Enhancing the Data from Cloud Data Base by Providing Assurance by Third Party

Girija Rani Suthoju[1], M. Suresh Babu[2]

[1]Assistant Professor, Department of CSE, NGIT, Hyderabad, TS
[2]Professor, Department of CSE, S K D Engineering College, Anantapur, AP

ABSTRACT

Large quantity of records is complex and expensive due to the necessities of excessive storage ability and qualified personnel. In the deliberate topic whilst a person requeststhe information to the statistics in the cloud, we offer security through police research theintruders among consumer and cloud database with relevance the cloud providersand consequently the owner. The proposedscheme affords safety from intruders bymeans of interference the content there anddetecting the intruders between user and cloud database with respect cloud provider carriers and the owner and lets in the authorized customers to verify that they're receiving the sourced data as a latest model. As a consequence, in the course of this paper, the thought is to outsource dynamic records that is based totally on the aid of cloud garage scheme, here the house owners of remote servers are capable of scaling data} that depends on them with the change and moreover get admission to the data by using archiving them, that is maintain cloud service carriers. The records proprietor physically releases sensitive records to an oversea cloud provider issuer, there are a few issues with reference to confidentiality,integrity and get entry to control of theinformation.

The projected subject has 5 important capa-bilities:

(i) it permits the owner to deliver sensitivefacts to a cloud service provider and performfull block-stage dynamic operations at the outsourced records i.e., block modification, insertion, deletion and append.

(ii) it ensures that authorised customers (i.e.,individuals who have the right to get admission to the proprietor’s file) get hold ofthe trendy model of the outsourced in- formation.

(iii) it lets in oblique mutual con-sider between proprietor and additionally the cloud carrier issuer.

(iv) it lets in the owner to grant or revoke access to the outsourced records and

(v) it detects the intrud-ers among consumer and cloud statistics with relevance the cloud service suppliers and proprietor.

We talk the safety troubles with theprojected topic. Except, we've a unethical tojustify its overall performance through theoretical analysis and an example implementation on Amazon cloud platform to decide garage, conversation and computation overheads.

Index Terms—Secure Data, Trusted Third Party, Storage of the Data, Access control and Dynamic data, Cloud database.

.

INTRODUCTION

SaaS supplied with the aid of cloud carrier providers (cloud provider carriers) emergedas a solution to mitigate the burden of hugenative information storage and scale back the preservation price by means of the manner that of outsourcing information storage. Because the statistics owner physically releases touchy facts to an remote places cloud service provider, there are a few issues referring to confidentiality,integrity and get right of entry to control of the statistics.

The confidentiality characteristic may be atease by way of the owner through encrypting the data before outsourcing to remote servers. For validating data integrity over cloud servers, researchers have projected obvious information ownership method to validate and extremely of statistics preserve on far flung websites. Sort of PDP protocols are bestowed to with efficiency validate the integrity of information, evidence of retrievability turned into brought as a stronger technique than PDP in the sense that the entire information file can be reconstructed from parts of the statistics which might be dependably hold at the servers. Normally, historic get entry to control strategies expects the existence of the factsproprietor and therefore the storage serversin the equal agree with domain. This assumption not holds once the information is sourced to remote places cloud carrier company, that takes the entire price of the outsourced facts control, and is living out ofdoors the agree with area of the statistics proprietor. A likely answer can be bestowedto adjust the owner to put in force access control of the records keep on an distant places untrusted cloud carrier company viathis answer, the statistics is encrypted underneath an specific key, that is shared totally with the certified users. The unauthorized customers, in addition to the cloud service company, are unable to get right of entry to the data seeing that they'redoing now not have the name of the game writing key. This trendy solution has been wide included into existing schemes, that aim at supplying information garage safetyon untrusted far away servers. Every other category of solutions utilizes attribute basedcoding to recognize fine-grained get admission to management.

The special approaches are investigated thatencourage the proprietor to outsource the records, and provide a few form of assure concerning the confidentiality, integrity andget admission to control of the outsourced knowledge. Those strategies will prevent and discover malicious moves from the cloud carrier provider facet. On the alternative hand, the cloud provider company needs to be safeguarded from a unethical owner, who tries to urge outlawed compensations via incorrectly claiminginformation corruption over cloud servers. This concern, if no longer well dealt with, can reason the cloud carrier provider to tourout of business. In this work, we have a tendency to advocate a subject that detects the intruders among person and cloud statistics with relation to the cloud service providers and owner also addresses vital troubles regarding outsourcing the storage offacts, specially dynamic information,newness, mutual trust, and get right of entryto control. The remotely preserve oninformation is not completely accessed by using authorized users, however conjointly updated and scaled with the aid of the owner. As soon as updating, authorized users ought to get the hold of the maximum current model of the statistics (newness belongings) i.e., a method is wanted to discover whether or no longer the receiveddata is stale. Mutual consider among the records proprietor and also the cloudprovider dealer is any other vital trouble thatis addressed inside the projected scheme. A mechanism is brought to look the cheating birthday celebration i.e., misconduct from any aspect is detected and also the responsible party is identified.

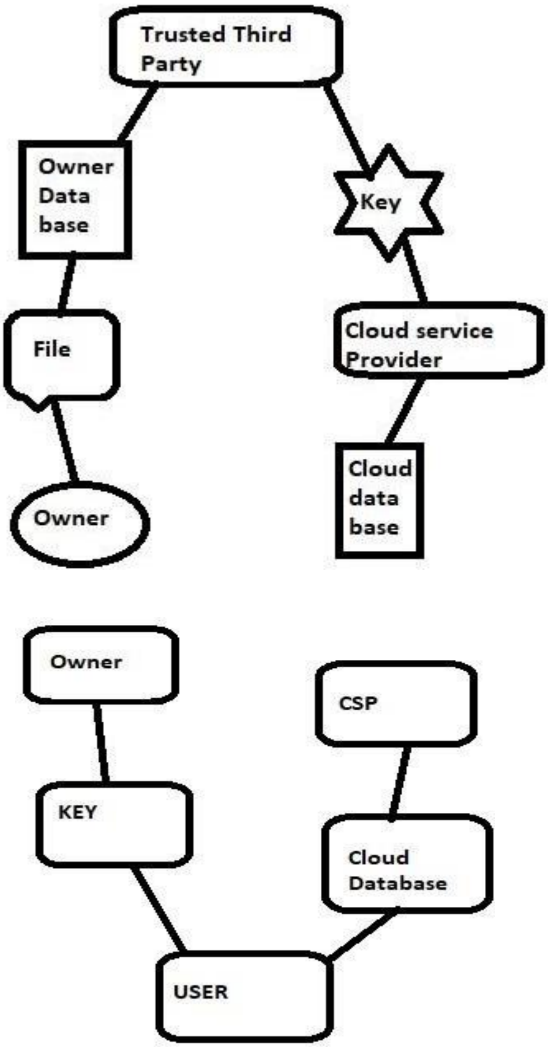

Fig. 1: Secure usage of cloud database

MAIN CONTRIBUTIONS

Layout and implementation of cloud basedtotally storage solutions with subsequentcapabilities:

(i) it permits an information owner to outsource the records to a cloud service provider and carry out full dynamic operations on the block-stage, i.e., it supports operations which includes block modification, insertion, deletion, and append;

(ii) it guarantees the newness property, i.e., the authorized users acquire the maximum latest version of the outsourced statistics;

(iii) it establishes mutual believe between the facts proprietor and the cloud service company because every birthday celebrationis living in a exclusive trust domain;

(iv) it enforces the access manage for the outsourced data; and

(v) it detects the intruders between person and cloud database with appreciate to the cloud carrier providers and owner;

We talk the safety functions of the proposed scheme. Besides, we justify its overall performance thru theoretical analysis and aprototype implementation on Amazon cloudplatform to evaluate garage, conversation, and computation overheads.

OUR SYSTEM AND ASSUMPTIONS

Device additives and members of the family: The cloud computing storage version taken into consideration in this workincludes five important additives as follows:

(i) a records proprietor that may be an organization producing touchy data to be stored inside the cloud and made to be had for controlled external use;

(ii) a cloud provider company who managescloud servers and presents paid storage space on its infrastructure to save the proprietor's files and make them to be had for legal users;

(iii) an authorized users - a set of proprietor's clients who have the right to get right of entry to the far flung facts;

(iv) a depended on 1/3 birthday celebration (TTP), an entity who is trusted with the aid of all different device components, and hasskills to come across/specify cheatingparties; and

(v) an outsider detection - detects the intruders among consumer and cloud database with appreciate to the cloudprovider carriers and proprietor;

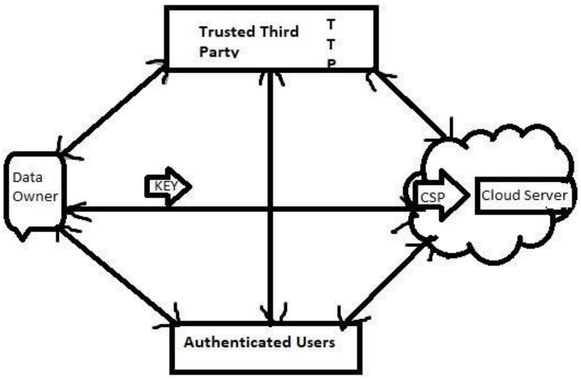

Fig. 2: Cloud data storage system model.

Within the above determine the relationbetween one of a kind system additives arerepresented by double-sided-arrows, in which stable and dashed arrows representbelieve and distrust familymembers,respectively.

As an example, the records owner, the legalusers, and the cloud service company agreewith the TTP. On the other hand, thestatistics proprietor and the authorized usershave mutual distrust family members with the cloud service provider. Thus, the TTP isused to allow indirect mutual accept as truewith betweenthese three components. Thereis an instantaneous accept as true withrelation among the statistics proprietor andthe authorized customers.

Outsourcing, updating, and gainingaccess to: The facts proprietor has a file F which include m blocks. For confidentiality, the proprietor encrypts the statistics before sending to cloud servers. Afterinformation outsourcing, the proprietor can have interaction with thecloud provider company to carry out blocklevel operations at the file. Further, the owner enforces get entryto manipulate with the aid of granting orrevoking get right of entry to rights to the outsourced information. To get admissionto the records, the authorized user sendsa data get admission to request to the cloud service provider, and gets the records file inan encrypted shape that may be decrypted using a mystery key generated by means ofthe legal person (extra details will be defined later). The TTP is an independent entity, and as a result has no incentive to collude with any party. However, any feasible leakage of statistics closer to the TTP need to be averted to preserve the outsourced data personal. The TTP and thecloud carrier provider are always online, atthe same time as the proprietor is intermittently on line. The authorized usersare capable of get right of entry to thestatistics file from the cloud carrier companyeven if the proprietor is offline.

Danger model: The cloud carrier provider is untrusted, and hence the confidentiality and integrity of statistics within the cloud can be at chance. For monetary incentives and retaining a recognition, the cloud service company might also hide information loss, or reclaim garage via discarding statistics that has not been or is hardly ever accessed. To keep thecomputational resources, the cloud providermay also completely forget about the information update requests, or execute onlysome of them. Therefore, the cloud carrier provider may also go back broken or stale records for any get right of entry to requestfrom the authorized users. Moreover, the cloud service company might not honor theaccess rights created via the proprietor, and allow unauthorized access for misuse ofconfidential facts.
Alternatively, an information proprietor and authorized customers may also collude and falsely accuse the cloud service company toget a sure quantity of compensation. They may dishonestly declare that data integrity over cloud servers has been violated, or thecloud provider issuer has lower back a stalefile that does not healthy the maximum current modifications issued by the proprietor.

Security requirements: Confidentiality: outsourced statistics ought to be included from the TTP, the cloud provider, and customers that aren't granted get right of entry to. Integrity: outsourced information isneeded to stay intact on cloud servers. The statistics owner and authorized customers must be enabled to understand information corruption over the cloud provider companyside.

Newness: receiving the maximum recent model of the outsourced statistics, file is an vital requirement of cloud-based totally storage structures. There must be a detection mechanism if the cloud service company ignores any statistics-update requests issuedvia the proprietor,

Get entry to manage: simplest authorized users are allowed to get right of entry to the outsourced information. Revoked users canread unmodified information, however, they need to now not be able to examine up to date/new blocks.

Cloud carrier company's defense: the cloud service company have to be safe guarded against fake accusations that can beclaimed through cheatingproprietor/customers, and this sort of malicious conduct is needed to be revealed.

SYSTEM PRELIMINARIES

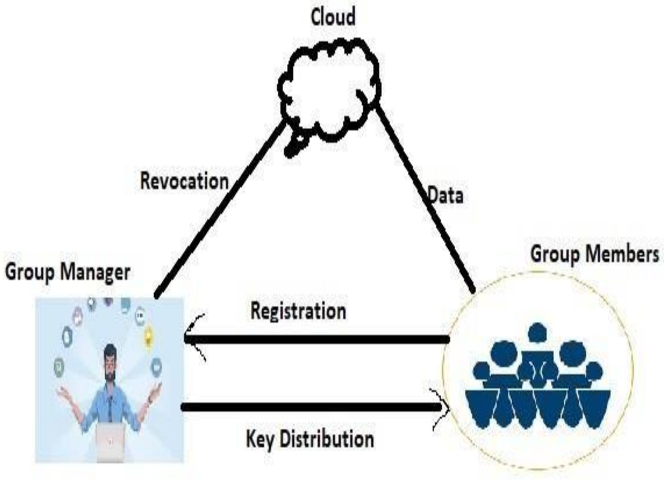

Fig .3: System preliminaries for proposed system

Revocation

The proposed scheme on these paintings letsin the facts proprietor to revoke the right ofsome customers for accessing the outsourced information. In lazy revocation, it's far acceptable for revoked users to examine unmodified information blocks. However, updated or new blocks have to notbe accessed by using such revoked customers. Lazy revocation trades re- encryption and statistics get entry to cost fora diploma of security.

Key Distribution
Key rotation is a way in which a series of keys may be generated from an initial key and a private key. The collection of keys haspredominant homes:

(i) Handiest the proprietor of the grasp secret key is able to generate the next key inthe sequence from the modern-day key, and

(ii) Any authorized consumer knowing a key within the collection is able to generateall preceding versions of that key.

In different phrases, given the ith key okayinside the sequence, it's miles computationally infeasible to compute keys {Ki} for l>I without having the master mystery key, but it is simple to compute keys {Ki} for j<i.

The proposed scheme in this work utilizesthe important thing j rotation technique.
Allow,

N = pq

denote the RSA modulus (p&q are highnumbers),

public key = (N,e)

private key d, the important thing d isknown simplest to the data owner, and

ed = 1 mod (p - 1)(q - 1)

Each time a person’s get right of entry to is revoked, the statistics owner generates a brand new key in the series (rotating ahead).

Allow ctr indicate the index/model quantityof the modern-day key within the keys series. The owner generates the following key as:

Kctr+1= okay(ctr,d) mod N

legal customers can recursively generateolder versions of the modern day key as okay

Kctr-1= k(ctr,e) mod N (rotating backward)

Broadcast Encryption
Broadcast encryption (bENC) lets in a broadcaster to encrypt a message for anarbitrary subset of a set of customers. The users within the subset are handiest allowedto decrypt the mes-sage. but, despite the factthat all users out of doors the subset colludethey can't access the encrypted message.

The proposed scheme makes use of bENC toput in force get right of entry to manipulatein outsourced information. The bENCconsists of 3 algorithms: SETUP, ENCRYPT and DECRYPT.

SETUP: This set of rules takes as input therange of device users n. It defines a bilinearinstitution G of prime order p with a generator g, a cyclic multiplicative organization Gt and a bilinear map ˆe :
G × G→ Gt
The algorithm choices a random a ∈ Z

ENCRYPT: This algorithm takes as input a subset S ⊆{1, 2,...,n}, and a public key PK. It outputs a couple (Hdr, okay), in which Hdr is called the header (broadcast ciphertext), and ok is a message encryptionkey. Hdr= (C0,C1) ∈ G is used to encrypt amessage M (symmetric encryption) to be broadcast to the subset S.

DECRYPT: This set of rules takes as entera subset S ⊆{1, 2,...,n}, a consumer-identityi ∈{1, 2,...,n}, the personal key di for user i, the header Hdr = (C), and the general pub- lic key PK.Ifi ∈ S, the set of rules outputs the key okay, which can be used to decryptthe encrypted model of M.

IMPLEMENTATION ANDEXPERIMENTALEVALUATION

Implementation
We have implemented the proposed schemeon top of Amazon Elastic Compute Cloud (Amazon EC2) and Amazon simple garage provider (Amazon S3) cloud systems. Our implementation of the proposed scheme consists of 5 modules:

1. OModule (proprietor module)
2. CModule (cloud service provider module)
3. UModule (user module)
4. TModule (TTP module) and
5. IModule(Intruder Detection module). **OModule**, which runs on the owner aspect,is a library to be utilized by the proprietor toperform the proprietor position within thesetup and file instruction segment. moreover, this library is utilized by theowner at some stage in the dynamicoperations on the outsourced records.

CModule is a library that runs on AmazonEC2 and is utilized by the cloud serviceissuer to keep, replace, and retrieve recordsfrom Amazon S3.

UModule is a library to be run at the legal users' side, and consist of functionalities that permit users to engage with the TTP and the cloud service provider to retrieve and get entry to the outsourced facts.

TModule is a library used by the TTP to carry out the TTP function in the setup andfile practise phase.

IModule is a module while a person requests the statistics to the cloud database,we offer security from intruders with the aidof blocking off the content there and detecting the intruders between user and cloud da-tabase with recognize to the cloudcarrier providers and owner. Furthermore, the TTP uses this library at some stage in thedynamic operations and to decide the cheating celebration within the device.

Experimental Evaluation

Here we describe the experimental assessment of the computation overhead the proposed scheme brings to a cloud garagedevice that has been handling static recordswith simplest confidentiality requirement.

Owner computation overhead: To experimentally compare the computation overhead on the proprietor facet because ofthe dynamic operations, we've got finishedone hundred special block operations(modify, insert, append, and delete) withquantity of authorized customers startingfrom 20,000 to 100,000. We've got run ourexperiment three times, each time with aspecial revocation percentage. Within thefirst time, 5% of 100 dynamic operations areaccomplished following revocations.

We elevated the revocation percentage to 10% for the second one time and 20% for the 1/3 time. For a large employer (information proprietor) with 100,000 customers, appearing dynamic operations and enforcing get right of entry to manipulate with 5% revocations add approximately 63 milliseconds of overhead.With 10% and 20% revocation possibilities,which can be high probabilities than a meanvalue in realistic packages, the proprietor overhead is zero.12 and 0.25 seconds, respectively. Scalability (i.e., how themachine plays while extra users are brought) is an critical feature of cloud storage structures. The access manipulate of theproposed scheme depends on the square rootof the full range of device customers.

Characteristic	**Experimental Overhead**	
Trusted third party	0.04 ms / 3.59 s Roles	0.55 s
Cloud Service Provider	6.04 s	

TABLE: Results of the Experimental overheads

TTP computation overhead: within the worst case, the TTP executes handiest four hashes in keeping with dynamic request to reflect the change at the outsourced facts. accordingly, the maximum computation overhead on the TTP aspect is set 0.04milliseconds, i.e., the proposed scheme brings mild overhead on the TTP during theeveryday system operations. To pick out the dishonest party within the system in case of disputes, the TTP verifies signatures (s), computes mixed hashes for the information(file and desk), and evaluate the computes hashes with the true values (THTTP and FHTTP). therefore, the computation overhead on the TTP facet is set 3.59 seconds. via our experiments, we use best one server to simulate the TTP and accomplish its paintings. The TTP may additionally choose to break up the work amongst a few devices or use a unmarried tool with a multi-core processor that is becoming popular in recent times, and as a consequence the computation time at the TTP side is significantly reduced in lots of packages.

User computation overhead: The computa- tion overhead at the consumer side due to records get admission to comes from five components divided into corporations. The first institution entails signatures verification and hash operations to confirm the acquired data (file and table). the second one institu- tion includes broadcast decryption, back- ward key rotations, and hash operations to compute the DEK. The first institution prices about 5.87 seconds, which can be without difficulty hidden inside thereceiving time of the statistics (1GB file and2MB desk). to research the time of thesecond one organi-zation, we get admissionto the file after walking 100 distinctive blockoperations (with 5% and 10% revocation percentages). furthermore, we put in force the backward key rotations within the optimized manner. the second one organization prices approximately 0.55 seconds, which can be taken into consideration because the user's computation overhead due to records get right of entry to.

Cloud service provider computation overhead: As a response to the statistics access request, the cloud provider companycom-putes signatures. consequently, the computation overhead on the cloud serviceissuer facet due to facts get admission to is set 6.04 seconds and may be without difficulty hidden within the transmission time of the information (1GB file and 2MBtable).

CONCLUSIONS

In this paper, we have got proposed a cloud primarily based garage scheme which helps outsourcing of dynamic records, wherein the proprietor is able to no longer only archiving and having access to the facts saved via the cloud provider corporation, however more over updating and scaling this facts on the remote servers. The proposed scheme presents safety from intruders with the useful resource of block adding the content material there and detecting the intruders among person and cloud database with apprehend to the cloud provider agencies and owner and allows the criminal customers to ensure that they're receiving the maximum modern version of the outsourced data. Furthermore, in case of dispute regarding records integrity/newness, a ttp is capable of decide the cheating party. The information owner enforces get admission to manipulate for the outsourced data through combining three cryptographicstrategies: broadcast encryption, revocation,and key distribution. We have studied the safety capabilities of the proposed scheme. We have got investigated the overheads delivered with the aid of our scheme while integrated proper into a cloud garage versionfor static statistics with first rate confidentiality requirement. The garage overhead is approximately 0.4% of the outsourced information duration, the communication overhead due to block degree dynamic changes on the informationis approximately 1% of the block duration,and the conversation overhead due to retrieving the statistics is approximately 0.2% of the outsourced data size. For amassive enterprise with 10 users, acting dynamic operations and imposing get right of entry to govern upload about 63 milliseconds of overhead. Consequently, crucial features of outsourcing records garage may be supported with outimmoderate overheads in storage,communication, and computation.

REFERENCES

[1]. G. Ateniese, R. Burns, R. Curtmola, J. Her-ring, L. Kissner, Z. Peterson, and D. Song, "Provable data possession at untrustedstores," in Proceedings of the 14th ACM Conference on Computer and Communica-tions Security, ser. CCS '07, 2007, pp. 598–609.

[2]. F. Seb´e, J. Domingo-Ferrer, A. Martinez-Balleste, Y. Deswarte, and J.-J. Quisquater, "Efficient remote data possession checking in critical informationinfrastructures," IEEE Trans. on Knowl.And Data Eng., vol. 20, no. 8, 2008.

[3]. G. Ateniese, R. D. Pietro, L. V. Mancini,and G. Tsudik, "Scalable and efficient prov- able data possession," in Proceedings of the4th International Conference on Security and Privacy in Communication Netowrks, 2008, pp. 1–10.

[4]. C. Erway, A. K¨upc¸ ¨ u, C. Papamanthou, and R. Tamassia, "Dynamic provable data possession," in Proceedings ofthe 16th ACM Conference on Computer andCom-munications Security, 2009, pp. 213–222.

[5]. Q. Wang, C. Wang, J. Li, K. Ren, and

[6]. W. Lou, "Enabling public verifiability and data dynamics for storage security in cloud com-puting," in Proceedings of the 14thEuro-pean Conference on Research inComputer Security, 2009, pp. 355–370.

[7]. A. F. Barsoum and M. A. Hasan,"Provable possession and replication of dataover cloud servers," Centre For AppliedCryptographic Research, Re- port.2010/32,2010,http://www.cacr.math. uwaterloo.ca/techreports/2010/cacr2010- 32.pdf.

[8]. K. D. Bowers, A. Juels, and A. Oprea, "HAIL: a high-availability and integrity layer for cloud storage," in CCS '09: Pro- ceedings of the 16th ACM conference on Computer and communications security. New York, NY, USA: ACM, 2009, pp. 187–198.

[9]. A. Juels and B. S. Kaliski, "PORs: Proofs of Retrievability for large files," in CCS'07: Proceedings of the 14th ACM conference on Computer and communications security. ACM, 2007, pp. 584–597.

[10]. H. Shacham and B. Waters, "Compact proofs of retrievability," in ASIACRYPT '08, 2008, pp. 90–107.

[11]. M. Kallahalla, E. Riedel, R.Swaminathan, Q. Wang, and K. Fu, "Plutus:Scalable se-cure file sharing on untrustedstorage," in Proceedings of the FAST 03:File and Sto-rage Technologies, 2003. [11]E.-J. Goh, H. Shacham, N. Modadugu,and D. Boneh, "Sirius: Securing remote un-trusted storage," in Proceedings of the Net-work and Distributed System Security Sym-posium, NDSS, 2003.

[12]. G. Ateniese, K. Fu, M. Green, and S. Ho-henberger, "Improved proxy re- encryption schemes with applications to secure distri-buted storage," in NDSS, 2005.

[13]. S. D. C. di Vimercati, S. Foresti, S. Jajodia, S. Paraboschi, and P. Samarati,"Over-encryption: Management of access control evolution on outsourced data," in Proceed-ings of the 33rd International Conference on Very Large Data Bases. ACM, 2007, pp. 123–134.

[14]. V. Goyal, O. Pandey, A. Sahai, and B.Wa-ters, "Attribute-based encryption for fine-grained access control of

encrypted data," in CCS '06, 2006, pp. 89–98.

[15]. S. Yu, C. Wang, K. Ren, and W. Lou,"Achieving secure, scalable, and fine-grained data access control in cloud compu-ting," in INFOCOM'10, 2010, pp. 534–542.

[16]. R. A. Popa, J. R. Lorch, D. Molnar, H.

[17]. J. Wang, and L. Zhuang, "Enabling security in cloud storage SLAs with cloudproof," inProceedings of the 2011 USENIX confe- rence, 2011.

[18]. K. E. Fu, "Group sharing and random access in cryptographic storage filesystems," Mas-ter's thesis, MIT, Tech. Rep.,1999.

[19]. W. Wang, Z. Li, R. Owens, and B. Bharga-va, "Secure and efficient access to out-sourced data," in Proceedings of the2009 ACM workshop on Cloud computingsecuri-ty, 2009, pp. 55–66.

[20]. M. Backes, C. Cachin, and A. Oprea, "Se-cure key-updating for lazy revocation,"in 11th European Symposium on Researchin Computer Security, 2006, pp. 327–346.

[21]. D. Boneh, C. Gentry, and B. Waters, "Col-lusion resistant broadcast encryption with short ciphertexts and private keys," inAd-vances in Cryptology - CRYPTO, 2005,pp. 258–275.

[22]. D. Boneh, B. Lynn, and H. Shacham, "Short signatures from the weil pairing," in ASIA-CRYPT '01: Proceedings of the 7th Interna-tional Conference on the Theory and Appli-cation of Cryptology and Information Secu-rity, London, UK, 2001, pp. 514–532.

[23]. P. S. L. M. Barreto and M. Naehrig, "IEEE P1363.3 submission: Pairing-friendlyelliptic curves of prime order with embedding degree 12," New Jersey: IEEE Standards Association, 2006.

[24]. P. S. L. M. Barreto and M. Naehrig, "Pair-ing-friendly elliptic curves of prime order," in Proceedings of SAC 2005,volume 3897 of LNCS. Springer-Verlag, 2005, pp. 319–331.

[25]. D. L. G. Filho and P. S. L. M. Barreto, "Demonstrating data possession and un- cheatable data transfer," Cryptology ePrintArchive, Report 2006/150, 2006.

[26]. D. Naor, M. Naor, and J. B. Lotspiech,"Re-vocation and tracing schemes forstateless receivers," in Proceedings of the 21st An-nual International Cryptology Conference on Advances in Cryptology, ser. CRYPTO '01. Springer-Verlag, 2001, pp. 41–62.

[27]. M. Blaze, G. Bleumer, and M. Strauss, "Di-vertible protocols and atomic proxy crypto-graphy," in EUROCRYPT, 1998, pp.127–144.

[28]. M. J. Atallah, K. B. Frikken, and M. Blan-ton, "Dynamic and efficient key manage-ment for access hierarchies," in Proceedings of the 12th ACM Conference on Computer and Communications Security,ser. CCS '05. ACM, 2005, pp. 190–202.

[29]. J. Feng, Y. Chen, W.-S. Ku, and P. Liu,"Analysis of integrity vulnerabilities and a non-repudiation protocol for cloud data sto-rage platforms," in Proceedings of the 201039th International Conference on Parallel Processing, 2010, pp. 251–258.

[30]. J. Feng, Y. Chen, and D. H. Summerville, "A fair multi-party non- repudiation scheme for storage clouds," in 2011 International Conference on Collaboration Technologies and Systems, 2011, pp. 457–465.

AUTHOR

[1] Ms. GIRIJA RANI SUTHOJU pursuing Ph.D in the Department of Computer Science and Engineering at JNTU Hyderabad. She received Masters degree (M.Tech) in the Department of CSE at Aurora's Technological and Research Institute belongs to JNTU, Hyderabad in 2014 and Bachelors degree (B.Tech) in the Department of Computer Science and Engineering from the same University in 2012. She worked as an Assistant Professor for 5years in Aurora's Technological and Research Institute affiliated to Jawaharlal Nehru Technological University, Hyderabad. She worked in KLEF (K L deemed to be University) Hyderabad from June 2019 to June 2022 and at present she is working in NGIT Hyderabad. She also received Teaching Excellence award for best teaching thrice from 2016 to 2018 from Aurora consortium and also in 2021 by KL University for her best performance in academics. She also received Global Eminent Teacher Award recently. Her area of research is Cryptography and network security.

[2] M. Suresh babu completed PhD (Computer Science) from Sri Krishnadevaraya University, Anantapur, M.Phil (Computer Science) from Bharthiar University in 2007, Master of Computer Applications from Osmania University,Hyderabad in 1997, PGDBA from Sri Krishnadevaraya University, Anantapur in 2002, DCOM from IGNOU, New Delhi and Bachelor of Science from Sri Krishnadevaraya University, Anantapur in 1993. His area of interests are Datamining, Cloud computing and Networks. He is a creative professional with around 18+ years of experience in Teaching & Student Management. Presently, he is working as Principal, in Y V Sivareddy college of Engineering, Ananthapur, AP. He worked as a Professor in Department of Computer Science & Engineering, S K D Engineering College, Ananthapur, AP and also as a Principal, Aurora's Technological Institute, Uppal, Hyderabad from Jan- 2015 Aug-2015, also as Principal, Intel Institute of Science, Anantapur,from October 1998 - December 2012. He worked as Professor & Head, Department of Computer Applications, Madanapalle Institute of Technology & Science, from December 2012 to December 2014.