

Electronic Products Marketing Store Application Design

Boggula Rajeswari¹, Marri Tanuja² and Sodagudi Suhasini³

¹⁻³Velagapudi Ramakrishna Siddhartha Engineering College/ Information Technology, Vijayawada, India
Email: rajeswari9864@gmail.com, {marritanuja@gmail.com, s.suhasini@vrsiddhartha.ac.in}

Abstract— In the rapidly evolving landscape of online commerce, the development of an e-commerce website that ensures a seamless and satisfying shopping experience for customers is paramount that focuses on addressing the issue of password security and complexity while also considering user-friendliness. Here's a breakdown of the key points that begins by highlighting the importance of security and privacy for individuals using online services. It acknowledges the prevalence of password authentication systems in protecting individual data. It emphasizes the growing significance of password security and authenticity due to factors like information sharing, internet popularity, electronic commerce transactions, and data transfer. The abstract acknowledged the common recommendation for complex password patterns by cybersecurity experts. It points out that users often forget complex passwords, suggesting a usability issue. The paper proposes a unique algorithm for generating strong passwords that are based on user-provided information (words and numbers). The objective is to create passwords that are both strong and memorable in order to provide the security for the website.

Index Terms— password security, Authentication, privacy, password Strength.

I. INTRODUCTION

The necessity of internet security has increased in light of the ever-expanding domain of online applications. Since most financial and business transactions now take place online, using platforms like online banking and e-commerce, information transmission security has become crucial [4]. The possible consequences of information breaches have increased significantly, perhaps leading to large losses. When it comes to protecting digital interactions in the open world of networked settings, user authentication is an essential component. On the other hand, using basic authentication techniques comes with significant drawbacks [1][5]. One such issue is people's propensity to choose readily guessed personal information as passwords, such as their phone number or ID, only for the ease.

In addition, in an attempt to reduce the amount of information that needs to be memorized, users commonly start using the same password across several platforms. The fact that users frequently find it difficult to create passwords that are both easy for them to remember and difficult for attackers to decipher is another important issue. Professionals have developed a number of rules and guidelines to help people choose secure passwords. Yet, intrinsic memory deficits in people are the root cause of many password authentication system flaws [3]. The most secure passwords should, in theory, have maximum entropy and be long sequences of random special characters, but human memory cannot handle that kind of complexity. Human memory is more adept at recalling

information when it comes to words or other commonly used symbols.

Moreover, memory is improved by encoding information in different ways. As such, the password authentication method requires a trade-off [1][2].

Certain passwords, like the names of family members or pets, could be simple to remember, but they are also susceptible to dictionary-based attacks. On the other hand, safe passwords could be hard for hackers to figure out but hard for users to remember. Some individuals choose to create unique passwords for each of their several internet accounts as a response to these issues [8]. Still, keeping track of several passwords may be confusing and time-consuming. Users may turn to writing down their passwords in such circumstances, however this is a risky security practice. Passwords that are written down are more vulnerable to password cracking attempts, which makes it easier for hackers to figure out what they are. The importance of internet security, particularly with regard to user authentication, has been highlighted by the growing domain of online activities and digital transactions [6][7].

In the quest for strong online security, addressing the many problems associated with password security—such as the conflict between rememberability and complexity—remains a complicated and continuous task. So in order to provide security to the E-Commerce website. So, We created a safe website that, by requiring strong credentials, can shield user data from cyber-attacks [5].

II. LITERATURE STUDY

Numerous types of research have been done in the field. Most of the time, academics focused on several approaches to guarantee password strength and create safe e-commerce websites.

[1] Using machine learning techniques, Sony Kuriakose, G Krishna Teja, Sravan Duggi, A Harshel Srivastava, and Venkat Jonnalagadda developed a unique way to assess the strength of passwords. The technique has been shown to be effective in predicting password strength and has the potential to improve the security of online accounts. explains a web application that uses machine learning techniques to analyse password strength in real time. By using different machine learning methods, including Decision Tree, Naive Bayes, Logistic Regression, and Random Forest, the authors hope to improve password security. The project's procedures, such as dataset collecting, preprocessing, model training, and real-time password analysis, are described in the methodology section. The significance of having a labelled dataset with weak, medium, and strong passwords is emphasised by the authors. They train models for password strength detection using machine learning methods, then they employ these models for in-the-moment analysis.

[2] Umar Farooq examines the weaknesses related to passwords and suggests a way to improve security by applying several machine learning techniques. Focuses on the common problem of weak passwords, which are vulnerable to dictionary and brute force assaults. Explains the issue and draws attention to how predictable passwords might be because of common patterns like typing patterns and dictionary terms and phrases. The suggested approach seeks to protect against online threats as well. It may be used to improve the security of web applications and is efficient in real-time password strength assessments. The study makes a contribution by addressing the widespread problem of weak passwords and offering a workable solution that incorporates machine learning methods. Offline threats by requiring users to use secure passwords.

[3] Wanda Li and Jianping Zeng explores the topic of password security, highlighting the common usage of text-based passwords as the main means of authentication. It emphasises the inherent difficulties brought about by people's tendency to use password combinations that are both simple to remember and frequently unsafe. A brief discussion is held about current methods for strengthening password security, such as the use of password meters and more stringent composition guidelines. In addition, the study adds to this unexplored area by introducing a thorough analysis of Leets peak replacements in passwords, covering definition, detection, dictionary construction, and usage. Nevertheless, the study identifies a significant gap in the literature regarding Leets peak, a method of changing password spellings by replacing letters with numbers or other characters.

[4] Zongda Wu, Haiping Zhou, Huxiong Li illustrated the increasing apprehension around the privacy of user behavior disclosure on e-commerce platforms. The emphasis is on limiting the disclosure of users' commodity viewing preferences due to the growing unreliability of the server-side in online commercial activities. Creating a set of fake queries on a reliable client and sending them to the untrusted server-side together with a user's commodity viewing request is the suggested method. This essentially seeks to obscure and bewilder user preferences. A privacy model for user commodity watching services is defined at the beginning of the research. To gauge how well dummy requests conceal and confuse user preferences, it presents ideas like entropy for commodity viewing likelihood and regional distance across commodity categories.

[5] Seyed Hamed, Jafarpour, Azam Andalib stated the importance of client loyalty and happiness in e-commerce is emphasized in the article. It investigates how infrastructure, electronic buying experiences, website quality, and service quality affect customer loyalty. The contributors stress the importance of client retention for the success of e-commerce businesses, pointing out the increased competition in this digital environment. Peter Drucker's customer-oriented approach to business is emphasized, stressing the requirement of comprehending and meeting the wants and desires of customers. The analysis provides strong data regarding the effects of customer-focused businesses, establishing a connection between market share, return on investment, and stock price increase and customer happiness. Now let's talk about electronic loyalty. According to the report, this is the state in which clients are more satisfied, make ongoing purchases, and show resistance to rivals.

III. METHODOLOGY

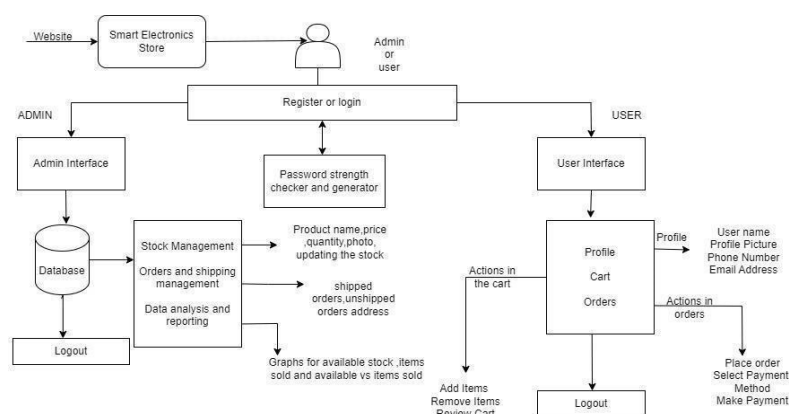


Fig:1 Architecture Diagram

A. Homepage and User Registration

Local The homepage of the website is inviting to new users and asks them to register. Users are required to provide their personal information, including name, email address, and password, after clicking the registration link. Regular expressions are used to assess password strength, and the system uses predetermined criteria to classify passwords as weak, strong, or extremely strong. The user's registration is finished as soon as they provide all required information.

B. User Login and Product Selection

Those who have registered can use their email address and password to access the website. Users may explore and choose electrical devices from a variety of categories after logging in

C. Shopping Cart Management

Select products can be added by users to their shopping carts. Users may check the list of things they have added, change the quantity, and delete products from the basket as needed.

D. Order Placement and Payment

The consumer can continue to the checkout procedure if they are happy with the items they have chosen for their basket. Users choose a payment option and enter shipping information throughout the checkout process. Credit cards may be one of the available payment methods. The order is processed by the system and a confirmation is sent to the user when the transaction is confirmed and payment is made.

E. Admin Panel

Site administrators can use the admin panel, which requires a separate login, to control the backend functions of the website.

F. Stock Management

The electronic product's current stock levels are visible to administrators. They have the power to change the inventory by adding new products and removing old ones.

G. Order and Shipping Management

Orders may be tracked by administrators, who can distinguish between pending and delivered orders. They may update the status of orders as they are processed and have access to shipment information.

H. Data Analysis and Reporting

Tools for assessing product sales data are available in the admin panel. In order to learn which goods are selling well and which may require attention, administrators can create graphical reports and charts.

One of the most crucial issues with password security is determining the strength of the password. There isn't a universally applicable answer, which makes it a difficult problem. The definition of a strong password varies throughout individuals. Regular expressions are an effective tool for text manipulation and search. They can be applied to define patterns in text strings that can be matched. Password security is one of the many applications for regular expressions.

Regular expressions can be used in password security to verify the strength of passwords. A password that is challenging to figure out or crack is considered strong. Strong passwords usually consist of a combination of capital and lowercase letters, numbers, and symbols, and are at least eight characters long.

Proposed algorithm

A straight forward approach for determining the strength of a password using a regular expression is as follows:

1. Establish a regular expression pattern that secure passwords ought to adhere to.
2. Incorporate the password into the regular expression pattern.
3. A strong password is one that satisfies the regular expression pattern.
4. The password is weak in other aspects.

The standard algorithm for the regular expression for checking password strength:

$$(?!^\{8,\}\$)(?=.*[a-z])(?=.*[A-Z])(?=.*[0-9])(?=.*[!@#\$%^&*()])$$

Explanation of each component:

- $(?!^\{8,\}\$)$: This part guarantees that the password consists of a minimum of eight characters.
- $(?=.*[a-z])$: This part makes assured that the password consists of a minimum of one lowercase letter.
- $(?=.*[A-Z])$: Having at least one capital letter in the password is ensured by this component.
- $(?=.*[0-9])$: This part makes sure the password has no less than of one digit.
- $(?=.*[!@#\$%^&*()])$: At least one special character must be present in the password, according to this component.

The following formula can be used to determine the password strength using regular expressions.

password strength = (password length + number_of_uppercase_letters + number_of_lowercase_letters + number_of_digits + number_of_special_characters) / 5

A higher number denotes a stronger password. The password strength value runs from 0 to 1. A strong password is often defined as one with a score of 0.8 or above.

IV. RESULTS AND OBSERVATIONS

A. The following shows the step wise result of our proposed system.

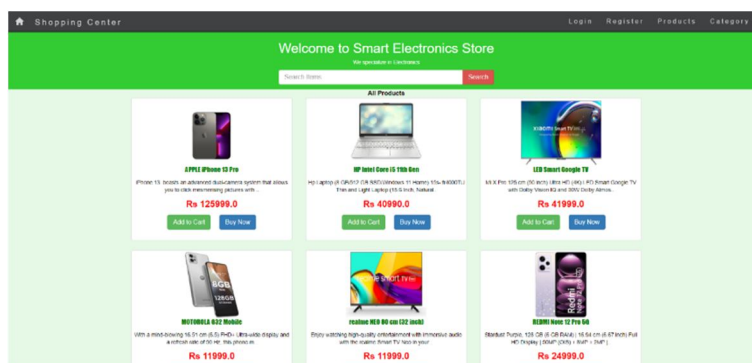


Fig:2 Home page of the website

At the time of registration, the password strength analysis is done and categorised the password as very weak, weak, strong, or very strong

Fig:3 Registration page.

Fig:4 Very Weak Password.

Fig:5 Weak password.

Fig:4 User entered password is detected as weak which is indicated by orange colour bar.

Fig: 5 User entered password is detected as Very weak which is indicated by red colour bar.

Fig:6 Strong password.

Fig:7 Very Strong password.

Fig: 6 User entered password is detected as Strong which is indicated by Light green colour bar.

Fig: 7 User entered password is detected as Very strong which is indicated by Dark green colour bar.

B. Data Analysis and Reporting

In Administrators can evaluate stock availability and products sold by using graphical data representations in the admin interface. This is made possible by separate graphs showing the availability of stock and each item sold separately, as well as a comparative graph showing the link between the two. This allows for effective and data-driven decision-making.

Fig:8 The graph shows the no of items of each product available in the electronic store

Fig: 9 The graph shows the no of items of each product sold in the store to the customres.

Fig:10 The graph shows the amount of stock available vs number of items sold.

Fig: 11 The graph shows the metrics distribution of the proposed work.

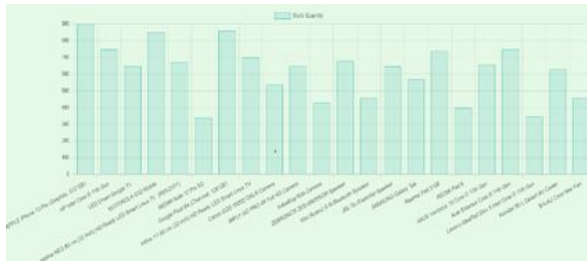


Fig: 8 Stock Available

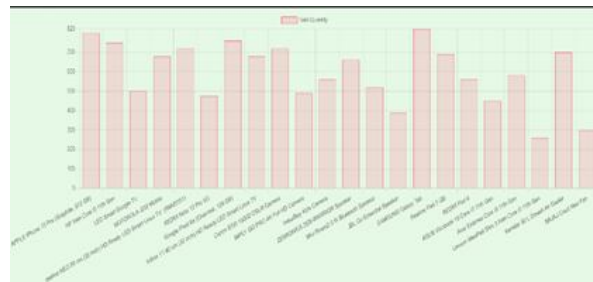


Fig:9 Items sold.

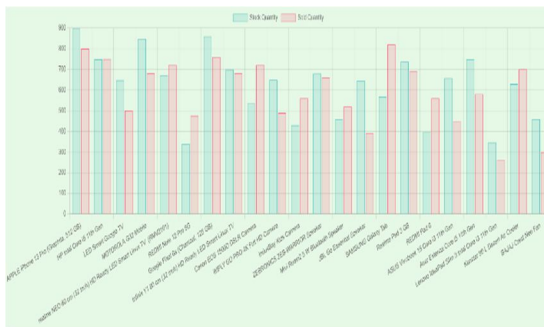


Fig:10 Stock available vs Items sold.

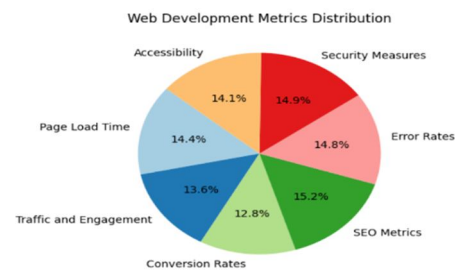


Fig:11 Metrics Distribution Graph.

V. CONCLUSION

In conclusion, building a secure e-commerce website through a thorough assessment of the validity of credentials supplied by users is not only a best practice, but also a need for safeguarding the interests of your business and your clients' trust. The importance of having a robust authentication system cannot be overstated in a time when cyber dangers are always evolving and the use of online commerce is becoming more and more common. By implementing stringent credential strength checks, you may protect your website from potential hacks and demonstrate your concern for the security of critical customer data. A strong authentication system protects user data integrity and confidentiality by acting as a strong deterrent to fraudulent behavior, unauthorized access, and data breaches. By increasing customer trust, a secure e-commerce platform also promotes enduring relationships and repeat business. It's clear that you respect their privacy and security, and it might do wonders for your standing and competitiveness in the market.

Ultimately, the cost of ignoring thorough credential strength checks can sometimes be substantially more than the cost of using them. As technology advances and cyberattacks get more complex, taking proactive steps to protect your e-commerce website and your customers is essential. Your company's success in the contemporary digital world is closely linked to the efficacy of your security measures. The development of a secure e-commerce website with extensive credential checks is therefore not only prudent, but also strategically necessary for success in the online market.

VI. FUTURE SCOPE

It is anticipated that authentication technologies will continue to advance. Biometrics, multifactor authentication (MFA), and adaptive authentication systems will proliferate in order to boost security without compromising user experience. As cyberthreats evolve, user awareness and education will become increasingly important. Companies will invest financial resources in educating customers about safe practices, which might lead to opportunities for cybersecurity education and training programs. As these laws become more stringent, there will be a greater demand for compliance experts and technology that helps e-commerce businesses comply with data protection and privacy rules (such as GDPR, CCPA). Businesses that prioritize and publicize their strong security protocols will have an advantage over competitors. Businesses engage in security as a marketing tactic to attract clients, in addition to security investments for protection.

REFERENCES

- [1] Grassi P.A., Garcia M., Fenton J. NIST Special Publication 800–63–3 Digital Identity Guidelines National Institute of Standards and Technology, Los Altos, CA (2020)
- [2] Zhou Huan, Liu Qixu, Cui Xiang, Zhang Fangjiao. Research on Targeted Password Guessing Using Neural Networks. *Journal of Cyber Security*. 2018. 3(5): p. 25-37.
- [3] M. Weir, S. Aggarwal, B. d. Medeiros and B. Glodek, "Password Cracking Using Probabilistic Context-Free Grammars," 2009 30th IEEE Symposium on Security and Privacy, Berkeley, CA, 2009, pp. 391-405, doi: 10.1109/SP.2009.8. [CrossRef]
- [4] J. Blocki, B. Harsha and S. Zhou, "On the Economics of Offline Password Cracking," 2018 IEEE Symposium on Security and Privacy (SP), San Francisco, CA, 2018, pp. 853-871, doi: 10.1109/SP.2018.00009. [CrossRef]
- [5] Melicher, W., et al., Better passwords through science (and neural networks). ; 2017. 42(4).
- [6] A LeCun, Y., Y. Bengio, and G. Hinton, Deep learning. *Nature*, 2015. 521(7553): pp. 436-444. [CrossRef]
- [7] Richard Shay, Saranga Komanduri, Adam L Durity, Phillip Seyoung Huh, Michelle L Mazurek, Sean M Segreti, Blase Ur, Lujo Bauer, Nicolas Christin, and Lorrie Faith Cranor. Designing password policies for strength and usability. *ACM Transactions on Information and System Security (TISSEC)*, 18(4): 13, 2016.
- [8] Cormac Herley and Paul Van Oorschot. A research agenda acknowledging the persistence of passwords. *IEEE Security & Privacy*, 10(1):28-36, 2011.