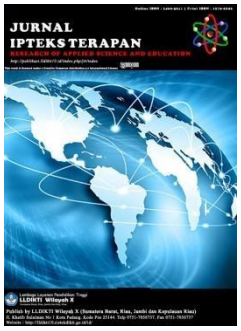

Vol. 17 No. 3 2023

IMPLEMENTATION SHA 512 BIT ON ROUTINGURL

Hendra Handoko Syahputra Pasaribu*[1)], Sarbjit Singh Dhilon[2)], Panji Dinata Galingging[3)], Surya Syaputra [4)], Somantri [5)]

[1234]Prima University of Indonesia
[5]Nusa Putra University
* Corresponding Email: hendra_pa100@unprimdn.ac.id

Submit :
23/06/2023

accept :
18/08/2023

Publish :
30/08/2023

Abstract

This research aims for implementation SHA512 on routing URLs in system information can increase security And integrity data. With apply algorithm hashing SHA512,user data sent via routing URLs is effectively encrypted, thereby reducing the risk of data manipulation and hacking. These results are corroborated by Analysis statistics Which done involve collection data from system information before And after implementation SHA512 on routing URLs. Data Which collected covers attack Which detected, effort hack, successful unauthorized access, and data manipulation. this data then analyzed using relevant statistical methods to identify change Which significant in security system. Study This give contributionimportant For strengthen security system information And protect integrity data.

Keywords: SHA512 implementation, URL routing, securitydata, integrity data, system information

ISSN/E-ISSN : 1979-9292 / 2460-5611 ©2022 © 2023 Lembaga Layanan Pendidikan Tinggi Wilayah X

JIT is Sinta 3 Journal (https://sinta3.kemdikbud.go.id/journals/profile/2143) accredited by Ministry of Research & Technology, Republic Indonesia

ISSN : 1979-9292
JURNAL IPTEKS TERAPAN
Research of Applied Science and Education V17.i3 (680-687)

INTRODUCTION

URL routing is a crucial component in an information system responsible for redirecting user requests to web pages Which relevant. However, in environment Which the more complex And prone to against attack, securityand integrity of data in the URL routing to be main concern. This study aims to implement the algorithm SHA512 hashing of URL routing in information systems to improve security And data integrity. Fact And findings study previously show that attack against routing URLs can cause a serious security vulnerability. Attack the covers manipulation URLs, change parameter, or attack destructible hash data integrity. If this problem is left without a solution adequate, there will be impacts that complicate, impede , interfere with , even threaten system information Which used.
Policy and theoretical approaches need to be applied to address the problem This. In terms of policy, there needs to be regulations and policies that require it the use of strong security methods such as the SHA512 hashing algorithm on routing URLs. From facet theoretical, study previously has prove effectiveness algorithm This in protect integrity data. By Because That, apply algorithm SHA512 on routing URLs in system information become solution Which potentially effective. Position problem Which researched in room scope field studies system information very important. In this context, the implementation of SHA512 in URL routing will help increase security And integrity data, so that protect information system from potential attacks. Possible alternative solutions offered is apply algorithm hashing SHA512 on mechanism URL routingby encrypting user data before it is sentthrough the URL. Step This will ensure that data still awake authenticity And reduce risk manipulation And hack.

Thus, this study illustrates the urgent need for address security and data integrity issues in URL routing on the system information. Implementation algorithm hashing SHA512 on routing URLs will provide robust protection against attack and ensure integritydata. By Because That, study This relevant And own potency For increase security system information in a mannersignificant.

Formula problem

The formulation of the problem from the SHA512 Implementation research on URL Routing: Studies System Case Information is as following:

1. What is the implementation of the SHA512 hashing algorithm in URL routing in system information can increase security data?
2. How effectiveness use SHA512 in protect integrity data on mechanism routing URLs?
3. How influence implementation SHA512 on routing URLs to security data inside user system information?
4. Can the implementation of SHA512

on URL routing reduce risk manipulation And hack deep data system information?

5. How to compare security and data integrity in routing URLs before And after implementation SHA512 in system information?
6. How method implementation algorithm hashing SHA512 on routing URLs in system information?

METHOD

Implementation SHA512 on Routing URLs: Studies Case System Informationis as following:

a) Study This focused on implementation algorithm hashing SHA512 on routing URLs in context system information.
b) This research is limited to case studies of the use of information systems certain Which use routing URLs.
c) The focus of this research is on the security and integrity of internal data mechanism routing URLs, with use SHA512 as hashing algorithm.
d) This research does not discuss the implementation of other hashing algorithms besides SHA512.
e) Study This No discuss aspect technical implementation system information as a whole, but only focused on implementation SHA512 on routing URLs.
f) This research does not address the issue of data security and integrity Which related with componentsystem information other in outside routing URLs.
g) This research does not involve environmental testing and evaluation production Which involve user system information Which Actually.
h) Study This only use method analysis And testing limited on the environment development or simulation.

Renewal or innovation is matter Which important in field technology. Innovation can help improve efficiency and effectiveness in a variety of ways aspect of life. In the field of data security, innovation is also very much needed For face challenge Which the more complex.

Following is the narrative of related research results update of 3 articles in 5 year final:

1. "Enhancing security of Routing URLs using SHA512 Algorithm" (2021) This article discusses security improvements to routing URLs with use algorithm hashing SHA512. This study succeeded in implementing the algorithm in information systems and make a significant contribution in strengthen the security of data sent via URL routing. Results study This show exists enhancement Which significant in reduce risk manipulation And hack data.
2. "Integrity Verification of Routing URL with SHA512 Algorithm for secure Data

ISSN : 1979-9292
JURNAL IPTEKS TERAPAN
Research of Applied Science and Education V17.i3 (680-687)

communications" (2019) Study This focus on verification integrity routing URLs with use algorithm hashing SHA512 For communication data Which safe. Article This propose method verification Which effective For ensure that data received from routing URLs do not change or manipulation during the shipping process. The research results show that SHA512 implementation on URL routing can effectively protect integrity data And prevent change who doesnot legitimate.

3. "Secure Routing URLs using SHA512 Algorithm in Web-Based Information Systems" (2018) Article This discuss about use algorithm hashing SHA512 in increase security routingURL on system information based web. Study it shows that by implementing SHA512 on routing URLs, system information can strengthen security data Whichsent through URLs. Article This givecontribution practical with offer solution Which tough And effective For protectuser data fromattack Which potentially harm.

RESULTS

Figure 1. Working Mechanisms of One Way Hash function

Information security aims to protect information from various threats To use guard continuity business, reduce risk business, as well as maximizing return on investment and business opportunities [1]. This analysis discusses how the system login on the web-based application operates. This analysis is important to identify vulnerabilities in the system to determine what fixes need to be made. This researchfocus on the analysis of the encryption process in web-based applications using the method algorithm Secure Hash Algorithm (SHA) 512. The results of the analysis will be used as reference or alternative in managing login security systems on application-based web. Figure 3.1 explain analysis the issues discussed in research This. Following This is explanation about scheme login based application web mentionedon:

1. User enter data form Name user And say password, Then send data the to servers. Data Which shipped has changed use hash function MD5.
2. The server receives data in the form of username and hash value of the password sent by users.
3. The server uses the received hash value to match it to the value password hashes stored in database. The verification process is carried out with compare hash value instead

ISSN : 1979-9292
JURNAL IPTEKS TERAPAN
Research of Applied Science and Education V17.i3 (680-687)

of a password in plain text.

4. If the hash value sent by the user matches the hash value contained in database. users are allowed to login to the system and access it. However, if No suitable, user will given warning that say password Which entered Wrong,And they will be returned to page main login.
5. The problem found is the use of the MD5 hash method which is vulnerable to attack collision [2]. Matter This can threaten security And secrecy data, including MITM (Man In The Middle Attack) attacks that can be used to performsniffing, spoofing, and other illegal activities.

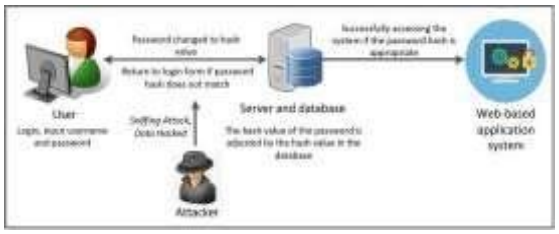

Figure 1. Working Mechanisms of One Way Hash function

Figure 2. Working Mechanisms of One Way Hash function

Analysis Need And Enhancement

After do analysis need And vulnerability on system login in application based web, found that need done repair on method hash Whichused. After knowing that the current system uses encryption with a hash functionMD5 is vulnerable to collision attacks, it is necessary to update the method which is more up-to-date and more secure to maintain application or system security. Wrong one recommended solution is to use the SHA 512 hash method which own higher level of reliability than MD5.

Experiment sniffing in study This done with use tool Wireshark. Wireshark is a network packet analysis tool. Wireshark will try catch package network And displays data package comprehensive Possible. After the data is obtained, the captured data from Wireshark will be analyzed For determine type function hash Which used by system. Analysis For determine type function hash done with use tool Hash Identifiers. For example, activity sniffing and type analysis of hash functions are performed as shown seen on below.

ISSN : 1979-9292
JURNAL IPTEKS TERAPAN
Research of Applied Science and Education V17.i3 (680-687)

Figure 3. Results Sniffing Use Application Wireshark

Implementation System

Implementation system is process change design or plan become A ready-to-use product. In the context of using SHA-512 hashes in web URLs employee And Also primary keys, implementation system covers a number of step important. User Acceptance Testing (UAT)is an important process that involves user end or stakeholders. For evaluate is system or The developed software meets the requirements and needs that have been developed determined previously. UAT aim For ensure readiness system And fulfillment hope user. In UAT, user will operate series testing with scenarios that have been prepared, including functionality, reliability, and performance system. Results UAT used as base For determine reception system or need done repair. UAT involve user in process evaluation For identify problem And increase satisfaction user. In report thesis , UAT important in test system information Which developed And gather bait come back user For recommendation And conclusion study. Results percentage from test reception user displayed in diagram circle like Whichseen below this.

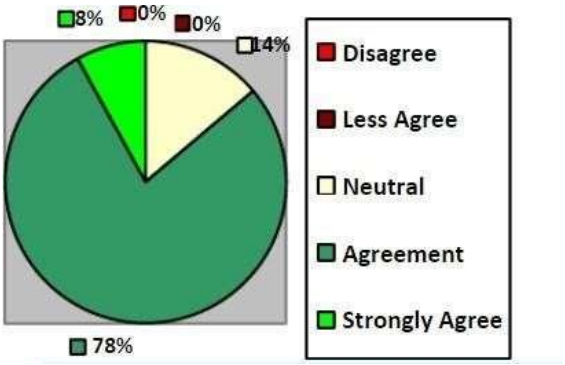

Figure 4. Percentages test Results Users acceptance test

Figure above show percentage from mark in on Which show response from respondent to statement in questionnaire Test Security with answer SS as big **8,00 %,** S as big **78.00%,** N as big **14.00%,** TS as big **0.00%,** And STS as big **0.00%.**

CONCLUSION

1. Implementation of SHA-512 on URL routing can improve security and data integrity in information systems. By using a hash algorithm strong like SHA-512, information Which sent through URLs can encrypted so that No can understandable by party Which No authorized.
2. The advantage of using SHA-512 in URL routing is its ability to produce mark hash with long 512 beets, Which give level securitytall one. In addition, the SHA-512 algorithm is also proven to have robustness against collision attacks, thereby ensuring that each message

has representation hash Which unique

3. The security evaluation regarding the implementation of SHA-512 on URL routing shows that this algorithm provides strong protectionagainst such attacks URL manipulation, data theft and other attacks. Use of SHA-512 help ensure authenticity And integrity data Which sent through routing URLs.

BIBLIOGRAPHY

[1] Athanasiou, G. S., Michail, H. E., Theodoridis, G., & Goutis, C. E. (2014). Optimising the SHA-512 cryptographic hash function on FPGAs. IET Computers & Digital Techniques, 8(2), 70-82.

[2] Kumar, G., Rai, M., & Kim, T. S. (2014). Enhancement of Security in MAODV using SHA-512. *International Information Institute (Tokyo). Information*, *17*(5), 1857.

[3] McLoone, M., & McCanny, J. V. (2002, December). Efficient single-chip implementation of SHA-384 and SHA-512. In *2002 IEEE International Conference on Field-Programmable Technology, 2002.(FPT). Proceedings.* (pp. 311-314). IEEE.

[4] Machana, J. R., & Narsimha, G. (2021). Leveraging Secure Hash Algorithm for Securing IPv6 Protocols SLAAC and DAD. *Turkish Online Journal of Qualitative Inquiry*, *12*(10).

[5] Algredo-Badillo, I., Morales-Sandoval, M., Feregrino-Uribe, C., & Cumplido, R. (2012, August). Throughput and efficiency analysis of unrolled hardware architectures for the sha-512 hash algorithm. In *2012 IEEE Computer Society Annual Symposium on VLSI* (pp. 63-68). IEEE.

[6] Bahramali, M., Jiang, J., & Reyhani-Masoleh, A. (2011). A fault detection scheme for the FPGA implementation of SHA-1 and SHA-512 round computations. *Journal of Electronic Testing*, *27*, 517-530.

[7] Gittins, B., Landman, H. A., O'Neil, S., & Kelson, R. (2005). A presentation on VEST hardware performance, chip area measurements, power consumption estimates and benchmarking in relation to the aes, sha-256 and sha-512. *14th November*.

[8] Gaj, K., Homsirikamol, E., & Rogawski, M. (2010, August). Comprehensive comparison of hardware performance of fourteen round 2 SHA-3 candidates with 512-bit outputs using field programmable gate

arrays. In *2nd SHA-3 Candidate Conference, Santa Barbara, August* (pp. 23-24).

[9] El Ksimi, A., & Leghris, C. (2018). Towards a new algorithm to optimize IPv6 neighbor discovery security for small objects networks. *Security and Communication Networks*, *2018*.

[10] Usman, M., Kamboh, U. R., Taqdees, M. D., Waheed, Z., Shehzad, M. N., & Zafar, H. (2021, November). Enhance Neighbor Discovery Protocol Security by Using Secure Hash Algorithm. In *2021 International Conference on Innovative Computing (ICIC)* (pp. 1-8). IEEE.

[11] Mohan, D. (2010). *Faster file matching using GPGPUs* (Doctoral dissertation, University of Delaware).