IJARIIT INTERNATIONAL JOURNAL OF ADVANCE RESEARCH, IDEAS AND INNOVATIONS IN TECHNOLOGY

ISSN: 2454-132X
Impact Factor: 6.078
(Volume 8, Issue 3 - V8I3-1425)
Available online at: https://www.ijariit.com

Secure pass – safe storage and password manager based on cryptanalysis

Krishna Yanmantram
krishnayanmantram@gmail.com
Vellore Institute of Technology, Vellore, Tamil Nadu

T. M. Vishnu Mukundan
tm.vishnu.m@gmail.com
Vellore Institute of Technology, Vellore, Tamil Nadu

Jama Surya Teja
jama.surya2019@vitstudent.ac.in
Vellore Institute of Technology, Vellore, Tamil Nadu

Atla Venkat Suhas
suhas.atla@gmail.com
Vellore Institute of Technology, Vellore, Tamil Nadu

ABSTRACT

Protecting the passwords that protect our information has become the main priority now a days as a lot of people are trying to crack into people's auto saved info on various applications to track out the passwords to their different accounts which is a major cybercrime that has been seen on an increased number. So we wanted to develop an mobile application that makes sure that no third party application can access the info saved in the app and this can only be accessed in a very particular way only the user can know. We are also trying to test out couple of algorithms which can help us to achieve the task with most efficiency and makes sure has the least time complexity in reacting to users interests.

Keywords: *Password Security, Mobile application, Cryptanalysis.*

1. INTRODUCTION

The organization of encryption is expanding in the current world. The organization of aggressors is likewise expanding, As the quantity of passwords are expanding in many spots, the motivation behind encryption is expanding all over. A typical human will in general fail to remember this large number of passwords as it is either undependable to have quite recently a solitary secret word or have recently an alternate means. We are fostering an application in which we will involve various sorts of encryption calculations for various kinds of passwords so a similar client can have an exceptionally protected capacity of the equivalent. Need of a solid secret word administrator is crucial that also making it productive is the principle key as the time intricacy ought to be thought of and we cannot continue to utilize a similar enormous calculation which will make the application extremely sluggish. The key is that everyone ought to have the option to use. As we as a whole realize that the world moving is towards security, there is encryption in numerous strategies which must be executed in the mean future. While us all notification, the use of passwords is expanding and thus we will derive the manner by which we can scramble and store so it is protected with the client. There are secret phrase vaults by numerous antivirus virtual products which are paid and they, when all is said and done, are not known to break down the best strategy to store. Aim of this is examine the most ideal calculation to securely store the secret word for the client in an android application so it is generally secure and wouldn't be feasible for any danger.

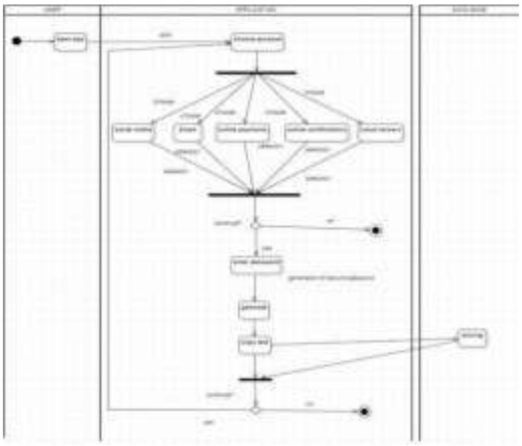
2. PROPOSED SYSTEM

With the proposed framework the client will actually want to remain safeguarded from assaults that are common nowadays. Part of individuals don't will quite often protect their record or any web-based subtleties with a solid and with serious level of entropy. This application is exceptionally helpful in light of the fact that the clients can enter the secret word existing or he/she can basically enter another secret key and the application will thoroughly take care of the end client. The client can pick among various choices gave once the application is opened. The primary module will request that the utilization select the reason for which he is utilizing. If he/she wishes to produce a solid secret key for email and Gmail purposes, he/she can pick the choice of "email" gave and can enter a current secret key to additionally solidify it, and this is additionally enlarged by scrambling calculations making them significantly more remarkable to be beaten and the secret word created to the client has serious level of entropy, which will debilitate the programmer/cryptanalyst. Level of irregularity makes the cryptanalyst depleted and this saves the clients records or anything they wish to store on the web. The calculations utilized are very much planned and there are no cases that they have been broken up tothis point. Then the clients can duplicate glue it to involve it in the sites or in some other
E-applications.

Subsequent to producing, one can duplicate the secret phrase created by tapping on duplicate button gave. Afterward assuming the client needs to see the historical backdrop of passwords created, they can see by tapping on "show passwords" on the upper right corner which is a choice inside the three-spot button. The client can see and furthermore clear the set of experiences byclicking "clear" button gave.

The application turned out great for practically all the experiments in the test suite. So there's no stress over any mistakes at this point. The planningof the application essentially comprises of use of
various calculations previously referenced and theyassume an indispensable part in changing over the secret phrase message into a solid and unbreachable secret key message as result.

3. MODEL

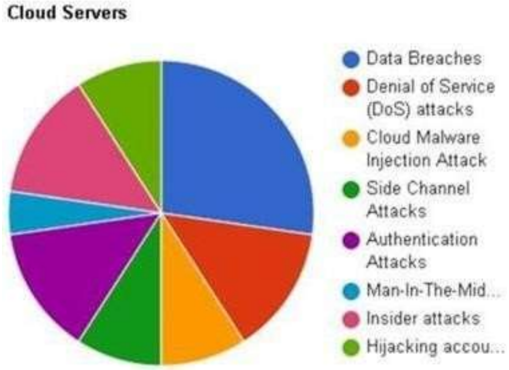


4. TYPES OF ATTACKS

- **Brute Force Attacks:** All combinations of Passwords are used.
- **Key Loggers:** Software thatmonitors the activity of user.
- **Dictionary Attacks**: This sort of Assault is somewhat quicker than beast force assault. Dissimilar to checking all prospects utilizing animal power assault, the word reference assault attempts to coordinate the secret phrase with most happening words or expressions of day to day existence utilization.
- **Shoulder Surfing**: Shoulder Surfingis "spying" in which the assailant sees the client's developments to get his/her secret word. In this sort of assault the aggressor notices the client; how he enters the secret key i.e., what keys of console the client has squeezed.

Replay Attacks: The replay assaultsare otherwise called the reflection assaults. It is a method for going after challenge reaction client validation system.

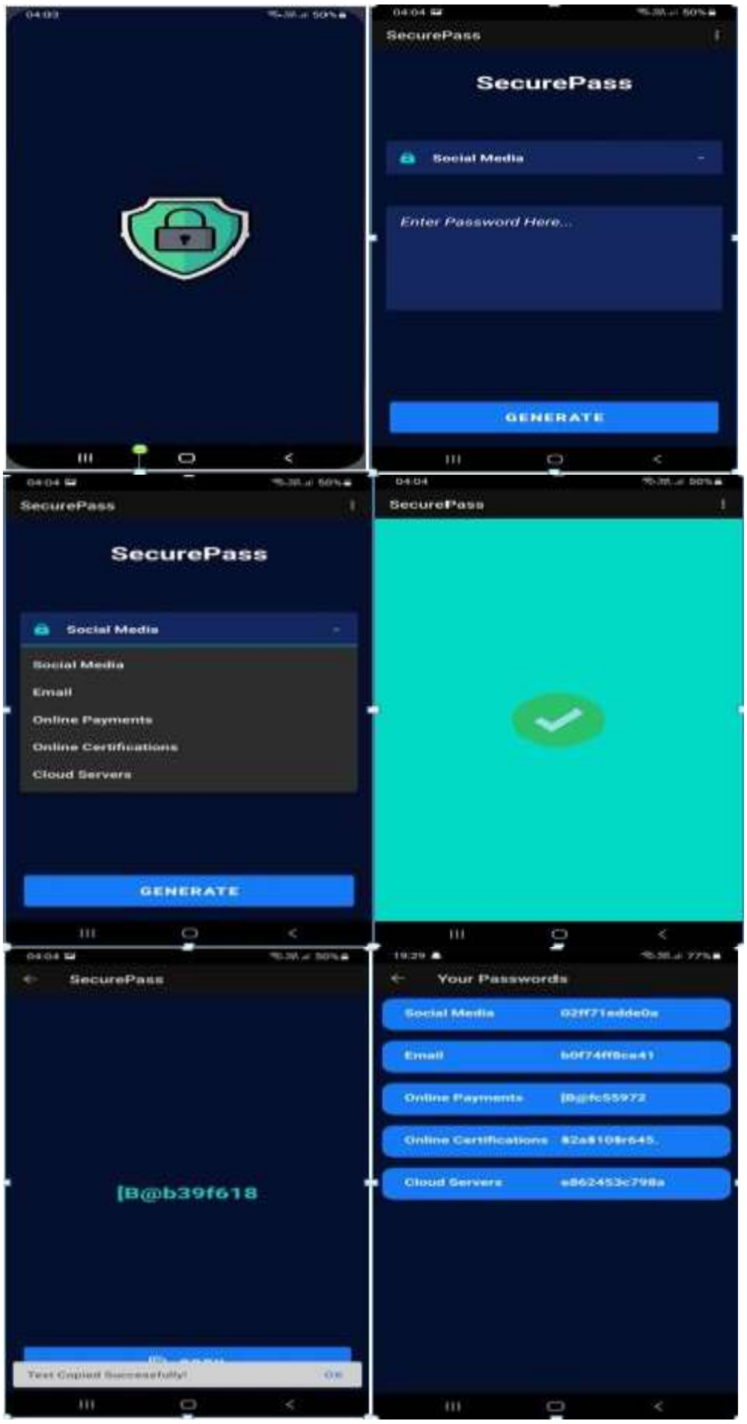
5. FRAMEWORK AND ARCHITECTURE OF PROPOSED SYSTEM



6. METHODOLOGY

- Developing Secure Mobile Applicationsfor Android.
- Developing and Benchmarking NativeLinux Applications on Android
- Cryptographic Hash functions: The Evaluation Report of SHA-256 CryptAnalysis Hash Function
- Application of SHA-256 in Formulation of Digital Signatures of RSA and El GamalCryptosystems
- Analysis of Secure Hash Algorithm (SHA) 512 for Encryption Process on WebBasedApplication
- Efficient Implementation of the SHA-512 Hash Function for 8-bit AVRMicrocontrollers
- Image Encryption Based on the Modified Triple-DES Cryptosystem by Victor ManuelSilva, R Flores, L Lopez
- Proposed Model for Triple-DES Encryption published in IBM Journal of Researchand Development by D. Coppersmith, D.B.

7. RESULTS



Social Media 02ff71edde0a
Email b0f74ff8ca41
Online Payments [B@fc55972
Online Certifications 82a8108r645.
Cloud Servers e862453c798a

Johnson, S.M. Martyas .Security Analysis ofMD5 algorithm in Password Storage

8. CONCLUSION

Subsequent to thinking about every single imaginable calculation, we have inferred that Argon2id is the best calculation that battles against such significant assaults. There are three unique adaptations of the calculation Argon2, and we have concluded that the Argon2id variation ought to be utilized, as it gives a decent way to deal with opposing bothside-channel and GPU-based assaults. While scrypt should be designed when utilized in heritage frameworks, more current frameworks ought to consider Argon2id for secret phrase hashing. As opposed to a basic work factor like different calculations, Argon2id has three unique boundaries that canbe designed. Argon2id should involve one of the accompanying design settings as a base least which incorporates the base memory size (m), the base number of emphasess (t) and thelevel of parallelism (p).

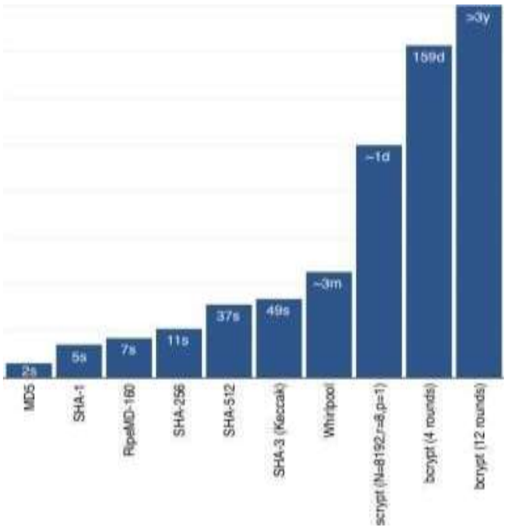
8.1) Social Media

Facebook uses SHA - 256 like most districts which was expected to be secure yet actually the example has changed and there are fresher hashing techniques for example PBKDF2, BCrypt, SCrypt estimations with salt. Instagram uses PBKDF2 or Bcrypt.

Online media objections in general use customary necessities for a decent mystery word which is - The mystery expression ought to be at any rate six characters and should be a mix of promoted and lowercasecharacters, numbers and complement.

In this way, the best hashing limit with regards to these are PBKDF2 - PBKDF2 (Secret phrase Based Key Deduction Capacity 2) are key surmising limits with a sliding computational cost, usedto decrease shortcomings of monster power attacks.

8.2) E:MAIL



To the extent that what we have seen now, we might presume that we will go with the calculation which is MD5 picked shrewdly among these assaults. With boundaries for email considered from what Gmail is really going after, MD5 is memory concentrated. This implies that more assetsare required while utilizing beast power and word reference assaults against the hashing calculation aswell as while hashing it. MD5 isn't as old and still can't seem to confront similar measure of time and investigation which implies it is conceivable that it has blemishes. Notwithstanding, this is not really set in stone. Subsequently for email hashing it would be best as far as we're concerned to pick a similar which would lead us to the end.

8.3) Personal Data:

There is in any case an interest for quick programming hashing for applications, for example, respectability checking and deduplicationin filesystems and distributed storage, have based interruption discovery, variant control frameworks, or secure boot plans. SHA-3 doesn't fit these requirements well-for instance on Qualcomm's Krait microarchitecture SHA-3-256 takes around 20% longer to hash a message than SHA-256 does, and on Intel's Ivy Extension microarchitecture2 SHA-3-512 accepts about two times the length SHA-512 does

BLAKE-2 is one more better form of SHA-3 for speeding the calculation. The designated applications incorporate distributed storage, interruption location and rendition control frameworks. This comes in 2 primary variations, the blake-2b which is enhanced for 64-bit stages and blake-2s for additional more modest structures.

9.REFERENCES

[1] A.V. Aho, J.E. Hopcroft, and J.D. Ullman, “TheDesign and Analysis of Computer Algorithms,” Addison- Wesley, 1974.

[2] D. Davies and W. L. Price, “Digital signatures, anupdate,” Proc. 5th International Conference on Computer Communication, October 1984, pp. 845–849.

[3] Bart Preneel, “CRYPTOGRAPHIC HASH FUNCTIONS”, 1993.

[4] Per Thorsheim, “Improving Usability of Password Management with Standardized Password Policies”, Conference Paper, · May 2012

[5] R. Venkatesan, S.-M. Koon, M. H. Jakubowski, and P. Moulin, “ROBUST IMAGE HASHING” ,2000

[6] Melima Sumagita, Analysis of Secure Hash Algorithm (SHA) 512 for Encryption Process on Web Based Application:

[7] Proposed Model for Triple-DES Encryption published in IBM Journal of Research and Development by

[8] D. Coppersmith, D.B. Johnson, S.M. Martyas Image Encryption Based on the Modified Triple- DES Cryptosystem by Victor Manuel Silva, R Flores, L Lopez

[9] Hao Cheng, Efficient Implementation of the SHA- 512 Hash Function for 8-bit AVR Microcontrollers

[10] Mary Cindy, Security Analysis of MD5 algorithm in Password Storage

[11] W. Hohl, X. Lai, Th. Meier, and C. Waldvogel, “Security of iterated hash functions based on block ciphers,” Advances in Cryptology, Proc. Crypto’93, LNCS, Springer- Verlag, to appear.

[12] “Hash Functions Using a Pseudo Random Algorithm,” ISO/IEC JTC1/SC27/WG2 N98, Japanese contribution, 1991

[13] Y.J. Huang and F. Cohen, “Some weak points ofone fast cryptographic checksum algorithm and its improvement,” Computers & Security, Vol. 7, 1988, pp. 503–505.

[14] “Digital Signature Standard,” Federal Information Processing Standard (FIPS), Draft, National Institute of Standards and Technology, US Department ofCommerce, Washington D.C., August 30, 1991.