International Journal of Computer Science
Scholarly Peer Reviewed Research Journal - PRESS - OPEN ACCESS
ISSN: 2348-6600
http://www.ijcsjournal.com Volume 6, Issue 1, No 2, 2018 ISSN: 2348-6600
Reference ID: IJCS-331 PAGE NO: 2196-2202

An Efficient and Secure Data Storage Using Two Different Cloud Storage Technique

V.Geetha[#1], Dr.M.V.Srinath[*2], K.Kanchikamatchi [*3]

[#]*Head of the Department of Computer Science, Sengamala Thayaar Educational Trust Women's College, Mannargudi, Thiruvarur, Tamil Nadu*

[*]*Department of Computer Science, Sengamala Thayaar Educational Trust Women's College, Mannargudi, Thiruvarur, Tamil Nadu*

[3]kanchikamatchi1894@gmail.com

Abstract— **Distributed storage empowers clients to remotely store their information and appreciate the on-request excellent cloud applications without the weight of nearby equipment and programming administration. In spite of the fact that the advantages are clear, such an administration is additionally giving up clients' physical ownership of their outsourced information, which definitely postures new security dangers toward the rightness of the information in cloud. Sensitive data is stored in the cloud, the corresponding private information may be exposed to cloud servers. Beside data privacy, client frequent queries will certainly and gradually reveal any private information on data statistic properties. Thus, data and queries of the outsourced database should be protected against the cloud service provider. In this research enhanced Shared-Ownership file access control Model. Our proposed secure database system includes a database administrator, and two non-colluding clouds. In this model, the database administrator can be implemented on a client side from the perspective of cloud service. The two clouds, as the server side, provide the storage and the computation service. The mechanism guarantees that knowing either of these two parts cannot obtain any useful privacy information, to conduct a secure database, data are encrypted and outsourced to be stored in one cloud, and the private keys are stored in the other one cloud. In our scheme, the knowledge of stored database and queries is partitioned into two parts, respectively stored in one cloud. Security analysis demonstrates that the protection of numerical data is unambiguously ensured against cloud suppliers in our proposed system.**

Index Terms— **Dual cloud, Security analysis, Shared-Ownership file access control**

I. INTRODUCTION

A Several patterns are opening up the time of distributed computing, which is an Internet-based improvement and utilization of PC innovation. The ever less expensive and all the more great processors, together with the Software as a Service (SaaS) figuring engineering, are changing server farms into pools of registering administration on a gigantic scale. The expanding system transmission capacity and dependable yet adaptable system associations influence it even conceivable that clients to would now be able to buy in excellent administrations from information and programming that dwell exclusively on remote server farms. Distributed storage is a distributed computing model in which information is put away on remote servers got to from the Internet, or "cloud." It is kept up, worked and overseen by a distributed storage specialist organization on a capacity server that are based on virtualization methods. Capacity support errands, for example, obtaining extra stockpiling limit, are offloaded to the obligation of a specialist organization. Distributed storage can be utilized as cataclysmic event verification reinforcement, as regularly there are a few distinctive reinforcement servers situated in better places far and wide.

A distributed computing is a kind of Internet-based enlisting that gives shared PC dealing with resources and data to PCs and distinctive contraptions on ask. It is a model for engaging ubiquitous, on-ask for access to a typical pool of configurable enlisting resources PC frameworks, servers, amassing, applications and organizations, which can be immediately provisioned and released with inconsequential organization effort. A limit courses of action outfit customers and tries with various capacities to store and process their data in outcast server cultivates that may be arranged far from the client going in expel from over a city to over the world. Distributed computing depends on sharing of assets to accomplish soundness and economy of scale, like an utility (like the power framework) over a power organize.

International Journal of Computer Science
Scholarly Peer Reviewed Research Journal - PRESS - OPEN ACCESS
ISSN: 2348-6600
http://www.ijcsjournal.com Volume 6, Issue 1, No 2, 2018 ISSN: 2348-6600
Reference ID: IJCS-331 PAGE NO: 2196-2202

Organizations can scale up as figuring needs increment and afterward downsize again as requests diminish. In 2013, it was accounted for that distributed computing had turned into a very requested administration or utility because of the upsides of high registering power, shabby cost of administrations, superior, versatility, openness and in addition accessibility. Some cloud merchants are encountering development rates of half every year except being still in a phase of early stages, it has entanglements that should be routed to make distributed computing administrations more dependable and easy to understand.

The essential inquiry any directing calculation needs to reply in this setting is "who makes a decent next bounce when no way to the goal as of now exists or potentially no other data about this goal may be accessible? In spite of various existing recommendations for artful directing the response to the past inquiry has as a rule been "everybody" or "nearly everybody". The lion's share of existing conventions are flooding-based that disseminate copy duplicates to all hubs in the system or a subset of them (e.g. tattling, and utility-based flooding). Despite the fact that flooding can be very quick in a few situations, the overhead associated with terms of transfer speed, support space, and vitality scattering is frequently restrictive for little remote gadgets (e.g. sensors). They call plans like these, which utilize in excess of one duplicate for every message, "multi-duplicate" plans. Single-duplicate plans that exclusive highway one duplicate for each message can extensively lessen asset squander. However, they can regularly be requests of size slower than multi-duplicate calculations and are naturally less solid. These last attributes may make single-duplicate plans exceptionally bothersome for a few applications (e.g. in a debacle recuperation systems or strategic systems past foe lines; regardless of whether correspondence must be irregular, limiting deferral or message misfortune is a need). Condensing, no steering plan for discontinuously associated conditions right now exists that can accomplish both little postponements and reasonable use of the system and assets.

In proposed system, Shared-Ownership file access control Model to characterize our thought of shared possession, and to formally express the given requirement issue. At that point propose two instantiations of the Shared-Ownership file access control model to uphold shared proprietorship arrangements in an appropriated form. They propose a first arrangement, called Commune, which distributively implements Shared-Ownership file access control and can be sent in a freethinker cloud stage. Cooperative guarantees that (i) a client can't read a record from a common archive except if that client is conceded perused access by in any event of the proprietors, and (ii) a client can't to compose a document to a mutual storehouse except if that client is allowed compose access by in any event of the proprietors. They propose a second arrangement, named Comrade, which use usefulness from the block chain innovation keeping in mind the end goal to achieve agreement on get to control choice. Friend enhances the execution of Commune, yet requires that the cloud can decipher get to control choices that achieved accord in the block chain into capacity get to control rules, in this way requiring minor alterations of existing mists. They fabricate models of Commune and Comrade and assess their execution as for the document estimate and the quantity of clients.

II. Related Work

A.Publicly Verifiable Remote Data Integrity

In this research, one plan and three calculations are utilized. That are Kegan, Copen, and Tegan. On the off chance that client transfer the information, consequently plan three duplicates at that point put away tin three servers that why for security and dodge server over-burden. That duplicate additionally scrambled so cloud specialist co-op or any others can't hack the information. On the off chance that clients transfer the information, server consequently change over to zip positions. So the server diminishes the document estimate naturally. The client share the record to approved client. At that point approved client send the document demand to cloud server again server send the encoded information to approved client. Also, approved client get the decode key from information proprietor. The fundamental point of this proposal is to store the information in the various server. That duplicates likewise encoded so the cloud specialist organization or any others can't hack the information. In the event that clients transfer the information, server naturally change over to zip positions. So the server diminish the record measure naturally. Client share the record to approved client. They contend that outsider inspecting is essential in making an online administration situated economy, since it enables clients to assess dangers, and it expands the effectiveness of protection based hazard moderation. They depict methodologies and framework snares that help both inner and outer evaluating of online stockpiling administrations, portray inspirations for specialist co-ops and reviewers to embrace these methodologies, and rundown challenges that should be settled for such examining to end up a reality. Empowering open unquestionable status

International Journal of Computer Science
Scholarly Peer Reviewed Research Journal - PRESS - OPEN ACCESS
ISSN: 2348-6600
http://www.ijcsjournal.com Volume 6, Issue 1, No 2, 2018 ISSN: 2348-6600
Reference ID: IJCS-331 PAGE NO: 2196-2202

and information progression for capacity security in distributed computing.

B.Provable Multi copy Dynamic Data Possession in Cloud Computing Systems

In this research, outsourcing information to remote servers has transform into a developing pattern for some, associations to facilitate the weight of neighborhood information stockpiling and security. In this work they have considered the trouble of making different duplicates of dynamic information record and affirm those duplicates put away on untrusted cloud servers. They have proposed another PDP conspire (alluded to as MB-PMDDP), which underpins outsourcing of multi-duplicate unique information, where the information proprietor is talented of not just filing and getting to the information duplicates put away by the CSP, yet additionally refreshing and scaling these duplicates on the remote servers. The proposed plot is the first to address numerous duplicates of dynamic information. The correspondence between the approved clients and the CSP is estimated in our framework, where the approved clients can easily get to an information duplicate got from the CSP utilizing a solitary mystery key imparted to the information proprietor. Besides, the proposed conspire bolsters open unquestionable status, permits self-assertive number of examining, and permits ownership free confirmation where the verifier has the ability to check the information honesty despite the fact that they neither has nor recovers the record obstructs from the server.

C.Efficient and Secure Data Storage in Cloud Computing RSA and DSE Function

In this research, under the security of remote stockpiling applications has been progressively tended to in the ongoing years, which has brought about different ways to deal with the plan of capacity check natives. The writing recognizes two primary classifications of confirmation plans. Deterministic confirmation plans check the protection of a remote information in a solitary, albeit possibly more costly task and probabilistic check plans depend on the irregular checking of segments of outsourced information. Deterministic Secure Storage Deterministic arrangements are checking the capacity of the whole information at every server. Descartes et al. also, Filo et al. are right off the bat proposed an answer for remote information respectability. Both utilize RSA-based capacities to the entire information petition for each confirmation challenge. They require pre-processed consequences of difficulties to be put away at verifier, where a test relates to the hashing of the information linked with an arbitrary number. Be that as it may, them two are wasteful for the substantial information records, which require more opportunity to process and exchange their qualities. Carmona et al. Portrayed a basic deterministic approach with boundless number of difficulties is proposed, where the verifier like the server is putting away the information. In this approach, the server needs to send MAC of information as the reaction to the test message. The verifier sends a new one of a kind arbitrary incentive as the key for the message verification code to keep the server from putting away just the aftereffect of the past of the information. Neck al. Proposed a SEC (Storage Enforcing Commitment) deterministic confirmation approach. Probabilistically Secure Storage In their framework, the customer pre-processes the labels for each square of a record utilizing holomorphic certain labels and stores the document and it labels with the server. At that point, the customer can check that server uprightness of the record by creating an arbitrary test, which determines the chose places of document squares. Utilizing the questioned squares and their relating labels and the server creates a proof of respectability. Joel's et al. proposed a formal meaning of POR (Proof of Retrievability) and its security demonstrate. In this model, the scrambled information is being partitioned into little information squares, which are encoded with Reed-Solomon codes. The "sentinels" are inserted among encoded information squares to distinguish whether it is unblemished.

D.Privacy-preserving external auditing for data storage security in cloud

In this research, TPA will check the uprightness or accuracy of the information which is put away by the customer. Where, the TPA won't take in any information on the information put away in the cloud server. Also, the customer will have the alternative to increment or decline the memory space required. The working can be clarified as: first the customer needs to enlist onto the cloud server utilizing TPA to profit the administration. In the wake of enrolling the TPA will keep the client ID and the full points of interest will be put away in the cloud server. In the event that customer needs to transfer a document then a demand is sent to TPA. The TPA will produce an open and a private key, sends people in general key to the customer and private key to the server. Presently the customer will scramble the information documents utilizing people in general key and send it to cloud server, in the meantime it will create the hash code of the information record and send that to TPA. At the point when client needs to check the uprightness of the information put away in the cloud server, the client will send a demand to TPA, now the TPA will request the mark from the server.

International Journal of Computer Science
Scholarly Peer Reviewed Research Journal - PRESS - OPEN ACCESS
ISSN: 2348-6600
http://www.ijcsjournal.com Volume 6, Issue 1, No 2, 2018 ISSN: 2348-6600
Reference ID: IJCS-331 PAGE NO: 2196-2202

The server will produce the mark of client information records upon ask for and send it to TPA. On the off chance that the mark from the server coordinates that of the hash code spared in TPA then the information records are secure and honesty is confirmed. Here the vital favorable position is that, even the outsider won't take in any learning on the information put away in cloud server.

E.Enhanced privacy of a remote data integrity-checking protocol for secure cloud storage

In this research, to produce a proof that the server has the file in its unique shape, the server processes a reaction to a test from the verifier. The verifier approves that the file isn't being altered through checking the rightness of the reaction. Participants additionally proposed two PDP conspires by using the RSA-based homomorphic direct authenticators. In the meantime, Jules et al. proposed the idea of verification of irretrievability, in which blunder rectifying codes and spot-checking are utilized to accomplish the properties of ownership and irretrievability records. PDP and POR have turned into an exploration hotspot of secure distributed storage and various plans have been proposed. Research, the explored information security issues in remote information honesty checking conventions. The demonstrated that the current protection saving remote information trustworthiness checking convention couldn't accomplish the coveted objective of "releasing no data to an outsider". The formalized the idea of "zero-information security" and propose denim demonstrated rendition of the convention in to accomplish this property. What's more, the demonstrated that our convention satisfied other security prerequisites. At long last, both the execution examination and the usage demonstrated that our change was viable.

III. Methodology

An Access control arrangement can't keep a client from appropriating content through an out-of-band channel. A client who legitimately peruses a record, can spill it to outsiders. On the other hand, a legitimate per user can impart the way to S and in this way release the document. Additionally, a vindictive essayist can compose a document and spread it through an out-of-band channel. For instance, a client can distribute records for him on S and make them accessible for others to peruse. Cooperative, be that as it may, should at any rate permit genuine per users, who tolerate to the convention particular, to recognize the substance composed by malignant scholars and the substance composed by fair journalists. Keen contracts allude to restricting contracts between at least two gatherings that are executed by all block chain hubs. In particular, shrewd contracts execute state machine replication. Brilliant contracts commonly comprise of an independent code and diligent stockpiling accessible to all block chain hubs. For instance, a decentralized stage that empowers the execution of self-assertive applications (or contracts) on its block chain. Inferable from its help for a Turing-finish dialect, Ethereum (which at present likewise depends on PoW-based accord) offers a simple means for engineers to send their dispersed applications as keen contracts.

A two clouds have been assigned distinct tasks in the database system: First cloud provides the main storage service and stores the encrypted database. Meanwhile, Second cloud executes the main computation task, to figure out whether each numerical record satisfies the client's query request with its own security key. With the assumption of no collusion between two clouds, the knowledge of application logic can be partitioned into two parts in our proposed scheme, where each one part is only known to one cloud. Analyse in this research, one single part of knowledge cannot reveal privacy of the data and the query.

A dual different cloud have been appointed particular undertakings in the database framework: First cloud gives the principle stockpiling administration and stores the scrambled database. In the mean time, Second cloud executes the primary calculation undertaking, to make sense of whether each numerical record fulfills the customer's inquiry ask for with its own particular security key. With the supposition of no agreement between two mists, the information of use rationale can be apportioned into two sections in our proposed conspire, where every one section is just known to one cloud. Break down in this research, one single piece of information can't uncover security of the information and the question.

The fundamental thought behind Comrade is that a brilliant contract can instantiate a confided in outsider that can assess client accreditations against proprietors get to arrangements in a reliable way. This is an essential arrangement of the block chain innovation that holds as long as the security presumptions on the block chain hold. Henceforth, in Comrade, a keen contract helps the cloud's PDP guaranteeing reliable treatment of strategies and accreditations.

International Journal of Computer Science
Scholarly Peer Reviewed Research Journal - PRESS - OPEN ACCESS
ISSN: 2348-6600
http://www.ijcsjournal.com Volume 6, Issue 1, No 2, 2018 ISSN: 2348-6600
Reference ID: IJCS-331 PAGE NO: 2196-2202

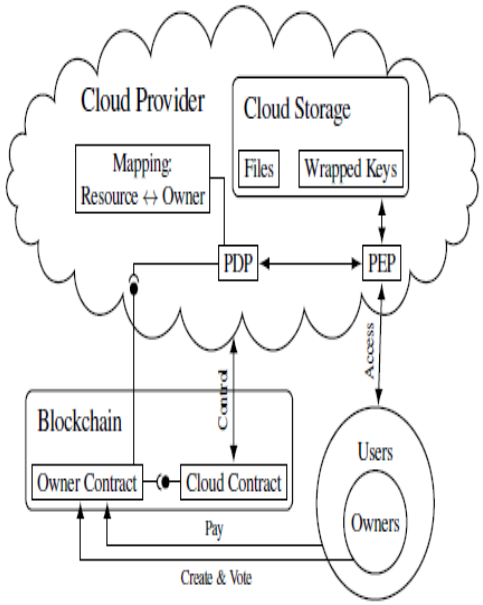

Fig. 1 Shared-Ownership file access control mechanism

Uniquely in contrast to Commune, be that as it may, Comrade needs the cloud to be shared-proprietorship mindful and implement the approaches characterized by the shrewd contract. At that point propose two conceivable Instantiations of our proposed shared ownership demonstrate. Our first Solution, called cooperative, depends on secure record dispersal and arrangement safe mystery sharing to guarantee that all entrance concedes in the cloud require the help of a concurred limit of proprietors. Thusly, Commune can be utilized as a part of existing mists without alterations to the stages. Our second arrangement, named friend, influences the block chain innovation keeping in mind the end goal to achieve accord on get to Control choice. Dissimilar to collective, confidant requires that the cloud can decipher get to control choices that achieve agreement. In the block chain into capacity get to control rules, in this manner requiring Minor adjustments to existing cloud.

Function V (O; U, A, F, D)
Votes [O; U, A, F] =D
end function
function HASACCESS(F, U, a)
Grant ← 0
O ← OWNERS [F]
for i ← 1 TO |O| do
if votes [O_i; U, a, F] == GRANT THEN
Grant ← Grant + 1
end if
end for
return (GRANT ← THRESHOLD[A, F])
end function

Review that all exchanges issued by the proprietors in Comrade are affirmed in the square chain by the validators/excavators. As required for the security of the basic square chain, accept the standard wellbeing conditions specific to the hidden square chain innovation. For example, since Ethereum depends on Proof-of-Work, accept that the foe can't control most of the figuring power in the system. By and by, expect that the enemy does not influence the mining procedure in Ethereum (i.e., does not go about as a digger). Notice that pernicious diggers can choose not to incorporate the exchanges issued by the proprietors in Comrade. Thusly, the enemy can endeavor to defer the affirmation of exchanges issued by substances in Comrade for a short measure of time. Adjusting with the present activity of Ethereum, accept that the guarantors of exchanges will re-communicate their exchanges on the off chance that they are excluded in the resulting square. This will guarantee that these exchanges will be in the end affirmed by fair mineworkers in the framework—as long as most of the processing power saddled in Ethereum is straightforward.

IV. Result and Discussion

In this exploration, demonstrate this Shared-Ownership document get to control show by breaking down the security of step. Note that, in these means, since everyone of the information got by first cloud is encoded and the calculation steps are altogether performed in the ciphertext area, and due to the semantic security of Paillier cryptosystem, first cloud can't find any private data from these three stages except if second cloud plots with it.

A.Efficiency

According to our experiment results, TBGR provide a 60% of efficiency in this research work. CSP approach provide a 50% of efficiency in this research work. MP-PMPDP 40% of efficiency in this research work. SOM provide a 76% of efficiency in this research work. Our proposed SOM Model provide more efficiency compared with other approach.

International Journal of Computer Science
Scholarly Peer Reviewed Research Journal - PRESS - OPEN ACCESS
ISSN: 2348-6600
http://www.ijcsjournal.com Volume 6, Issue 1, No 2, 2018 ISSN: 2348-6600
Reference ID: IJCS-331 PAGE NO: 2196-2202

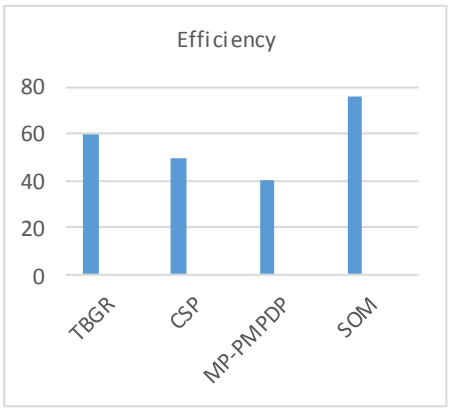

Fig. 2 Efficiency analysis

B.Accurate Result

According to our experiment results, TBGR provide a 40% of accurate result in this research work. CSP approach provide a 50% of accurate result in this research work. MP-PMPDP 60% of accurate result in this research work. SOM provide a 76% of accurate result in this research work. Our proposed SOM Model provide more efficiency compared with other approach.

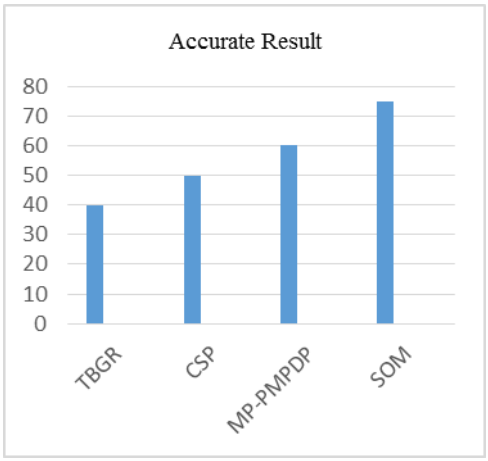

Fig. 3 Accurate result analysis

C. Security

According to our experiment results, TBGR provide a 60% of security in this research work. CSP approach provide a 50% of security in this research work. MP-PMPDP 40% of accurate result in this research work. SOM provide an 80% of security result in this research work. Our proposed SOM Model provide High security compared with other approach.

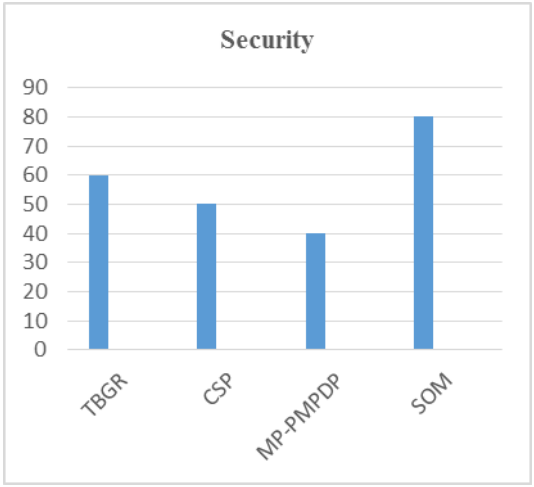

Fig. 4 Security analysis

V. Conclusions

In this research, presented a novel idea of shared possession and portrayed it through a formal access control display, called SOM. At that point propose two conceivable instantiations of our proposed shared possession display. Our first arrangement, called Commune, depends on secure document dispersal and conspiracy safe mystery sharing to guarantee that all entrance concedes in the cloud require the help of a concurred edge of proprietors. All things considered, Commune can be utilized as a part of existing freethinker mists without alterations to the stages. Our second arrangement, named Comrade, influences the block chain innovation keeping in mind the end goal to achieve accord on get to control choice. Not at all like Commune, Comrade requires that the cloud can decipher get to control choices that accomplished agreement in the block chain into capacity get to control rules. The friend, in any case, demonstrates preferred execution over Commune. Our exhibited a two-cloud design with a progression of connection conventions for outsourced database benefit, which guarantees the security conservation of information substance, factual properties and inquiry design. In the meantime, with the help of range questions, it ensures the classification of static information, as well as tends to potential security spillage in measurable properties or after vast number of inquiry forms. Security investigation demonstrates that our plan can meet the protection safeguarding

International Journal of Computer Science
Scholarly Peer Reviewed Research Journal - PRESS - OPEN ACCESS
ISSN: 2348-6600
http://www.ijcsjournal.com Volume 6, Issue 1, No 2, 2018 ISSN: 2348-6600
Reference ID: IJCS-331 PAGE NO: 2196-2202

prerequisites. Moreover, execution assessment result demonstrates that our proposed plot is effective.

REFERENCES

[1] G. Ateniese, R. D. Pietro, L. V. Mancini, and G. Tsudik, "Scalable and efficient provable data possession," in Proc. 4th Int. Conf. Secur. Privacy Commun. Netw. (SecureComm), New York, NY, USA, 2006, Art. ID 9.

[2] M. A. Shah, R. Swaminathan, and M. Baker, "Privacy-preserving audit and extraction of digital contents," IACR Cryptology ePrint Archive, Tech. Rep. 2006/186, 2006.

[3] F. Sebé, J. Domingo-Ferrer, A. Martinez-Balleste, Y. Deswarte, and J.-J. Quisquater, "Efficient remote data possession checking in critical information infrastructures," IEEE Trans. Knowl. Data Eng., vol. 20, no. 8, pp. 1034–1038, Aug. 2005.

[4] K. Zeng, "Publicly verifiable remote data integrity," in Proc. 10th Int. Conf. Inf. Commun. Secur. (ICICS), 2005, pp. 419–434.

[5] G. Ateniese et al., "Provable data possession at untrusted stores," in Proc. 14th ACM Conf. Comput. Commun. Secur. (CCS), New York, NY, USA, 2005, pp. 598–609.

[6] M. A. Shah, M. Baker, J. C. Mogul, and R. Swaminathan, "Auditing to keep online storage services honest," in Proc. 11th USENIX Workshop Hot Topics Oper. Syst. (HOTOS), Berkeley, CA, USA, 2004, pp. 1–6.

[7] E. Mykletun, M. Narasimha, and G. Tsudik, "Authentication and integrity in outsourced databases," ACM Trans. Storage, vol. 2, no. 2, pp. 107–138, 2004.

[8] D. L. G. Filho and P. S. L. M. Barreto, "Demonstrating data possession and uncheatable data transfer," IACR (International Association for Cryptologic Research) ePrint Archive, Tech. Rep. 2006/150, 2004.

[9] Y. Deswarte, J.-J. Quisquater, and A. Saïdane, "Remote integrity checking," in Proc. 6th Working Conf. Integr. Internal Control Inf. Syst. (IICIS), 2003, pp. 1–11.

[10] P. Golle, S. Jarecki, and I. Mironov, "Cryptographic primitives enforcing communication and storage complexity," in Proc. 6th Int. Conf. Financial Cryptograph. (FC), Berlin, Germany, 2003, pp. 120–135.

[11] Yong Jian Chin; Thian Song Ong; Michael K. O. Goh; Bee Yan Hiew, "Integrating Palmprint and Fingerprint for Identity Verification", Network and System Security, 2009. NSS '09. Third International Conference on Year: 2009.

[12] Ahmed Elnakib; Ayman El-Baz; Manuel F. Casanova; Georgy Gimel'farb; Andrew E. Switala, "Image-based detection of Corpus Callosum variability for more accuratediscrimination between autistic and normal brains", 2010 IEEE International Conference on Image Processing Year: 2010.

[13] V. D. Mhaske; A. J. Patankar, "Multimodal biometrics by integrating fingerprint and palmprint for security", Computational Intelligence and Computing Research (ICCIC), 2013 IEEE International Conference on Year: 2013.

[14] Lei Zhang; D. Zhang, "Characterization of palmprints by wavelet signatures via directional context modeling", IEEE Transactions on Systems, Man, and Cybernetics, Part B (Cybernetics) Year: 2004.