JAYPEE INSTITUTE OF INFORMATION TECHNOLOGY, NOIDA, SECTOR-62

WEB TECH AND CYBER SECURITY

SYNOPSIS

AI-POWERED SECURE AUTHENTICATION SYSTEM

SUBMITTED TO:

Dr. SHARDHA PORWAL

BY:

TEAM MEMBERS (B6 BATCH):

- ***SAUMIL GUPTA (22103179)***
- ***TANUSH (22103157)***
- ***KARAN PATHAK (22103176)***
- ***KARTIK GARG (22103158)***

(6th Semester)

TABLE OF CONTENT

1. Problem Statement
2. Solution
3. Flowchart
4. Algorithms
5. Tools and Technologies used
6. Conclusion
7. References

PROBLEM STATEMENT

With the increasing reliance on online platforms for education and communication, ensuring secure authentication for students in AI-powered applications is crucial. Traditional login methods relying solely on passwords are vulnerable to breaches, phishing, and unauthorized access.

This project aims to develop a secure and intelligent authentication system for an AI-powered calculator, meeting, and chatting application for students. The login system will implement Kerberos authentication, hashing, OTP, and location-based verification to enhance security. The location-based authentication will analyze the user's geographical access patterns and trigger extra verification steps (such as OTP or security

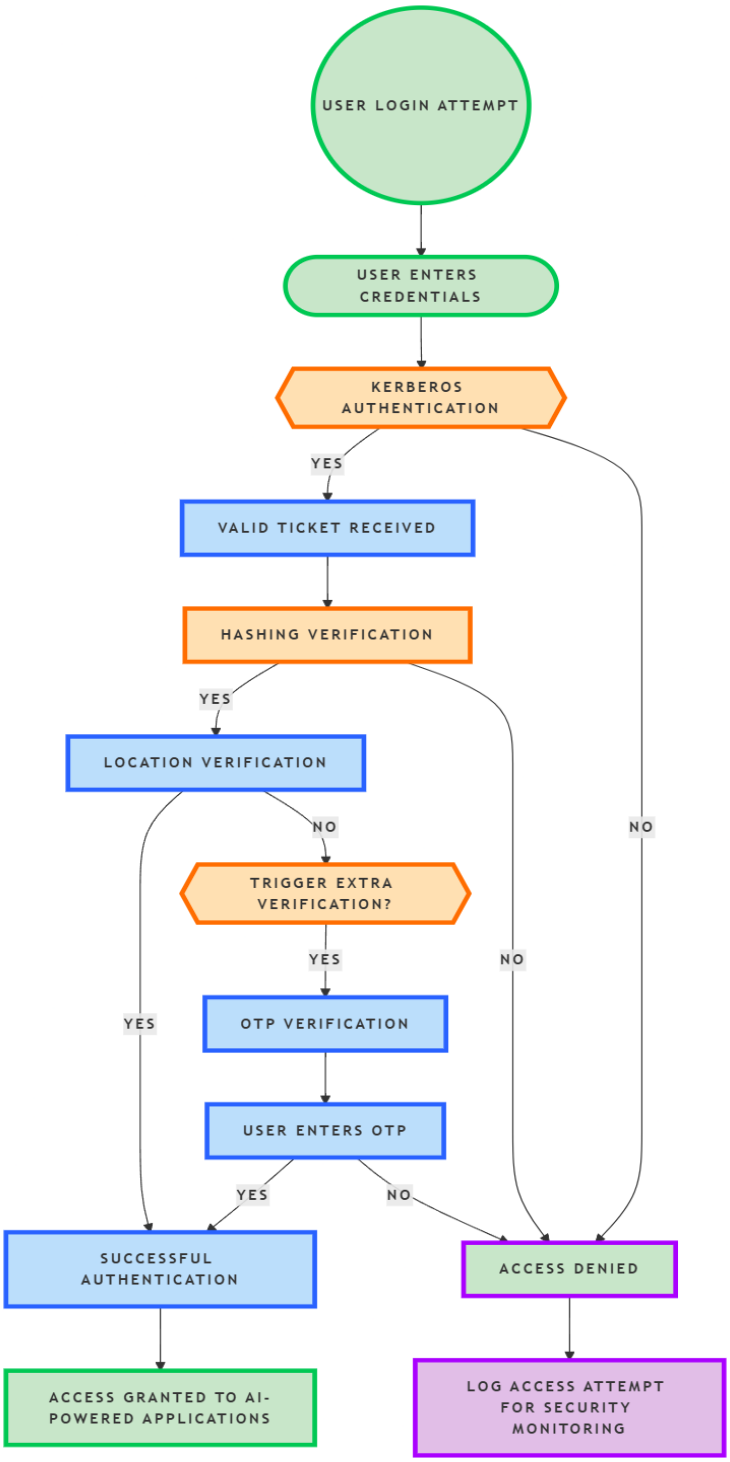
questions) when an attempt is made from an unusual or suspicious location.

By integrating multi-factor authentication and Zero-Knowledge Proof (ZKP) mechanisms, this system seeks to minimize security risks while ensuring a seamless user experience. The solution will protect users against credential theft, unauthorized logins, and location spoofing, making authentication both secure and context-aware

SOLUTION

Our solution integrates robust security protocols and modern web technologies to address fragmented digital services and cybersecurity threats. By employing Kerberos, hashing, OTP, and location detection, we ensure secure, authenticated access to the platform. The chat application, built with the MERN stack and Socket.io, facilitates real-time communication, while Stream.io supports seamless video streaming for online meetings. NextJS delivers an optimized, fast frontend, and the AI-powered calculator offers precise computational support. Together, these technologies form a unified, secure platform that enhances user collaboration and protects sensitive data.

FLOWCHART


USER LOGIN ATTEMPT
USER ENTERS CREDENTIALS
KERBEROS AUTHENTICATION
YES
NO
VALID TICKET RECEIVED
HASHING VERIFICATION
YES
NO
LOCATION VERIFICATION
NO
YES
TRIGGER EXTRA VERIFICATION?
YES
NO
YES
OTP VERIFICATION
USER ENTERS OTP
YES
NO
SUCCESSFUL AUTHENTICATION
ACCESS DENIED
ACCESS GRANTED TO AI-POWERED APPLICATIONS
LOG ACCESS ATTEMPT FOR SECURITY MONITORING

TOOLS AND TECHNOLOGIES USED

- **Kerberos:**
  A network authentication protocol that uses secret-key cryptography to verify user identities through a trusted ticketing system.
  It ensures secure, mutual authentication between clients and servers in a networked environment.
- **Hashing:**
  A method that converts data into a fixed-size string of characters, providing a unique digital fingerprint.
  It guarantees data integrity by detecting any alterations, making it vital for secure storage.
- **OTP (One-Time Password):**
  A temporary, dynamically generated code that enhances security during authentication.
  It minimizes the risk of unauthorized access by ensuring credentials are used only once.
- **Location Detection for Security:**
  A technique to verify user access based on geographical location, adding an extra layer of authentication.
  It helps identify and prevent suspicious login attempts from unrecognized or high-risk regions.
- **MERN Stack:**
  A full-stack development framework combining MongoDB, Express.js, React, and Node.js for robust web applications.
  It enables seamless integration between the frontend and backend, ensuring scalability and efficiency.
- **Socket.io:**
  A library that facilitates real-time, bi-directional communication

between clients and servers.

It is essential for the chat application, providing low-latency and event-driven messaging capabilities.

- **Stream.io:**

  A service designed for real-time video streaming and interactive media content delivery.

  It supports high-quality, scalable video experiences ideal for live online meetings.

- **NextJS:**

  A React framework that offers server-side rendering and static site generation for enhanced performance.

  It improves SEO and user experience by delivering fast, optimized, and scalable web frontends.

ALGORITHMS

- **Kerberos Authentication** (For Secure Login Without Sending Passwords)

  Instead of sending passwords over the internet, Kerberos uses a special ticket system to verify users. When you log in, a trusted server gives you a ticket that proves your identity. This ticket is used instead of your password to log into the app securely. Protects against hackers stealing passwords while they travel across the internet.

- **Hashing** (For Password Protection in the Database)

  When you set a password, it is converted into a secret code (hash) before being saved in the database. Even if a hacker gets into the database, they only see coded versions of passwords. Extra random data (salt) is added to make hacking even harder. Stops hackers from easily figuring out passwords.

- **One-Time Password (OTP)** (For Extra Security at Login)
  If something seems suspicious (like a login from a new device), the system sends a temporary secret code (OTP) to your email or phone. You must enter this code to prove it's really you. The OTP expires quickly, so hackers can't reuse old codes. Even if someone steals your password, they can't log in without the OTP.

- **Location-Based Authentication** (For Detecting Unusual Logins)
  When you try to log in, the system checks where you are. If you're logging in from a new or suspicious location, extra verification (like OTP) is required. Uses your device's GPS or IP address to detect your location. Blocks hackers from logging in from a far-away place.

CONCLUSION

This project successfully integrates an AI-powered calculator, meeting app, and chatting app for students with a robust, multi-layered authentication system. By implementing Kerberos authentication, hashing, OTP verification, and location-based authentication, it ensures a secure

This security framework ensures a balance between strong protection and user convenience. The project can be further expanded by incorporating AI-driven security, blockchain-based authentication, and adaptive authentication techniques.

In conclusion, this project not only provides essential AI-powered tools for students but also establishes a highly secure authentication system that safeguards user data and ensures safe and efficient access to digital educational platforms.

REFERENCES

https://ieeexplore.ieee.org/document/5590521

https://www.ijert.org/research/hash-based-dynamic-password-authentication-mechanism-for-kerberos-environment-IJERTV2IS70115.pdf

https://ieeexplore.ieee.org/document/1592297

https://www.diva-portal.org/smash/get/diva2%3A576463/FULLTEXT01.pdf