IJIRCCE

e-ISSN: 2320-9801 | p-ISSN: 2320-9798

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

Volume 12, Issue 3, March 2024

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 8.379

International Journal of Innovative Research in Computer and Communication Engineering

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.379 | Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 3, March 2024 ||

| DOI: 10.15680/IJIRCCE.2024.1203023 |

Securing Digital Vaults: Advanced Tactics for Protecting Personal Information Online

[1] Khush Shah, [2] Raghavendra R

[1] PG Student, Department of MSc CS-IT, Jain(Deemed-to-be University), Bangalore, India.

[2]Assistant Professor, School of CS & IT, Jain(Deemed-to-be University), Bangalore, India.

ABSTRACT: Abstract: This research explores the critical significance of robust password security in protecting personal and sensitive data on digital platforms. It emphasizes key factors contributing to password vulnerability, including length, structure, recycling, and irregular updates. The paper stresses the paramount importance of creating strong, unique passwords while avoiding personal details and refraining from password reuse. Additionally, it discusses advanced techniques like the Honeyword technique and HoneyEncryption to enhance password security. User education on mobile authentication and preventing shoulder-surfing attacks is highlighted. Privacy implications related to sensitive personal data usage are also examined. Moreover, the potential benefits of graphical passwords in improving security and user convenience are explored. Ultimately, this paper provides valuable insights and practical recommendations for individuals and organizations to prioritize and strengthen password security, thus safeguarding their personal information online.

KEYWORDS: Password security, Honeyword technique, HoneyEncryption, Shoulder-surfing prevention, Privacy considerations, Sensitive personal data, Graphical passwords, Security enhancement.

I. INTRODUCTION

The pervasive integration of information technology, particularly catalyzed by the advent of mobile Internet and e-commerce, has revolutionized the fabric of modern living. Alongside this digital transformation, concerns pertaining to information security have surged, taking center stage in the domain of the Internet. As a stalwart bastion in the realm of user information protection, password authentication reigns supreme and finds widespread adoption among major Internet service providers [1].

This investigation embarks on an intricate exploration of the precarious landscape of mobile authentication, specifically scrutinizing the vulnerabilities inherent in password exposure during shoulder-surfing incidents. By dissecting the strategies employed by adversaries aiming to decipher passwords through clandestine observation [2], this study uncovers crucial insights into the depth of password susceptibility. At its core, this inquiry underscores the pivotal role of forging robust passwords as a linchpin in fortifying personal data integrity and preserving account sanctity [3].

Seeking to illuminate prevailing vulnerabilities in password practices, this research endeavors to gauge users' apprehensions concerning password strength, shedding light on the prevalent concerns and areas warranting immediate attention [3]. Diving deeper, this exploration traverses a diverse array of methodologies employed to assess password robustness within authentication frameworks. It confronts the prevalent trend where users, driven by convenience, often opt for simplicity in crafting their passwords, thereby inadvertently exposing themselves to security risks. As a countermeasure, Internet service providers have proactively instituted a Password Strength Metric (PSM) framework, poised to offer guidance and encourage the creation of resilient passwords, effectively mitigating inherent security vulnerabilities [4]

Steering away from conventional text-based schemes, the proposal of graphical password systems emerges as a compelling alternative, leveraging the human brain's innate capacity for visual memory. Through intuitive graphical patterns, users bypass the need for grappling with lengthy character sequences, leading to heightened security levels vis-à-vis their text-based counterparts [5].

Moreover, the Internet's darker facets—encompassing perils like spam, malware proliferation, hacking exploits, phishing attempts, and insidious invasions of privacy—accentuate the acute necessity of fortifying user data. Techniques such as Honeyencryption are introduced as formidable fortifications, rendering pilfered passwords virtually

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.379 | Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 3, March 2024 ||

| DOI: 10.15680/IJIRCCE.2024.1203023 |

irretrievable. This study's overarching ambition encompasses a holistic fortification of password security by integrating multifaceted elements including honeywords, Honeyencryption, and distributed security mechanisms. The paper will delve into various key aspects, including:

A. BACKGROUND

The pervasive integration of information technology, particularly catalyzed by the advent of mobile Internet and e-commerce, has transformed modern living significantly. With the exponential growth of digital interactions, concerns surrounding information security have become increasingly prominent. Among the various security measures, password authentication has emerged as a cornerstone in protecting user data across online platforms.

B. MOTIVATION

The motivation behind this investigation stems from the escalating importance of understanding and addressing vulnerabilities in mobile authentication, particularly concerning password exposure during shoulder-surfing incidents. As more aspects of daily life transition to digital platforms, the need to safeguard personal information from malicious actors becomes paramount. By delving into the strategies employed by adversaries to exploit password vulnerabilities, this study aims to shed light on the depth of the issue and propose effective countermeasures.

C. OBJECTIVE

The primary objective of this research is to comprehensively analyze the landscape of password security, with a focus on mobile authentication and the vulnerabilities associated with password exposure. By assessing user apprehensions and prevailing trends in password practices, the study seeks to identify areas requiring immediate attention and propose practical solutions. Furthermore, the objective encompasses exploring alternative authentication methods, such as graphical password systems, and evaluating their efficacy in enhancing security while maintaining user convenience. Additionally, the research aims to investigate the effectiveness of proactive measures, including Password Strength Metric (PSM) frameworks, in guiding users towards creating stronger passwords. Moreover, the study intends to examine the potential of advanced security techniques like Honeyencryption to mitigate the risks associated with password theft. By synthesizing these findings, the objective is to contribute to the development of comprehensive strategies for fortifying password security in the digital landscape, ultimately safeguarding personal information and enhancing user trust in online platforms. Furthermore, the research seeks to disseminate its findings through academic publications and industry collaborations to foster broader awareness and adoption of robust password security practices. The main objectives of this research are outlined as follows:

1. **Comprehensive Analysis:** Conduct a thorough examination of password security, focusing on mobile authentication and vulnerabilities related to password exposure.
2. **User Assessment:** Assess user apprehensions and prevalent trends in password practices to identify areas requiring immediate attention.
3. **Solution Proposals:** Develop practical solutions to address identified vulnerabilities and enhance password security.
4. **Exploration of Alternatives:** Explore alternative authentication methods, such as graphical password systems, to evaluate their effectiveness in bolstering security while maintaining user convenience.
5. **Evaluation of Proactive Measures:** Investigate the effectiveness of proactive measures, including Password Strength Metric (PSM) frameworks, in guiding users towards creating stronger passwords.
6. **Advanced Security Techniques:** Examine the potential of advanced security techniques like Honeyencryption to mitigate risks associated with password theft.
7. **Synthesis of Findings:** Synthesize research findings to develop comprehensive strategies for fortifying password security in the digital landscape.
8. **Dissemination of Results:** Share research findings through academic publications and industry collaborations to increase awareness and adoption of robust password security practices.

By pursuing these objectives, this research seeks to contribute to the advancement of password security practices in the digital realm, offering more effective and user-friendly approaches to safeguarding personal information. By enhancing the understanding of password vulnerabilities and proposing practical solutions, this effort aims to bolster online security measures and foster greater trust among users in their digital interactions. Ultimately, the research strives to promote a safer online environment, thereby supporting broader initiatives aimed at protecting user privacy and maintaining the integrity of digital platforms.

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.379 | Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 3, March 2024 ||

| DOI: 10.15680/IJIRCCE.2024.1203023 |

II. LITERATURE SURVEY

Password security plays a pivotal role in ensuring data privacy and protecting individuals' online accounts and sensitive information. Traditional methods of password authentication, such as alphanumeric passwords, have long been the primary means of securing digital assets. However, these methods are increasingly vulnerable to sophisticated cyber threats, including brute-force attacks and phishing scams. The advent of biometric authentication and advanced encryption techniques presents new opportunities to enhance password security and mitigate these risks. This literature review explores recent research and developments in biometric authentication and encryption technologies, with a specific focus on their application in bolstering password security. By examining advancements in these areas, this review aims to provide insights into potential strategies for improving password security measures and safeguarding user data in the digital age.

A. [1] "Behaviours of Unwarranted Password Identification via Shoulder-Surfing during Mobile Authentication" by Lina Zhou, Kanlun Wang, Jianwei Lai, and Dongsong Zhang - Presented at the 2021 IEEE International Conference on Intelligence and Security Informatics (ISI)

This meticulous study meticulously examines the vulnerability of password-based mobile user authentication to the pernicious threat of shoulder-surfing attacks. These surreptitious attacks harbor the potential to compromise the sanctity of mobile devices or applications by illicitly accessing them. By meticulously dissecting the methodologies and intricacies involved in unraveling passwords through shoulder-surfing, encompassing varied observation distances and multiple attempts, this research strives to unveil the nuanced strategies and dynamics that govern password identification behaviors. The resultant insights aim not only to fortify the security of user passwords but also to refine the very fabric of mobile authentication methodologies.

The central aspiration of this investigation is twofold: to fortify user password security and to augment the design of mobile authentication techniques. These revelations stand as a beacon to heighten user awareness regarding the multifaceted security risks entrenched within password-based mobile authentication. Furthermore, they serve as a catalyst for pioneering the development of anti-shoulder-surfing authentication approaches, aiming to erect robust defenses against these insidious intrusions.

In light of the ubiquitous utilization of passwords within mobile applications and their susceptibility to a panoply of threats, including the stealthy incursions of shoulder-surfing attacks, this research diligently endeavors to address lacunae existing within empirical studies. While prior research has predominantly focused on comparative analyses involving various permutations of PIN and pattern lock, PIN and ForcePIN, or alphanumeric and graphical passwords, empirical evidence underscores an alarming reality. Replicating low-security passwords typically demands adversaries to observe a login attempt more than three times on average, with the complexity of high-security passwords demanding an even greater number of attempts.

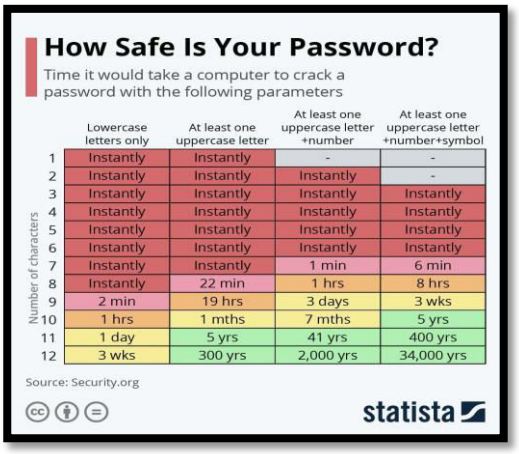

Fig. 1. How safe is your password?

B. [1] "Level of Password Vulnerability" by Indira Mannuela, Michael, Maria Susan Anggreainy, and Jessy Putri - Presented at the 2021 1st International Conference on Computer Science and Artificial Intelligence (ICCSAI)

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.379 | Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 3, March 2024 ||

| DOI: 10.15680/IJIRCCE.2024.1203023 |

This study places paramount importance on password security, recognizing it as an integral component within security technologies and the most widely adopted authentication method. To gauge the current vulnerability of user passwords, the study investigates password reusability and the frequency of password changes, identifying them as pivotal facets of password security. Parameters such as password length, composition, reuse frequency, and regular changes significantly influence password security, with shorter passwords being prone to easier guessing while longer ones fortify defenses against potential attackers. Despite prevalent security concerns, passwords, in use for over half a century, persist in maintaining their relevance and foresee continued utilization in the future.

Notably, findings from the study reveal that 61 percent of participants rely on memory for password recall. While biometric sensors offer enhanced security measures, they come with their own set of challenges. Alarmingly, 43 percent of users tend to reuse passwords or make minor alterations, potentially leading to financial losses, stress, and embarrassment. Addressing online attacks targeting passwords, the study distinguishes between live system estimation and offline attack models, involving the theft of hashed password files.

Employing qualitative methodologies, particularly survey research, this study quantitatively describes the populace's perceptions regarding password vulnerability. It emphasizes the critical role of authentication in accessing online accounts and upholding information security. Additionally, it delves into various authentication categories such as knowledge-based, biometrics, token-based authentication, and two-way authentication. It highlights Gmail's extensive user base of 1.8 billion globally, underscoring the prevalence of password leaks and theft incidents.

C. [2] "A Password Strength Evaluation Algorithm based on Sensitive Personal Information" by Xueqing Li, Yiming Qin, and Ding Yong - Presented at the 2020 IEEE 19th International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom).

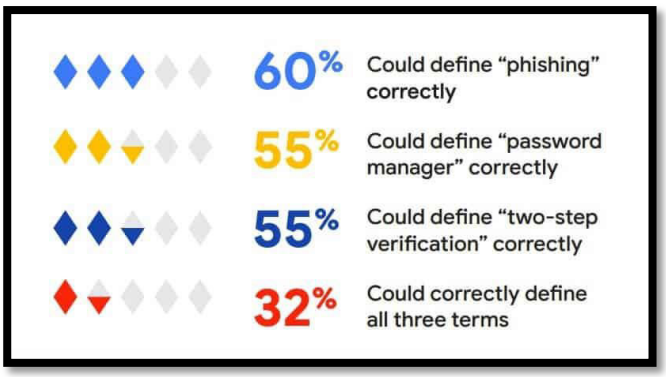

Fig. 2. Password statistics

Conventional password strength evaluation methods, susceptible to social engineering attacks, encounter vulnerabilities. This paper introduces an innovative approach to password strength evaluation anchored in sensitive personal information. Comprising three stages—pre-processing, prediction dictionary generation, and password strength evaluation—the method scrutinizes the incorporation of users' personal information within passwords.

The proposed methodology leverages structure segmentation and bidirectional matching algorithms to investigate the integration of personal information into user passwords. It introduces a sensitivity personal information coverage evaluation function, illustrating the correlation between users' passwords and their personal information.

Existing methodologies, including rule-based evaluation, pattern detection-based evaluation, and attack algorithm-based evaluation, have been critiqued to enhance user password security. While exhibiting varying degrees of rigor and efficiency, these methodologies often rely on subjective weight assignments, presenting limitations. This paper introduces an innovative evaluation method aiming for precise password strength assessment, a critical factor in bolstering password security.

D. [3] "The Security Analysis of Graphical Passwords" by Wei Hu, Xiaoping Wu, Guoheng Wei - Presented at the 2010 International Conference on Communications and Intelligence Information Security

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.379 | Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 3, March 2024 ||

| DOI: 10.15680/IJIRCCE.2024.1203023 |

Graphical passwords, emerging as an alternative to text-based authentication methods, boast ease of memorization and reduced user effort. This paper undertakes a comprehensive examination of diverse graphical password authentication schemes, assessing their security based on predetermined criteria. The conclusions drawn from this analysis affirm the superior memorability and security of graphical passwords compared to textual counterparts. These graphical schemes exhibit heightened resilience against major password attacks.

Categorized into recognition-based and recall-based techniques, graphical password authentication methods offer distinctive user interaction paradigms. Notable schemes under scrutiny include PassFaces and Pass-Objects. PassFaces, crafted by Real User Corporation, prompts users to select specific human faces during registration, necessitating correct identification for authentication. Conversely, Pass-Objects, developed by Sobrado and Birget, involves selecting faces from a grid for authentication purposes.

E. [4] "Strengthening Password Security through Honeyword and HoneyEncryption Technique" by Mrs. Vasundhara R. Pagar and Mrs. Rohini G. Pise - Presented at the International Conference on Trends in Electronics and Informatics 2017

Honeyword and Honeyencryption techniques serve as robust tools fortifying password security. Honeywords, pseudo passwords stored alongside authentic ones, act as decoys to confound attackers. Simultaneously, Honeyencryption bolsters security by furnishing misleading or false plaintext during password decryption, safeguarding websites against breaches stemming from weak passwords. These techniques play instrumental roles in securing online communication, thwarting the misuse of user financial and personal data by malevolent attackers.

This paper accentuates the necessity of deploying Honeywords in tandem with other authentication mechanisms to fortify online services against theft or misuse. Leveraging Honeywords to mislead attackers by injecting spurious passwords into databases, Honeyencryption encrypts passwords, rendering post-theft recovery virtually infeasible.

HoneyEncryption strategically employs Distribution-transforming encoders (DTE) on passwords to derive seed space, subsequently encrypting it using a key. At the core of this approach lies distributed security, with Honeychecker interfacing with the primary authentication server to authenticate user credentials. After three unsuccessful attempts, the account automatically locks, and genuine users are promptly notified.

F. From [6] "Behaviors of Unwarranted Password Identification via Shoulder-Surfing during Mobile Authentication" by Lina Zhou, Kanlun Wang, Jianwei Lai, and Dongsong Zhang (2021):

The paper likely investigates the vulnerabilities of mobile authentication to shoulder-surfing attacks, where attackers obtain passwords by observing users.
It may explore the various tactics and behaviors employed by attackers during shoulder-surfing incidents to identify passwords.
Possible findings could include insights into common patterns or strategies used by attackers and recommendations for mitigating the risks of shoulder-surfing attacks in mobile authentication systems.

G. From [7] "Level of Password Vulnerability" by Indira Mannuela, Jessy Putri, Michael, and Maria Susan Anggreainy (2021):

The paper likely assesses the overall vulnerability of passwords in various contexts, such as online accounts or authentication systems.
It may analyze factors contributing to password vulnerability, such as password complexity, reuse, and exposure to phishing attacks.
Possible outcomes could include a quantitative or qualitative assessment of the level of vulnerability across different password types or user behaviors, along with recommendations for improving password security.

H. From [8] "A Password Strength Evaluation Algorithm based on Sensitive Personal Information" by Xinchun Cu, Ding Yong, Xueqing Li, and Yiming Qin (2020):

The paper likely proposes an algorithm or methodology for evaluating password strength based on sensitive personal information.
It may introduce novel techniques for incorporating personalized or context-specific data into password strength

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.379 | Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 3, March 2024 ||

| DOI: 10.15680/IJIRCCE.2024.1203023 |

assessments.
Possible contributions could include the development of a robust algorithm for assessing password strength that considers individual user characteristics and potential security risks.

I. From [9] "The Security Analysis of Graphical Passwords" by Wei Hu, Xiaoping Wu, and Guoheng Wei (2010):

The paper likely provides a comprehensive analysis of the security implications of graphical passwords.
It may evaluate the strengths and weaknesses of graphical password systems compared to traditional text-based passwords.
Possible findings could include insights into the susceptibility of graphical passwords to various attacks, such as shoulder-surfing or pattern analysis, and recommendations for enhancing their security.

J. From [10] "Strengthening Password Security through Honeyword and HoneyEncryption Technique" by Mrs. Vasundhara R. Pagar and Mrs. Rohini G. Pise (2017):

The paper proposes the use of Honeywords and HoneyEncryption techniques to enhance password security.
It likely discusses the implementation details and effectiveness of these techniques in protecting against password breaches and unauthorized access.
Possible contributions could include insights into the practical applications of Honeywords and HoneyEncryption in real-world scenarios and their potential impact on password security practices.

III. METHODOLOGY

Passwords, often the initial layer of protection against unauthorized access, serve as a fundamental validation of identity, ensuring that individuals seeking entry are the rightful owners of their respective accounts or systems. However, the vulnerability of a weak password can serve as a gateway for attackers, risking the compromise of personal information, financial assets, and critical corporate data.

To bolster password security, comprehending the array of techniques employed by malicious entities becomes imperative. Tactics like brute force attacks, dictionary attacks, and password sniffing capitalize on the weaknesses inherent in weak passwords, enabling unauthorized access.

Moreover, safeguarding against these threats entails exploring multifaceted approaches and innovative strategies. Advancements in authentication technologies, such as biometrics, token-based systems, and multi-factor authentication, extend security measures beyond traditional password-based methods. Additionally, proactive measures like scoring algorithms, graphical passwords, honeywords, and encryption mechanisms fortify defenses against unauthorized access and mitigate risks even in cases of password compromise.

Beyond mere password creation, educating users on best practices and the importance of robust password hygiene emerges as a crucial aspect of fortifying overall security measures. Regularly updating passwords, avoiding common or easily guessable phrases, and utilizing multi-factor authentication add layers of protection.

In essence, fortifying password security involves a multi-faceted approach encompassing technological advancements, user education, and the implementation of innovative strategies to create a robust defense against unauthorized access.

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.379 | Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 3, March 2024 ||

| DOI: 10.15680/IJIRCCE.2024.1203023 |

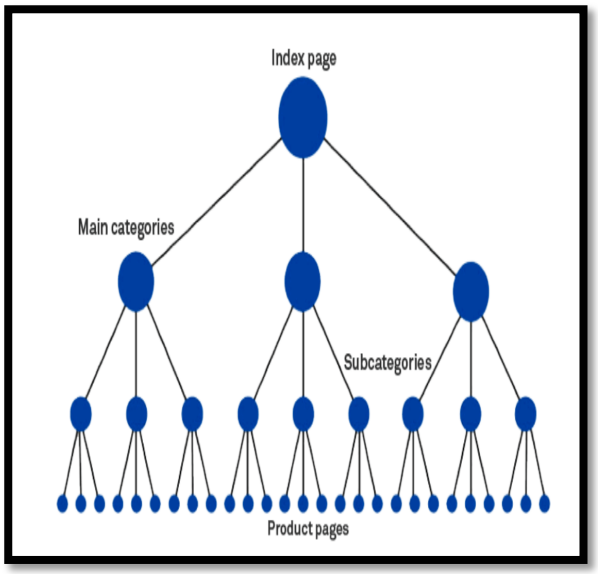

Fig. 3. Scoring algorithm

Moreover, the evolution of authentication technologies, such as biometrics, token-based systems, and two-factor authentication, significantly augments the security landscape. These innovations transcend traditional password-based authentication and complement strategies like scoring algorithms, graphical passwords, honeywords, and encryption mechanisms. The integration of these technologies provides an extra layer of defense against unauthorized access, ensuring a more robust shield even if passwords are compromised.

1. Scoring Algorithm - A Detailed Methodology:
The scoring algorithm, a meticulous methodology for assessing password strength by incorporating sensitive personal information, operates through a systematic process to curate password recommendations and ascertain their robustness [3].

i. **Collection of Personal Information:** This methodology initiates by gathering sensitive personal details from users, including their name, birthdate, or other pertinent information. This data serves as the foundation for crafting personalized password suggestions, catering specifically to each user's contextual requirements.
ii. **Password Generation:** Leveraging the gathered personal information, the algorithm employs predefined rules and heuristic mechanisms to generate a diverse array of password candidates. These rules may entail combining personal data with additional characters, symbols, or variations to create intricate and diverse passwords.
iii. **Scoring Algorithm Assessment:** The generated password candidates undergo evaluation via a scoring algorithm that takes into account several critical factors like password length, complexity, uniqueness, and the integration of personal information. Scores are assigned to each password candidate, quantifying their strength based on these pivotal criteria.
iv. **Strength Assessment:** Following the scoring process, the methodology proceeds to evaluate the strength of each password against predefined criteria. This evaluation may involve establishing minimum score thresholds or comparisons with recognized password strength standards, determining whether the generated passwords meet the desired level of robustness.
v. **User Feedback and Recommendations:** A significant aspect of this methodology lies in providing comprehensive feedback to users regarding the strength of their passwords. Users receive detailed information about the strengths and weaknesses of their generated passwords, along with suggestions for improvements or alternative approaches.

This comprehensive methodology aims to elevate password robustness by harnessing sensitive personal information. Through a systematic assessment, it facilitates the generation of stronger, more secure, and personalized passwords, aligning precisely with individual user profiles and preferences.

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.379 | Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 3, March 2024 ||

| DOI: 10.15680/IJIRCCE.2024.1203023 |

2. Exploration of Graphical Passwords: A Comprehensive Analysis
Graphical passwords, utilizing images, patterns, or symbols instead of conventional text-based credentials, represent a dynamic field of study aiming to bolster password security. This investigative endeavor delves into evaluating the effectiveness of graphical passwords, emphasizing aspects like usability, memorability, and resilience against diverse attacks, encompassing shoulder-surfing and dictionary attacks [4].

i. **Selection and Diversification of Graphical Password Schemes:** The methodology initiates by meticulously selecting a range of graphical password schemes for thorough examination. This assortment may encompass prevalent approaches such as recognition-based, recall-based, or hybrid methods, each showcasing distinct attributes and security paradigms.
ii. **Identification and Assessment of Vulnerabilities:** An essential facet involves scrutinizing potential attack vectors that could potentially compromise the integrity of the chosen graphical password schemes. This analysis encompasses threats like shoulder-surfing, smudge attacks, brute-force attempts, and known vulnerabilities inherent in graphical password systems.
iii. **Scenario Development for Rigorous Testing:** Based on identified vulnerabilities, the methodology constructs an array of simulated attack scenarios. These diverse scenarios aim to assess the susceptibility of various graphical password schemes to a spectrum of attacks, thus discerning the efficacy and resilience of each scheme under different threat landscapes.
iv. **Structured Experimentation and Implementation:** The methodology meticulously designs and executes experiments to rigorously evaluate the selected graphical password schemes within defined attack scenarios. This phase might entail the establishment of controlled environments, participant recruitment, and precise instructions for password creation and authentication utilizing graphical schemes.
v. **Data Collection and Multifaceted Analysis:** Throughout the experimental phase, a comprehensive array of metrics is meticulously gathered, including authentication success rates, authentication timing, and detailed user feedback on both usability and security aspects. The collated data is subjected to in-depth analysis to ascertain the strengths, weaknesses, and idiosyncrasies of each graphical password scheme under diverse attack scenarios.
vi. **Thorough Security Evaluation and Recommendations:** Drawing from the analyzed data, the methodology critically evaluates the security posture of each graphical password scheme. It meticulously identifies vulnerabilities, weaknesses, and potential areas for enhancement within each scheme. Additionally, the methodology offers robust recommendations and strategic suggestions aimed at bolstering the security and usability facets of graphical password schemes.

3. Honeywords and Honey-Encryption: Honeywords are decoy passwords designed to confuse attackers. This technique involves generating a set of plausible decoy passwords alongside the real password to deceive attackers attempting to crack passwords. It evaluates the impact on password guessing resistance and discusses potential use cases [5].

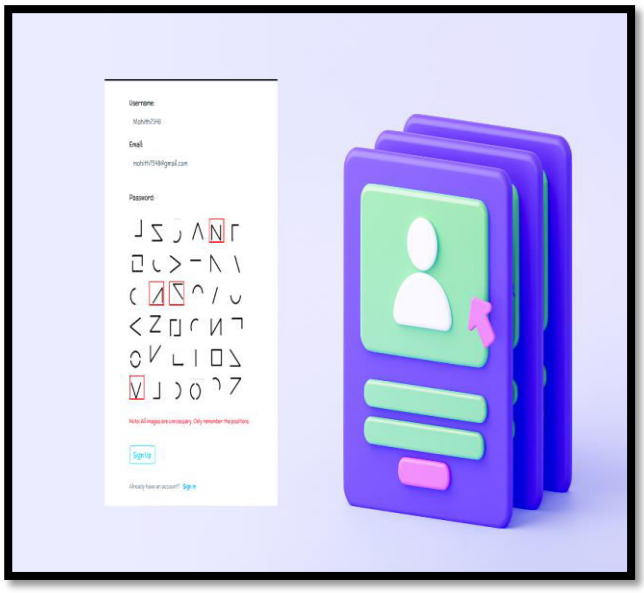

Fig. 4. Graphical Password Authentication

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.379 | Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 3, March 2024 ||

| DOI: 10.15680/IJIRCCE.2024.1203023 |

Honey-encryption emerges as a potent strategy within the realm of password security, encrypting sensitive data using algorithms that intricately generate deceptive outputs when incorrect keys are employed. This advanced methodology necessitates a comprehensive exploration to ascertain its efficacy in fortifying password protection amidst potential security breaches.

i. **Participant Selection and Diverse Representation:** The selection of participants was meticulously curated, emphasizing familiarity with password security measures and a willingness to actively engage in the study. The deliberate inclusion of a diverse cohort, spanning various demographics such as age, professional backgrounds, and technical expertise, ensures a comprehensive representation of user perspectives and experiences.

ii. **Rigorous Experimental Design:** An intricately controlled experimental environment was established to rigorously evaluate the practical application and effectiveness of honeyword and honey-encryption techniques within password management systems. This setup encompassed a secure platform facilitating participants to create, modify, and manage passwords while meticulously recording their interactions and associated data for comprehensive analysis.

iii. **Holistic Data Collection and In-Depth Analysis:** A multifaceted approach to data collection was adopted, encompassing both quantitative and qualitative metrics:

a. **Password Creation and Management:** Participants actively engaged in generating and managing passwords within the password management system. This practical involvement allowed for an assessment of the application's usability and real-time viability.

b. **User Feedback and Comprehensive Surveys:** Through structured surveys and questionnaires, participants conveyed their experiences, gauging aspects such as usability, effectiveness, and security perception. This qualitative feedback enables a deeper understanding of user perspectives and challenges encountered during practical implementation.

The gathered data undergoes meticulous analysis to unveil insights into the effectiveness of honey-encryption techniques. The assessment encompasses not only the security enhancements rendered but also the usability and practical implications of incorporating such techniques within password security paradigms. Resultant recommendations aim to refine and optimize the application of honey-encryption, aligning it with user expectations and security imperatives.

This comprehensive evaluation aims not only to scrutinize the technical prowess of honey-encryption but also to ascertain its practical viability and user-centric attributes within the realm of password security.

c. Comprehensive Data Logging and Evaluation Metrics: System logs played a pivotal role in recording essential information, encompassing timestamps for password creation/modification, usage patterns, and user interactions with honeyword or honey-encryption functionalities. These recorded metrics form the bedrock for an exhaustive evaluation of the implemented techniques.

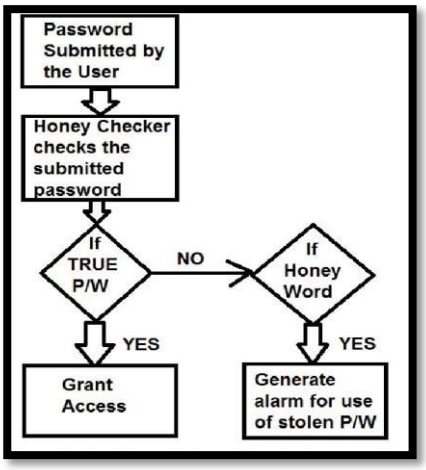

Fig. 5. Honey Checker

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.379 | Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 3, March 2024 ||

| DOI: 10.15680/IJIRCCE.2024.1203023 |

iv. Thorough Analysis Framework: Upon collating the extensive dataset, a meticulous analysis was undertaken to gauge the influence of honeyword and honey-encryption techniques on password security, consisting of two fundamental phases:

a. Quantitative Analysis: The quantitative dataset, comprising success rates of password attacks, password strength metrics, and user satisfaction ratings, underwent a rigorous statistical examination. This quantitative scrutiny offered invaluable insights into the tangible effects of integrating honey- word and honey-encryption techniques. Analyzing success rates of attacks provides a quantitative gauge of the system's resilience against various intrusion attempts, while assessing password strength metrics delineates the robustness of the passwords generated through this mechanism.

b. Qualitative Analysis: Qualitative data, derived from user feedback and survey responses, underwent a thematic analysis approach. This qualitative exploration aimed to identify recurring themes and patterns embedded within user perceptions, experiences, and challenges encountered while engaging with honeyword and honey-encryption techniques. By unearthing user sentiments and experiences, this qualitative analysis contributes invaluable insights into the nuanced aspects of user acceptance, usability, and areas for potential enhancement.

The amalgamation of quantitative and qualitative findings offers a comprehensive panorama:

The quantitative results provide an empirical understanding of how the integration of honeyword and honey-encryption techniques influences password strength, resilience against potential attacks, and user satisfaction metrics. These quantifiable outcomes offer a clear delineation of the efficacy of these techniques in fortifying the security landscape.

On the other hand, the qualitative findings delve into the subjective realm, unraveling user perceptions, experiences, and offering nuanced suggestions for potential refinements or augmentations. These insights pave the way for refining the user experience and tailoring the implementation of these techniques in line with user expectations and preferences.

Utilizing Insights for Continuous Improvement:

The amalgamated insights, derived from both quantitative and qualitative analyses, serve as guiding beacons for refining and evolving password security paradigms. These insights underpin a continuous improvement cycle, ensuring that the integration of honeyword and honey-encryption techniques evolves in consonance with user needs, technological advancements, and emergent threat landscapes.

IV. EXPERIMENTAL RESULTS

The statistical analysis of shoulder-surfing behaviors indicated a tendency among participants to iterate upon previous identification attempts rather than initiating from scratch. Specifically, findings revealed that observation distance significantly influenced character alterations, with distant observations leading to more substantial changes compared to closer observations. Moreover, intervals between attempts notably affected alterations in password length, showcasing increased modifications between initial and subsequent attempts relative to later attempts [1].

Numerous strategies associated with password identification behaviors surfaced, encompassing divide-and-conquer methodologies, layout-dependent replacement tactics, and the pivotal choice between modifying existing content and commencing anew [2]. Notably, adapting previous results emerged as a more effective strategy than starting from a clean slate.

In the analysis of password characteristics, a predominant pattern emerged, indicating that a majority of passwords fell within the range of 8 to 12 characters, likely in adherence to minimal length criteria stipulated by various websites. These passwords commonly comprised a combination of uppercase and lowercase letters, numerals, and a smaller fraction incorporated symbols. Passwords inclusive of personally identifiable information (PII) exhibited higher vulnerability, while those devoid of dictionary words were deemed comparatively more secure. The study underscored a prevalent trend of password reuse among respondents, with convenience often taking precedence over security measures. Furthermore, a significant portion of users displayed infrequent password updates, potentially heightening risks associated with account security [4].

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.379 | Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 3, March 2024 ||

| DOI: 10.15680/IJIRCCE.2024.1203023 |

Password Popularity – Top 20

Rank	Password	Number of Users with Password (absolute)
1	123456	290731
2	12345	79078
3	123456789	76790
4	Password	61958
5	iloveyou	51622
6	princess	35231
7	rockyou	22588
8	1234567	21726
9	12345678	20553
10	abc123	17542

Fig. 6. Commonly used passwords

V. DISCUSSION

Absolutely, in the realm of shoulder-surfing attacks targeting password-based authentication, the findings unveiled an intriguing pattern of adversary behavior. The utilization of divide-and-conquer strategies by these attackers signifies a shrewd approach, reducing cognitive burdens while maximizing their chances of successful identification. Their preference for character substitution, favoring adjacent keys on the keyboard, underscores the deep-rooted reliance on the layout of the keyboard itself. Interestingly, the research indicated that starting anew with password identification might not yield optimal outcomes; instead, adversaries tend to pivot towards modifying prior observations due to the complexity inherent in deciphering passwords. This insight not only underscores the efficiency of prior knowledge but also the nuanced nature of these identification tasks.

The study also underscored the pivotal influence of observation distance and intervals between attempts on the strategies employed by shoulder-surfing adversaries. This influence extended to the extent of alterations made in both character usage and password length. Such revelations carry significant implications for both users and developers in fortifying mobile authentication systems. It highlights the need for users to be mindful of their physical proximity during authentication sessions and encourages them to minimize the frequency of such interactions to mitigate the risk of shoulder-surfing attacks. Simultaneously, developers can leverage these adversary behaviors as crucial insights in crafting more robust and secure mobile authentication methods, aiming to counter such vulnerabilities.

As this study provides a glimpse into the behavior and tactics of shoulder-surfing adversaries, it beckons further exploration in the domain of password security. The call for future research echoes the necessity for larger and more diverse sample sizes, encompassing varying password lengths and encompassing broader demographics. This expansion aims not only to enrich our understanding of adversary strategies but also to bolster the fortifications against such attacks. Insights gleaned from a more expansive study could pave the way for enhanced security measures, catering to the multifaceted challenges posed by shoulder-surfing attacks on password-based authentication in mobile environments.

VI. CONCLUSION

Safeguarding personal and sensitive information online hinges significantly on robust password security. Several contributing factors, such as password length, composition, reuse, and the inclusion of personal identifiable information (PII), heighten the vulnerability of passwords. Strengthening password security necessitates the creation of unique, complex passwords devoid of easily guessable patterns or personal information. Consistently changing passwords and refraining from reusing them across multiple accounts are imperative practices. While password management systems

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.379 | Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 3, March 2024 ||

| DOI: 10.15680/IJIRCCE.2024.1203023 |

offer convenience, the compromise of a master password can pose inherent risks.

The advent of mobile authentication introduces new threats, notably shoulder-surfing attacks. Educating users on the significance of unique passwords and employing strategies like screen covering or randomized keyboard layouts can deter unauthorized observation. Key practices include avoiding password sharing, using identical passwords across accounts, writing down passwords, or transmitting them insecurely. Additional authentication mechanisms, like Honeyword and HoneyEncryption, bolster password storage and fortify defenses against brute force attacks.

The research underscores the evolution of password evaluation techniques, highlighting the vulnerability of traditional methods to social engineering attacks. The incorporation of sensitive personal information in password strength assessment offers promise but demands careful consideration of privacy and data accuracy concerns. Furthermore, the recommendation of graphical passwords as a more secure alternative emphasizes their resistance to common password attacks and ease of user recollection.

In conclusion, prioritizing robust password security is paramount for individuals and organizations alike. This involves creating, safeguarding, and regularly updating strong, unique, and complex passwords. Augmenting these practices with additional security measures and diverse authentication mechanisms strengthens overall password protection in an ever-evolving digital landscape.

REFERENCES

[1] Behaviors of Unwarranted Password Identification via Shoulder-Surfing during Mobile Authentication Lina Zhou, Kanlun Wang, Dongsong Zhang, Jianwei Lai 2021 IEEE Inter- national Conference on Intelligence and Security Informatics (ISI) — DOI: 10.1109/ISI53945.2021.9624730
[2] Level of Password Vulnerability Indira Mannuela, Jessy Putri, Michael, Maria Susan Anggreainy in 2021 1st International Conference on Computer Science and Artificial Intelligence (ICCSAI)
[3] A Password Strength Evaluation Algorithm based on Sensitive Personal Information Xinchun Cu, Ding Yong ,Xueqing Li ,Yiming Qin in 2020 IEEE 19th International Con- ference on Trust, Security and Privacy in Computing and Communications (TrustCom) DOI 10.1109
[4] The Security Analysis of Graphical Passwords Wei Hu,Xiaoping Wu, Guoheng Wei in 2010 International Conference on Communications and Intelligence Information Security DOI 10.1109
[5] Strengthening Password Security through Honeyword and HoneyEncryption Technique Mrs.Vasundhara R.Pagar, Mrs.Rohini G.Pise in International Conference on Trends in Electronics and Informatics ICEI 2017
[6] Lina Zhou, Kanlun Wang, Jianwei Lai, Dongsong Zhang (2021). "Behaviors of Unwarranted Password Identification via Shoulder-Surfing during Mobile Authentication." In 2021 IEEE International Conference on Intelligence and Security Informatics (ISI). DOI: 10.1109/ISI53945.2021.9624730
[7] Mannuela, I., Putri, J., Michael, & Anggreainy, M. S. (2021). "Level of Password Vulnerability." In 2021 1st International Conference on Computer Science and Artificial Intelligence (ICCSAI).
[8] Cu, X., Yong, D., Li, X., & Qin, Y. (2020). "A Password Strength Evaluation Algorithm based on Sensitive Personal Information." In 2020 IEEE 19th International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom). DOI: 10.1109
[9] Hu, W., Wu, X., & Wei, G. (2010). "The Security Analysis of Graphical Passwords." In 2010 International Conference on Communications and Intelligence Information Security. DOI: 10.1109
[10] Pagar, V. R., & Pise, R. G. (2017). "Strengthening Password Security through Honeyword and HoneyEncryption Technique." In International Conference on Trends in Electronics and Informatics (ICEI) 2017.

INNO SPACE
SJIF Scientific Journal Impact Factor

Impact Factor: 8.379

doi cross ref

ISSN INTERNATIONAL STANDARD SERIAL NUMBER INDIA

निस्केयर NISCAIR

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

9940 572 462 6381 907 438 ijircce@gmail.com

www.ijircce.com

Scan to save the contact details