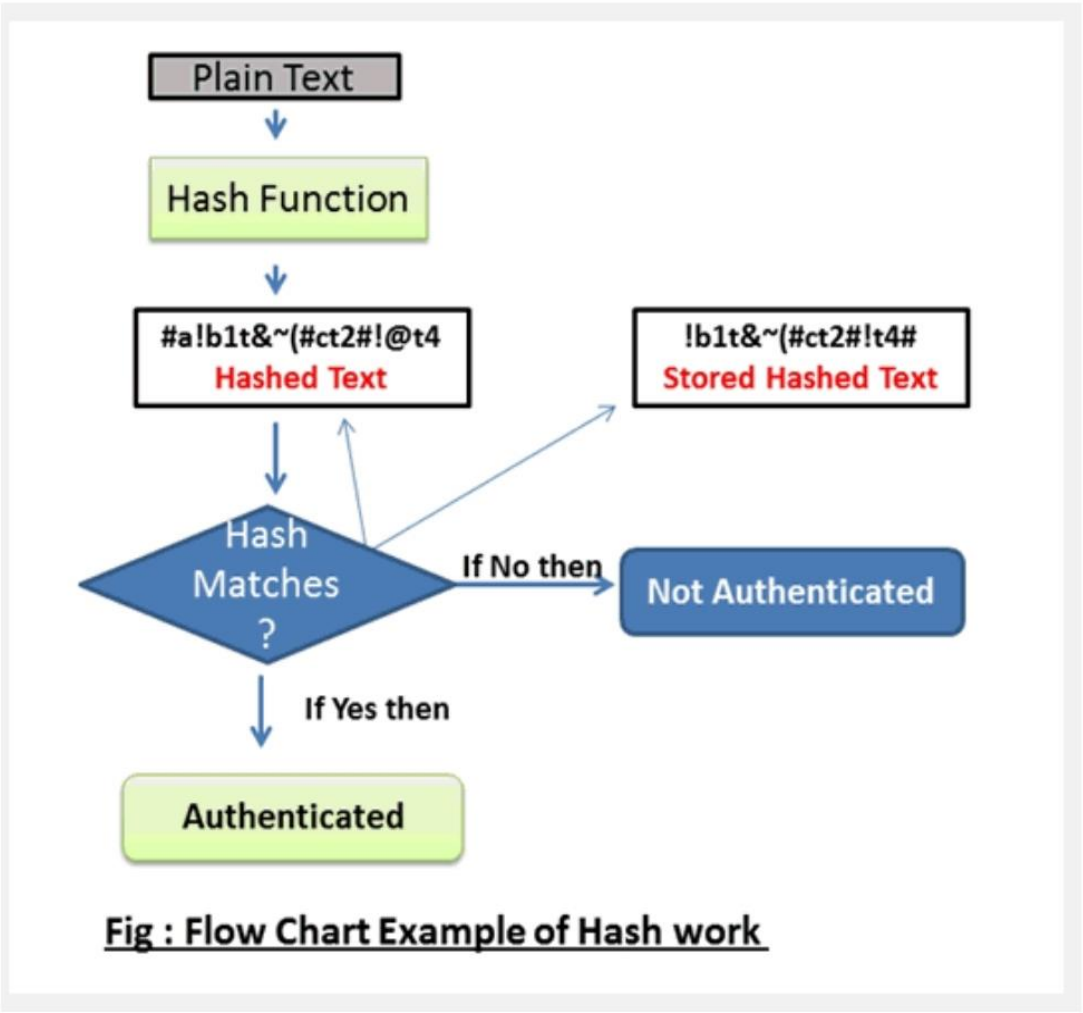


Fig : Flow Chart Example of Hash work

2.4 COMPARISON BETWEEN PROPOSED SOLUTION

Proposed Solution	Strength	Weakness
Two factor authentication	• Increase the step for attackers to success	• If the email is hijacked, the process cannot continue until the email is been recovery.
Hash Function	• The password is not reversible • The password with the similar hashes is very rare • Time exhausting to crack the password	• Vulnerable to rainbow table attack

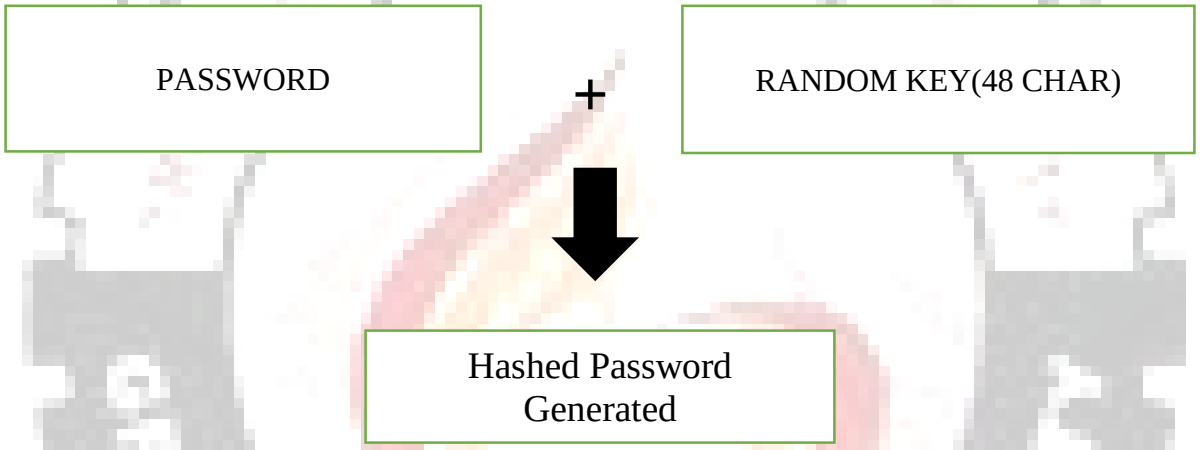
Chapter 3 :

PROPOSED METHOD/APPROACH

3.1 DESIGN SPECIFICATIONS

Due to the importance to secure the password, I had implemented an enhanced version of the login authentication from the existing proposed solution. Under the existing system, the password whether it is encrypted or hashed, it still exists in the network traffic to reach the service. Once the attackers get the encrypted or hashed password, the attacker will have the chance to succeed to discover the algorithm to retrieve back the plain text.

This project needs 2 things which are the desktop sites and mobile application. The desktop designed to have 2 type of user input with username and Password. The website will require the username first then only the password. Next, the system will need the implementation of server-side scripting. The server-side scripting will retrieve the password from database and generate the random key with 48 characters. The password and random key then combine and hashed.



3.2 SYSTEM REQUIREMENT

The device requires respectives system requirement.
For the laptop requirement suggested will be as listed as below.

- OS Window XP and later/Mac OS
- RAM 2GB
- Processor Intel's dual-core Core i3-4130
- Hard drive 1GB of free space

3.3 SOFTWARE REQUIREMENT

The Software we require are :

- Visual Studio code (VS CODE)
- Web Browser (CHROME,EDGE ,etc)
- NodeJS (SERVER)
- MongoDB (DATABASE)
- AWS (HOSTING)

3.4 IMPLEMENTATION ISSUES AND CHALLENGES

The major challenge of the project is the shortage of time because time is needed to learning the code and need to implement the system. The time also uses to find out the better solution from the others proposed solution. The proposed solution needed to study and find out their strength and weaknesses to be improved so that can learn from their problem. The next challenge of the project will be the limitation of understanding the code used to implement the system. The coding will be a very fresh programming language for me since it is very new for me.

Chapter 4 :

DISCUSSION

4.1 SECURITY ISSUES OF CURRENT LOGIN SYSTEM

In the current existing login authentication system, the password is still will be flowing in the network. The attackers are able to obtain the packet contain the username and password and grant access to the service.

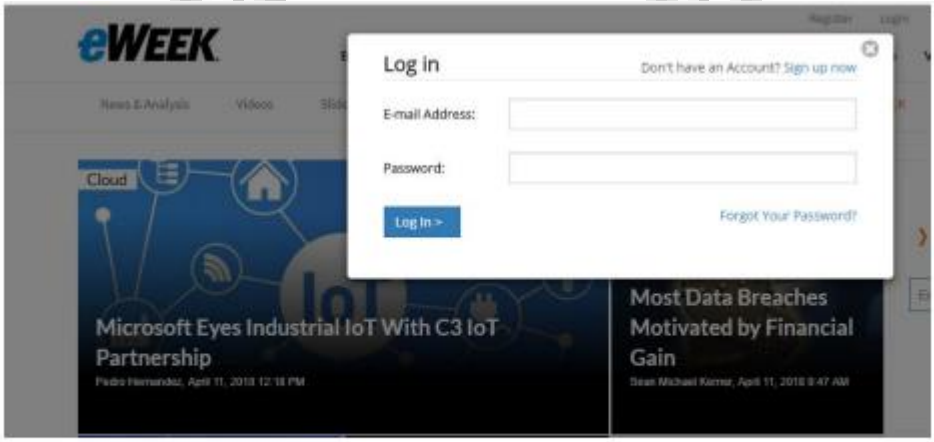


Figure 5-1 Login interface of the existing system

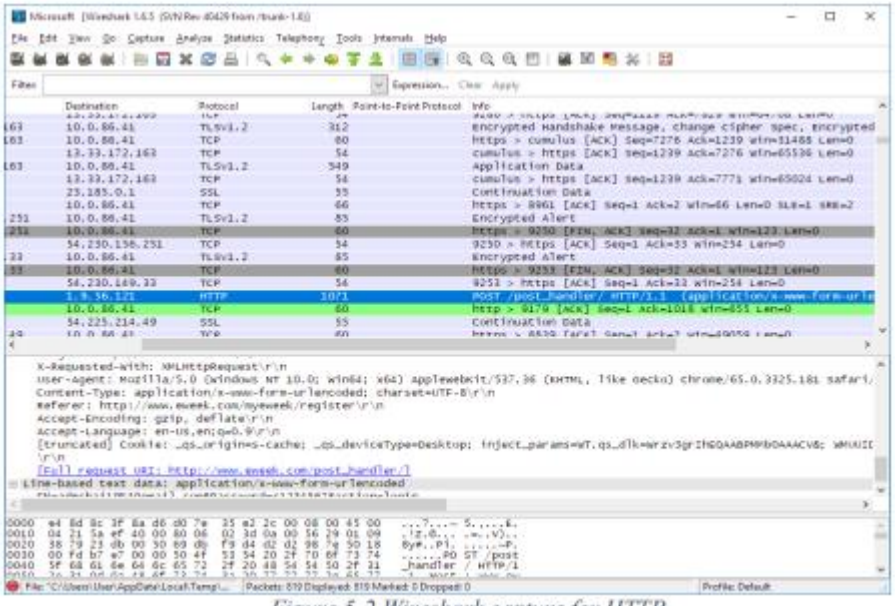


Figure 5-2 Wireshark capture for HTTP

Some of the users also tend to save password using the cookies in the browser. It is danger when the attackers able to retrieve the cookies since they able to get the username and password of the user on the site.

4.2 REASON FOR SELECTION TOOLS

4.2.1 Reason of choosing MongoDB:

MongoDB is a document database built on a scale-out architecture that has become popular with developers of all kinds who are building scalable applications using agile methodologies.

MongoDB was built for people who are building internet and business applications who need to evolve quickly and scale elegantly.

Simply to go further and faster when developing software applications that have to handle data of all sorts in a scalable way.

Thousands of companies like Bosch, Barclays, and Morgan Stanley run their businesses on MongoDB, and use it to handle their most demanding apps in areas like IoT, Gaming, Logistics, Banking, e-Commerce, and Content Management.

MongoDB is a great choice if you need to:

- Represent data with natural clusters and variability over time or in its structure
- Support rapid iterative development.
- Enable collaboration of a large number of teams
- Scale to high levels of read and write traffic.
- Scale your data repository to a massive size.
- Evolve the type of deployment as the business changes.
- Store, manage, and search data with text, geospatial, or time series dimensions.

MongoDB as a company has grown because the number of use cases with these characteristics keep growing.

4.2.2 Reason of choosing VS CODE:

At its heart, Visual Studio Code features a lightning fast source code editor, perfect for day-to-day use. With support for hundreds of languages, VS Code helps you be instantly productive with syntax highlighting, bracket-matching, auto-indentation, box-selection, snippets, and more. Intuitive keyboard shortcuts, easy customization and community-contributed keyboard shortcut mappings let you navigate your code with ease.

For serious coding, you'll often benefit from tools with more code understanding than just blocks of text. Visual Studio Code includes built-in support for IntelliSense code completion, rich semantic code understanding and navigation, and code refactoring.

And when the coding gets tough, the tough get debugging. Debugging is often the one feature that developers miss most in a leaner coding experience, so we made it happen. Visual Studio Code includes an interactive debugger, so you can step through source code, inspect variables, view call stacks, and execute commands in the console.

VS Code also integrates with build and scripting tools to perform common tasks making everyday workflows faster. VS Code has support for Git so you can work with source control without leaving the editor including viewing pending changes diffs.

VS Code includes enriched built-in support for Node.js development with JavaScript and TypeScript, powered by the same underlying technologies that drive Visual Studio. VS Code also includes great tooling for web technologies such as JSX/React, HTML, CSS, SCSS, Less, and JSON

4.2.3 Reason of choosing NODE JS:

Node.js is a cross-platform runtime environment, built on V8, high-performance open-source JavaScript engine. To ensure outstanding performance, Node.js applies event-driven, non-blocking I/O paradigm. In the past years, it gained a lot of popularity in various Node.js development circles.

Node.js really shines in building fast, scalable network applications, offers benefits in performance, faster development, and other perks. Today's requirements for processing and consuming real-time information are paramount, and Node.js is exceptionally fast for multi-user real-time data situations. No surprise, that a lot of startups lean toward it.

Node.js is best suitable for:

- Real-time web applications
- Streaming applications
- Messaging apps
- Chat programs
- Social media apps
- Virtual emulators
- Multiplayer games
- Collaboration tools
- API