Annals of R.S.C.B., ISSN:1583-6258, Vol. 25, Issue 3, 2021, Pages. 8606 - 8615
Received 16 February 2021; Accepted 08 March 2021.

Public Auditing for Shared Data Hierarchical Attribute based on Encryption

S.Indumathi[1], V.Harshini[2], M.Madhan Kumar[3], Dr.N.Saravanan[4], Dr.M.Somu[5]

[1]Student, Department of Computer Science and Engineering, K.S.R College of Engineering, Anna University, Tiruchengode, Tamil Nadu, India.

[2]Student, Department of Computer Science and Engineering, K.S.R College of Engineering, Anna University, Tiruchengode, Tamil Nadu, India.

[3]Student, Department of Computer Science and Engineering, K.S.R College of Engineering, Anna University, Tiruchengode, Tamil Nadu, India.

[4]Assistant Professor, Department of Computer Science and Engineering, K.S.R College of Engineering, Anna University, Tiruchengode, Tamil Nadu, India.

[5]Assistant Professor, Department of Computer Science and Engineering, K.S.R College of Engineering, Anna University, Tiruchengode, Tamil Nadu, India.

ABSTRACT

Data integrity, a core security issue in reliable cloud storage, has received much attention. Data auditing protocols enable a verifier to efficiently check the integrity of the outsourced data without downloading the data. Provable Data Possession (PDP) empowers cloud clients to check the information uprightness without recovering the whole record. all the current PDP plans depend on the Public Key Infrastructure (PKI).The conspire is effective, adaptable and upholds private check, designated confirmation and public verification.ID-DPDP is defective since it neglects to accomplish sufficiency. Fix the blemish by introducing a nonexclusive development. Another ID-DPDP convention is acquired by stretching out the fundamental ID-PDP to various mists climate.

With information stockpiling and sharing administrations in the cloud, clients can undoubtedly alter and share information as a gathering. To guarantee shared information honesty can be confirmed openly, clients in the gathering need to register marks on all the squares in shared information. Various squares in shared information are by and large endorsed by various clients because of information alterations performed by various clients. For security reasons, when a client is repudiated from the gathering, the squares which were recently endorsed by this disavowed client should be re-endorsed by a current client. The direct strategy, which permits a current client to download the relating part of shared information and re-sign it during client disavowal, is wasteful because of the huge size of shared information in the cloud.

In this work, we propose a novel public inspecting instrument for the respectability of imparted information to productive client denial as a top priority. By using the possibility of intermediary re-marks, we permit the cloud to re-sign squares for the benefit of existing clients during client denial, so that current clients don't have to download and re-sign squares without anyone else.

KEYWORDS

Public Auditing, PKI, PDP.

Introduction

Distributed storage is a help where information is distantly kept up, oversaw, and upheld up. Distributed computing, another sort of Internet-based figuring, gives helpful, on-request network access. Provable Data Possession (PDP) confirms the information respectability by testing irregular arrangements of squares.

Public Sector Auditing

The public-area review climate is that wherein governments and other public-area elements practice duty regarding the utilization of assets got from tax collection and different sources in the conveyance of administrations to residents and different beneficiaries. These substances are responsible for their administration and execution, and for the utilization of assets, both to those that give the assets and to those, including residents, who rely upon the administrations conveyed utilizing those assets. Public-area inspecting assists with making reasonable conditions and

Annals of R.S.C.B., ISSN:1583-6258, Vol. 25, Issue 3, 2021, Pages. 8606 - 8615
Received 16 February 2021; Accepted 08 March 2021.

fortify the assumption that public-area substances and community workers will play out their capacities successfully, productively, morally and as per the relevant laws and guidelines.

Types of Public-sector Audit

The three fundamental sorts of public-area review are characterized as follows:

Financial Audit

It centers around deciding if an element's monetary data is introduced as per the pertinent monetary revealing and administrative system. This is refined by getting adequate and fitting review proof to empower the evaluator to communicate an assessment concerning whether the monetary data is liberated from material misquote because of extortion or blunder.

Performance Audit

It centers around whether mediations, projects and organizations are acting as per the standards of economy, proficiency and adequacy and whether there is opportunity to get better. Execution is inspected against reasonable models, and the reasons for deviations from those rules or different issues are examined. The point is to address key review questions and to give suggestions to progress.

Compliance Audit

It centers around whether a specific topic is in consistence with specialists recognized as measures. Consistence inspecting is performed by evaluating whether exercises, monetary exchanges and data are, in all material regards, in consistence with the specialists which oversee the examined element. These specialists may incorporate standards, laws and guidelines, budgetary goals, strategy, set up codes, concurred terms or the overall standards overseeing sound public-area monetary administration and the lead of public authorities.

The auditor: In open area reviewing the part of evaluator is satisfied by the Head of the SAI and by people to whom the errand of leading the reviews is assigned. The general duty regarding public-area inspecting stays as characterized by the SAI's command.

The responsible party: In open area evaluating the significant duties are dictated by protected or administrative game plan. The people in question might be answerable for the topic data, for dealing with the topic or for tending to proposals, and might be people or associations.

Intended users: The people, associations or classes thereof for whom the examiner readies the review report. The proposed clients might be administrative or oversight bodies, those accused of administration or the overall population.

Materiality

Materiality is significant in all reviews. A matter can be made a decision about material if information on it is probably going to impact the choices of the planned clients. Deciding materiality involves proficient judgment and relies upon the examiner's understanding of the clients' necessities. Materiality contemplations influence choices concerning the nature, timing and degree of review methods and the assessment of review results.

Evidence

Review proof is any data utilized by the evaluator to decide if the topic follows the appropriate models. Proof may take numerous structures, for example, electronic and paper records of exchanges, composed and electronic correspondence with pariahs, perceptions by the inspector, and oral or composed declaration by the examined substance. Strategies for acquiring review proof can incorporate examination, perception, request, affirmation,

Annals of R.S.C.B., ISSN:1583-6258, Vol. 25, Issue 3, 2021, Pages. 8606 - 8615
Received 16 February 2021; Accepted 08 March 2021.

recalculation, reperformance, insightful systems as well as other exploration procedures.

The structure and substance of a report will rely upon the idea of the review, the planned clients, the pertinent principles and legitimate necessities. The SAI's order and other significant laws or guidelines may determine the format or phrasing of reports, which can show up in short structure or long structure.

Long-structure reports by and large portray in detail the review scope, review discoveries and ends, including likely results and helpful proposals to empower therapeutic activity. Short-structure reports are more consolidated and for the most part in a more normalized design.

Shared Data

The Cloud anyway is vulnerable to numerous protection and security assaults. As featured in, the greatest snag impeding the advancement and the wide reception of the Cloud is the protection and security issues related with it.. Obviously, numerous protection and security assaults happen from inside the Cloud supplier themselves as they typically have direct admittance to put away information and take the information to offer to outsiders to acquire benefit. There are numerous instances of this occurrence in reality as featured. In this day and age, there is a solid need to share data to gatherings of individuals around the planet. Since the Cloud is loaded with so numerous protection issues, numerous clients are as yet uncertain about offering their most basic information to different clients.

Some of significant necessities of secure information partaking in the Cloud are as per the following. Initially the information proprietor ought to have the option to determine a gathering of clients that are permitted to see their information. Any part inside the gathering ought to have the option to access the information whenever, anyplace without the information proprietor's intercession. Nobody, other than the information proprietor and the individuals from the gathering, should access the information, including the Cloud Service Provider. The information proprietor ought to have the option to add new clients to the gathering. The information proprietor ought to likewise have the option to repudiate access rights against any individual from the gathering over their shared information. No individual from the gathering ought to be permitted to disavow rights or join new clients to the gathering.

Types of Attacks on the Cloud

There are various sorts of protection and security assaults in the Cloud. The accompanying contains a rundown of the normal kinds of assaults that may happen in the Cloud.

- XML Signature Wrapping Attacks
- Cross site scripting assaults
- Flooding Attack Problem
- Denial-of-Service Attacks
- Law Enforcement Requests
- Data Stealing Problem

It is significant that the engineering of the Cloud is grown with the end goal that it guarantees protection and security as aggressors are consistently watching out for security openings in Cloud design.

- Identity and Access Management
- Software Isolation
- Data Protection
- Availability
- Incident Response

While including information in the Cloud, encryption in this manner gets significant. Numerous works in writing recommend the requirement for encoding information in the Cloud in some structure or another. The states that encryption should happen on the way, very still and on reinforcement

Annals of R.S.C.B., ISSN:1583-6258, Vol. 25, Issue 3, 2021, Pages. 8606 - 8615
Received 16 February 2021; Accepted 08 March 2021.

media. Upper class proposes the utilization of homomorphic encryption to keep information secure and classified. With homomorphic encryption, it is conceivable to perform activities, for example, questioning and looking on scrambled information while never unscrambling the information and consequently uncovering protection. It propose a framework called 'TrustStore' which encodes and parcels information on the customer side and sends each segment to various Cloud stockpiling suppliers. This significantly upgrades the privacy of information as the possibility of trading off at least two stockpiling suppliers is low.

While considering information sharing and coordinated effort, basic encryption procedures don't do the trick, particularly when thinking about key administration. To empower secure and classified information sharing and cooperation in the Cloud, there necessities to initially be appropriate key administration in the Cloud.

Information sharing is getting progressively significant for some clients and some of the time a urgent prerequisite, particularly for organizations and associations meaning to acquire benefit. Truly, numerous individuals saw the PC as "unoriginal goliaths" who took steps to eliminate positions of numerous individuals through robotization.

With the progressions in Cloud processing, there is presently a developing spotlight on executing information sharing abilities in the Cloud. With the capacity to share information by means of the Cloud, the quantity of advantages increments multifold. As organizations and associations are presently re-appropriating information and tasks to the Cloud, they advantage further with the capacity to divide information among different organizations and associations.

Data Confidentiality: Unauthorized clients (counting the Cloud), ought not have the option to get to information at some random time. Information ought to stay secret on the way, very still and on reinforcement media. Just approved clients ought to have the option to access information.

User revocation: When a client is denied admittance rights to information, that client ought not have the option to access the information at some random time. In a perfect world, client renouncement ought not influence other approved clients in the gathering for productivity purposes.

Scalable and Efficient: Since the quantity of Cloud clients will in general be very huge and now and again capricious as clients join and leave, it is basic that the framework keep up productivity just as be adaptability.

User Revocation

In distributed computing client can without much of a stretch share and change information inside gathering. Here information honesty can be effectively guaranteed by utilizing the public mark of existing clients in the cloud gathering. By utilizing information sharing administrations in cloud client can capable change information as a gathering on cloud.

Cloud Computing

Distributed computing can be characterized as a registering climate where figuring needs by one gathering can be moved to another gathering and when need be emerge to utilize the processing force or assets like data set or messages, they can get to them by means of web. Distributed computing is a new pattern in IT that moves figuring and information away from work area and compact PCs into enormous server farms. The principle favorable position of distributed computing is that clients don't need to pay for framework, its establishment, required labor to deal with such foundation and support.

The expression "cloud" begins from the universe of broadcast communications when suppliers started utilizing virtual private organization (VPN) administrations for information interchanges. Distributed computing manages calculation, programming, information access and capacity benefits that may not need end-client information on the actual area and the design of the framework that is conveying the administrations. Distributed computing is a new sever in IT that moves processing and information away from work area and versatile PCs into enormous server farms.

Annals of R.S.C.B., ISSN:1583-6258, Vol. 25, Issue 3, 2021, Pages. 8606 - 8615
Received 16 February 2021; Accepted 08 March 2021.

Characteristics of Cloud Computing

In distributed computing, clients access the information, applications or some other administrations with the assistance of a program paying little heed to the gadget utilized and the client's area. The framework which is by and large given by an outsider is gotten to with the assistance of web. Cost is diminished to a critical level as the framework is given by an outsider and need not be procured for intermittent escalated figuring undertakings.

Dependable help can be gotten by the utilization of various destinations which is appropriate for business congruity and fiasco recuperation. Notwithstanding, at times many distributed computing administrations have endured blackouts and in such occasions its clients can scarcely do anything.

Sharing of assets and expenses among an enormous assortment of clients permits proficient usage of the foundation. Support is simpler if there should be an occurrence of distributed computing as they need not be introduced on every client's PC.

Deployment a/Cloud Computing Service

For conveying a distributed computing arrangement, the significant undertaking is to settle on the kind of cloud to be actualized. As of now three kinds of cloud arrangement happens - public cloud, private cloud and crossover cloud.

- **Public Cloud**

Public cloud permits clients' admittance to the cloud by means of interfaces utilizing internet browsers. Clients need to pay just for the time term they utilize the help, i.e., pay-per-use. Anyway open mists are less secure contrasted with other cloud models as all the applications and information on the public cloud are more inclined to noxious assaults.

- **Private Cloud**

A private mists activity is inside an association's inward endeavor server farm. The fundamental preferred position here is that it is simpler to oversee security, support and overhauls and furthermore gives more authority over the arrangement and use. Private cloud can be contrasted with intranet. Contrasted with public cloud where all the assets and applications were overseen by the specialist co-op, in private cloud these administrations are pooled together and made accessible for the clients at the authoritative level.

- **Hybrid Cloud**

In this model a private cloud is connected to at least one outside cloud administrations. It is safer approach to control information and applications and permits the gathering to get to data over the web. It empowers the association to serve its necessities in the private cloud and if some intermittent need happens it asks the public cloud for escalated processing assets.

- **Community Cloud**

At the point when numerous association mutually build and offer a cloud foundation, their necessities and approaches then such a cloud model is called as a local area cloud. The cloud framework could be facilitated by a third-gathering supplier or inside one of the associations locally.

The support of the framework, be it equipment or programming is rearranged, subsequently, less cerebral pains for the IT group. Additionally applications that are very capacity broad are more simpler to use in the cloud climate contrasted with a similar when utilized by the association by its own. Additionally at the client level, what you generally need is a basic internet browser with web network.

Annals of R.S.C.B., ISSN:1583-6258, Vol. 25, Issue 3, 2021, Pages. 8606 - 8615
Received 16 February 2021; Accepted 08 March 2021.

Related Work

In this work, M. Armbrust, A. Fox, R. Griffith, et.al[2] has proposed Cloud Computing, the since quite a while ago held fantasy about figuring as a utility, can possibly change a huge piece of the IT business, making programming significantly more appealing as an assistance and forming the manner in which IT equipment is planned and bought. Designers with imaginative thoughts for new Internet benefits presently don't need the huge capital costs in equipment to convey their administration or the human cost to work it.

The actual administrations have for quite some time been alluded to as Software as a Service (SaaS).At the point when a Cloud is made free in a pay-more only as costs arise way to the overall population, we consider it a Public Cloud; the help being sold is Utility Computing. We utilize the term Private Cloud to allude to inward server farms of a business or other association, not disclosed accessible to the general.

Distributed computing is related with another worldview for the arrangement of figuring framework. This changes in outlook the area of this foundation to the organization to lessen the expenses related with the administration of equipment and programming assets.

In this work, G. Ateniese, R. Consumes, et.al[3] has proposed provable information ownership (PDP) that permits a customer that has put away information at an untrusted worker to confirm that the worker has the first information without recovering it. The model creates probabilistic evidences of ownership by examining irregular arrangements of squares from the worker, which definitely decreases I/O costs. The customer keeps a consistent measure of metadata to check the confirmation. The test/reaction convention sends a little, consistent measure of information, which limits network correspondence.

Provable Data Possession (PDP) that gives probabilistic confirmation that an outsider stores a document. The model is special in that it permits the worker to get to little segments of the document in producing the evidence; any remaining procedures should get to the whole record. Inside this model, we give the first provably-secure plan for far off information checking. The customer stores a little O(1) measure of metadata to confirm the worker's confirmation.

The customer pre-figures labels for each square of a document and afterward stores the record and its labels with a worker. Sometime in the not too distant future, the customer can confirm that the worker has the record by producing an arbitrary test against an arbitrarily chosen set of document blocks.

In this work, H. Shacham and B. Waters, et.al [4] has proposed In a proof-of-retrievability framework, an information stockpiling focus should demonstrate to a verifier that he is really putting away the entirety of a customer's information. The focal test is to construct frameworks that are both proficient and provably secure. A proof-of-retrievability convention in which the customer's question and worker's reaction are both incredibly short.

Cryptographic frameworks that would permit clients of rethought stockpiling administrations (or their representatives) to confirm that their information is as yet accessible and prepared for recovery if necessary. Such a capacity can be imperative to capacity suppliers too. Clients might be hesitant to depend their information to an obscure startup; a reviewing component can promise them that their information is in reality still accessible.

The most significant crypto basis is this: Whether the convention really sets up that any worker that passes a confirmation check for a record even a vindictive worker that displays subjective, The early cryptographic papers did not have a proper security model, not to mention verifications.

In this work, C. Wang, Q. Wang, et.al [5] has proposed Cloud Computing moves the application programming and information bases to the huge server farms, where the administration of the information and administrations may not be completely reliable. Cloud information stockpiling security, which has consistently been a significant part of nature of administration.

The information put away in the cloud might be as often as possible refreshed by the clients, including inclusion,

Annals of R.S.C.B., ISSN:1583-6258, Vol. 25, Issue 3, 2021, Pages. 8606 - 8615
Received 16 February 2021; Accepted 08 March 2021.

erasure, alteration, annexing, reordering, and so on To guarantee stockpiling rightness under powerful information update is thus of central significance. a powerful and adaptable dispersed plan with express unique information backing to guarantee the rightness of clients' information in the cloud.

Security dangers looked by cloud information stockpiling can emerge out of two unique sources. From one perspective, a CSP can act naturally intrigued, untrusted and perhaps noxious. The foe is keen on adulterating the client's information records put away on individual workers.

In this work, Q. Wang, C. Wang, et.al[6], has proposed, The help for information elements by means of the most broad types of information activity, for example, block adjustment, inclusion and erasure, is additionally a huge advance toward common sense, since administrations in Cloud Computing are not restricted to document or reinforcement information as it were. The Proof of Retrievability model by controlling the exemplary Merkle Hash Tree (MHT) development for block label verification.

"Cloud" achieves many testing configuration issues which have significant impact on the security and execution of the general framework. Perhaps the greatest worry with cloud information stockpiling is that of information trustworthiness confirmation at untrusted workers.

Proposed Methodology

In Cloud Computing, the distantly put away electronic information may not exclusively be gotten to yet in addition refreshed by the customers, e.g., through square alteration, cancellation and inclusion. Tragically, the cutting edge with regards to far off information stockpiling chiefly center around static information documents and the significance of this unique information refreshes has gotten restricted consideration in the information ownership applications.

An epic multi-cloud Authentication convention, specifically CP-HABE, including two plans. Every subgroup is dealt with practically like a different multi-cloud gathering and is overseen by a confided in gathering security middle person character Hierarchal Attribute based circulated provable information ownership (CP-HABE). This is an attractive component particularly for the huge scope network frameworks, since it limits the issue of focusing the outstanding task at hand on a solitary substance.

Multi Cloud Group Member Registration & Login

The primary User entered the username, secret word, and picks any one gathering id at that point register with Data Cloud Server. This client included this specific gathering. At that point entered the username, secret phrase and pick the client's gathering id for login.

Efficient Key Generation & Controller Using CP-HABE

In Key Generation module, each client in the gathering creates public key and private key. Client produces an irregular, and yields public key and private key. Without loss of consensus, In the methodology, expect client u1 is the first client, who is the maker of shared information. The first client additionally makes a client list (UL), which contains ids of the relative multitude of clients in the gathering. The client list is public and endorsed by the first client.

Upload File to Data Multi Cloud Server

The client needs to transfer a record. So the client split the records into numerous squares. Next scramble each squares with the public key. At that point, the client create mark of each squares for validation reason. At that point transfer each square code text with signature, block id and endorser id. These metadata and Key Details are put away in Public Verifier for public inspecting.

Annals of R.S.C.B., ISSN:1583-6258, Vol. 25, Issue 3, 2021, Pages. 8606 - 8615
Received 16 February 2021; Accepted 08 March 2021.

Download File from Data Multi Cloud Server

The following client or gathering part needs to download a record. So the client gives the filename and gets the mystery key. At that point entered this mystery key. In the event that this mystery key is legitimate, at that point the client ready to decode this downloaded document. Else, the following client entered wrong mystery key then the user1 hindered by Public Verifier. On the off chance that this mystery key is substantial, at that point unscramble each impede and confirm the mark. On the off chance that the two marks are equivalent, at that point join all squares at that point get the first document.

Public Auditing with User Collision in Public Verifier

In Public verifier technique, the User who entered some unacceptable mystery key at that point obstructed by the public verifier. Next the client added public verifier crash client list. At that point the client needs to attempts to download any record, the Data Cloud Server answers his obstructed data. At that point the client needs to un crash, so they ask the public verifier. At last the public verifier unrevoked this client. Next the client ready to download any document with its comparing mystery key. In this methodology, by using the possibility of intermediary re-marks, when a client in the gathering is impact, the Data Cloud Server can re-sign the squares, which were endorsed by the crash client, with a leaving key.

Experimental Setup

In certain situations, the customers need to store their information on multi-cloud workers to permit parallelism and gigantic information stockpiling. Thus, the honesty checking convention should be effective to save the verifier's expense. The creator Wang, H. proposed a novel PDP model as ID-DPDP (personality based circulated provable information ownership) in multi-distributed storage. In light of the bilinear matching idea, the total IDDPDP convention is planned. The proposed ID-DPDP convention is provably secure under the hardness supposition of the standard CDH (computational Diffie-Hellman) issue as tried by creator. Notwithstanding the underlying preferred position of end of overseeing authentication, the IDDPDP approach is productive and adaptable. Contingent upon the customer's approval, the proposed ID-DPDP convention can recognize private check and public confirmation.

The examination of above PDP plans will assist with distinguishing the most appropriate methodology for given business setting. The accompanying table gives relative investigation of PDP plans. The primary table indicates varieties of PDP calculation alongside the methods utilized and whether it underpins single or multi distributed storage. The second table we have analyzed the varieties of PDP plots by determining preferences and drawbacks of them.

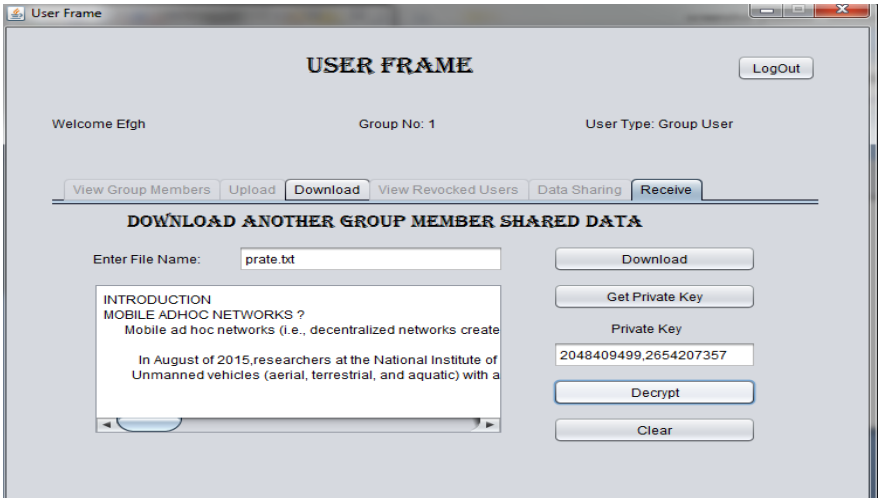

Fig. 1. Receiver side decrypt form

Annals of R.S.C.B., ISSN:1583-6258, Vol. 25, Issue 3, 2021, Pages. 8606 - 8615
Received 16 February 2021; Accepted 08 March 2021.

The above PDP plans need customer inceptions for information respectability checking. Likewise, in the event of organization situated climate, it will be helpful if the framework is following the information uprightness confirmation exchanges for future improvements. The model can be intended to accomplish self started approach of PDP and log-based methodology can be utilized for organization reason. As per above PDP plans, the proposed framework will assist customer with keeping up the information trustworthiness confirmation records for additional procedures and furthermore customer will be liberated from starting the information uprightness checking measure. In detail, we will plan a framework where there will be a clock which will continue to create hinders and because of these intrudes on the information honesty confirmation solicitation will get produced in the interest of the customer. The solicitation at that point will be served by cloud worker as typical PDP approach and will restore the evidence back to customer.

Conclusions

Returned to the personality based circulated provable information ownership plot in multi-distributed storage. The worker can in any case create a substantial evidence to demonstrate that the information are put away flawless. A conventional development of ID-PDP conventions by utilizing general mark plans and customary PDP conventions and demonstrated its security. Assembled a solid ID-PDP convention and an all-inclusive variant that is reasonable for the multi-distributed storage climate we proposed another public reviewing component for imparted information to productive client denial in the cloud. At the point when a client in the gathering is denied, we permit the semi-confided in cloud to re-sign squares that were endorsed by the disavowed client with intermediary re-marks. Trial results show that the cloud can improve the proficiency of client repudiation, and existing clients in the gathering can save a lot of calculation and correspondence assets during client renouncement.

References

[1] Wang, B., Li, B., & Li, H. (2013). Public Auditing for Shared Data with Efficient User Revocation in the Cloud. *In the Proceedings of IEEE INFOCOM 2013*, 2904–2912.

[2] Armbrust, M., Fox, A., Griffith, R., Joseph, A.D., Katz, R., Konwinski, A., &Zaharia, M. (2010). A view of cloud computing. *Communications of the ACM*, *53*(4), 50-58.

[3] Ateniese, G., Burns, R., Curtmola, R., Herring, J., Kissner, L., Peterson, Z., & Song, D. (2007). Provable data possession at untrusted stores. *In Proceedings of the 14th ACM conference on Computer and communications security*, 598-609.

[4] Shacham, H., & Waters, B. (2008). Compact Proofs of Retrievability. *In the Proceedings of ASIACRYPT*, 90-107

[5] Wang, C., Wang, Q., Ren, K., & Lou, W. (2009). Ensuring Data Storage Security in Cloud Computing. *In the Proceedings of ACM/IEEE IWQoS 2009*, 1–9.

[6] Wang, C., Wang, Q., Ren, K., & Lou, W. (2010). Privacy-Preserving Public Auditing for Data Storage Security in Cloud Computing. *In the Proceedings of IEEE INFOCOM 2010*,525–533.

[7] Wang, Q., Wang, C., Li, J., Ren, K., & Lou, W. (2009). Enabling public verifiability and data dynamics for storage security in cloud computing. *In European symposium on research in computer security*, *Springer, Berlin, Heidelberg*, 355-370.

[8] Zhu, Y., Wang, H., Hu, Z., Ahn, G.J., Hu, H., &Yau, S.S. (2011). Dynamic audit services for integrity verification of outsourced storages in clouds. *In Proceedings of the 2011 ACM Symposium on Applied Computing*, 1550-1557.

[9] Saravanan, N., Subramani, A., &Sivakumar, P. (2016). Mobile Agents based Reliable and Energy Efficient Routing Protocol for MANET. *International Journal of Intelligent Engineering and Systems*,5*(*2), 220–232.

[10] Zhu, Y., Ahn, G.J., Hu, H., Yau, S.S., An, H.G., & Hu, C.J. (2011). Dynamic audit services for outsourced storages in clouds. *IEEE Transactions on Services Computing*, *6*(2), 227-238.

[11] Saravanan, N., Subramani, A., & Balamurugan, P. (2017). Optimal route selection in MANET based on

Annals of R.S.C.B., ISSN:1583-6258, Vol. 25, Issue 3, 2021, Pages. 8606 - 8615
Received 16 February 2021; Accepted 08 March 2021.

particle swarm optimization utilizing expected transmission count. *Cluster Computing the Journal of Networks, Software Tools & Applications, 6*(1).

[12] Somu, M., &Rengarajan, N. (2012). Particle swarm intelligence approach for enhanced hierarchical cache optimization in IPTV networks. *European Journal of Scientific Research, 76*(3), 366-378.

[13] Somu, M., &Rengarajan, N. (2013). A Hybrid Model of Swarm Intelligence Algorithm to Improve the Hierarchical Cache Optimization in IPTV Networks. *International Review on Computers and Software,* 1460.

[14] Yuan, J., & Yu, S. (2013). Proofs of Retrievability with Public Verifiability and Constant Communication Cost in Cloud. *In Proceedings of ACM ASIACCS-SCC'13.*

[15] Tate, S.R., Vishwanathan, R., & Everhart, L. (2013). Multi-user Dynamic Proofs of Data Possession Using Trusted Hardware. *In Proceedings of ACM CODASPY'13,* 353–364.