British Journal of Applied Science & Technology
18(6): 1-10, 2016; Article no.BJAST.30798
ISSN: 2231-0843, NLM ID: 101664541

SCIENCEDOMAIN *international*
www.sciencedomain.org

T.R.P Mechanism to Secure E-learning Information that Shared with Cloud Storage

Khalid Muhammad Al-Khafaji[1*] and Meltem Eryilmaz[2]

[1]Department of Computer Engineering, Graduate School of Natural and Applied Sciences, Atilim University, Ankara, Turkey.
[2]Department of Computer Engineering, Faculty of Engineering, Atilim University, Ankara, Turkey.

Authors' contributions

This work was carried out in collaboration between both authors. Author KMAK designed the study, performed the statistical analysis, wrote the protocol, wrote the first draft of the manuscript, managed the analyses of the study and the literature searches. Author ME supervised the study and the methodology of workflow. Both authors read and approved the final manuscript.

Article Information

DOI: 10.9734/BJAST/2016/30798
Editor(s):
(1) Kleopatra Nikolopoulou, School of Education, University of Athens, Athens, Greece.
Reviewers:
(1) Dexin Zhao, Tianjin University of Technology, China.
(2) S. Vaithyasubramanian, Sathyabama University, Chennai, India.
(3) Radosław Jedynak, Kazimierz Pulaski University of Technology and Humanities, Malczewskiego, Poland.
(4) Ajay Auddy, The University of Burdwan, West Bengal, India.
Complete Peer review History: http://www.sciencedomain.org/review-history/17788

Original Research Article

Received 30th November 2016
Accepted 26th January 2017
Published 10th February 2017

ABSTRACT

The aim of the study is establish and implement a safe mechanism is: Technique Relationship Protected (TRP), by using a privacy control with the Auditor on the information shared between two of the most important services offered by modern technology, namely the E-learning systems and service of cloud storage, as a matter of fact these technologies require relevant features of the databases made up of information that need safety. This study aims to shed light on the concept of ensuring privacy to protect information shared between the E-learning system and Cloud platform by proposing a mechanism to preserve the privacy of quite distinctive between these important technologies. It is worth mentioning that the study has a tendency to need to pick advantage of looping the signatures to verify the authenticity of the information required to review the validity the information shared encrypted. With our mechanism, entity location on each block of the joint information is unbroken figure of the year investigators, administrative body is able to check the efficiency of the safety of the common information, without retrieving the entire file.

**Corresponding author: E-mail: alkhafajik@gmail.com;*

The propose system, keep a privacy of auditing a mechanism for shared information about cloud keeping-safe. With AES an encryption algorithm for protecting the shared information by applying an encryption a mechanism on the information that is being uploaded from its owners. They have been certified by the E-learning system administrators and the application of a decrypt the encrypted information after users' requested, they trusted users has E-learning system after sponsorship by the owners of the information they need. We have to take advantage of ring autographs to build homomorphism authenticators so that a general verifier has the capacity to audit shared information integrity without retrieving the complete data or access to content. Addition to it cannot recognize who's the signer on files, this means that the power to administrator to reveal the identity of the signer. As well as the presence of additional functions of the work of the Auditor that contribute to the consolidation of this technique relationship protected TRP.
This is for the protect and the success of that relationship between the technical services which has become an urgent necessity in the modern technical world that contains a very massive amount of data and information those shared and transmitted daily between branches of our technological world.

Keywords: TRP; E-learning; cloud; audit; privacy; shared data.

1. INTRODUCTION

The aim at the study is establishing and implement a methodology safe is TRP (Technique Relationship Protected) by using a privacy control with the Auditor and apply TRP to ensure the transmission of information and save them in a reliable way. The researcher is thought it is the way of the right direction for the advancement of modern technology services through earning the confidence in the beneficiary and the reduction of cost and easy availability of the information access and preserve the security and privacy of Information [1]. Of the most popular services provided by modern technology is the E-learning and cloud computing platforms, these techniques require the relevant features in the information consist of data that need to safety basics and privacy. In order to take advantage of modern technology services for the development of the reality of E-learning which is one of the means of modern technological advancement as it provides the services and features contributed to the creation of useful learning environment in the various joints of the electronic life, conditions of that security issues have become an important concern with the growing popularity of these technique services.

In addition to the idea of paper, this study suggests to implement the proposed a mechanism TRP on shared data onto E-learning systems and cloud computing platforms, It seeks to clarify the fact of taking security measures and precautions to ensure the performance and operation of the required level and gain the confidence of the educational institutions, companies and recipients. E-learning in the environment of Cloud storage faces many dangers and challenges in the process of deciding to work [2,3], like in the circumstances of outsourcing more traditional it makes many of these concerns more acute. Data level of privacy is the key concern, users do not have control or do not know where their data is stored and a few see an information not be safe only when management of the internal network, while some believe necessary to provide security to ensure the maintenance of information and safety is the responsibility of the service provider [4], it is necessary to provide a strong infrastructure and tools and storage depots safe, particularly if it should take a corresponding materially them. Suppliers of cloud services provide storage of economic information and scalable services to the user with the lowest value of the old curriculum approach [5]. It's a regimen for users to take good thing about cloud storage services to talk about data onto others about the stop, as it becomes standard data exchange feature generally in most cloud storage solutions, start box drop, the iCloud In Google Drive also. Safety knowledge in cloud storage [2], however, is subject matter to suspicion and examination, and the info held on the cloud can simply loss or damage as the inevitable consequences of the failure of the hardware / software and human error [6,7]. To help make the matters more serious, the suppliers of cloud services are in addition reluctant to users of data with regard to these details errors and so to keep your name of their services and prevent the damage to earnings. Therefore, you should examine the safety of cloud data prior to any use of the data, such as search or an account on the cloud data [8]. Specific approach to examine the validity of

the data to retrieve the full data onto the cloud, and therefore verify the honesty of the info by examining the validity of autographs.

It is important that the decision makers in the E-learning have a deep understanding of cloud computing and how they evolve [9], and trends that can adapt to them, and that between the costs and benefits are in the budget of each approach, and the level of confidence in the key factors which must be taken into account.

2. RELATED WORKS

1. C. Wang, S Chow, Q Wang, St, K. Ren, and W. Lou, (2010), "Privacy-Preserving Public Auditing for Secure Cloud Storage".

Advantages:

- A privacy of public auditing system for data storage security in Cloud Computing.
- Use the homomorphism linear authenticator and random masking to guarantee that the TPA would not learn any knowledge about the data content stored on the cloud server during the efficient auditing process.
- It is provably secure and highly efficient.

Techniques:

Homomorphic linear authenticator, and implement a random masking using MAC.

Disadvantage:

- The individual auditing of these growing tasks can be tedious and cumbersome.
- The technique of public key based homomorphism linear authenticator, which enables TPA to perform the auditing without demanding the local copy of data and thus drastically reduces the communication and computation overhead as compared to the straightforward data auditing approaches.

2. Y. Prasanna, Ramesh (2012), "Efficient and Secure Multi-Keyword Search on Encrypted Cloud Data".

Advantages:

- The efficient and secure ranked multi-keyword search on remotely stored encrypted database model where the database users are protected against privacy violation.
- We appropriately increase the efficiency of the scheme by using symmetric-key encryption method rather than public- key encryption for document encryption.
- The ranking method proves to be efficient to return highly relevant documents corresponding to submitted search terms.

Techniques:

Ranking method, Symmetric key Encryption.

Disadvantages:

- The computation and communication costs of this method are quite large since every search term in a query requires several homomorphism encryption operations both on the server and the user side.
- They retrieving all files containing the queried keyword further incurs unnecessary network traffic.

3. B. Wang, B. Li, and H. Li, (2014), "Oruta: Privacy-Preserving Public Auditing for Shared Data in the Cloud".

Advantages:

- Oruta, the TPA is able to efficiently audit the integrity of shared data, yet cannot distinguish who is the signer on each block, which can preserve identity privacy for users.
- We exploit ring signatures to compute the verification information needed to audit the integrity of shared data.
- The identity of the signer on each block in shared data is kept private from a third party the Auditor (TPA), who is still able to verify the integrity of shared data without retrieving the entire file.
- They share the data effectively and competent.

Techniques:

Ring Signature.

Disadvantages:

- To preserve identity privacy from the TPA, because the identities of signers on shared

data may indicate that a particular user in the group or a special block in shared data is a more valuable target than others.
- The information is confidential to the group and should not be revealed to any third party.

4. B. Wang, B. Li, and H. Li, (2015), "Panda: Public Auditing for Shared Data with Efficient User Revocation in the Cloud".

Advantages:

- A new auditing mechanism for shared information with efficient user revocation in the cloud.
- When a user in the group is revoked, we allow the semi-trusted cloud to re-sign blocks that were signed by the revoked user with proxy re-signatures.
- The group can save a significant amount of computation and communication resources during user revocation.

Techniques:

Resigned Techniques.

Disadvantages:

- This revoked user should no longer be able to access and modify shared data.
- The integrity of the entire data can still be verified with the public keys of existing users only.

5. Bo Chen, R. Curtmola, G. Ateniese, R. Burns (2010), "Remote Data Checking for Network Coding-based. Distributed Storage Systems".

Advantages:

- A secure and efficient RDC scheme for network coding-based distributed storage systems that rely on untrusted server.
- RDC-NC scheme can be used to ensure data remains intact when faced with data corruption, replay, and pollution attacks.
- The RDC-NC is inexpensive for both clients and servers.

Techniques:

Remote Data Checking.

Disadvantages:

- The code is not systematic; it does not embed the input as part of the encoded output.
- Small portions of the file cannot be read without reconstructing the entire file.
- Online storage systems do not use network coding, because they prefer to optimize performance for read (the common operation).
- They use systematic codes to support sub-file access to data. Network-coding for storage really only makes sense for systems in which data repair occurs much more often than read.

6. D. Boneh, X. Boyen, and H. Shacham (2004), "Short Group Signatures".

Advantages:

Signatures in our scheme are approximately the size of a standard RSA signature with the same security.

- The group signature is based on the Strong Diffie-Hellman assumption and a new assumption in bilinear groups called the Decision Linear.

Techniques:

RSA Algorithm.

Disadvantages:

Signature generation requires no pairing computations, and verification requires a single pairing.

3. THE PROPOSED SYSTEM

The importance of this study can be seen in establish and implement a safe mechanism is TRP by using a privacy control and the Auditor and apply TRP on two of most important services in modern technology, namely the E-learning systems and service of cloud storage, to secure E-learning information that shared with Cloud storage.

How? By taking advantage of ring signatures to create authenticators. Accordingly, a verifier can audit that distributed data integrity without retrieving the complete data or access to content.

Addition to it cannot recognize who's the signer on files, this means that the power to administrator to reveal the identity of the signer. As well as the presence of additional functions in the work of the Auditor that contribute to the consolidation of this technique relationship protected.

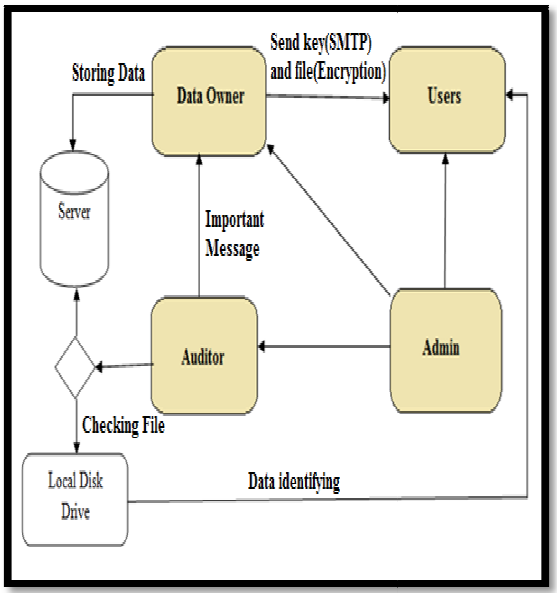

Fig. 1. Structure of the mechanism proposed

Where this model consists of the following functions, with the interface to perform work Control for each one:

- Admin of the System
- Data Owner
- User of Information
- Auditor

4. OBJECTIVE

Because privacy and security matters are becoming main worry with the growing circulation use of E-learning in the environment of Cloud, became objective of this study to applying a methodology safe TRP to keep a mechanism that supports privacy control with auditor on shared information between E-learning systems and Cloud storage.

5. ADVANTAGES

- The system can expected to perform multiple tasks in a similar audit time.
- Improve the efficiency of verification tasks checking multiple.
- Provides high security for file sharing.

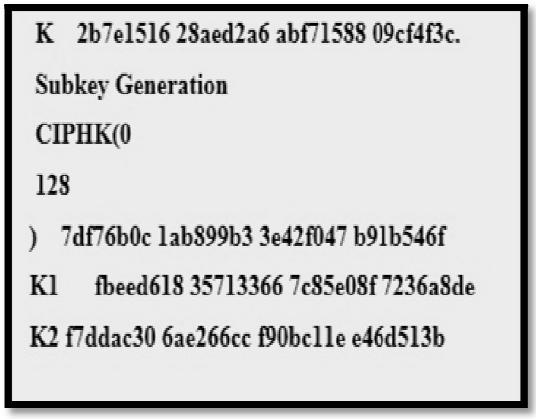

Fig. 2. Block cipher

6. REGISTER AND CONTROL

By use E-learning system, this usually Unity addition unusual for users to register custom modules that support customization and ease of a particular deal. If users want to form their own user accounts, any recording, then checks Salary dexterity user name and assign a distinctive identity. It suggests that the dominant user management login with reference to the user's name and the words of unity given throughout the recording methodology. Once you log in, the user encrypts the initial information and keep it in the information, so the user retrieve the initial information that gets to unpack once verification of distinct identity and researched information. Supported the login data, they need to look at the rights of, or edit, update or delete the contents of resources. Neighborhood information remain confidential, but once these institutions store information on devices offered by cloud computing service provider, priority access to information is not the owner, but the supplier cloud computing service. Therefore, there is a chance to keep the wind cannot be ruled out being leaked. In addition, there is no danger to trace the initial information to hackers.

7. CRM SERVICE

This unit is the managing relationships shopper, wherever the user will move with the device. CRM cares with the creation and development of desalination dedicated shopper relations with the targeted buyers precisely team's shopper

Fig. 3. The correspondence management cycle

thereby increasing the total value of the consumer at the time of their lives. CRM will be the commercial strategy which aims to understand the desires associated with existing and potential customers of the Foundation. It is a comprehensive approach that provides the integration of each house of business that touches the customer specifically promote sales and shopper services and field support through the mixing of individuals, methodology and technology. CRM will be a shift from the old to strengthen as the results focuses on retaining the shoppers in addition to the acquisition of the latest customers. Shopper expression CRM sound in the word and the old, and replace the wide looked as if it'd be a little tricky period, strengthening the relationship (RM). More importantly, the purpose of CRM is:

- Most of the focus [of CRM] - to create value for the consumer and the addition to the companies about the future.
- Allows CRM - organizations that appreciate the "competitive advantage" over competitors that offer similar goods or services. CRM consists of an index page, registration page, login page, etc. Through this, the user can register with the details of the user, once registered user can send preliminary information that gets encrypted and inventory information base; as well as the user can retrieve the initial knowledge they keep only once decode the encrypted information is encrypted by giving secret key writing.

8. ENCRYPTION / DECRYPTION SERVICE

This module describes with respect to writing and technical writing confidential preliminary data key. Key technical writing is required while the information and data are stored together required secret writing while information retrieval. Once it has been the user's login with success verified, and if the CRM service system wants to consumer information from the user, it sends you need to share data (for writing and secret encryption) to the storage service system.

8.1 Encryption

Throughout this (data) storage service, and CRM service system transmits the user's identity storage system service wherever it looks for user data and compelled the original data, once found, and the participation of the need to send to / decryption service system in the side of the user's identity. It shows the death storage of consumer data transmission service system and penalty along on the user's encryption / decryption service system identity. Here, the user gets sent to the original data encryption, and keeps in storage service according to the user's request. You cannot break through that data from

one side of the unauthorized and this is a lot of confidential and encrypted.

8.2 Decryption

Throughout this (data retrieval service), if the user demand CRM service to retrieve information unit area on the contract in the storage service, and customer relationship management sends the user's identity and together research data to the encryption / decryption service system. It approves or not the unity of the user's identity and the search data in hand by the user are identical. If documented, and data encryption of the storage service system to send / decryption technology service system, the key to writing. Throughout the system, it checks for the key to the secret of writing, if it is OK, and thus decrypt the encrypted data and compilation of the raw data that was retrieved and sent to the user.

9. ARRIVE AT THE STORAGE SERVICE

It describes this unit as but the information gets to hold and retrieve information. Gets the first data that is given by the user and the application to store encrypted, and the system of encrypted data is stored with the user's identity to avoid the misuse of information storage service. Along throughout the retrieval, the user to retrieve knowledge and application by giving the search data, and verify the user's identity storage system research unit of menstruation identical data, if thus it sends encrypted / decryption service system data writing key technology for, it decrypt the information and sends to the user. User interacts with information on each occasion through the CRM service completely. Used to work in customer relationship management service system, the goal is supposed to remain part of the customer data and therefore, it must be compelled to take the maintenance of information at the thought of the boom system. Vogue strategies for achieving embrace matching consumer data encrypted with the user identity of the interview and consumer ID, so a variety of user IDs allowing consumers to urge the corresponding data. Then it goes to the customer's identity be familiar with customer data index the user must keep it. Due to the huge amount of consumer data, and can improve search potency by combining the user's identity and the identity of the consumer to make the subscriber identity used to identify a particular client data.

In the new business model, multiple cloud services operator's purchaser service through existing data techniques on the aspect of the different systems of application such as E-Learning systems, ERP, Accounting icon, and choose the governor and operations money that could require the user's identity to be combined with a completely IDs a completely different lineup to hold or retrieve data. In addition, the preceding description of the two systems use the online service technology related to understanding the operational synergies and objectives of the exchange of data.

10. AUDITING

Homomorphic authenticators are unforgeable confirmation metadata made from specific data blocks, which is often securely aggregated so to make sure the Auditor a linear combo of data blocks is appropriately computed by check only the aggregated authenticator. Summary to accomplish privacy-preserving general public auditing, we propose to assimilate the Homomorphic authenticator with arbitrary cover up strategy exclusively.

And the likelihood of new has been added to this study of the Auditor in addition to his work, which is its capability to compute and show how big is the uploaded record storage, and the right time that put in the Auditor to complete this technique.

11. SHARING INFORMATION

The canonical software is data showing. The auditing property is particularly useful whenever we expect the delegation to be versatile and effective. The schemes permit a content provider to share her information in a selective and confidential way, with a set and short ciphertext expansion, by distributing to each authorized user a small and single aggregate key.

12. INTEGRITY CHECKING

Hence, helping data dynamics for privacy-preserving general public danger auditing is also very important. Now we show how our main scheme can be adapted to develop after the prevailing work to aid data dynamics, including block level functions of modification, insertion and deletion. We are able to adopt this system inside our design to accomplish privacy-preserving public danger auditing with support of

data dynamics. An individual download this document not download whole file.

13. FEATURE

The likelihood of new has been added to this study, its capability to show name, size of the uploaded file and the time spent for upload from E-learning system to the Cloud.

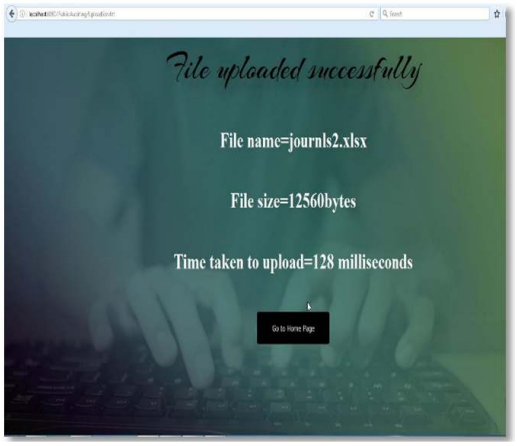

Fig. 4. Files information & elapsed time for upload (Image)

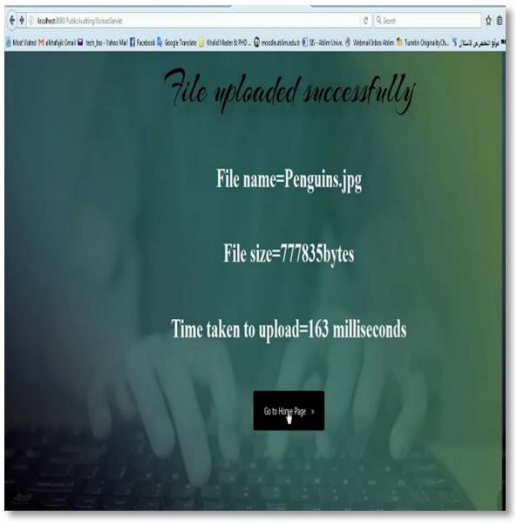

Fig. 5. Files information & elapsed time for upload (Excel sheet)

14. MESSAGE DIGEST-FIVE (MD5)

MD5 can be an algorithm that used to confirm data integrity through the creation of 128-bit message break down from data suggestions (which might be a note of any period) that is stated to be as unique compared to that specific data as a fingerprint is to the precise individual. MD5, that was developed by Teacher Ronald L. Rivest of MIT, is supposed for use with digital personal applications, which need to the large data must be compressed with a protect method before being encrypted with a hidden knowledge key, under a open public key cryptosystem. MD5 is a typical presently, Internet Engineering Task Force (IETF) Obtain Feedback (RFC) 1321. Based on the standard, it is "computationally infeasible" that any two text messages that contain been suggestions to the MD5 algorithm may have as the outcome the same meaning digest, or a false concept could be created through apprehension of the communication digest. MD5 is the 3rd algorithm created by Rivest absorb. This algorithm can be an expansion of MD4, that your critical review found to be fast, however, not absolutely secure possibly. Compared, MD5 is nearly as fast as the MD4 algorithm, but offers a lot more assurance of data security [10].

15. EXPERIMENTAL RESULTS

The study assess at present strength of Oruta in experiments. In our tests, the study has a tendency to take advantage of multiple calculation accuracy (GMP) bovid Library and the Library of pairing encryption based primarily (PBC). Each unit area of successive experiments supported C and tested on a quest gig of 26 in the second cycle of the program more than 1.000 times the UNIX system. As a result, for Oruta need further exponentiations pairing operations throughout the audit strategy, and the curve Oval our tendency to the election in our tests is Associate in Nursing MNT curve with the size of the base field of 159 bits, which contains the best performance is much different curves quite perfectly exponentiations computing. The study have a tendency to elect |p| = One hundred and sixty bits bit and |P| = Eighty bits. The study have a tendency to tend to the whole assumption is different from the blocks in the shared data is n = 1.000.000 | N | = Twenty bits. The size of the shared data is 2GB. The survival probability of detection greater than 9ty nine, the study have a tendency to the amount of line-elect. Blocks in Associate in Nursing audit function as c = 460 [9]. If exactly three hundred units of blocks measuring team, chances are high detection that are larger than 95. The study have a tendency to cluster together assuming the dimensions d Є (2-20) in the following experiments. Sure, if you

use a much larger block, and the price of the entire account size could increase as results to differ from the increasing exponentiations and coupling processes.

16. PERFORMANCE OF SIGNATURE GENERATION

In accordance with section 6, while the generation of the signing of the hoop on the block is about by different users within the bloc and collectively amount of ingredients in each block. Once is mounted K, generation time of the signing of the hoop increases linearly with the dimensions of the group; once d is mounted, the generation time of a hoop signature is linearly increasing with the quantity of components in every block. Specifically, once d = ten and k = one hundred, a user within the cluster needs regarding thirty seven milliseconds to reason a hoop signature on a block in shared knowledge.

17. COMPARED OF STUDIES

This study proposes a mechanism to solution a series of problems and obstacles that faced by other studies that have reported detailed in (Section 2) which have a related work with the current study. As well as take advantage of the good features that referred to in those studies and make some improvements and modifications to the methods used and complementary to those studies and propose a mechanism may serving the technical modern world.

The current study indicated to a mechanism safe is TRP to maintain the privacy of quite distinctive by using a privacy control with the Auditor and apply TRP on two of most important services in modern technology, What distinguishes this study from recent studies referred to, which have a related work with the current study and makes it semi-integrated is:

- Proposed TRP (Technique Relationship Protected) between and implement with E-learning systems and Cloud Storage platforms by designing module simulates the work of the proposed mechanism.
- Ability of administrative body to check the efficiency of the safety of the common information without the need to view file contents in full.
- The Auditor can expected to implement multiple tasks at a time.
- The control and distribution of tasks and the separation of powers between the members of the proposed system.
- Use signatures gang to build notaries and increase the privacy.
- Support the principle of the privacy and protection of information shared electronically.
- Build a module system to perform tasks above to show the proposed mechanism and be clearer to the recipient and close to reality.

In addition to the privacy management is ensures performance through user's distribution in the form of groups independent of each other, each group linked only prime one is the data owner who has the permittivity to upload the files and stored in the cloud after being signed on that block during the procedure, as well as the creation of a special key with members his group, this key send to them by each user's e-mail. Use the e-mail in the security and privacy of shared information is one of the successful ways to increase the security and privacy of data shared information and traded. The sender key is created from 16 key character, used by user when downloading any of the files that have been uploaded by the owner of the private data for the Group.

18. CONCLUSION

This study provided an electronic protected policy advanced by the distribution of tasks and the separation of powers between the members of the proposed system process. It led to the principle of the privacy and protection for information shared electronically.

In this study the researcher tried to proposed TRP (Technique Relationship Protected) between two of the most important services offered by modern technology, namely the E-learning systems and Cloud Storage environment by applying the mechanism to maintain the privacy of quite distinctive by using a privacy control with the Auditor on the information shared between the E-learning platform and cloud storage to ensure the transmission of information and save them in a reliable way. The researcher is thought it is the way of the right direction for the advancement of modern technology services through earning the confidence in the beneficiary and the reduction of cost and easy availability in the information

access and preserve the security and privacy of Information.

The study takes advantage of signatures gangs to build notaries homomorphism and that the public patron is over the position exceedingly to check the integrity of information shared without retrieving the entire file though it can not be distinguished between the site of each block [11]. It is important to mention that the decision-makers in the the electronic educational institutions have a deep understanding of cloud computing and The speed of evolution and trends that can adapt to them. The costs and benefits are in the budget of each approach and the level of confidence in the key factors which must be taken into account to help in the success of this technology relationship are protected.

ACKNOWLEDGEMENT

Many thanks to my country "Republic of Iraq", for giving me the opportunity and funding to complete a master's study outside Iraq.

COMPETING INTERESTS

Authors have declared that no competing interests exist.

REFERENCES

1. Wang B, Li B, Li H. Oruta: Privacy-preserving public auditing for shared data in the cloud. Proc. IEEE Fifth Int'l Conf. Cloud Computing. 2012;295-302.
2. Ren K, Wang C, Wang Q. Security challenges for the public cloud. IEEE Internet Computing. 2012;16(1):69-73.
3. Song, Shi, Fischer, Shankar. Cloud data protection for the masses. Computer. 2012;45(1):39-45.
4. Armbrust, Fox, Griffith, Joseph, Katz, Konwinski, Lee, Patterson, Rabkin, Stoica, Zaharia. A view of cloud computing. Comm. ACM. 2010;53(4):50-58.
5. Wang, Ren, Lou. Privacy-preserving public auditing for data storage security in cloud computing. Proc. IEEE INFOCOM. 2010; 525-533.
6. Wang B, Li M, Chow SSM, Li H. Computing encrypted cloud data efficiently under multiple keys. Proc. IEEE Conf. Comm and Network Security (CNS' 13). 2013;90-99.
7. Rivest, Shamir, Adleman. A method for obtaining digital signatures and public key cryptosystems. Comm. ACM. 1978;21(2): 120-126.
8. Simon Marechal. Etat de l'art sur le cassage de mots de passe, Actes du symposium SSTIC07; 2007.
9. Wang B, Li B, Li H. Panda: Public auditing for shared data with efficient user revocation in the cloud. Proc. IEEE. 2015; 8:1.
10. Wikipedia, "MD5".
Available:https://en.wikipedia.org/wiki/MD5
11. Christopher Schultz. Information security trends and issues in the Moodle E-learning platform: An ethnographic content analysis. Winter. 2012;23:4. E-learning platform: An ethnographic content analysis. Winter. 2012;23:4.
E.ISSN: 1948-9447

Peer-review history:
The peer review history for this paper can be accessed here:
http://sciencedomain.org/review-history/17788