Journal of Computer Science

Original Research Paper

Security based Approach of SHA 384 and SHA 512 Algorithms in Cloud Environment

Thambusamy Velmurugan and Sivakumar Karthiga

Department of Computer Science, D. G. Vaishnav College, Chennai-600106, Tamil Nadu, India

Article history
Received: 12-08-2020
Revised: 10-10-2020
Accepted: 28-10-2020

Corresponding Author:
Thambusamy Velmurugan
Department of Computer Science, D. G. Vaishnav College, Chennai-600106, Tamil Nadu, India
Email: velmurugan_dgvc@yahoo.co.in

Abstract: Cloud computing is going to be the next big thing in the era of internet world. As the world moves ahead towards enhancement of the cloud features we also have to take a serious consideration of the enhancing cloud securities to protect the end-user's data. The major usage of this cloud feature are widely applied in the cloud based IT sector for operation advancement, Data storage; on-demand software delivery and many more operations which also requires the scrutiny of the data that is being shared. This research work is carried out to enhance the security of the end-users using secured hashing algorithm. In this, the principles of hash utility are applied that makes the intruders difficult to decode the encrypted password of the user. Even if the intruder or even the administrator of the server tries to decode the encryption for multiple attempts to decode the password the hash codes of the server keeps on changing for multiple attempts. This research work gives a new solution for the concern that is getting raised on the data privacy. The usage of the secured hashing algorithm helps to develop platform that ensure data security for the end-user in the cloud environment. For that the Secure Hashing Algorithm (SHA) 384& SHA 512 is taken and implemented by a practical approach in cloud. For the implementation of these two algorithms, the major attacks faced by end user namely Brute force attack, Man in Middle attack and Rainbow attack are experimented under cloud platform. From the experimental results, it is identified that the best algorithm to protect the data.

Keywords: Network Security, Hash Technique, Secure Hashing Algorithm 384, Secure Hashing Algorithm 512

Introduction

Cloud computing is extensively preferred platform across management. The fluid data swap and the leisure of 24*7 approach to data admittance firms to engage frequently. Here are a few tips of security issues discussed in the research paper Cloud computing - Issues, research and implementations. Security involvement correlate with cloud computing ease into two sections: Security concerns suffered by cloud providers and security issues abide by their consumer. The provider must secure their framework is defended and their consumer data and utilization are guaranteed, while the end user must yield allotment to protect their application and use tough password and testimonial dimension (Vouk, 2008).

When a framework resolves to store data or host utilization on the public cloud, it bereaves its competence to have substantial approach to distributers hosting its material. Figure 1 shows Cloud end users contact data from disparate equipment therefore, possibly delicate data is at fortuity from confederate attacks. Sun *et al*. (2011) canvass about Cloud service distributors must protect that through attainment audit are control for apprentice who have physical path to the servers and the data center in its survey paper. Additionally, (Hayes, 2008) reveal about data centers and its security. Data centers must be usually observed for suspicious action. In regulation to sustain methods, carving tariff and manage productivity, cloud service distributors generally backlog more than one user information on the compatible server. Consequently, there is a prospect that one user's infantry data can be discern by alternative customer. To crank such tricky position, cloud service providers should assure decent data confinement and coherent storage segregation in its cloud computing research paper.

DOI: 10.3844/jcssp.2020.1439.1450

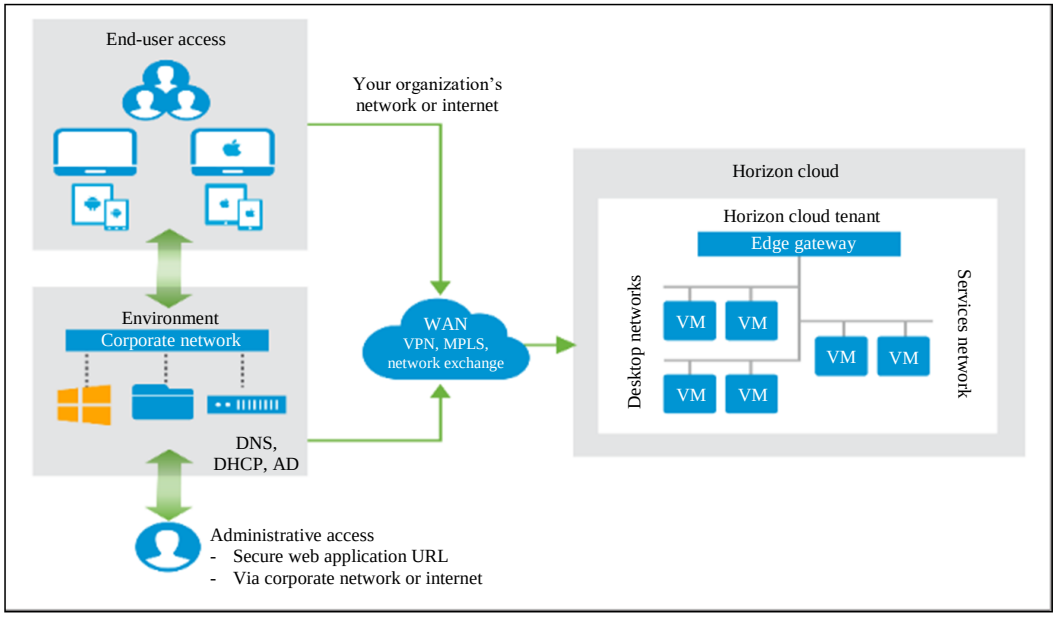

Fig. 1: Cloud users and administrator access

Cryptography Technique with Modular Multiplication Block Cipher and Playfair Cipher research paper discussed about Secure Hash Algorithms, are a progeny of cryptographic objective invent to keep data guaranteed. These algorithms are produced to be one-way operate, that once they're commute into their various hash values, it's virtually inaccessible to alter them back into the authenticated data. A few algorithms of concern are SHA-1, 2 and 3 was consecutively described with advance secure encryption in return to hacker incursion. SHA-0, for occasion, is now antiquated due to the widely defined vulnerabilities (Rahim and Ikhwan, 2016).

Cryptography and data security in cloud computing is discussed about pre-image resistance. The keystone of cryptographic conservation deceit in the draft of pre-image resistance, which compose it resilient and future-draining for an assailant to find an primitive message, p,*m*, given the respective hash value, r_p*hm*. This preservation is afforded by the humor of reward functions, which is a key peripheral of Secure Hashing Algorithm. Pre-image resistance is required to parish off brute force attacks from impressive appliance (Yan *et al*., 2017).

Mittelbach (2012) discusses about second pre-image resistance. The second harmlessly aspect is known as second pre-image resistance, assumed by Secure Hashing Algorithm when a directive is known, d_1d1, yet it's tough to find another regulation, d_2d2 that hashes to the exact value: $H\_\{d\_1\} = H\_\{d\_2\}Hd1 = Hd2$. Without this tendency, dual component password would revenue the exact hash equivalent, assuming the pattern password unnecessary in order to approach secured data.

The last harmlessly characteristic is collision resistance, which is contributed by finding that make it intensely tough for an attacker to find duple broadly dissimilar mandate that hash to the exact hash value: $H\_\{d\_1\} = H\_\{d\_2\}Hd1 = Hd2$. To contribute this distinctive, there must be a comparable figure of desirable inputs to conceivable outputs, will convincingly incur possible collisions. An Improved Cryptographic Technique to Encrypt Text using Double Encryption reviewed in its research paper (Jensen *et al*., 2009).

The research paper is organized as follows. Section 2 provides related work through literature survey. Section 3 demonstrates material and methods of this research. Experimental work is given in section 4. Finally, the conclusion of this research work is pointed out in section 5.

Literature Survey

Cloud computing security assign to the set of methods, operations and requirement lay out to provide security assertion in a cloud computing circumstances. Cloud security addresses both logical and physical security controversy across all the disparate assistance models of platform, infrastructure and software. It also addresses how these benefits are conveyed public, private or hybrid delivery models on professional security concern in cloud computing review in this research paper Big Data and cloud computing: Innovation opportunities and challenges (Yang *et al*., 2017). Subashini and Kavitha (2011) canvass about Cloud computing security operation should address the security to maintain the user data privacy, security and compliance with necessary settlement. The development

will also likely include a trade persistence and data substitute intention in case of a cloud security breach.

Encrypting data before transferring into a cloud is an admirable protection against threats from undesirable hackers. We use narrow encryption as an appended overlay of safeguard. Known as zero-knowledge testimonial in cryptography, this scheme will even conserve our data across service providers and administrators themselves. Therefore, it is accepted a service distributor who distribute an expedient data encryption. Exploit prudence and do not make your password predictable discussed in its paper Hash algorithms for security on GSM system (Rababaa *et al*., 2009). Ali *et al.* (2015) discussed in his research paper. Additionally, recommended a two-step authentication technique to augment the safeguard level of our information. Even if there is a breach in one surveillance stride, the other safe guard the data. We use modernize rebuild levels so that hackers cannot interrupt efficiently. There are diverse tips on the Internet to make a good password. Use your ingenuity to enlarge the password another and keep dynamic it at routine interruption.

Toward trusted cloud computing research paper discussed about password protection, although password is good for observance data encrypted, applying further allotment are also necessary. Encryption stops unauthorized approach of data, but it does not secure its survival. There is likelihood that your data capability gets depraved over the time or that manifold users will have access to your data and password security seems undependable. Cloud must be safeguard with antivirus automation, admin authority and other appearance that convenience safeguard data. A secure cloud system and its enthusiastic servers must use the right security tools and must activity according to privilege restriction to move data (Santos *et al*., 2009). Testing might accent like an adolescent effect, but it can make a compelling exception. Testing may include criticize your cloud to see how well it is operating in alliance with its guarantee structure. We can also select intruders to test our organization security level and check if it has ruined over allotment; this may also afford a window to the desirable loopholes that may grant disfigure from unknown expert. Never estimate that our cloud infrastructure is always secure. Keeping cloud data secure requires continual activity canvass in named research paper Cloud approach for short chain admission (Contò *et al*., 2013).

Cloud Security authority is a portion of security command that assure cloud environments against susceptibility and reduces the consequence of malicious attacks. In cloud computing, a cloud service distributor hosts a company utilization on its assistant and make vacant over the internet while cloud service provider attempt the cloud spectrum of cloud security tools and service to defended the user networks and operation to the cloud.

Materials and Methods

The major objection that IT environment face in cloud security is a reduction of clarity of services and applications that are expanded in cloud organization. Cloud data center are deeply protected. Different cloud vendors use different access to each of the aspect. The administrators must appliance the necessary security controls.

Description and Data Set

Cloud Computing administration is responsible for working in a mixed of windows and unix software environment. The responsibility of the individual is to manage the instances of cloud infrastructure of service and the multiple cloud servers is discussed by (Contò *et al*., 2013). Figure 2 shows structure of Administration and their roles. There are three types of Administration in IT Organizations: Security administration, domain administration and cloud administration.

Lloret *et al*. (2016) discussed about cloud servers, all Administrative tasks are centrally managed through a single administrative interface. The cloud administrator will report to the directors of cloud operation, in its arrangement is pledged for setup and ongoing support of cloud infrastructure.

Cloud Computing Security Controls

IT organization and cloud service providers, they do trade with claim authority for achieve security command to preserve utilization and data restoration and trade survival methods, encrypting data and governing cloud approach are all the security authority described by (Mital *et al*., 2015) in its research paper. While manifold categories of cloud computing security controls endure, they commonly fall into one of four division.

Deterrent Control

Ramachandra *et al*. (2017) discussed about Deterrent control invent to intimidate nefarious attacks from cloud system. These manipulate may act as a alert that an attack will be meet issues. Insider attacks are a authority of risk for cloud service providers. For example, this control could be a cloud service provider attend corrupt backdrop of attendant.

Preventive Control

Preventive controls make the cloud infrastructure more volatile to attacks by defeat susceptibility. A control could be scripting a fragment of code that exhaust inactive ports to secure that there is no applicable access point for hackers. Preserve active customer security system is alternate way of contraction vulnerability to attack designed by (Zhang *et al*., 2010).

DOI: 10.3844/jcssp.2020.1439.1450

Detective Control

Rafal *et al*. (2013) discussed about the purpose of detective controls to analyse and act to security threats and action. The examples of detective control are Intrusion detection network security and software monitoring tools their appearance to audit the network to determine when an attack could be happening.

Corrective Control

Secure hash algorithm discussed about Corrective controls are alerted in the event of a security attack. Their aspect is to check the disturbance caused by circumstance. A planner might write a fragment of cipher so that when a certain type of threat is encounter, data servers are detached from the network to inhibit data theft in the book (Mukta and Azad, 2014).

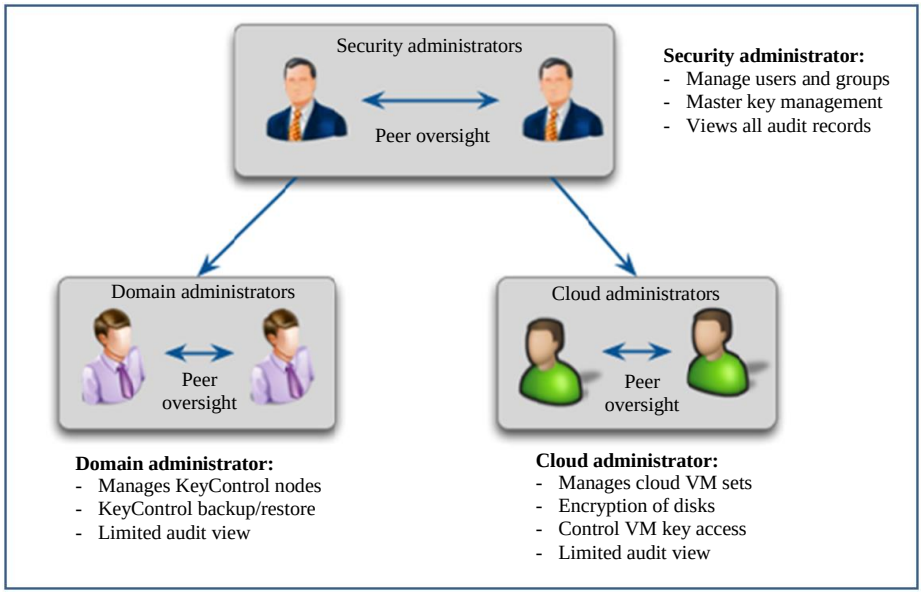

Fig. 2: Administrator and their roles

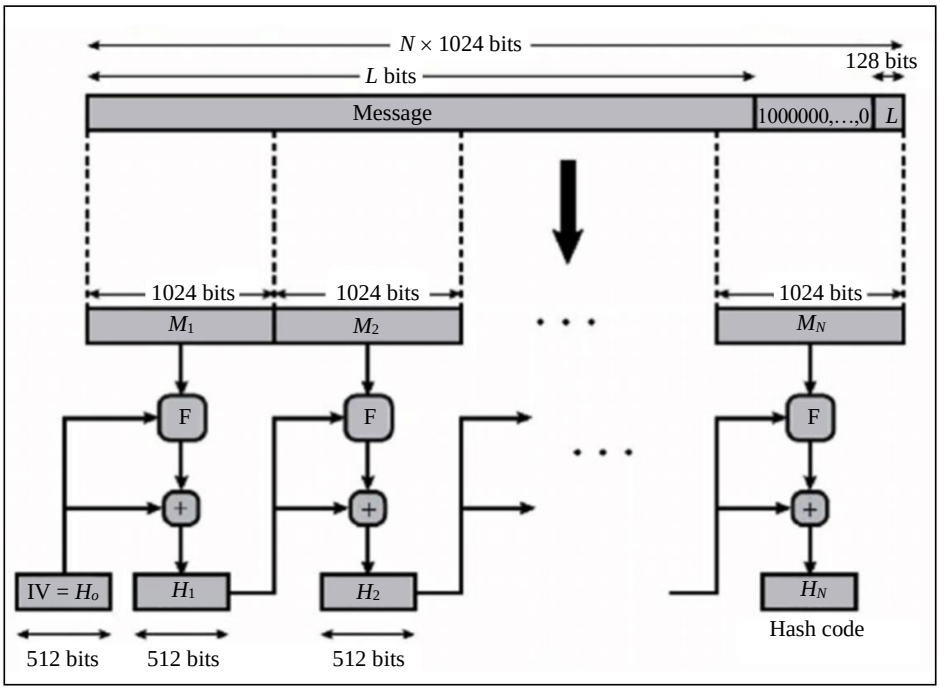

Fig. 3: Message digest Generation using SHA 512

SHA Algorithms and Data Set

Secure Hashing Algorithm is a hash function in cryptography which holding an input and yields a 20-byte (160-bit) hash equivalent known as a message digest consistently concluded as a hexadecimal number, 40 digits long. In this research paper implemented SHA-384 and SHA- 512 using SHA general formula (1):

$$hash(s) = \sum s(i).pi \bmod m \quad (1)$$

where, $s(i)$ means hash value, $p(i)$ is password and m mean message digest. A familiar utilization of SHA is to encrypting password, server only needs to direct path of a definite customer's hash value, relatively than the substantial identification. This is accessible in case assailant drudge the directory, as they find the hashed operation and not the substantial identification, so if they allowed hashed value input as a password, the hash function will switch it into another cord and finally contradict approach. SHA 384 exist to the SHA 2 group of cryptographic hashes. Its goods the 384 digests of a information. SHA-384 is approximately 50% quickly than SHA-224 and SHA-256 on 64- bit appliance, even if its digest enlarged. The expedite is due to the private automation being enforce with 8 byte words, whereas the other two hash objective engage 32-bit words designed by (Mukta and Azad, 2014).

Figure 3 shows the process of message digest bearing using SHA 512. The Secured Hashing Algorithm (SHA-512) is the technique subsists of the ensuing steps:

- Append padding bits
- Append length
- Initialize hash buffer
- Convert the password in 1024 bits (128 words) blocks which forms the hash
- Output the final state value of resulting hash

Secure Hashing Algorithm exhibit the deluge consequence, where the adjustment of very lean alphabets being encrypted causes a big adjustment in output; or diversely distant strings produce comparable hash values. This aftermath causes hash values to not accord any report regarding the input string, such as its authentic segment. In addition, SHA is also used to disclose manipulate of data by attackers, where if a text file is marginally changed and almost obvious, the altered file's hash value will be divergent than the primitive file's hash value canvass in the named research paper analysis and comparison of MD5 and SHA-1 algorithm implementation in Simple-O authentication based security system. Li *et al*. (2012) discussed about Cryptographers converted the innovation to produce SHA-2, which subsists of not one, but two hash operate known as SHA-256 and SHA-512, using 32- and 64-bit words, respectively (Omran and Jumma, 2017).

Research Experiments

In Cloud computing, SHA 256 provides security in cloud server. It protects data from several attacks. Using this concept, SHA 384/512 implemented in this research article. Alshaikhli *et al*. (2012) discussed about new algorithm helps to protect data from Brute force attack, Man in Middle attack and Rainbow attacks. In cloud computing the user face security issues while storing data in cloud server. Secure Hashing algorithm protect user password in server site, administrator also did not find customer passwords. So, secure hashing algorithm is very useful to protect user security.

In cloud data storage is highly used by business clients and students. Sometime data can be leaked by own cloud administrators and data can be hacked by attackers by using different attacks. By using SHA 384 the data can be highly protected. Even cloud administrators cannot guess the client passwords. Figure 4 shows example of some passwords encrypted in SHA 384 and SHA 256. The existing SHA 256 is used in cloud administrators is easily hacked and data can be leaked easily. The proposal of SHA 384 is highly recommended for Cloud business users.

Figure 5 shows the comparison of SHA 256 and SHA 512. The distant amidst these two algorithms is security. SHA 512 is highly recommended for protecting files in cloud storage. The cloud service providers and cloud administrators also cannot identify user information and file directory. SHA 512 is more secure by comparing SHA 256 and it occupy less memory space. SHA 512 is cannot easily hack by attackers. SHA 384 and SHA 512 provide more security for cloud users to store data and files.

Brute Force Attack in SHA 384/512

A brute force attack is a crypt-analytic attack to be used to attempt decrypt any encrypted data when password guessing is occurred. This SHA cryptography the password considered as every clear text bit has an own corresponding key from random sequence of key bits. A familiar intimidation web planner aspect is password guessing attack. Comparative and security performance analysis of SHA-3 discussed about brute force attack is an endeavour to detect a password by consistently trying every conceivable aggregate of alphabet, numbers and symbols until discover the one combination that works.

Hackers discharge brute force attacks using extensively usable device that handle word classify and smart conduct sets to guess customer password reasonably and approximately. Figure 6 explain some hash functions for number values that encrypted in cloud server. The most accessible approach to block brute force attacks is to easily hasp out narrative after a specify

DOI: 10.3844/jcssp.2020.1439.1450

number of improper passwords attempts. Account lock outs can bust a definite continuation, such as one hour or the version could endure sealed until manually unlock by an authority (Lin *et al*., 2003).

Man in Middle Attack in SHA 384/512

In cloud server each login credential stored in server database, so once the storage is done the hacker and administrator easily find user passwords. SHA 384/512 protect user credential from Man in middle attack. In this research work trying to protect user data via secure hashing algorithm by using cryptography SHA 1 algorithm. Using SHA 384 & SHA 512 algorithm to protect user passwords is very effective. The user login information stored in database is 32-bit hashing password.

Attackers have many different reasons and methods for using a man in middle attack, without encrypted WIFI connections are easy to eavesdrop. Another WIFI eavesdropping attack happens when a hacker creates its own WIFI hot spot called Evil twin.

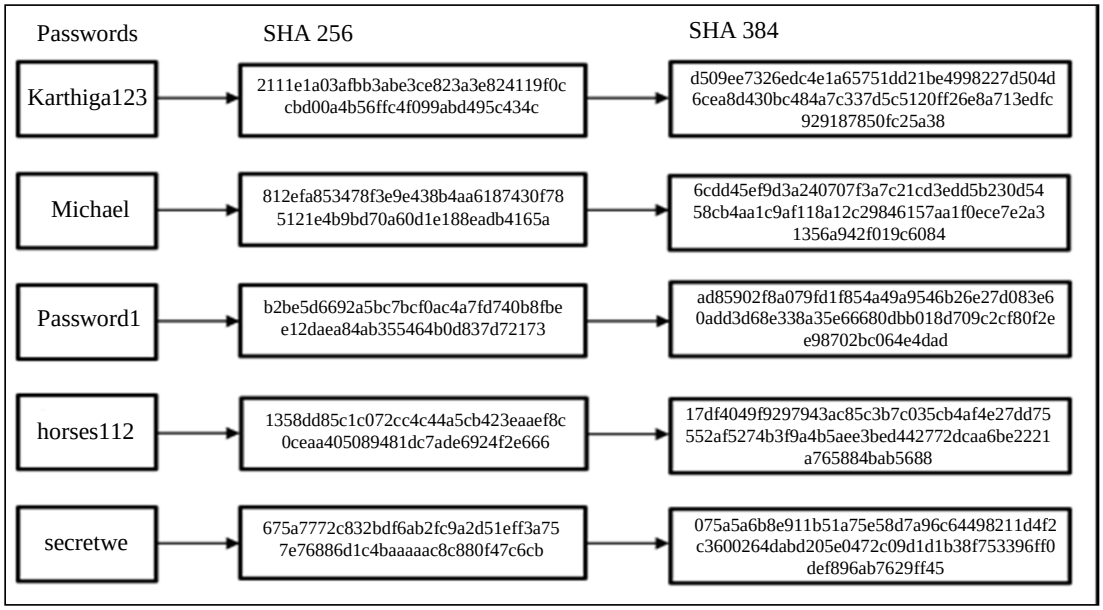

Fig. 4: SHA algorithm for data storage

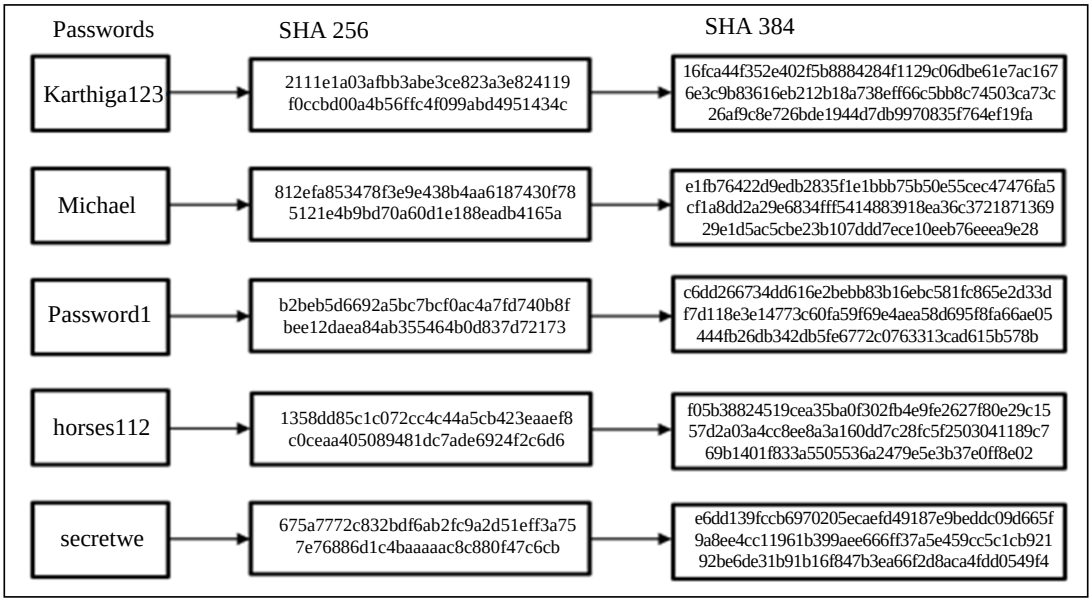

Fig. 5: SHA algorithm in cloud files storage

DOI: 10.3844/jcssp.2020.1439.1450

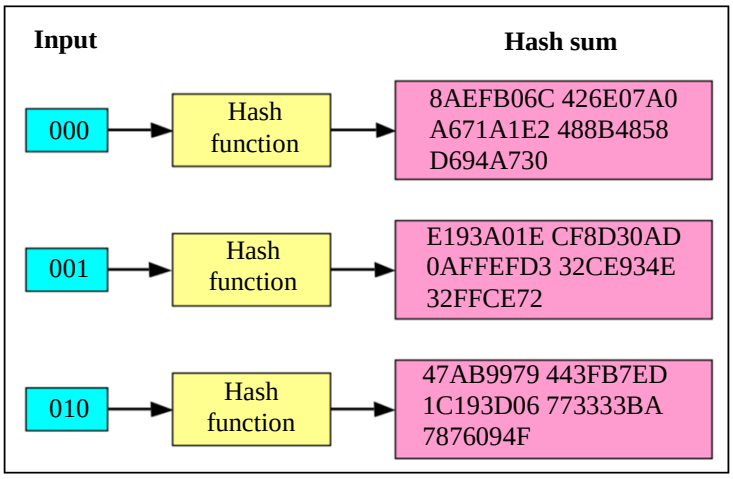

Fig. 6: Result of Brute force attack in hash function

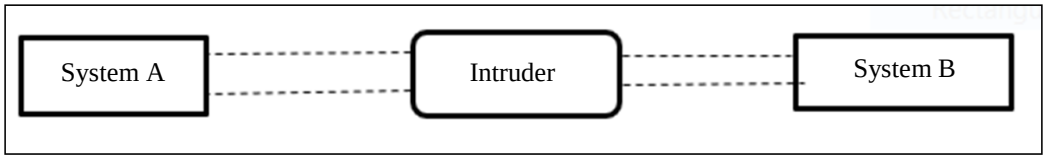

Fig. 7: Man in Middle attack

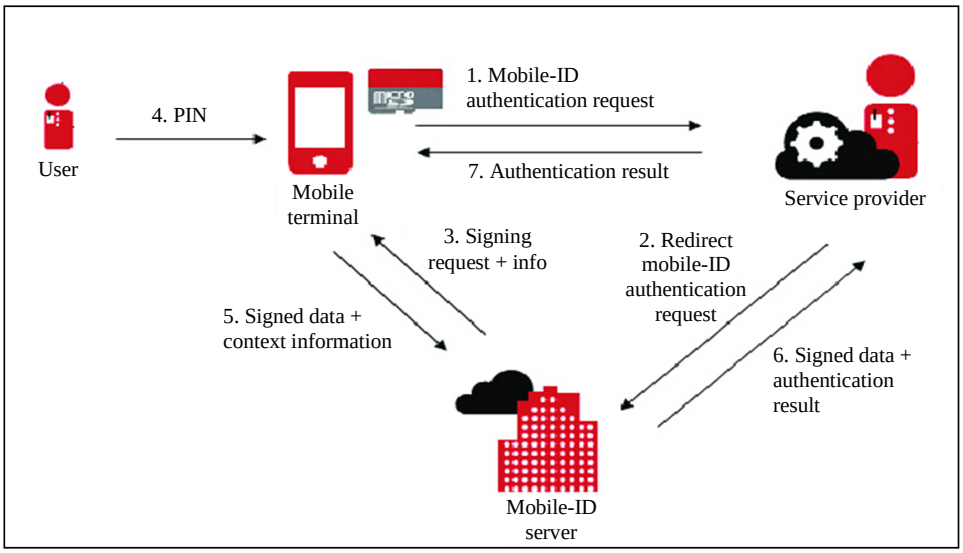

Fig. 8: Example for authenticating data from Man in Middle attack

Figure 7 explains how Man in Middle attack works in between systems and intruders. System A and System B thinks they are talking to each other but the hacker is intercepting and talking to both. C.-H. Lin described about session hijack occurs when an attacker steals a session cookie. This can happen if the user system is attacked with malware or browser hijackers. It can also happen when an attacker uses Cross- Scripting XSS attack where the attacker injects malicious code into a frequently used website with SSL striping the hacker intercepts and forwarding traffic from users.

Figure 8 explains how data can be access through mobile, each process can be recorded and checked by administrator then the access given to the user. The process can be done internally and protect user information from intruders (Tulyakov *et al*., 2007).

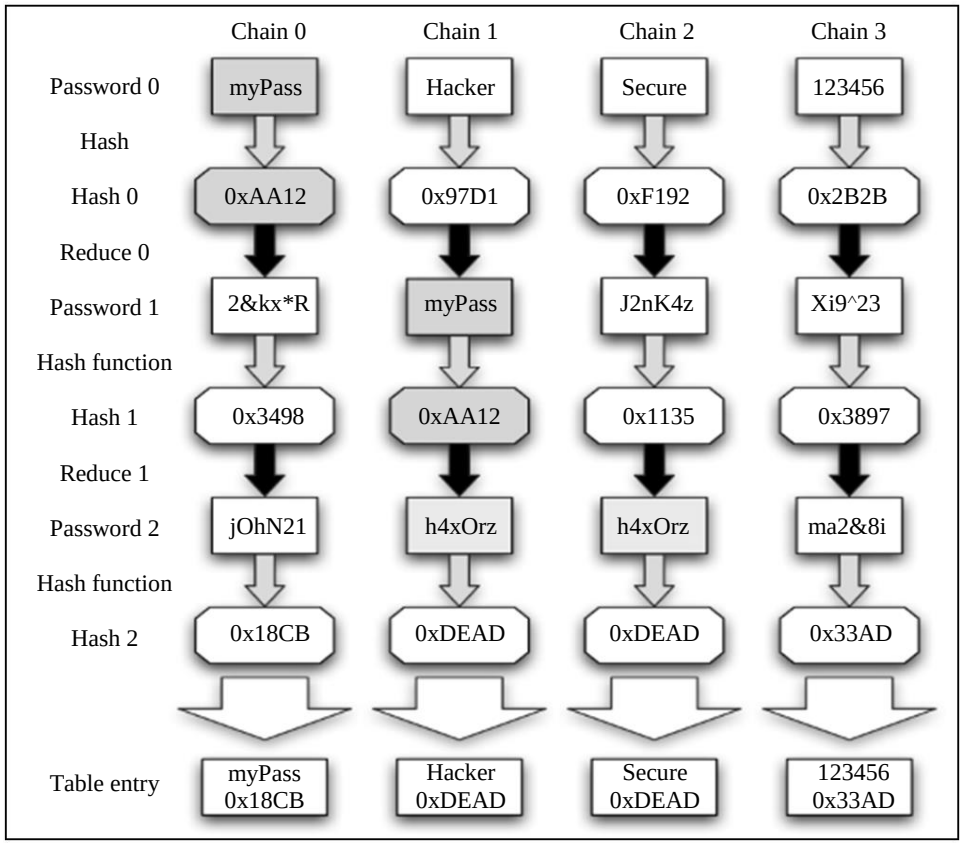

Fig. 9: Rainbow attack table formation

Rainbow Attack in SHA 384/512

A rainbow attack is a figure out table for overturns cryptographic hash function usually for cracking password hashes tables are uses in recovering a password up to a convinced segment subsist of a defined set of aspects. System that requires password testimonial must enclose a database of identification, either in plaintext or various methods of password storage exist. Instead when a customer invades a password for verification, the scheme measures the hash value for the administer password and that hash value is co related to the gathered hash for the user.

A rainbow table is impotent across one-way hashes that combine huge salts. Figure 9 shows rainbow attack table formation. A huge salt value inhibits precomputation attack, counting rainbow tables by assure that each customer password is hashes alone. This means that two customers with the same identification will have different password hashes. The larger salt values make precomputation attack across these scheme absurd for around any dimension of the password in the research paper Symmetric hash functions for secure fingerprint biometric systems (Johnson and Ramchandran, 2003).

The change in hash value suggests that the data has been modified and data integrity has been compromised. This same method can be used in cloud computing environment to check the data integrity files stored in the cloud. This method is suggested to be applied on the customer side; the hash values calculated can be saved in secure hash repositories which can be later checked by the customer at the time of retrieving the file from the cloud.

Results and Discussion

Cloud computing infrastructure admits harmless complication since the initial phase of its advancement agenda. It concludes paramount to an additional strong, secure and scattering fault inclined to system than those scheme that assort security texture only on one moment, once the pattern is dispatch. SHA 1 & SHA 2 is the base of Secure Hashing Algorithm 256& 384& 512 and Message Digest. In Secured Hashing Algorithm 384 and 512 is play vital role cloud computing security. By comparing SHA 384& 512, SHA 512 is providing high protection for cloud data preventing attacks from hackers. The hashing password cannot be decrypt easily so hackers find difficulties to decrypt the code. Each year the security threats are increased in the world. Frequently hashing is assigning to as one-way encryption. Hashes are beneficial for

DOI: 10.3844/jcssp.2020.1439.1450

direction where computers may wish to determine, contrast or differently run estimate against files and string of data. It is obvious for the computer to first figure out a hash and then correlate the values than it would be to correlate the authentic files.

The SHA 384 algorithm does minor activity than SHA 512. It is not summarized easily curtail the SHA 512 with distant original values security perspective, SHA 384 has resistance to length extension attack, but SHA 512 does not have. Secured Hashing Algorithm 384 has 128-bit support against the length development attacks since the attacker need to inference the 128-bit to execute the attack. This is due to the truncation. The distant leading value implement authority split with 384 domain splits by using Equation (2):

$$SHA384(m) \neq SHA512(m) \mid 384 \quad (2)$$

where, |384 is the truncation, the generic attacks in hash algorithm is implemented to convince using Pre-image resistance, Secondary pre-image resistance and Collision resistance.

Therefore, Secured Hashing Algorithm 512 is improved in the case of Pre-image, Secondary pre-image and Collision resistance. SHA 512 is only failing is that it is prone to duration adjunct attacks in Table 1 (Weng and Preneel, 2011).

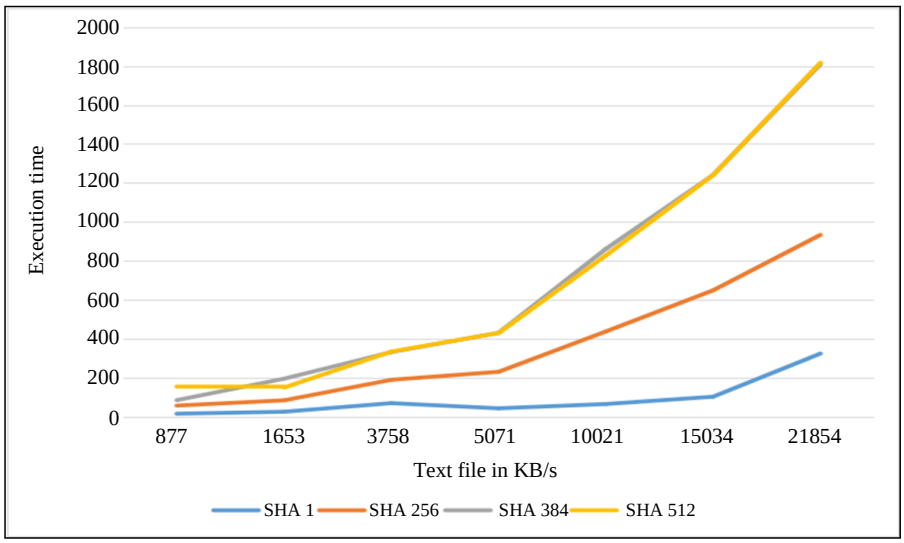

Fig. 10: Run time for Hashing Algorithm

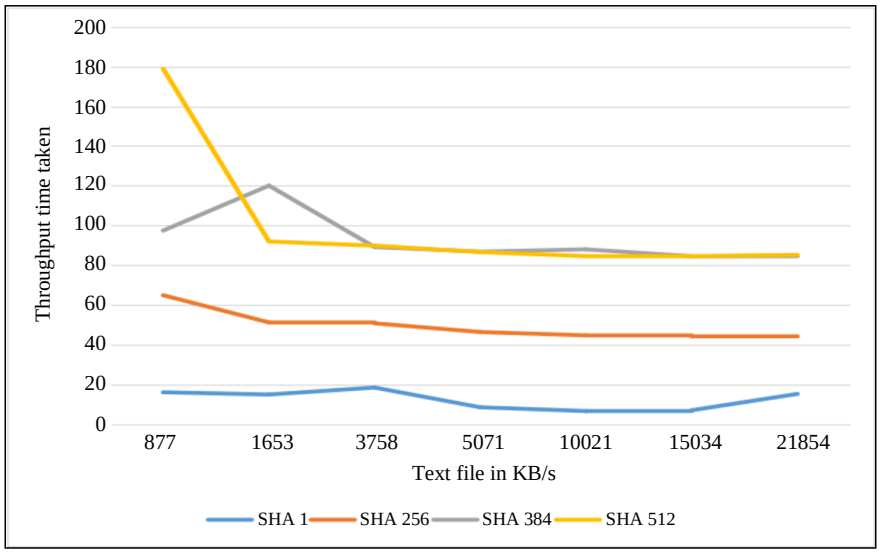

Fig. 11: Result for throughput of various Hash Algorithm in m/s

DOI: 10.3844/jcssp.2020.1439.1450

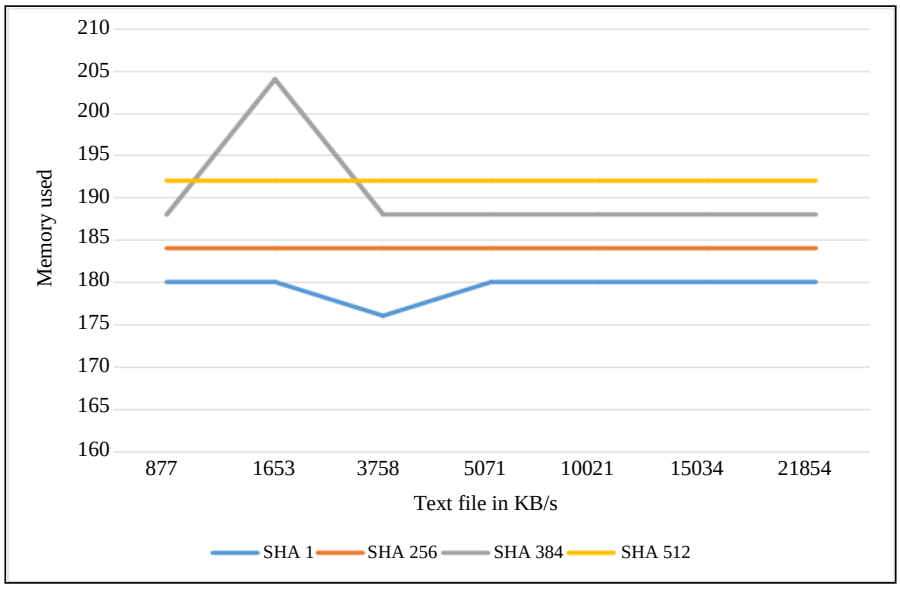

Fig. 12: Results of Memory used in Hashing Algorithm

Table 1: Generic attack in hash algorithm

SHA	Pre-image resistance	Secondary pre-image resistance	Collision resistance
SHA-384	O (2^{384})	O (2^{384})	O (2^{192})
SHA-512	O (2^{512})	O (2^{512})	O (2^{256})

Table 2: Execution time for hashing algorithm

Text files (KB)	SHA 1	SHA 256	SHA 384	SHA 512
877	13.646	55.478	83.386	153.072
1653	23.913	82.523	193.794	148.347
3758	67.958	187.98	330.43	333.079
5071	41.488	229.214	429.757	428.764
10021	63.46	436.442	860.639	827.1413
15034	101.0388	647.784	1240.463	1240.36
21854	322.522	932.596	1809.111	1817.312

Table 3: Throughput of various hash algorithm

Text file (KB)	SHA 1	SHA 256	SHA 384	SHA 512
877	15.944	64.81	97.426	178.84
1653	14.815	51.126	120.063	91.906
3758	18.324	50.689	89.09	89.81
5071	8.378	46.29	86.79	86.59
10021	6.484	44.598	87.94	84.523
15034	6.88	44.123	84.494	84.48
21854	15.11	43.698	84.768	85.153

Table 4: Memory used by various hash algorithm (KB)

Text file (KB)	SHA 1	SHA 256	SHA 384	SHA 512
877	180	184	188	192
1653	180	184	204	192
3758	176	184	188	192
5071	180	184	188	192
10021	180	184	188	192
15034	180	184	188	192
21854	180	184	188	192

The execution time was obsessed Fig. 10. From this SHA-512 and SHA-384 are acquired highest execution time (Table 2). The SHA-1 takes lowest time to produce hash code even for the biggest text file. The SHA1 also consumes least time. SHA 384 and SHA 512 speed is moreover identical.

Throughput is an essential measured of an algorithm's administration detecting. It is a computation that bits/s conveyed through a network and the bandwidth abundance of the network. The throughput Fig. 11 shows that SHA-512 and SHA-384 have chief throughput. But SHA-256 and SHA-1 are engraved as flat throughput. SHA-512 and SHA-384 have the enormous length of output but these are acquiring excellent throughput. SHA 256 and SHA1 have minimum output length also accept bottom throughput. Here the files content is not anxious. As a result of all the algorithms have the comparable field of bits relocated when the file content are commuted except SHA-512 (Table 3) designed in the research paper A secure perceptual hash algorithm for image content authentication.

The achievement of an algorithm is also disturbed with the capacity that takes for the progress. The remembrance used for hash algorithms are computed and proven that whatever may be the file content, the algorithms SHA-1, SHA256, SHA-384, SHA-512 used balanced field to enumerate hash (Fig. 12). If 180 kb has been seized for 877 kb content, the exact field has been worn for the file contented 21854. Here SHA-1 used least field when combine to other algorithm and SHA 512 takes extreme field for the process in Table 4.

Conclusion

Cloud computing still needs to be advanced to provide a more protected and secure platform for the customer to use. The method used and discussed in this study is very basic and easy with the embracement of user itself. The directory of user can be downloaded at any moment from the cloud locker and compute hash value can be balanced with the hash value stored in archive. This can be very capable and competent to an extent to check the faithfulness and security of cloud and already developed SHA. This research work finds the covenant point of cloud computing act with data probity audit of the customer data. The SHA 384 and SHA 512 methods discussed, implemented and provided additional security for users and automation for administrators. Both the algorithms are implemented in brute force attack, man in the middle attack and rainbow attack. From the experimental results, it is observed that in every attack, SHA 512 gives best security for password protection compared with SHA 384. In cloud server, SHA use less memory usage and execution time also reduced in SHA 512. Hence, it is concluded that the SHA 512 algorithm provided more security than the SHA 384. In future additional security can be implemented by Message Digest Authentication. This intern will enhance the security by providing additional protection against several attacks.

Acknowledgement

We would like to thank D. G Vaisnav College Chennai and Madras University which is moral supported for research and developing hashing security in cloud computing.

Author's Contributions

Thambusamy Velumurugan: Contributing to the literature review with the related fields. He designs the study, developing the methodology, collecting the data, performing the data analysis and approving the final manuscript.

Sivakumar Karthiga: Inventing the idea, designing the hashing algorithm in cloud computing and the research plan, writing the manuscript, hashing algorithm, designing the data dictionary, database design and coding the program.

Ethics

The research article is originally licensed and still contains the unpublished sections in author confirms that all the other authors have read and approved the manuscript and no ethical issues concerned.

References

Ali, M., Khan, S. U., & Vasilakos, A. V. (2015). Security in cloud computing: Opportunities and challenges. Information sciences, 305, 357-383.

Alshaikhli, I. F., Alahmad, M. A., & Munthir, K. (2012, November). Comparison and analysis study of SHA-3 finalists. In 2012 International Conference on Advanced Computer Science Applications and Technologies (ACSAT) (pp. 366-371). IEEE.

Contò, F., Faccilongo, N., La Sala, P., & Dicecc, R. (2013). Cloud approach for short chain administration. Procedia Technology, 8, 600-605.

Hayes, B. (2008). Cloud computing.

Jensen, M., Schwenk, J., Gruschka, N., & Iacono, L. L. (2009, September). On technical security issues in cloud computing. In 2009 IEEE International Conference on Cloud Computing (pp. 109-116). IEEE.

Johnson, M., & Ramchandran, K. (2003, September). Dither-based secure image hashing using distributed coding. In Proceedings 2003 International Conference on Image Processing (Cat. No. 03CH37429) (Vol. 2, pp. II-751). IEEE.

Li, J., Isobe, T., & Shibutani, K. (2012, March). Converting meet-in-the-middle preimage attack into pseudo collision attack: Application to SHA-2. In International Workshop on Fast Software Encryption (pp. 264-286). Springer, Berlin, Heidelberg.

Lin, C. H., Yeh, Y. S., & Lee, C. Y. (2003). Keyed/Unkeyed SHA-2. Journal of Discrete Mathematical Sciences and Cryptography, 6(1), 45-58.

Lloret, J., Sendra, S., Jimenez, J. M., & Parra, L. (2016). Providing security and fault tolerance in P2P connections between clouds for mHealth services. Peer-to-Peer Networking and Applications, 9(5), 876-893.

Mital, M., Pani, A. K., Damodaran, S., & Ramesh, R. (2015). Cloud based management and control system for smart communities: A practical case study. Computers in Industry, 74, 162-172.

Mittelbach, A. (2012, September). Hash combiners for second pre-image resistance, target collision resistance and pre-image resistance have long output. In International Conference on Security and Cryptography for Networks (pp. 522-539). Springer, Berlin, Heidelberg.

Mukta, S. H., & Azad, S. (2014). Secure hash algorithm. in Practical Cryptography: Algorithms and Implementations Using C++.

Omran, S. S., & Jumma, L. F. (2017, May). Design of multithreading SHA-1 & SHA-2 MIPS processor using FPGA. In 2017 8th International Conference on Information Technology (ICIT) (pp. 632-637). IEEE.

Rababaa, M. A., Kofahi, M. A., Saqqar, F. A., & Rababavh, S. A. (2009). Hash algorithms for security on GSM system. International Review on Computers and Software, 4, 698-703.

Rafal, L., Dave, S., Bryan, S., & Luciano, J. S. (2013). The notorious nine: cloud computing top threats in 2013. Cloud Security Alliance, Top Threats Working Group and Others.

Rahim, R., & Ikhwan, A. (2016). Cryptography technique with modular multiplication block cipher and playfair cipher. Int. J. Sci. Res. Sci. Technol, 2(6), 71-78.

Ramachandra, G., Iftikhar, M., & Khan, F. A. (2017). A comprehensive survey on security in cloud computing. Procedia Computer Science, 110, 465-472.

Santos, N., Gummadi, K. P., & Rodrigues, R. (2009). Towards Trusted Cloud Computing. HotCloud, 9(9), 3.

Subashini, S., & Kavitha, V. (2011). A survey on security issues in service delivery models of cloud computing. Journal of network and computer applications, 34(1), 1-11.

Sun, D., Chang, G., Sun, L., & Wang, X. (2011). Surveying and analyzing security, privacy and trust issues in cloud computing environments. Procedia Engineering, 15, 2852-2856.

Tulyakov, S., Farooq, F., Mansukhani, P., & Govindaraju, V. (2007). Symmetric hash functions for secure fingerprint biometric systems. Pattern Recognition Letters, 28(16), 2427-2436.

Vouk, M. (2008). Cloud computing–issues, research and implementations. Journal of computing and information technology, 16(4), 235-246.

Weng, L., & Preneel, B. (2011, October). A secure perceptual hash algorithm for image content authentication. In IFIP International Conference on Communications and Multimedia Security (pp. 108-121). Springer, Berlin, Heidelberg.

Yan, Z., Deng, R. H., & Varadharajan, V. (2017). Cryptography and data security in cloud computing.

Yang, C., Huang, Q., Li, Z., Liu, K., & Hu, F. (2017). Big Data and cloud computing: innovation opportunities and challenges. International Journal of Digital Earth, 10(1), 13-53.

Zhang, S., Zhang, S., Chen, X., & Huo, X. (2010, January). Cloud computing research and development trend. In 2010 Second international conference on future networks (pp. 93-97). IEEE.