Discourse Journal of Educational Research
www.resjournals.org/IJER
ISSN: 2346-7045
Vol. 4(1): 1-4, May, 2018

Enhancing Web security using Hash Algorithms: A Comparative Analysis

***Jarikre Amos O.[1] and Rakesh Rathi[2]**

[1]Doctoral Research Scholar,Shri JJT University, Jhunjhunu, Rajasthan, India
[2]Head, Computer Engineering and IT, Government Engineering College, Ajmer, Rajasthan, India

*Email for Correspondence: jarky4u2c@gmail.com, rathirakesh4@gmail.com

Abstract

Security of the web is tantamount to any organization due to the nature of information the web is hosting. Many individuals and organisation now totally depend on the web for storing and retrieval of their information due to the vital importance the web is currently playing in information handling, storing and transmission. But how secure is the web and the information content herein is a paramount issued to many such as organisations that uses the web for the entire college management. In other to strengthen the security of web usage, this paper discusses a comparative analysis of the various hash algorithms that could strengthen web service application such as MD-5, SHA-1, SHA-2, SHA-3 as well as SHA-192 in web security.

Keywords: Web security, Hash Algorithm, Hash function, Web information

INTRODUCTION

Over the years, computing had been experiencing various innovations and advancement that brought about modern computing and the emergence of modern computing has currently change the entire computing environment with innovations of technologies and tools to enhance its usage. The combination of many technologies like virtualization, utility computing, web, clustering, networks and others make the computing environment suitable to create new paradigms to encourage the use of technology and enhance its efficiency (Ennajjar, Tabii, andBenkaddour, 2015). With the web, data can be easily share, process and transmitted faster and more effective but one major predominant concerns encountered with the web is the security of data and information content.

According to Bhargavan, Fournet, Gordon andPucella (2003), a basic motivation for web services is to support programmatic access to web data, and also protect data against hackers and unauthorized users using hash function. The Hash function works better when is used for secured information encryption. Hash functions are the most widespread among all cryptographic primitives, and are currently used in multiple cryptographic schemes and in security protocols(Lakshmananand Muthusamy, 2012). Hence, using hash algorithm to secure web service can be considered to be more protected since data will be encrypted. The hash Algorithm can be considered to be Message-Digest algorithm 5 (MD-5) and Secured Hash Algorithm (SHA) as modern algorithms. The MD5-(Message-Digest algorithm 5), a widely used cryptographic hash function with a 128-bit hash value, processes a variable-length message into a fixed-length output of 128 bits (Suresh and Prasad, 2012). One may encounter SHA as; SHA-1 which is an algorithm that produces a 160-bit hash value; SHA-2 as sets of cryptographic hash functions with different digest sizes (SHA-224, SHA-256, SHA-384, and SHA-512); SHA-3 with robust protocols as compare to SHA-1 and SHA-2 which is not sensitive to extension attacks and SHA-192 as proposed by (Lakshmananand Muthusamy, 2012) being similar algorithm to SHA-1 in structure except that it has one an extra 32-bit word (Lakshmananand Muthusamy, 2012), without an Output Size (Bits) of 192 against 160 of SHA-1.

Hash function

A hash function algorithm is a one way algorithm which is used as a value with a unique size that represents a data. Such data can be file or web password meant to protect web authentication access which have effect in the hash once

there is a change in the data which is fixed. Jacob (2016) pointed out that a hash function is usually considered a way to generate a digest of messages, by making comparison of the digested messages to into order to systematically ascertain if the messages are from same value. Unlike other cryptography algorithms, such as secret key and public key algorithms, the hash functions has not specific key since it's a one-way encryption algorithm. This put the hash function in cryptography as a way of message integrity.Hash functions were introduced in cryptology as a tool to protect the integrity of information (Gupta and Sharma, 2013). Hash functions are generally classified into two main types namely; keyed hash function and unkeyed hash function. While the unkeyed hash function handles the modification detection codes which is also used in cryptography, the keyed hash functions are used in the Message Authentication Code (MAC) whose specification are dictates two distinct inputs a message and a secret key (Lakshmananand Muthusamy, 2012). Again, a dedicated hash function is designed only for hashing by optimized processing and never uses existing system elements (Yang, Kim and Jang, 2012).

Characteristics of Secured Hash Algorithms

The ideal cryptographic hash function has four main or significant properties; it is easy to compute, but it is unlikely to: generate a message that has a given hash, change a message and not change the hash, or find different messages with the same hash (Chandersekaranand Simpson, 2013). There are different types of Hash Algorithm suitable for web service securities which are Message Digest 5 (MD-5) and Secured Hash Algorithm (SHA – SHA-1, SHA-2, SHA-3 and currently SHA-192). Their comparative and distinct functions are discussed below in 3.1, 3.2, 3.3 and 3.4.

MD-5

MD-5 is a widely used cryptographic hash function with a 128-bit hash value processes a variable-length message into a fixed-length output of 128 bits (Kaur and Mahajan, 2013) and less secured hash function compare to SHA. Although, it has a faster speed, MD-5 has only 64 iterations in operation and vulnerable to collisions. As a general purpose hash algorithm, MD-5 had been considered cryptographically broken and shouldn't also be considered for further usage by United States Computer Emergency Readiness Team (US-CERT) due to its vulnerability to attack.

SHA-1

SHA-1 which is fast and input-sensitive, is an evolution of SHA-0 that differs in message expansion. According to Manuel (2011), SHA-1 is a 160-bit dedicated hash function based on the design principle of Merkle-Damg˚ard paradigm (MD4).It is a more secured algorithm than MD-5 in terms of security. Furthermore, SHA-1 provides less collision resistance than was originally expected (Polk, Chen, Turner and Hoffman, 2011), when introduced by National Institute of Standards and Technology (NIST) as a cryptographic hash functions to tackle information handing in the web.SHA has altogether, 80 iterations which consists of 4 x 20(rounds x iterations) as show in Fig. 1. For each operation, the iterations displays are as follows;

abcde - (e +Process P + S^5(a) + W[t] + K[t]), a, S^{30}(b), c, d

Where,

abcde = Register which consists of five(5) variables
Process P = Operational logic
s^t = Circular-left shift of 32-bits sub-block by t bits
W[t] = A 32-bit derived from the 32-bits sub-block
K[t] = Additive constants

SHA-2

SHA-2 is a set of cryptographic hash functions (SHA-224, SHA-256, SHA-384, and SHA-512) designed by the National Security Agency (NSA) and published in 2001 by the NIST as a U.S. Federal Information Processing Standard [8]. In terms of message digest, Moh'd, Aslam, MarziandTawalbeh (2010) suggested that SHA-2 functions have larger message digests, when compared to MD-5 and SHA-1 with 128-bit and 160-bit respectively. The SHA-2 family (SHA-256 and SHA-512) is the object of very intensive cryptanalysis in the world of hash functions (Khovratovich, RechbergerandSavelieva, 2012). Although differs in word size (SHA-256 has 32 bits while SHA-512 has 64bits), SHA-256 have 64 iterations and use 64 different constants, K_t, instead of 80 iterations and 4 constants for SHA-1 (Moh'd*et al,* 2010).

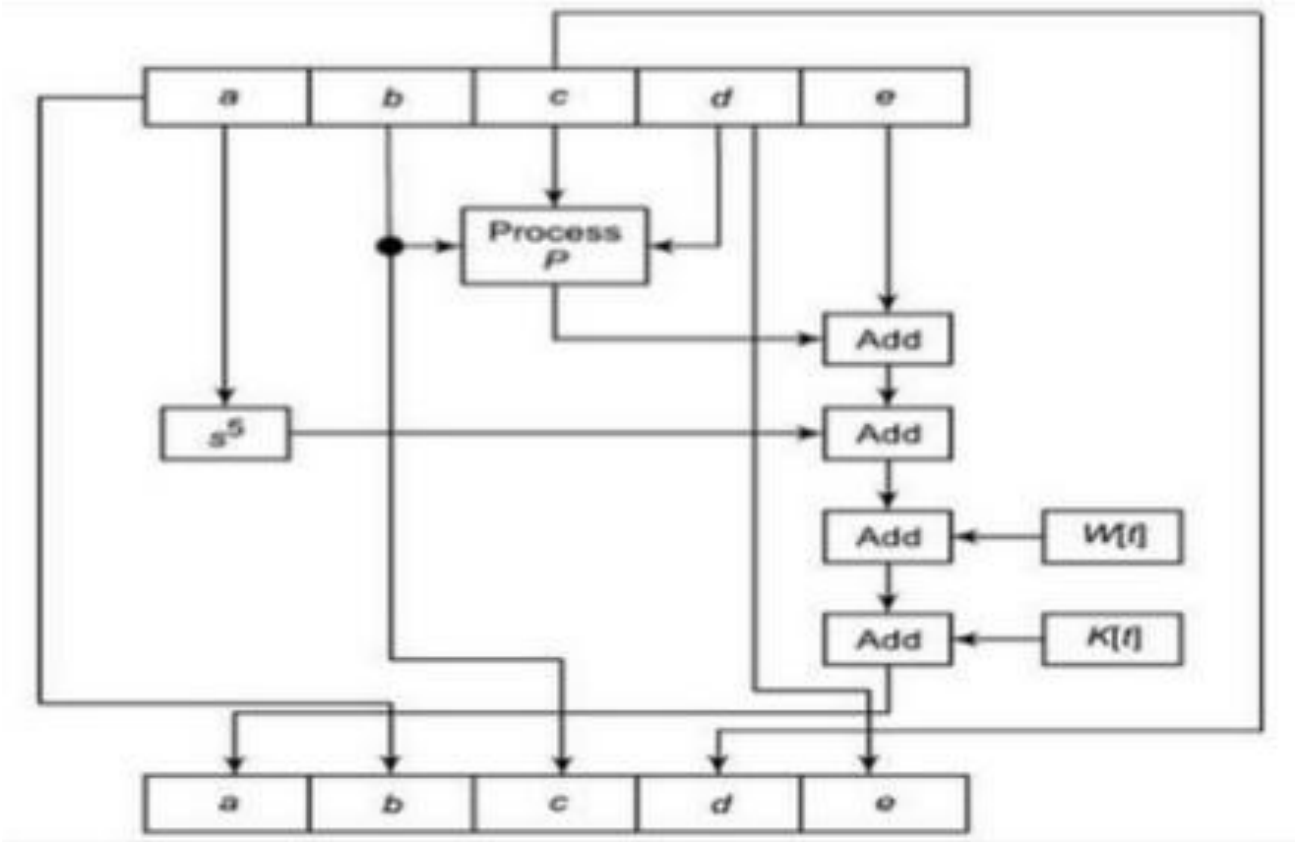

Figure1. SHA-1 iteration

SHA-3

SHA-3 Hash Algorithm was recommended to replace SHA-1 and SHA-2 by US National Institute for Standards and Technology (NIST) due to its ability to provide resistance to attacks and collisions. The call prescribes that SHA-3 must allow for message digests of length 224, 256, 384 and 512 bits, it should be efficient, and most importantly it should provide an adequate level of security (Andreeva, Mennink, PreneelandŠkrobot, 2012). SHA-3is more resistance against implementation attacks than its predecessors. Such implementation attacks are for instance side channel attacks, which utilize all kinds of physical leaking information, e.g. the execution time of the algorithm, the power consumption of the device, or even the electromagnetic emission, in order to recover secret information (Zohner, Kasper, Stöttingerand Huss, 2012). In speed determination, SHA-3 is faster than SHA-1and SHA-2

SHA-192

For SHA-192, its designed was based on the fact that the previous SHA (SHA-1, SHA-2 and SHA-3) are more vulnerable to attacks so therefore it was developed to properly handle such and advanced attacks (pre-image, second preimage and collision) by enhancing web application security. For similarity, SHA-192 has same word size (bits) with the previous SHA and same iterating process (Eighty rounds) with SHA-1 and SHA-2.The modified SHA [SHA-192] uses the padding algorithm, breaking the message into 512 blocks and adding the length as a 64 bit number at end (Lakshmananand Muthusamy, 2012). SHA-192 has been considered to have longer time to generate message digest compared to SHA-1.SHA-192 is considered more secured and useful against attacks associated with its predecessors (SHA-1, SHA-2 and SHA-3) making it more viable to be, used in many applications such as public key cryptosystem, digital signcryption, message authentication code, random generator and in security architecture of upcoming wireless devices like software defined radio etc. (Lakshmananand Muthusamy, 2012).
Some of these key characteristics of hash algorithms which help in analysing their comparison are shown in Table 1 below.

Table 1. Key characteristics of Hash algorithms

Name	Security bits (Info)	Round	Block Size (Bits)	WordSize (Bits)	OutputSize (Bits)
MD-5	<64	64	512	32	128
SHA-1	<32	80	512	32	160
SHA-2	112, 128, 192, 256	80	512	32	224
SHA-3	112, 128, 192, 256	24	512	32	224
SHA-192	64	80	512	32	192

Conclusion

Currently, hash functions are regards to be very important tool in handling information security base on its ability in ensuring organisationstores, process and shares data over the web using secured and preserve means. With SHA, an encryption of user's authentication and preservation of user's information is effective. With the introduction of SHA-192 with a much larger bit difference having 192 bits length of message digest, it reduces the security issue on SHA-1 and MD-5 which are associated with collision attacks. Hence, it is evidence for the analysis discussed above that the web requires strong cryptographic serviceswhich poses as high security assurance for stored, processing and shared data in order to cope with the ever-increasing computation threats

References

Andreeva, E., Mennink, B., Preneel, B., andŠkrobot, M. (2012).Security analysis and comparison of the SHA-3 finalists BLAKE, Grøstl, JH, Keccak, and Skein. Progress in Cryptology-AFRICACRYPT 2012, 287-305.

Bhargavan, K., Fournet, C., Gordon, A. D., andPucella, R. (2003, November).TulaFale: A security tool for web services. In International Symposium on Formal Methods for Components and Objects (pp. 197-222).Springer, Berlin, Heidelberg.

Chandersekaran, C., and Simpson, W. R. (2013).Cryptography for a High-Assurance Web-Based Enterprise.In Proceedings of the World Congress on Engineering and Computer Science (Vol. 1).

Ennajjar, I., Tabii, Y., andBenkaddour, A. (2015). Improving Data Sharing Security in Cloud Computing. In BDCA (pp. 46-50).

Gupta, G., and Sharma, S. (2013, April). Enhanced SHA-192 Algorithm with Larger Bit Difference. In Communication Systems and Network Technologies (CSNT), 2013 International Conference on (pp. 152-156). IEEE.

Jacob Su (2016). “Hash functions in web security.” Available online at https://medium.com/@zpcat/hash-functions-in-web-security-61d287aa1307.

Kaur, G., and Mahajan, M. (2013).Analyzing Data Security for Cloud Computing Using Cryptographic Algorithms.International Journal of Engineering Research and Application, ISSN, 2248-9622.

Khovratovich, D., Rechberger, C., andSavelieva, A. (2012).Bicliques for preimages: attacks on Skein-512 and the SHA-2 family. In Fast Software Encryption (pp. 244-263).Springer Berlin/Heidelberg.

Lakshmanan, T., and Muthusamy, M. (2012).A novel secure hash algorithm for public key digital signature schemes. Int. Arab J. Inf. Technol., 9(3), 262-267.

Manuel, S. (2011). Classification and generation of disturbance vectors for collision attacks against SHA-1. Designs, Codes and Cryptography, 59(1), 247-263.

Moh’d, A., Aslam, N., Marzi, H., andTawalbeh, L. A. (2010, July). Hardware implementations of secure hashing functions on FPGAs for WSNs.In Proceedings of the 3rd International Conference on the Applications of Digital Information and Web Technologies (ICADIWT).

Polk, T., Chen, L., Turner, S., and Hoffman, P. (2011). Security considerations for the sha-0 and sha-1 message-digest algorithms (No.RFC 6194).

Suresh, K. S., and Prasad, K. V. (2012). Security issues and security algorithms in cloud computing. International Journal of Advanced Research in Computer Science and Software Engineering, 2(10).

Yang, H. S., Kim, S. S., and Jang, H. S. (2012). Optimized security algorithm for IEC 61850 based power utility system. Journal of Electrical Engineering and Technology, 7(3), 443-450.

Zohner, M., Kasper, M., Stöttinger, M., and Huss, S. A. (2012, March).Side channel analysis of the SHA-3 finalists. In Proceedings of the Conference on Design, Automation and Test in Europe (pp. 1012-1017). EDA Consortium.