|| Volume 3 || Issue 2 || February 2018 || ISSN (Online) 2456-0774
INTERNATIONAL JOURNAL OF ADVANCE SCIENTIFIC RESEARCH
AND ENGINEERING TRENDS

Survey Paper on Different Type of Hashing Algorithm

Mahesh A. Kale[1], Prof. Shrikant Dhamdhere[2]
Student, Department Computer Engineering, P.G.M.C.O.E, Pune, India[1]
HOD, Department Computer Engineering, P.G.M.C.O.E, Pune, India[2]
maheshkale11196@gmail.com[1], dhamdhere2007@gmail.com[2]

***Abstract*— Hash Functions are vital apparatus in data security over the web. The hash capacities that are utilized as a part of different security related applications are called cryptographic hash capacities. They acknowledge subjective length of information and create a normally little, settled size yield, known as message process. They are intended to give message uprightness, i.e. on the off chance that the message has been changed after transmission from sender and before it might be gotten by the comparing recipient, can be followed by the collector, and along these lines, such a altered message can be disposed of. This property is moreover helpful in may different applications, for example, production of computerized signature and arbitrary number age and so forth. The vast majority of the hash capacities depend on Merkle-Damgard development, for example, MD-5, SHA-1, SHA2, SHA3 and so forth, which are definitely not hundred percent safe from assaults. The paper examines a few of the assaults that are conceivable on this development, and subsequently on these hash capacities likewise confront same assaults.**

Keywords: *Hashing Algorithms, SHA-1, SHA-2, SHA-3, MD5*

I INTRODUCTION

A cryptographic hash work is an extraordinary class of hash work that has certain properties which make it appropriate for use in cryptography. It is a numerical calculation that maps information of subjective size to a bit string of a settled size (a hash) and is intended to be a restricted capacity, that is, a capacity which is infeasible to modify. The best way to reproduce the info information from a perfect cryptographic hash capacity's yield is to endeavor a beast constrain inquiry of conceivable contributions to check whether they create a match, or utilize a rainbow table of coordinated hashes. Bruce Schneier has called one-way hash works "the workhorses of current cryptography".The info information is regularly called the message, and the yield (the hash esteem or hash) is frequently called the message process or basically the process. The perfect cryptographic hash work has five principle properties:

(1)It is deterministic so a similar message dependably brings about a similar hash.

(2) It rushes to register the hash an incentive for any given message.

(3) It is infeasible to create a message from its hash an incentive with the exception of by attempting every single conceivable message.

(4) A little change to a message should change the hash esteem so broadly that the new hash esteem seems uncorrelated with the old hash esteem

(5) It is infeasible to discover two distinct messages with a similar hash esteem

1.1 Hashing

Hashing is a sort of algorithm that takes information of any size and changes over it into information of settled size. The principle contrast between hashing and encryption is that a hash is irreversible. Hash capacities are utilized for hashing. A hash work is any capacity that can be utilized to delineate of subjective size to information of settled measure. The yield of the hash work is called hash codes, hash values, hash entireties, or hashes.

A hash function should satisfy the following:

a) Two distinct messages ought not have a similar hash esteem. In this manner, the hash capacity ought to be safe against impact.

b) Given a hash esteem, it ought to be troublesome or for all intents and purposes difficult to create the relating message. In this manner, the hash capacity ought to have pre-picture protection.

1.2 Hashing Algorithms

a) MD5:

This algorithm takes information of self-assertive length and produces message process of 128 bits (i.e. 16 bytes). In this algorithm, the info message is broken into pieces of 512-piece squares. The message is cushioned by a 1 took after by zeros so that the message length is 64 bits not exactly a different of 512. The rest of the bits are loaded with 64 bits speaking to the length of unique message. This hashing algorithm is comprehensively used yet, it is slanted to crashes. Nonetheless, by and by, the impact assault is too ease back to possibly be valuable. This is softened up respect to crashes however not as

to pre-pictures or second-pre-pictures.

b) SHA1:

Creating SHA-1 crashes isn't that simple. It appears to be sensible that the assault with has been depicted on SHA-1 truly works with a normal cost of 261, considerably speedier than the non specific birthday assault (which is in 280), yet at the same time very troublesome. With a considerable measure of hand-waving, I could assert that SHA-1 is more powerful than MD5 in light of the fact that it has more adjusts and on the grounds that the induction of the 80 message words in SHA-1 is substantially more "blending" than that of MD5. While there are some known assaults on SHA1, they are considerably less genuine than the assaults on MD5.For this reason, SHA1 is a greatly improved decision than MD5 in numerous settings.

c) SHA2:

Secured hash work 2 is a hash algorithm that takes a string of any length and diminishes it to a message process. The SHA-2 family includes six hash capacities with hash esteems that are 224, 256, 384 or 512 bits: SHA-224, SHA-256, SHA-384, SHA- 512, SHA-512/224, and SHA-512/256. In this algorithm, message is "cushioned" with a 1 and the same number of 0's as important to bring the message length to 64 bits not exactly an even various of 512. 64-bits showing the length of unique message are attached to the finish of cushioned message. Cushioned message is prepared in 512-piece squares.

d) SHA3:

SHA-3 is a cryptographic hashing algorithm that was picked by the NSA in 2012 after an open rivalry among non-NSA planners . The earlier name of the SHA-3 hashing algorithm preceding the consequences of the opposition was keccak. Whenever keccak developed as the victor of the SHA-3 rivalry, it was renamed to SHA-3. While SHA-3 bolsters a similar hash lengths as SHA-2, the inward structure altogether different and is resistant to assaults like length expansion which both the MD5 and SHA-1 were ended up being defenseless to. The primary purpose behind the creation of the SHA-3 algorithm is because of the hypothetical assaults that are conceivable against SHA-2. While there no down to earth confirmation has been submitted uncovering the imperfections of SHA-2, one can't deny that it is in fact conceivable.

II LITERATURE SURVEY

1) This review paper thinks about various hashing algorithms what's more, their disadvantages. The client must know the sorts of assaults and should apply suitable hashing calculation to stay away from assaults [1].

2)This exploration paper comprises of examinations between distinctive secure hashing algorithms. Every algorithm takes the ideal opportunity for the algorithm of hash esteem. By registering the time required from each of these algorithm and finding the algorithm which will require the less measure of time for algorithm of the hash esteem we can consolidate the best secure hashing algorithm with organize security algorithm so as to expand the security of the information being sent [7].

3) In this review we have talked about various cryptographic hash algorithms and the fundamental rationale behind them. It is anything but difficult to process the hash an incentive for any given messages and it is infeasible to adjust a message without changing the hash. Cryptographic hash capacities have numerous data security applications, prominently in computerized marks, message verification codes (MACs), and different types of verification. It is particular that cryptographic hashing algorithms can be made non cryptographic by making reasonable changes in the hashing plans. This audit paper will profit the investigate group working in the fields of systems administration also, data security [6].

4) This paper recommends that the SHA algorithms ought to be given vital significance in contrast with MD5 as SHA algorithms' execution is outperforming other cryptographic hash algorithm capacities. Soon, new inquires about would be ropounded proposing a similar conclusion and more data would be amassed which could be utilized as a driving element in the innovative testing of the cryptographic hashing algorithms. This would bring about a definitive endorsed predominance of SHA algorithms most importantly cryptographic hash algorithms [5].

5) This relative examination helped us to comprehend that the SHA algorithm assumes an essential part in contrast with MD5 on the grounds that SHA algorithms' execution rate is similarly superior to other cryptographic hash algorithm capacities. As a future work, we propose to execute twofold hashing to store passwords in order to outdo both universes. More data would be developed which could be utilized as a thought process in the mechanical testing of the cryptographic hashing algorithms. This would bring about an extreme consequence of utilizing both hashing and securing secret word substantially more proficiently [4].

6) The Secure Hash Algorithm (SHA-1) is utilized for processing a packed portrayal of a message. In the event that we give an info message of discretionary length < 264 bits, it creates a 160-piece yield called the message process. The SHA-1 algorithm is asserted to be secure since it is for all intents and purposes infeasible to figure the message comparing to a given message process. Additionally it is to a great degree unlikely to recognize two messages hashing to a similar esteem. In this way, nowadays the vast majority still utilize SHA1 or even MD5, broken or not. Since the present condition of the workmanship in hashing is that we have a few capacities that we know have hypothetical vulnerabilities however no genuine down to earth breaks, and some problematic capacities that we

know next to no about by any means. Regardless of whether there has never been an effective finish impact with SHA1, the development of our PCs' estimation limits will before long make it conceivable. Along these lines, mammoth organizations like Google, Microsoft, and so on intending to murder SHA-1in close future to make web more secure [2].

7) This work closed the general view about the leaving hash work based algorithms. It is discovered that all the uprightness algorithms have demonstrated brittle with the exception of SHA-2 yet it isn't time effective. SHA-1 hashing algorithm regarding the quantity of savage power assaults expected to break it and additionally it is quick when contrasted with the other secure hash algorithms. Numerous scientists have proposed their own algorithms however none of them are time productive as SHA-1 and furthermore there are odds of enhancing the inward quality of these algorithms. In not so distant future we can build up a algorithm that is more secure, less time expending, and better piece distinction when contrasted with existing algorithms [8].

Table 1: Algorithms and Limitations

Sr No	***Hashing Algorithms***	***Limitations***
1	SHA-1	This requires a lot of computing power and resources
2	SHA-2	Increased resistance to collision means SHA256 and SHA512 produce longer outputs (256b and 512b respectively) than SHA1 (160b). Those defending use of SHA2 cite this increased output size as reason behind attack resistance.
3	SHA-3	SHA-3 is designed to be a good hash-function, not a good *password-hashing-scheme* (PHS), whereas bcrypt is designed to be a PHS and was analyzed in this direction as well.
4	MD5	Using salted md5 for passwords is a bad idea. Not because of MD5's cryptographic weaknesses, but because it's fast. This means that an attacker can try billions of candidate passwords per second on a single GPU.

III CONCLUSION

In this review we have written about various cryptographic hash algorithms and the fundamental rationale behind them. We maintain the hash value by using different hashing algorithm in different situation to check whether the message is modified or not. Which algorithm is more suitable for the particular message is discussed here. We discussed some limitations of SHA-1, SHA-2, SHA-3 and MD5 in this paper.

ACKNOWLEDGMENT

I would like to express my special thanks of gratitude to our HOD Prof. Shrikant Dhamdhere for guided me and help me to understand algorithms of hashing algorithm. Which also helped me in doing a lot of Research and I came to know about so many new things I am really thankful to them.

.REFERENCES

[1] G. Tejaswini Bhorkar, "A Survey of Password Attacks and Safe Hashing Algorithms International Research Journal of Engineering and Technology (IRJET), Volume: 04 Issue: 12 Dec-2017

[2] Chaitya B. Shah, Drashti R. Panchal "Secured Hash Algorithm-1: Review Paper" International Journal For Advance Research In Engineering And Technology, Volume 2, Issue X, Oct 2014

[3] Ankit Kumar Jain, Rohit Jones, Puru Joshi, "Survey of Cryptographic Hashing Algorithms for Message Signing" IJCST Vol . 8, Issue 2, April - June 2017

[4] C.G Thomas, Robin Thomas Jose, "A Comparative Study on Different Hashing Algorithms" International Journal of Innovative Research in Computer and Communication Engineering, Vol. 3, Special Issue 7, October 2015

[5] Surbhi Aggarwal, Neha Goyal, Kirti Aggarwal, "A review of Comparative Study of MD5 and SHA Security Algorithm", International Journal of Computer Applications (0975 – 8887) Volume 104 – No.14, October 2014

[6] K. Saravanan and A. Senthilkumar, "Theoretical Survey on Secure Hash Functions and issues", International Journal of Engineering Research & Technology (IJERT) ISSN: 2278-0181 Vol. 2 Issue 10, October - 2013

[7] Priyanka Vadhera , Bhumika Lall, "Review Paper on Secure Hashing Algorithm and Its Variants" International Journal of Science and Research (IJSR) ISSN (Online): 2319-7064 Impact Factor (2012): 3.358

[8] Sandhya Verma, G. S. Prajapati "A Survey of Cryptographic Hash Algorithms and Issues", International Journal of Computer Security & Source Code Analysis (IJCSSCA), 2015, Vol1, Issue3, ISSN (O): 2454-5651