**Enhancing User Authentication and Authorization for E-commerce**

**Project Proposal**

**Background**

The necessity for safe transactions has never been more pressing because e-commerce has become an integral aspect of contemporary life. E-commerce security problems are harming firms severely, both financially and reputationally. More than 30% of all e-commerce websites, from small to major firms, are progressively becoming targets of assaults.

**Step-1: Finding a problem**

Due to the rising usage of e-commerce, there are more cyberattacks and fraudulent activities taking place, which increases the risk of sensitive data being compromised, including login passwords, personal identity information, and financial information. E-commerce platforms must have strong security measures in place to guard against these risks and guarantee the confidentiality of customer data.

Unauthorized access to user accounts is one of the biggest dangers to e-commerce security. To access user accounts, attackers employ a variety of techniques, such as phishing, brute-force attacks, and social engineering. Once a user's account has been compromised, an attacker can use it to carry out a variety of fraudulent acts, including stealing money, making illegal purchases, and even launching new attacks.

User accounts no longer have enough protection against these risks from the typical username-and-password user authentication technique. Users frequently use the same password across numerous platforms, making their accounts vulnerable. Passwords are simple to guess or hack. In order to improve user security, a more sophisticated method to authentication is required.

As a result, a solution to improve user authentication and authorization for e-commerce systems is required. This solution must be safe, simple to use, and adaptable to the demands of diverse users. In order to safeguard user accounts from unwanted access and fraudulent activity, the solution must solve the shortcomings of MFA and security questions and offer a more reliable authentication method.

**Step-2: Method and Solution**

We suggest designing and implementing a safe login system that makes use of multi-factor authentication and security questions in order to address the issues with poor user authentication and authorization in e-commerce. With its suggested login method, e-commerce websites' client-server architecture would be made less vulnerable while also enhancing the security and privacy of online transactions.

Designing a safe login screen that asks users for their credentials—such as usernames and passwords—is the first step in our suggested procedure. To store passwords safely in the database, we will use password encryption methods that use hash algorithms like SHA-256. We'll also put in place a mechanism for managing passwords that will encourage users to pick secure passwords and to change them often.

A multi-factor authentication system will then be put into place, requiring users to present two or more pieces of identity in order to access their accounts. This might contain both something the person holds and something they are aware of, such a security token or a password. The system will be more secure and resistant to unwanted access if it requires more than one factor for authentication.

We'll also use security questions to further strengthen the security of our login process. Users will be prompted to set up security questions as part of the account creation process, and in order to access their accounts, they must provide the proper answers. By doing this, extra protection is added and account access by unauthorized individuals is made more challenging.

We will simulate several potential assaults, such as brute force attacks, password guessing attacks, and phishing attacks, to evaluate the performance of our suggested login method. The efficacy of the system's functioning and the security measures put in place to prevent attacks will next be assessed.

The deployment of a secure login system, as part of our suggested technique for improving user authentication and authorization in e-commerce, is intended to lower the risk of unwanted access, data theft, and damage to computer networks.

**Step-3: Result and Analysis and Outcome Expectation**

The main objective of this project is to develop and deploy a secure login system that uses security questions and multi-factor authentication to improve user authentication and authorization for online transactions. This project's goal is to dramatically lower the danger of illegal access to e-commerce websites, which will protect firms' finances and reputations.

We will first create a secure login system using multi-factor authentication and security questions in order to obtain the desired result. Users must submit various kinds of authentication to the system, such as a password and one-time passcodes delivered to their registered email address or cellphone number. By forcing users to respond to particular questions before using the service, the security questions will create an extra layer of protection against unwanted access.

We will test the login system to make sure it is reliable and safe when it has been created and put into place. To find any potential flaws in the system, we will do penetration testing, vulnerability assessment, and other security testing. Then, we will take the appropriate action to remediate any found vulnerabilities.

The project's last stage will be to examine the findings and assess how well the new login mechanism worked. To assess if the new system has had an effect on lowering the danger of unauthorized access, we will compare the number of successful login attempts made before and after its deployment. By gathering opinions via surveys or user testing, we'll also assess how well users are responding to the new system.

A more secure and user-friendly login system that considerably lowers the danger of illegal access to e-commerce websites is the anticipated result of this project. Users will have more faith in the security of the system by utilizing multi-factor authentication and security questions, which will boost trust and customer satisfaction. A lower chance of financial and reputational harm brought on by security breaches will be advantageous to the company, resulting in more sales and a better reputation for the brand.