International Journal of Future Generation Communication and Networking
Vol. 13, No. 1, (2020), pp.758-764

A Novel Framework to Enhance Security Features in Social Media Network

Roopini. J* and N. Anuradha
Assistant Professor, Department of Computer Science and Applications, Krupanidhi Degree College, Bangalore

Abstract

With the progression of innovation, the Social Media has become a generally utilized medium of correspondence. Million quantities of individual all over on the planet can get the usage of innovation. Novel issues like Cyber stalking have been expanding worldwide consideration. Cyber stalking can be clarified as risking conduct or bothersome advances expected for another utilizing the Internet and other method for online correspondences and also different associations and organizations are additionally utilizing the web so as to present their items or administrations around the globe. This paper centers on giving security to users information by utilizing the argon2 and bcrypt hashing algorithms. The framework of Argon 2 hashing method along with bcrypt algorithm has been proposed to strength the security of the user data.

Keywords: *Security, Hashing, Argon 2, Bcrypt*

Introduction: Millions of people are hooked on to Social networking sites. However, allows people to socialize nevertheless of distance. Usage of social media has its own pros and cons as per the studies. With the development of social media, a common problem surfaced is fake online profiles. It allows one to steal the identity of another and take advantage on it. Social Media is the chief means of communication which allows the user to post their thoughts, ideas, news in no time etc. It plays a vital role and has remarkable place in globalization. Though Social Media has its superiority, there is always a question in users mind over social media – whether it is boon or curse for us. This question arisen because of anti- social activities which are charged by social media.

Online social associations have made enormous amounts of information inside the systems. Such information contains numerous private and delicate insights concerning people. Subsequently, Data anonymization is required before the information are made generally accessible for commercial or logical research. Sensitive data must be protected in order to overcome the cyber-crimes such as cyberbullying, Cyber stalking, scams, harassments, robbery etc.

On the off chance that putting away secret key (passwords) in a plain content or is undermined through simple encryption technique then there are potential outcomes of unscrambling of secret word and stolen.

To protect the sensitive data of the users, cryptographic hashing algorithms are used. Hashing capacities are a fundamental piece of cyber security. Hashing the secret key is better technique than encryption because hashing is a one way function. Hash capacities are very valuable and show up in practically all data security applications. Hashing is a strategy for cryptography that changes over any type of information into a remarkable string of content. Any bit of information can be hashed, regardless of its measure or type.

ISSN: 2233-7857 IJFGCN

The cryptographic hashing algorithm such as Scrypt, Sha_256, Sha_512, PBKDF2, Bcrypt, MD5, Argon2 are the most recommended password hashing algorithms. This paper proposed the framework of Argon 2 hashing method along with bcrypt algorithm to strength the security of the sensitive data.

Review of Literature

The research compared and analyzed the performance of three types of algorithm i.e; PBKDF2, Scrypt, Bcrypt in mobile platforms by developing the android application. It has found that among all these three types of algorithms PBKDF2 is faster but not strong as it has been cracked. Hence, Bcrypt and Scrypt is strongest and is depends on memory hard and takes more time and computational power to crack the password [1].

Another methodology is utilizing dispersed preparing to register different hashes at an exceptionally fast, making one of the most generally utilized hashing calculation SHA-512 which is not used excessively, and not considering all cryptographic parameters. And this framework proved that Bcrypt is the fastest algorithm with 3310 hashes per second [2].

A 256 Bit Hash function designed i.e; FORK-256 which provides more security against attacks and faster computation than SHA_256 algorithm [3].

Another research focused on solving the two major features like authenticity and privacy for the network users which uses strong password, salt, key stretching and chaining method to minimize the data attacks [4].

Research based on cryptographic algorithm focused on Bcrypt hashing algorithm using Advanced Encryption Standard (AES) encryption technique to check whether the hashed password could be cracked using brute force attack and word reference table. This research applied Bcrypt algorithm on the original password and to undergo through the AES algorithm to get the final hashed password [5].

The architecture, operation and features of Argon2 are simplified, compact in size and clear to understand which has been selected as the winner of PHC [6].

Argon2

Argon2 is cryptographic hashing calculation, for secret key hashing. Argon2 has 3 variations: Argon2d, Argon2i and Argon2id. Argon2i is improved for secret key hashing. Argon2 has six information parameters such as secret key, salt, memory cost, execution time cost, parallelism factor based on quantity of parallel strings and hash length. Argon 2i is preferred for password hashing which uses data independent memory access. It is also suitable for password based key derivation method. Argon 2i is best in protecting the tradeoff attacks as it makes more passes over the memory [7] [8].

The values of the parameters of Argon2 are hash length is 16, memory cost is 102400, Parallelism is 8, salt length is 16 and time cost is 2. As the values of the parameters are visible in the function to any individual, security of the password is reduced. The parameters should not be invisible as the values are required for recalculation of hash value and also if the parameters are hidden, the verification process of the hash value is also gets difficult. Considering these points, the disadvantage of visible parameters has to overcome and the mechanism has to be improvized.

ISSN: 2233-7857 IJFGCN

The Fig.1 shows working of Argon2, it depicts the working process of Argon2 where the password and salt value is given to the Argon2 hash function which uses the visible parameters with the password for encrypting which in turn generates the hash value.

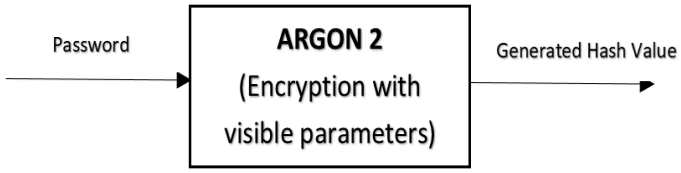

Fig.1 Working of Argon2

In the existing system, it is found that the generated hash value is less secured because of visible parameters of the hash function which is not preferable for storing the user data. Hence hackers can easily trap the parameters values and hack the passwords. So, to eliminate this scenario, a new framework for enhancing the security is proposed.

Proposed Framework

In the proposed framework, the two best algorithms such as bcrypt and argon2 has used to provide greater mechanism of protecting the private data.

The Fig.2: shows Proposed Framework, it projects that the original password is initially passes to the Bcrypt hash function for the encryption which uses two parameters password and salt (random generated value), the resultant hash value and salt will be given as an input to the argon2 hash function to get the final hash value which are stored.

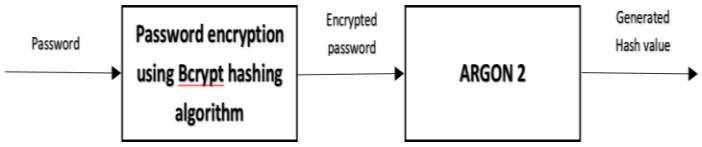

Fig.2: Proposed Framework

By applying this method, the chances of hacking private data can be reduced. Though hackers found the value of the parameters and try to crack, the resultant value will be hash value again. Hence, this will lead hackers to be perplexed.

Result and Analysis of Argon 2

Tab.1 shows Parameters in Argon2 to depict the default values of Argon2 Parameters.

Tab.1: Parameters in Argon2

Argon2 Parameters	
SALT Size (In terms of Bytes)	
Default Size	16
Minimum Size	8
Maximum Size	4294967295

ISSN: 2233-7857 IJFGCN

Rounds	
Default Rounds	2
Minimum Rounds	1
Maximum Rounds	4294967295
Rounds Cost	Linear
User Defined	Yes
Encoding Method	
Encoded Checksum Size	16 bytes
Encoding Scheme	Base 64
Encrypted Password Size	77

Tab.2 shows the Hashed Values and Time Taken to generate the Hash Values to project the generated hash values from the password and the time taken to generate the values and also shows that the time is increasing based on the size of the password.

Tab.2: Hashed Values and Time Taken to generate the Hash Values.

Size of Password (In terms of Bytes)	**Password**	**Hash Value**	**Time Taken to Hash**
5	a@123	'$argon2id$v=19$m=102400,t=2,p=8$89kmLhPZub8aT4EgzPuhwQ$OPdpjAGAjFhVn36jMq3qew'	1.7
14	abcdefghij@123	'$argon2id$v=19$m=102400,t=2,p=8$Mzb0BuClpZgacACvHv6LGA$x4fBM0py+wrdpw4F8v	1.8

ISSN: 2233-7857 IJFGCN

		byZQ'	
20	abcdefghijklmnop@123	'$argon2id$v=19$m=102400,t=2,p=8$F2uugHtbDjnnNjjKR+CkiA$zlj17FXl+Jlk+d38AJeueg'	1.9
27	abcdefghijklmnopqrstuvw@123	'$argon2id$v=19$m=102400,t=2,p=8$GZoETum/B0T/pUOps+JW1w$nYAUXPFxZgRFkOoa86n9SA'	2.4

The Fig.3 Time Analysis to Hash the Password shows that how the time is increasing based upon the password's size.

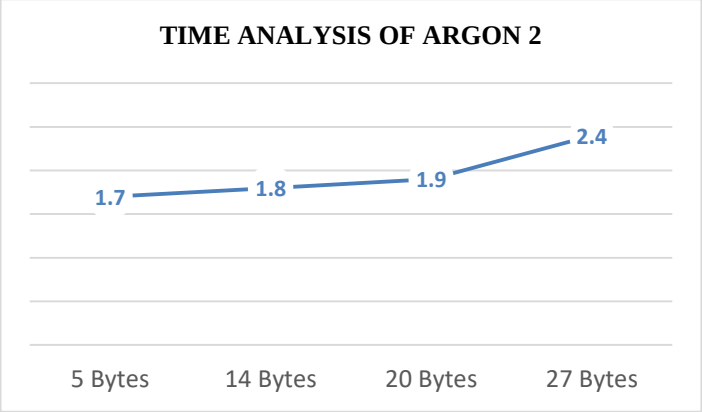

Fig.3: Time Analysis to Hash the Password.

Conclusion

In the study of Argon2 has been observed that there is a disadvantage of visible parameters in the hash function, due to which the security mechanism of user data is reduced. To overcome this problem, a new framework has been introduced by using two algorithms such as Bcrypt and Argon2. In this process, two hash values are generated wherein, the first hash value gets generated by passing the password through the Bcrypt hash function and the second hash value is generated by passing the hash value and salt to the Argon2 hash function and stored. Therefore, though the parameters of the hash function of Argon2 is

ISSN: 2233-7857 IJFGCN

visible to the hackers, the process of cracking the password will be challenging. Hence, the security of user data has been enhanced.

Acknowledgement

The authors express their sincere gratitude to The Management, Krupanidhi Group of Institutions for supporting the work through Krupanidhi Research Incubator Centre (K-RIC) under Krupanidhi Degree College and the Research Mentors, Accendere, CL Educate Ltd.

References

[1] Zhiyong Zhang, Brij B. Gupta, Social media security and trustworthiness: Overview and new direction, Elsevier B.V., ISSN No-0167-739X, DOI:dx.doi.org/10.1016/j.future.2016.10.007, 2016, pp 1-12
[2] W.Akram, R.Kumar, A Study on Positive and Negative Effects of Social Media on Society, International Journal of Computer Sciences and Engineering, ISSN No-E-ISSN: 2347-2693, Volume-5, Issue No-10, 2017, pp 347-354
[3] A.T.M Shahjahan, Kutub Uddin Chisty, Social Media Research and Its Effect on Our Society, International Journal of Information and Communication Engineering, ISNI: 0000000091950263, Volume-8, Issue No-6, 2014, pp 2009-2013
[4] Markku-Juhani O. Saarinen, Cryptanalysis of Block Ciphers Based on SHA-1 and MD5, International Association for Cryptologic Research, 2003, pp 36-44
[5] Levent Ertaul, Manpreet Kaur, Venkata Arun Kumar R Gudise, Implementation and Performance Analysis of PBKDF2, Bcrypt, Scrypt Algorithms
[6] Atishay Aggarwal, Pranav Chaphekar, Rohit Mandrekar, Cryptanalysis of bcrypt and SHA-512 using Distributed Processing over the Cloud, international Journal of Computer Applications, Volume 128 – No.16, 2015, pp 13-16
[7] A.Arul Lawrence Selvakumar, C.Suresh Ganandhas, The Evaluation Report of SHA-256 Crypt Analysis Hash Function, International Conference on Communication Software and Networks, DOI 10.1109/ICCSN.2009.50, 2009
[8] P. Sriramya and R. A. Karthika, Providing password security by salted password hashing using bcrypt algorithm, ARPN Journal of Engineering and Applied Sciences, Volume. 10, NO. 13, 2015, pp 5551-5556
[9] Narander Kumar and Priyanka Chaudhary, Password Security Using Bcrypt with AES Encryption Algorithm**,** Springer Nature Singapore Pte Ltd, doi.org/10.1007/978-981-10-5544-7_37, 2018, pp 385-392
[10] Alan Kaminsky , Michael Kurdziel , Stanisław Radziszowski, An Overview of Cryptanalysis Research for the Advanced Encryption Standard, pp 1-8
[11] Ashish Kumar Kendhe, Himani Agrawal, A Survey Report on Various Cryptanalysis Techniques, International Journal of Soft Computing and Engineering (IJSCE) ISSN: 2231-2307, Volume-3, Issue-2, May 2013, pp 287-293

ISSN: 2233-7857 IJFGCN

[12] Detchasit Pansa, Thawatchai Chomsiri, Web Security Improving by using Dynamic Password Authentication, International Conference on Network and Electronics Engineering, IPCSIT vol.11, 2011, pp 32-36
[13] Alex Biryukov, Daniel Dinu, Dmitry Khovratovich, Argon2: new generation of memory-hard functions for password hashing and other applications, IEEE European Symposium on Security and Privacy, ISSN No: 978-1-5090-1752-2/16, DOI:10.1109/EuroS&P.39, 2016, pp 292-302
[14] white paper, Argon2.online, November 20th, 2019
[15] Alex Biryukov, Daniel Dinu, and Dmitry Khovratovich, Argon2: the memory-hard function for password hashing and other Applications, 2017, pp 1-20
[16] white paper, statista.com, November 22nd , 2019
[17] white paper, cybintsolutions.com, November 22nd 2019
[18] white paper, betanews.com, November 22nd , 2019
[19] white paper, consumeraffairs.com, November 22nd , 2019
[20] white paper, gartner.com, November 22nd , 2019
[21] white paper, securityintelligence.com, November 22nd , 2019
[22] white paper, thycotic.com, November 22nd , 2019

ISSN: 2233-7857 IJFGCN