##### Title

**A PROJECT REPORT**

###### *Submitted by*

**Anjul Kumar** (2XBCY10XXX)

**Ayushman Bhatia** (2XBCY10300)

**Pranjal Jamwant** (2XBCY10084)

**Pushpa Thungu** (2XBCY10268)

**Jassi Kumar Saadho** (2XBCY10111)

*in partial fulfillment for the award of the degree*

*of*

##### BACHELORS OF TECHNOLOGY

*In*

**COMPUTER SCIENCE AND ENGINEERING**

**(Cyber Security and Digital Forensics)**



**SCHOOL OF COMPUTING SCIENCE ENGINEERING AND ARTIFICIAL INTELLIGENCE (SCAI)**

**VIT BHOPAL UNIVERSITY**

**KOTHRI KALAN, SEHORE**

**MADHYA PRADESH - 466114**

SEP – JAN 2024

**VIT BHOPAL UNIVERSITY, KOTHRI KALAN, SEHORE**

**MADHYA PRADESH – 466114**

**BONAFIDE CERTIFICATE**

Certified that this project report titled **“Title”** is the Bonafide work of **Sam Thungu (2xBCY10441), Ayush Singh (2XBCY10121** who carried out the project work under my supervision. Certified further that to the best of my knowledge the work reported at this time does not form part of any other project/research work based on which a degree or award was conferred on an earlier occasion on this or any other candidate.

|  |  |  |
| --- | --- | --- |
| **PROGRAM CHAIR**  **Dr. D. Saravanan**  Assistant Professor,  School of Computing Science Engineering and Artificial Intelligence (SCAI)VIT BHOPAL UNIVERSITY | **PROGRAM CHAIR**  **Dr. Adarsh Patel**  Assistant Professor,  School of Computing Science Engineering and Artificial Intelligence (SCAI)VIT BHOPAL UNIVERSITY | **PROJECT GUIDE**  **Dr. Anshul Kumar,**  Assistant Professor,  School of Computing Science Engineering and Artificial Intelligence (SCAI)VIT BHOPAL UNIVERSITY |

The Project Exhibition I is held on \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**ACKNOWLEDGEMENT**

First and foremost I would like to thank the Lord Almighty for His presence and immense blessings throughout the project work.

I wish to express my heartfelt gratitude to **Dr D. Saravanan** and **Dr. Adarsh Patel**, Program Chairs, Cyber Security and Digital Forensics for much of his valuable support encouragement in carrying out this work.

I would like to thank my internal guide **Dr Anshul Kumar** for continually guiding and actively participating in my project, giving valuable suggestions to complete the project work.

I would like to thank all the technical and teaching staff of the School Computing Science and Engineering, who extended directly or indirectly all support.

Last, but not least, I am deeply indebted to my parents who have been the greatest support while I worked day and night for the project to make it a success.

**LIST OF ABBREVIATIONS**

* UI – User Interface
* UX - User Interface
* HTML – Hyper Text Markup Language
* CSS – Cascading Style Sheet
* JS – JavaScript
* DPPG – Dynamic Password Policy Generator
* OP Grid – Operational Grid
* UsForm - Using a Formula
* PCFG - Probabilistic Context-Free Grammar

# **LIST OF FIGURES AND GRAPHS**

|  |  |  |
| --- | --- | --- |
| **FIGURE NO.** | **TITLE** | **PAGE NO.** |
| 1.1 | Characteristic of different password manager | 15 |
| 1.2 | Comparison between different password manager | 16 |
| 1.3 | Proportion of different character structure | 19 |
| 1.4 | Personal information in group password | 19 |
| 1.5 | Splash Screen PassGuardian app | 18 |
| 1.6 | Registration Screen PassGuardian app | 19 |
| 1.7 | Login Screen PassGuardian app | 22 |
| 1.8 | Password Generator PassGuardian website | 23 |
| 1.9 | Password Generator PassGuardian app | 24 |
| 1.10 | Password Validator PassGuardian app | 26 |

**LIST OF TABLES**

|  |  |  |
| --- | --- | --- |
| Table No. | Title | Page No. |
| Table 1.1 | Security evaluation of password managers , including quantitative value | 15 |
| Table 2.1 | Popular group password analysis | 18 |
| Table 3.1 | Working of PassGuardian | 18 |

**ABSTRACT**

Research shows that password managers contribute to network security by encouraging the use of complex and unique passwords to reduce the risk of unauthorized access. The research also shows the impact of password managers on user experience and highlights the need for better understanding and integration of existing systems. This study identified potential vulnerabilities and issues associated with some password managers.  
  
Research announces Dynamic Password Policy Generator (DPPG) as an alternative to password strength checkers to ensure uniformity of password space OPGrid technology for secure password entry using authentication methods with different models for each login. It examines today's password management systems, evaluating their encryption methods, user interface, cross platform compatibility. The concept of "group password" is introduced to analyze the password characteristics of different users. SPHINX is a new way to manage passwords that stay safe even if your password manager is compromised. It prevents attackers from learning this information by keeping the information on the device separate from the user's master password. It was all about comparing different successful, secure and widely used password managers under different categories.

**TABLE OF CONTENTS**

|  |  |  |
| --- | --- | --- |
| CHP  NO. | TITLE | PAGE NO. |
|  | List of Abbreviations  List of Figures and Graphs  List of Tables  Abstract | ii  iii  iv  v |
| 1 | **CHAPTER 1: INTRODUCTION**  1.1 Introduction  1.2 Motivation for the work  1.3 Problem Statement  1.4 Objective of the project  1.5 Organization of the project  1.6 Summary | 1  1  1  2  2  2  3 |
| 2 | **CHAPTER 2: RELATED WORK INVESTIGATION**  2.1 Introduction  2.2 Existing Approaches/Methods  2.3 Approaches/Methods -2  2.4 Approaches/Methods -3  2.5 Pros and cons of the stated Approaches/Methods  2.6 Issues/Observation from investigation  2.7 Summary | 4  4  6  6  7  8  12  12 |
| 3 | **CHAPTER 3: METHODOLOGY**  3.1 Methodology | 12  12 |
| 4 | **CHAPTER 4: REQUIREMENT AND IMPLEMENTATION**  4.1 Essential Function  4.2 Password Creation and Verification  3.3 Safe Storage  3.4 Dynamic Password Policy System (DPPGS)  3.5 User Interface  3.6 Non – Functional Needs  3.7 Security  3.8 Usability  3.9 Dependability  3.10 Legal and Compliance  3.11 Documentation Requirement  3.12 Technical Records | 13  13  13  13  13  13  13  13  14  14  14  14  14  14 |
| 5 | **CHAPTER 5: TECHNICAL IMPLEMENTATION & ANALYSIS**  5.1 Splash Screen  5.2 Registration Page  5.3 Login Page  5.4 Password Generator  5.5 Password Validator | 18  18  19  22  23  25 |
| 6 | **CHAPTER 6: RESULTS AND DISCUSSION**  6.1 Outline  6.2 Applicability | 28  28  28 |
| 7 | **CHAPTER 7: CONCLUSION AND FUTURE WORK**  7.1 Outline  7.2 Limitations/Constraints of the System  7.3 Future Enhancements  7.4 Inference | 29  29  29  29  30 |
|  | **References** | 31 |

# **Chapter 1**

## **Introduction**

* 1. **Introduction**:

This project exhibition centers around two key components: research paper and app development, with a primary focus on creating a cutting-edge password manager. This innovative solution aims to enhance online security and user convenience by securely storing and managing passwords [1]. The research paper delves into the latest advancements in password security and management, while the app development segment involves the creation of a user-friendly, cross-platform application that offers robust encryption, auto-generation, and seamless integration with various devices [2].

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| A | B | C | D | E |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

Table 1.1 - Security evaluation of password managers, including quantitative value

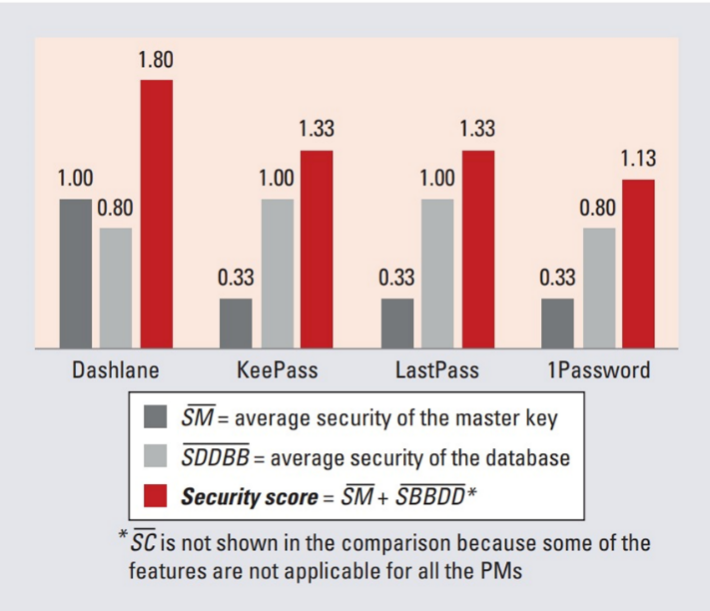


Fig 1.1 Comparison between different password manager

**REFERENCES**

[1]. DPPG: A Dynamic Password Policy Generation System Shukun Yang, Member, IEEE, Shouling Ji, Member, IEEE, and Raheem Beyah, Senior Member, IEEE

[2]. Patricia Arias-Cabarcos; Andrés Marín; Diego Palacios; Florina Almenárez; Daniel Díaz-Sánchez: Comparing Password Management Towards Usable and secure enterprise authentication: 28 September 2016

[3]. Syed Shabih Ul Hasan; Anwar Ghani; Muhammad Bilal; Alireza JolfaeiMacquarie University, Australia :Multi-Factor Pattern Implicit Authentication: 25 January 2021

[4]. Daojing He, Beibei Zhou, Xiao Yang, Sammy Chan, Yao Cheng, and Nadra Guiana: Group Password Strength Meter Based on Attention Mechanism: 19 February 2020

[5]. Jianhua Song; Degang Wang; Zhongyue Yun; Xiao Han: A Password Generation Strategy Based on mnemonic Shape: 23 August 2019

[6]. Maliheh Shirvanian; Nitesh Saxena; Stanislaw Jarecki; Hugo Krawczyk: Building and Studying a Password Store that Perfectly Hides Passwords from Itself: 14 March 2019