MIT-ADT UNIVERSITY
PUNE, INDIA
A leap towards World Class Education

MIT SCHOOL OF COMPUTING

Class : TY-CSF-1
Group Id: 6

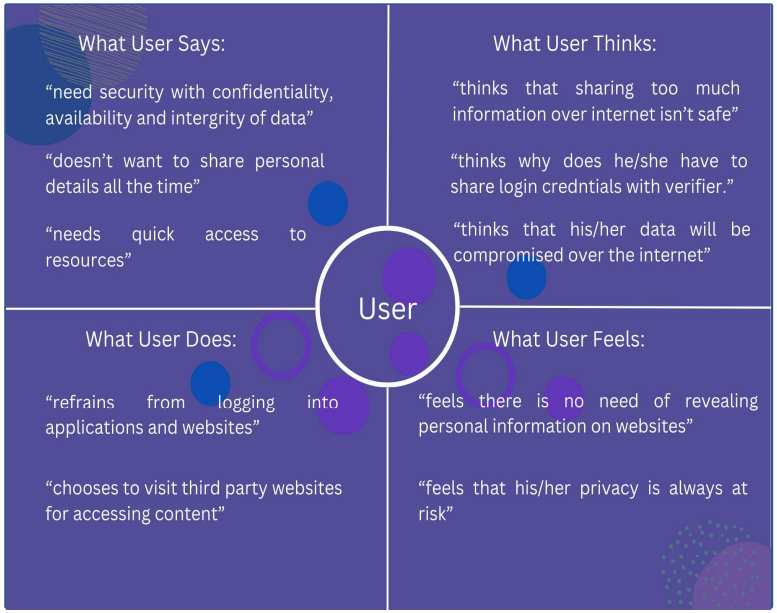
DEPARTMENT OF COMPUTER SCIENCE & ENGINEERING

Zero Knowledge Proof Authentication

Yogesh Thakur, Pradnya Khore, Kaushal Chordiya and Gaurang Sharma

Faculty Guide:

Prof. Smita Gumaste



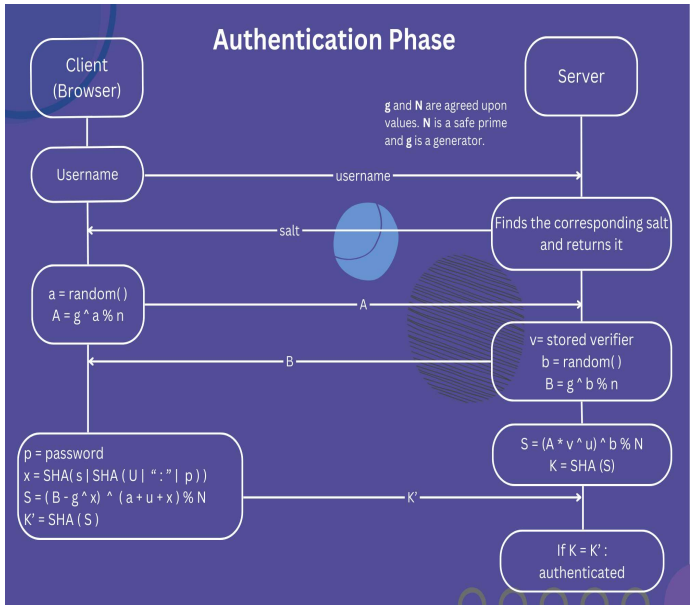
Problem Statement:

Traditional authentication methods, such as passwords and biometrics, expose sensitive information, making them vulnerable to attacks. Zero Knowledge Proof (ZKP) offers a secure alternative by allowing a user to prove knowledge of a secret without revealing the secret itself. This project aims to develop an authentication system using ZKP, ensuring that no sensitive data is transmitted during the authentication process.

Sr. No.	Requirement	Proposed Solution
1.	Authentication	
	Available Solutions - In the traditional solutions that exist, there is always high possibilities of compromisation of personal information.	Proposed Solution - Creating a similar encryption systems that can help users login within minimum possible exposure of personal information.
2.	Compatibility	
	Available Solutions - Traditionally, these systems work only with compatible devices so not all devices support ZKPs and thus are at risk.	Proposed Solutions - We shall be creating a similar system but incorporate an extra layer at the communication level which will overcome the compatibility issues present in various devices.

Proposed Solution:

As a solution we will develop a additional filter to counter the problem of interoperability. One of the major problems with this method is that different systems are not compatible with each other so we will add one extra layer where we will develop a solution to implement ZKP as a mediator between different systems.



Scope:

This method can be implemented in college libraries and ERP system to enhance security and consider privacy of students.