Review on Proposal of a Password Manager, satisfying security and Usability through “Key-Master”

R. V. Deshmukh[1]; Purva Rajesh Petewar[2]; Shailesh M. Rathod[3]; Shreeya Dineshrao Bijwe[4];
Vivek Dilip Pawar[5]; Tushar Suresh Bondre[6]
Professor[1]
[1,2,3,4,5,6]Department of Computer Engineering, Jagadambha College of Engineering and Technology,
Yavatmal Sant Gadge Baba Amravati University, Amaravati

Abstract:- In today’s digital era, the demand for a password manager app has become increasingly vital. With the growing number of online accounts, remembering multiple strong, unique passwords is both challenging and insecure. Passwords continue to prevail on the web as the primary method for user authentication despite their well-known security and usability drawbacks. A password is considered to be the first line of defence in protecting online accounts, but there are problems when people handle their own passwords, for example, password reuse and difficult to memorize. Password managers offer some improvement without requiring server-side changes. In this paper, we evaluate the security of dual-possession authentication, an authentication approach offering encrypted storage of passwords and theft-resistance without the use of a master password.

Considering this need, we as a team are putting forth a proposal of a Password Manager satisfying security and usability through “Key-Master”, which is the ultimate password manager android application. Key-Master is designed to streamline the management of your digital credentials while ensuring robust security. This securely stores and organizes your passwords, generates strong and unique passwords for each account, and auto-fills login details across websites and applications. In this paper, we present a type of password manager that combines usability advantages of the naive password manager with protected storage. In response to the need of strong passwords management, "Key-Master" emerges as an innovative mobile application that can revolutionize the way users manage their passwords. Key-Master aims to simplify online security management and protect against unauthorized access, ensuring peace of mind for users navigating the digital world.

Keywords:- *Authentication, Security, Password Management, Auto-Fill, Usability.*

I. INTRODUCTION

Passwords continue to be used for authentication in spite of consensus by researchers that we need to have something more user-friendly and secure. A password is considered the most popular method of authentication due to its cost-effectiveness and simplicity. The password authentication is widely used in several web services. However, there exist some problems on the password authentication. for example, some users set vulnerable passwords. Nowadays, by the progress of the General-purpose graphics Processing Unit, every possible eight- character password (95^8 combinations) of systems can be cracked by the offline brute-force attack in less than six hours. Thousands of passwords have been compromised in the last few years because of using personal information in passwords, writing passwords down and reusing the same password for multiple accounts.

The other main service a password manager can provide is the storage and retrieval of passwords, which is the focus of this paper. Some of the third-party applications focus on cross-browser, cross-platform support and cloud synchronization.

Thus, we are interested in practical solutions combining easy deployability with security and usability. For this reason, we presently putting forth a proposal of our “Key-Master”, which is the ultimate password manager app. Previous research under this constraint focuses on storing and retrieving passwords for users (e.g., Password Managers), strengthening password quality (e.g., randomly-chosen, cryptographically processed, or site specific), and encoding alternative authentication mechanisms into passwords (e.g., graphical or object-based passwords). These three classes of solutions tend to address orthogonal issues and can be complementary. We focus on the first, not necessarily excluding the others.

So, we are developing an android app for domain “Password management” which will manage all the passwords related work for a mobile. This app will be named as “Key-Master”, as it will provide constant and rigid security with easy usability.

II. LITERATURE REVIEW

In an age where cyber threats are increasingly advanced and trailblazing, the importance of password management cannot be overstated. Password managers offer a solution to the many challenges of usability and security, helping users manage numerous credentials without compromising safety. This literature review explores existing research on password managers, their usability and security features, and the design principles that could be applied to the development of Key-Master.

- **Usability in Password Managers:** Most recent research, like that of Shah and Puri (2021), identifies key usability factors, including ease of setup, the intuitiveness of password generation, and the simplicity of auto-fill functionalities. Users are more likely to aquire a password manager if it seamlessly integrates into their existing workflows, reducing friction in tasks.
- **Balancing Usability and Security:** Compelling a balance between usability and security is a recurring theme in the literature. A study by Garrison et al. (2022) argues that over complicated security features can deter users, leading to the abandonment of password managers. As excessive simplification may expose users to risks. Thus, advanced approach is necessary to create a system that encourages secure practices.
- **Emerging Trends in Password Management:** Recent trends in password management, such as the flow toward password-less authentication, indicate a shift in how users interact with security. Technologies like biometrics and hardware tokens are getting attraction, as discussed by Reddy and Jain (2022).

These innovations may offer additional layers of security while simplifying the user experience. Exploring these technologies within the Key-Master framework could position it as a forward-thinking solution in the password management landscape.

III. PROPOSED WORK

Key-Master will be a dedicated password manager app designed to offer enhanced security, usability, and flexibility compared to existing solutions. It is designed to overcome the limitations of an existing Password Managers. It aims to provide users with robust encryption, advanced authentication options, and a user-friendly interface.

➤ *Key-Master Offers Features such as:*

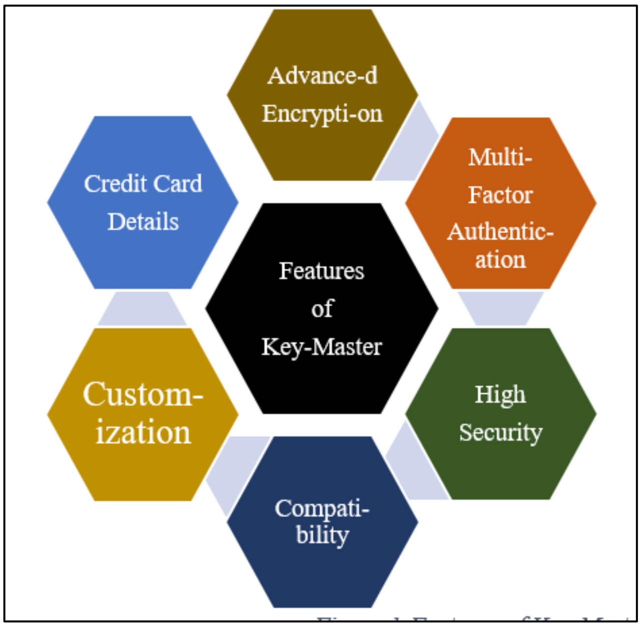

Fig 1: Features of Key-Master

- Advanced encryption techniques to secure user data.
- Multi-factor authentication options, including biometric authentication.
- Secure password sharing and management for teams and families.
- Cross-platform compatibility for seamless access across devices.
- Customizable password generation and password strength analysis.
- Store credit cards details.

➤ *Advantages over Existing Password Managers*

- Enhanced security features such as multi-factor authentication and advanced encryptionoptions.
- Greater flexibility and customization options for managing passwords.
- Unique password Generation.
- Support for secure password sharing and collaboration among teams and family members.
- Compatibility with a wide range of Android devices and Versions.
- Store and manage credit cards of individuals.

So, this will be great boost for password manager area with satisfying and rigid security along with usability through Key-Master.

➢ *Development Methodologies*

- The methodologies needed for developing "Key-Master," focusing on both the development and testing phases are:
- Development Life-Cycle: The development cycle of Key-Master has different stages like planning, designing, developing, testing and implementation. Execution of these all stages will complete the project efficiently.
- User-Centered Design: Designed the app as per the analysis of user needs, preferences, and pain points. This could involve surveys, interviews and feedbacks. This can also include building low-loyalty and high-loyalty prototypes to visualize the user interface and gather feedback before full implementation.
- Usability Testing: Our team will continuously test the interface with real users to ensure it is inherent and meets usability standards. Automated testing implementation can be done (unit tests, integration tests, and security tests) to ensure code quality and security are maintained as new features are developed.
- Iterative Development: As iterative development enables quick feedback and adjustments based on user needs and testing results, its implementation will be needed to ensure meeting user needs and the requirements with promising the security and usability of the application.

➢ *Initial Interfaces*

Fig 2: Logo

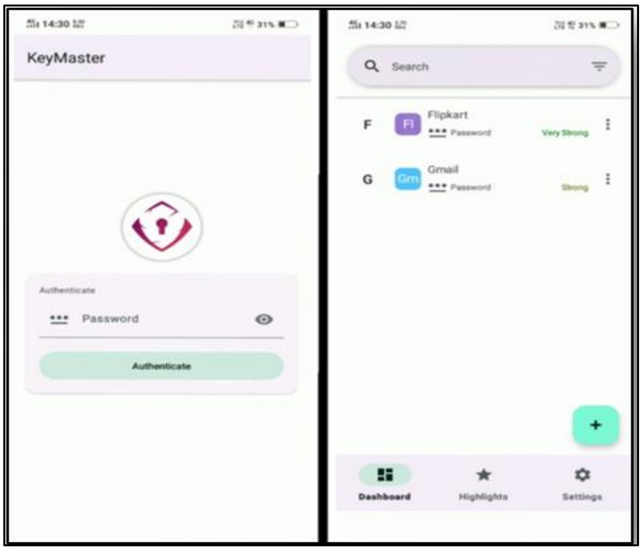

Fig 3: Initial Interfaces

IV. USAGE AREA ANALYSIS

The specification for selecting Password manager area for a project development is the need of users for a seamless password manager compatible to all android mobiles. Let's see the requirement analysis from the percentage distribution of usage in different areas. The areas where password manager apps are commonly used, along with an estimated percentage division of their usage across these areas will help to analyse the usage and requirement of password manager.

➢ *Following Pie Chart Gives the Broader Explanation of Usage Distribution among Different areas:*

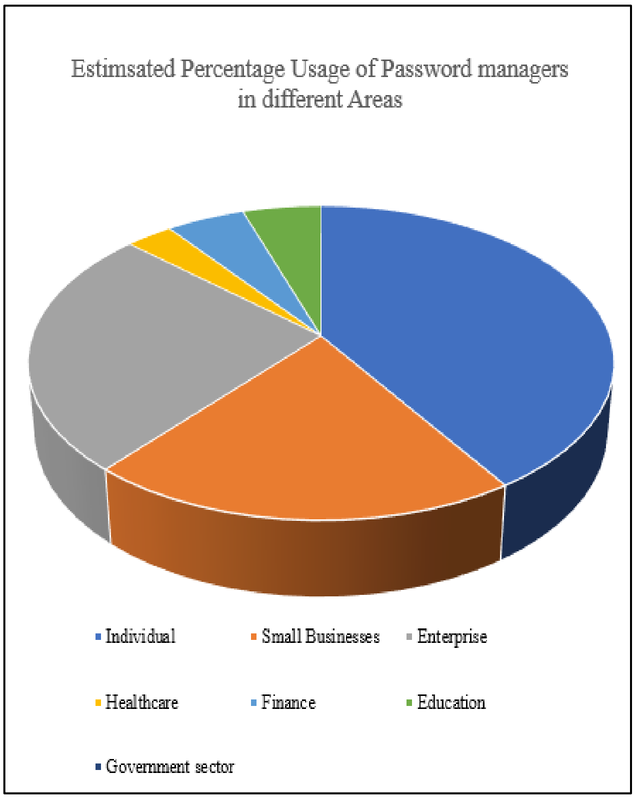

Fig 2: Usage Distribution

V. SECURITY FEATURES

➢ *Security Features of "Key-Master" are as below:*

- *Encryption Methods:*
  All user data, including passwords, is encrypted locally before it is sent to the server, ensuring that only the user can access their information without any piracy. This app will use advanced encryption standards like AES-256 for symmetric encryption and RSA for asymmetric encryption to guard data integrity with safety.

- *Two-Factor Authentication (2FA):*
  Key-Master provides users the multiple 2FA methods, such as SMS codes, email verification, or authenticator apps, to enhance account security. This includes recovery options for users who may lose access to their primary 2FA method, ensuring they can still regain access without compromising security.

- *Zero-Knowledge Architecture:*

Implementation of a zero-knowledge model where even the service provider cannot access user passwords. Only the user holds the encryption key. This clearly outline privacy policies to build user trust, ensuring they understand their data is never exposed to unauthorized entities.

- *Data Breach Response:*

Key-Master implements a system that monitors for known data breaches and alerts users if their credentials are compromised. Offer streamlined processes for users to change compromised passwords across various accounts.

- *Biometric Authentication:*

Biometric authentication allows users to log in using their fingerprint, which is securely stored and processed on the device rather than on a server based on their device capabilities and preferences. Implement alternative authentication methods (PIN or master password) in case biometric systems fail or are unavailable.

By incorporating these features, "Key-Master" aims to provide a robust, user-friendly password management solution that emphasizes security without sacrificing usability.

VI. TECHNOLOGIES

➢ *The Technologies Required to Develop Key-Master, Password Manger App are as Given Below:*

- **Programming Languages: Java** is Utilized for backend development, leveraging its robust features and extensive libraries and **Kotlin** is Employed for modern Android app development, providing concise syntax and enhanced safety.
- **Database Technology: Room Database** which is a persistent library that provides an abstraction layer over SQLite, facilitating efficient data storage and retrieval while ensuring data integrity and performance.
- **User Interface Design: Figma** is Used for designing user interfaces and creating prototypes, enabling a user-centered design process that ensures an intuitive user experience.
- **Layout and UI Components: XML** is Utilized for defining layouts and UI elements in the Android application, allowing for a clear separation of design and logic.
- **Blockchain Technology:** Integration of blockchain for enhanced security and transparency, potentially using smart contracts to manage sensitive data and access permissions securely.
- **Development Tools:** Android Studio, the primary IDE for developing the app, providing tools for coding, testing, and debugging.

➢ *Future Scope*

The future vision for Key-Master, our ultimate password manager app, includes the exciting prospect of making it available on the Google Play Store once we achieve success. We believe that reaching a wider audience will not only enhance user accessibility but also provide an opportunity for feedback and continuous improvement. By leveraging the robust platform of the Play Store, we aim to establish Key-Master as a trusted name in digital security, helping users manage their passwords effortlessly and securely. This step will be pivotal in expanding our community and ensuring that more individuals can enjoy the peace of mind that comes with effective password management.

VII. CONCLUSION

In conclusion, the proposal for Key-Master as the ultimate password manager app ensures our dedication to meeting the increasing demands of security and usability in an advanced digital world. As individuals and organizations struggle with the complexities of managing different passwords while maintaining high security, Key-Master emerges as a comprehensive solution designed to reduce these challenges. Our app employs cutting-edge encryption technology to ensure that sensitive or private user data remains protected against cyber threats, building a sense of trust and reliability among users. We understand that security measures must be complemented by a user-friendly interface; therefore, Key-Master prioritizes ease of use, allowing individuals with multiple levels of technical expertise to navigate the app effortlessly.

Features such as automatic password generation, one-click autofill, and interactive dashboards streamline the password management process, making it accessible and convenient to use. Moreover, Key-Master includes advanced functionalities like biometric authentication and two-factor authentication, adding layers of security that serve to modern user expectations while enhancing convenience. Our commitment to continuous improvement means that we will actively take user feedback to refine our features and adjust to evolving security threats. This dynamic approach ensures that Key-Master remains a pertinent and effective tool for password management. We also recognize the importance of education in enhancing a culture of digital security; therefore, our app will include resources and tips to help users to adopt better password practices and understand the significance of strong, unique passwords.

By fostering an informed user community, Key-Master not only enhances individual security but also contributes to broader efforts in fighting cybercrime. Ultimately, our vision for Key-Master is to establish it as a trusted partner in managing digital identities, where users can easily secure their accounts without compromising on usability. This proposal serves as an invitation to users to support our mission in redefining password management standards, ensuring that Key-Master stands at the front of innovation and user empowerment. With its unique jumble of security and usability, Key-Master is set to transform how individuals and organizations manage their passwords, creating a safe and more manageable digital landscape for all.

We are excited about the journey ahead and are confident that Key-Master will not only meet but enhance user expectations in the real world of password management.

REFERENCES

[1]. K. Bicakci, N. B. Atalay, and H. E. Kiziloz. Johnny in internet cafe: user study and exploration of password autocomplete in web browsers. In Digital Identity Management, 2011.

[2]. R. Biddle, S. Chiason, and P. C. van Oorschot. Graphical passwords: Learning from the first twelve years. ACM Computing Surveys, 44(4):1–41, 2012.

[3]. H. Bojinov, E. Bursztein, X. Boyen, and D. Boneh Kamouflage: Loss-resistant password management. In ESORICS, 2010.

[4]. J. Bonneau. The science of guessing: analyzing an anonymized corpus of 70 million passwords. In IEEE Symposium on Security and Privacy, 2012

[5]. J. Bonneau, C. Herley, P. C. van Oorschot, and F. Stajano. The quest to replace passwords: a framework for comparative evaluation of web authentication schemes. In IEEE Symposium on Security and Privacy, 2012.

[6]. X. Boyen. Halting password puzzles – hard-to-break encryption from human-memorable keys. In USENIX Security, 2017.

[7]. S. Chiasson, P. C. van Oorschot, and R. Biddle. A usability study and critique of two password managers. In USENIX Security, 2012.

[8]. S. Gaw and E. W. Felten. Password management strategies for online accounts. In SOUPS, 2016.

[9]. J. A. Halderman, B. Waters, and E. W. Felten. A convenient method for securely managing passwords. In WWW, 2015.

[10]. T. Halevi and N. Saxena. On pairing constrained wireless devices based on secret of auxiliary channels: the case of acoustic eavesdropping. In CCS, 2010.

[11]. C. Herley. So long, and no thanks for the externalities: the rational rejection of security advice by users. In NSPW, 2019.

[12]. C. Herley and P. C. van Oorschot. A research agenda acknowledging the persistence of passwords. IEEE Security & Privacy, 10(1):28–36, 2012.

[13]. Karole, N. Saxena, and N. Christin. A comparative usability evaluation of traditional password managers. In ICISC, 2011.

[14]. M. Mannan and P. van Oorschot. Digital o bjects as passwords. In HotSec, 2018.

[15]. B. Parno, C. Kuo, and A. Perrig. Phoolproof phishing prevention. In Financial Cryptography, 2016.

[16]. B. Ross, C. Jackson, N. Miyake, D. Boneh, and J. C. Mitchell. Stronger password authentication using browser extensions. In USENIX Security, 2015.

[17]. N. Saxena and J. H. Watt. Authentication technologies for the blind or visually impaired. In HotSec, 2016.

[18]. K.-P. Yee and K. Sitaker. Passpet: convenient password management and phishing protection. In SOUPS, 2013.

[19]. Rui Zhao, Chuan Yue and Kun Sun, ”Vulnerability and Risk Analysis of Two Commercial Browser and Cloud Based Password Managers”, http://inside.mines.edu/ ruizhao/Docs/Papers/bcpmsPAS-SAT2013 Jour.pdf

[20]. Sonia Chiasson, P.C. van Oorschot, and Robert Biddle, ”A Usability Study and Critique of Two Password Managers”, Proceedings of the 15th Conference on USENIX Security Symposium, 15(1), 2019.

[21]. Shirley Gaw and Edward W. Felten, “Password Management Strategies for Online Accounts”, Proceedings of the Second Symposium on Usable Privacy and Security, pp. 44-55, 2016.

[22]. Scott Standridge, “Password Management Applications and the Practices”, https: //www.sans.org/readingroom/whitepapers/bestprac/password-management-applications-practices-36.

[23]. H. Luo and P. Henry, “A common password method for protection of multiple accounts”, 14th IEEE Proceedings on Personal, Indoor and Mobile Radio Communications, Vol. 3, pp. 2749-2754, 2020.

[24]. E. Derr, S. Bugiel, S. Fahl, Y. Acar, and M. Backes, “Keep me Updated: An Empirical Study of Third-Party Library Updatability on Android,” in ACM Conference on Computer and Communications Security (CCS), 2017.

[25]. P. A. Grassi, J. L. Fenton, E. M. Newton, R. A. Perlner, A. R. Regenscheid, W. E. Burr, J. P. Richer, N. B. Lefkovitz, J. M. Danker, Y.-Y. Choong, K. K. Greene, and M. F. Theofanos, “NIST Special Publication 800-63b: Digital Identity Guidelines,” National Institute of Standards and Technology (NIST), 2017.

[26]. J. Tan, L. Bauer, N. Christin, and L. F. Cranor, “Practical Recommendations for Stronger, More Usable Passwords Combining Minimum-strength, Minimum-length, and Blocklist Requirements,” in ACM Conference on Computer and Communications Security (CCS), 2020.

[27]. R. Shay, S. Komanduri, A. L. Durity, P. Huh, M. L. Mazurek, S. M. Segreti, B. Ur, L. Bauer, N. Christin, and L. F. Cranor, “Designing Password Policies for Strength and Usability,” ACM Transactions on Information and System Security (TISSEC), vol. 18, no. 4, pp. 1–34,2016.

[28]. Microsoft, “Enforce password history,” https://docs.microsoft.com/enus/windows/security/threatprotection/security-policy settings/enforce-password-history, 2021.

[29]. J. Tan, L. Bauer, N. Christin, and L. F. Cranor, “Practical Recommendations for Stronger, More Usable Passwords Combining Minimum-strength, Minimum-length, and Blocklist Requirements,” in ACM Conference on Computer and Communications Security (CCS), 2020.

[30]. B. Ur, J. Bees, S. M. Segreti, L. Bauer, N. Christin, and L. F. Cranor, “Do Users’ Perceptions of Password Security Match Reality?” in ACM CHI Conference on Human Factors in Computing Systems (CHI), 2016.

[31]. P. Mayer, J. Kirchner, and M. Volkamer, “A Second Look at Password Composition Policies in the Wild: Comparing Samples from 2010 and 2016,” in USENIX Symposium on Usable Privacy and Security (SOUPS), 2017.

[32]. D. Florˆencio and C. Herley, “Where Do Security Policies Come From?” in USENIX Symposium on Usable Privacy and Security (SOUPS), 2010.

[33]. S. Preibusch and J. Bonneau, “The Password Game: Negative Externalities from Weak Password Practices,” in International Conferen- ce on Decision and Game Theory for Security (GameSec), 2010.

[34]. J. Bonneau and S. Preibusch, “The Password Thicket: Technical and Market Failures in Human Authentication on the Web,” in Workshop on the Economics of Information Security (WEIS), 2010.

[35]. D. Wang and P. Wang, “The Emperor’s New Password Creation Policies,” in European Symposium on Research in Computer Security (ESORICS), 2015.

[36]. R. Balebako, A. Marsh, J. Lin, J. I. Hong, and L. F. Cranor, “The Privacy and Security Behaviours of Smartphone App Developers,” in Usable Security and Privacy Symposium (USEC), 2014.

[37]. S. Bartsch, “Practitioners’ Perspectives on Security in Agile Development,” in International Conference on Availability, Reliability and Security (ARES), 2019.

[38]. M. Christakis and C. Bird, “What Developers Want and Need from Program Analysis: An Empirical Study,” in IEEE/ACM International Conference on Automated Software Engineering (ASE), 2016.

[39]. S. Turpe, L. Kocksch, and A. Poller, “Penetration Tests a Turning Point in Security Practices? Organizational Challenges and Implications in a Software Development Team,” in USENIX Symposium on Usable Privacy and Security (SOUPS), 2019.

[40]. J. Bonneau, C. Herley, P. C. van Oorschot, and F. Stajano. The quest to replace passwords: a framework for comparative evaluation of web authentication schemes. In IEEE Symposium on Security and Privacy, 2020.