International Journal of Science Engineering and Advance Technology

Collective Conviction Based Confidentiality Sustain Endorsement Procedure in Cloud Computing

Saisaran Anumalasetty[1], I.Sapthami[2]
[1]PG Scholar, [2]Assistant Professor in Department of Computer Science and Engineering,
Visvodaya Engineering College, Kavali, SPSR Nellore D.t., India.

Abstract —
Cloud computing is consistently growing as a typical for sharing the knowledge over the remote warehousing in a web cloud server. Cloud administrations offers awing enhancements for the purchasers to understand the on-interest cloud applications with no commitments known with data. Amid the knowledge ill , numerous purchasers is also in a pleasant relationship, and henceforward data appropriation gets to be essential. In this paper, we have concentrated on protection protecting confirmation convention (SAPA) to address the said security issue for cloud putting away furthermore attempting to deliver to the effectiveness expanded by this SAPA convention. It likewise assigns that the planned convention acknowledging security safeguarding data access power sharing is most encouraging for multi-client synergistic cloud applications. Amid cloud data aiming to, the consumer independent connects with the cloud server while not outside impedances, and is allotted with the total and autonomous power on their lonesome data fields. it's necessary to confirm that the purchasers' outsourced data cannot be unapproved gotten to by completely different clients, and is of discriminating significance to ensure the non-public knowledge amid the clients' data access challenges. during this paper, we have a tendency to address the antecedently declared security issue to propose a typical power primarily based protection protecting confirmation convention (SAPA) for the cloud data warehousing, that acknowledges verification and approval while not commerce off a client's non-public knowledge. Propose a confirmation convention to upgrade a client's entrance solicitation connected protection, and also the common access power is accomplished by mysterious access solicitation coordinative mechanism.

Index Terms - Cloud computing, authentication, shared authority, universal composability, accountability

1. INTRODUCTION

Cloud computing empowers exceptionally adaptable administrations to be effortlessly expended over the Internet on an as-required premise. A critical advantage of the cloud administrations is that clients' information are typically prepared remotely in obscure machines that clients don't have or utilization. While appreciating the accommodation brought by this innovation, clients' get terrified of missing their information. It can turn into a noteworthy obstruction to the wide selection of cloud administrations. A novel profoundly dispersed data responsibility system to stay informed concerning the real utilization of the clients' information in the cloud. We present an article focused methodology that empowers encasing our logging instrument together with clients' information and approaches. We impact the JAR coding abilities to both make a dynamic and moving item, and to verify that any entrance to clients' information will trigger confirmation and robotized logging nearby to the JARs. To make the client's control more grounded, we give disseminated instruments to reviewing. We give far reaching trial studies that exhibit the effectiveness and viability of the proposed methodologies. It is commonly a kind of figuring that depends on sharing processing assets as opposed to having nearby servers or individual gadgets to handle applications.

In cloud computing, the word cloud (additionally stated as "the cloud") is utilized as an allegory for "the Internet," so the expression distributed computing signifies "a sort of Internet-based processing," where distinctive administrations —, for example, servers, stockpiling and applications —are conveyed to an association's PCs and gadgets through the Internet. At the point when contrasted with matrix figuring, a processing sort where preparing cycles that are unused for all PCs in a system are saddles to take care of issues excessively serious for any stand-alone machine. Cloud computing is a kind of figuring where unused handling cycles of all PCs in a system are saddles to tackle issues excessively escalated for any stand-alone machine.

The focal points are

- Scalability and Storage
- Cost Efficient
- Backup and calamity recuperation
- Enable IT Innovation
- Unlimited stockpiling
- Easy access of data

Development and Test - Develop and test applications in on-interest environment utilizing reliably designed assets, bringing down expenses and shortening discharge cycles.

• Disaster Recovery – Public and private cloud empower financially savvy answers for keep up very accessible applications with flexible multi-datacentre and multi-supplier architectures, minimizing down time and information misfortune. Foundation -as-a-Service furnishes the client with virtual server occurrences, stockpiling, and additionally application program interfaces permits the client to begin, stop, get to and design the virtual servers and capacity. Designers start applications on the supplier's stage over the Internet. In the product as-an administration cloud demonstrates, the

venders supplies the equipment base, the product item and speaks with the client.

II. CLOUD SERVICES

Data privacy a lot of study has been done on the potential of cloud and the services that cloud computing can and could deal. These services can be characterized into four main sections: Storage as a Service (StaaS), Platform as a Service (PaaS), Infrastructure as a Service (IaaS) and Software as a Service (SaaS). Following section highlights these services and their usage in depth. A. Storage as a Service Cloud offers a storage space that is huge, seemingly boundless, and rising every day. Storage as a Service (StaaS) allows cloud applications to gauge beyond their inadequate servers. Cloud storage systems needs to focus on requirements for upholding users' data and information, considering high performance, availability, replication, data reliability and reliability.

The accountability to individual is maintained and upholds customer's own computer storage as cloud vendors deal them the choice of loading their information in the cloud which is reachable whenever they need [11].

Security Issues:

Companies are promptly moving onto cloud because they can now use the greatest capitals available on the market in the blink of an eye and also decrease their operations' cost radically. But as more and more information is moved to the cloud the security concerns have continuing to grow. Data breaking is the biggest security issue. A capable hacker can easily get into a client side application and get into the client's intimate data [2].

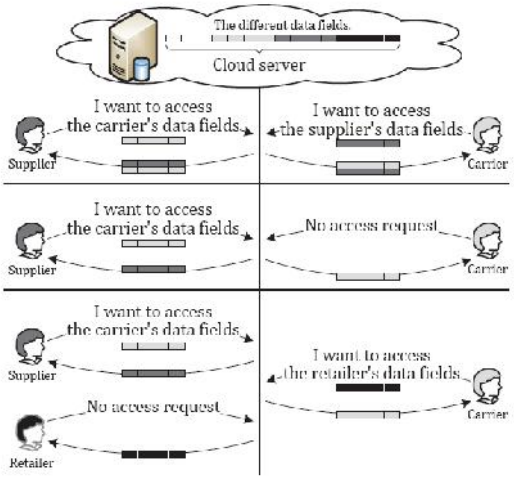

Fig1: Possible cases during data accessing and sharing in cloud applications.

Incompetent and faulty APIs and interfaces become the target. IT companies which provide cloud services allow third party companies to alter the APIs and familiarize their own functionality which in turn allows these companies to comprehend the internal workings of the cloud[2].Denial of Service (DoS) is also a major menace wherein the user is approved partial or not at all access to their data. Companies now use cloud very frequently say all days and DoS can root huge increase in cost both for the user and service provider. A malicious hacker can wipe out the data or any natural/man-made disaster can destroy your data. In such cases having an offline copy is a big advantage. Carelessness of the service provider can also lead to data loss [3].Compatibility between different cloud services is also an issue. If a user decides to move from one cloud to another the compatibility ensures that there is no loss of data. Cloud can also be used for wrong purposes i.e. cloud abuse. Due to the availability of latest technologies on the cloud it can be used for high end calculations which cannot be done on a standard computer [2], [3].

Insufficient understanding of cloud technologies can lead to unknown levels of risk. Companies move to cloud because it provides substantial reduction in cost but if transfer is done without proper background learning, the problems that arise can be even greater. Internal intruders are able to use the data for harmful purposes. Safe storage of encryption keys is also a problem. Even if you are using encryption for enhanced security, keeping a key a safe asset becomes an issue.

III. RELATED WORK

In the cloud environments, a reasonable security protocol should achieve the following requirements.

A. Authentication A legal user can access its own data fields, only the authorized partial or entire data fields can be identified by the legal user, and any forged or tampered data fields cannot deceive the legal user.

B. Data anonymity any irrelevant entity cannot recognize the exchanged data and communication state even it intercepts the exchanged messages via an open channel.

C. User privacy any irrelevant entity cannot know or guess a user's access desire, which represents a user's interest in another user's authorized data fields. If and only if the both users have mutual interests in each other's authorized data fields, the cloud server will inform the two users to realize the access permission sharing.

D. Forward security any adversary cannot correlate two communication sessions to derive the prior interrogations according to the currently captured messages. Researches have been worked to strengthen security protection and privacy preservation in cloud applications including security architectures, data possession protocols data public auditing protocols , secure data storage and data sharing protocols, access control mechanisms and key management which ignores the case that different users may want to access and share each other's authorized data fields to achieve productive benefits.

When a user challenges the cloud server to request other users for data sharing, the access request itself may reveal the user's privacy no matter whether or not it can obtain the data access permissions. In this work, we aim to address a user's sensitive access desire related privacy during data sharing in the cloud environments, and it is significant to design a humanistic security scheme to simultaneously achieve data access control, access authority sharing, and privacy preservation.

IV.PRIVACY PRESERVING AUTHENTICATED ACCESS CONTROL SCHEME

In this section we propose our privacy preserving authenticated access control scheme. According to our

scheme an user can create a file and store it securely in the cloud. This scheme consists of use of the two protocols ABE and ABS, as discussed in Section III-D and III-E respectively. We will first discuss our scheme in details and then provide a concrete example to demonstrate how it works. We refer to the Fig. 2. There are three users, a creator, a reader and writer. Creator Alice receives a token γ from the trustee, who is assumed to be honest. A trustee can be someone like the federal government who manages social insurance numbers etc. On presenting her id (like health/social insurance number), the trustee gives her a token γ. There are multiple KDCs (Key distribution centre), which can be scattered. For example, these can be servers in different parts of the world. A creator on presenting the token to one or more KDCs receives keys for encryption/decryption and signing. In the Fig. 1, SKs are secret keys given for decryption, Kx are keys for signing. The message MSG is encrypted under the access policy X. The access policy decides who can access the data stored in the cloud. The creator decides on a claim policy Y, to prove her authenticity and signs the message under this claim. The cipher text C with signature is c, and is sent to the cloud. The cloud verifies the signature and stores the ciphertext C. When a reader wants to read, the cloud sends C. If the user has attributes matching with access policy, it can decrypt and get back original message. Write proceeds in the same way as file creation. By designating the verification process to the cloud, it relieves the individual users from time consuming verifications. When a reader wants to read some data stored in the cloud, it tries to decrypt it using the secret keys it receives from the KDCs. If it has enough attributes matching with the access policy, then it decrypts the information stored in the cloud.

A. Data storage in clouds an user Uu first registers itself with one or more trustees. For simplicity we assume there is one trustee. The trustee gives it a token γ = (u, Kbase, K0, ρ), where ρ is the signature on u||Kbase signed with the trustees private key T Sig (By Equation 6). The KDCs are given keys PK[i], SK[i] for encryption/decryption and ASK[i], APK[i] for signing/verifying. The user on presenting this token obtains attributes and secret keys from one or more KDCs. A key for an attribute x belonging to KDC Ai is calculated as Kx = K1/ (a+bx) base, where (a, b) ∈ ASK[i]. The user also receives secret keys skx,u for encrypting messages. The user then creates an access policy X which is a monotone Boolean function. The message is then encrypted under the access policy as

$$C = ABE.Encrypt(MSG, X)$$

The user also constructs a claim policy Y to enable the cloud to authenticate the user. The creator does not send the message MSG as is, but uses the time stamp τ and creates H(C)||τ. This is done to prevent replay attacks. If the time stamp is not sent, then the user can write previous stale message back to the cloud with a valid signature, even when its claim policy and attributes have been revoked. In their scheme, a writer can send its message and correct signature even when it no longer has access rights. In our scheme a writer whose rights have been revoked cannot create a new signature with new time stamp and thus cannot write back stale information. It then signs the message and calculates the message signature as

σ = ABS.Sign(Public key of trustee, Public key of KDCs, token, signing key, message, access claim)

The following information is then sent in the cloud.

c = (C, τ, σ, Y). (13) The cloud on receiving the information verifies the access claim using the algorithm ABS.verify. The creator checks the value of V = ABS.verify(T PK, σ, c, Y). If V = 0, then authentication has failed and the message is discarded. Else, the message (C, τ) is stored in the cloud.

B. Reading from the cloud When an user requests data from the cloud, the cloud sends the ciphertext C using SSH protocol. Decryption proceeds using algorithm ABE.Decrypt(C, {ski,u}) and the message MSG is calculated as given in Section III-D4.

C. Writing to the cloud to write to an already existing file, the user must send its message with the claim policy as done during file creation. The cloud verifies the claim policy, and only if the user is authentic, is allowed to write on the file.

V. PROPOSED WORK

Data access control of data stored in cloud so that only authorized users with valid attributes can access them. The architecture is decentralized, meaning that there can be several KDCs for key management. The access control and authentication are both collusion resistant, meaning that no two users can collude and access data or authenticate themselves, if they are individually not authorized. Revoked users cannot access data after they have been revoked. The proposed scheme is resilient to replay attacks. A writer whose attributes and keys have been revoked cannot write back stale information. The protocol supports multiple read and writes on the data stored in the cloud. The costs are comparable to the existing centralized approaches, and the expensive operations are mostly done by the cloud. Authentication of users who store and modify their data on the cloud. The identity of the user is protected from the cloud during authentication.

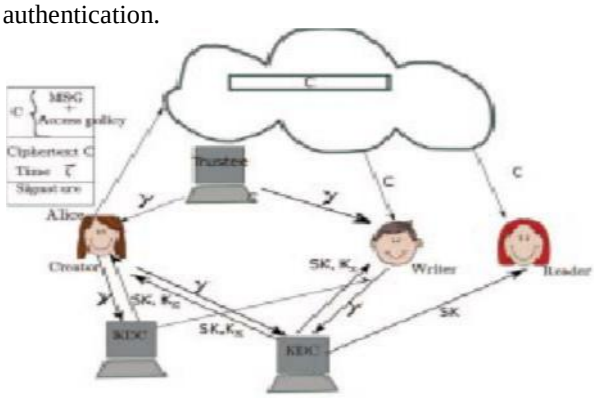

Fig. 2 Cloud authentication access control scheme

The architecture is decentralized, meaning that there can be several KDC's for key management. There are three users, a creator, a reader and writer. Creator Alice receives a token γ from the trustee, who is assumed to be

honest. A trustee can be someone like the federal government who manages social insurance numbers etc. On presenting her id the trustee gives her a token γ.. For example, these can be servers in different parts of the world. A creator on presenting the token to one or more KDCs receives keys for encryption/decryption and signing. In the Fig. 1, SKs are secret keys given for decryption, Kx are keys for signing. The message MSG is encrypted under the access policy X. The access policy decides who can access the data stored in the cloud. The creator decides on a claim policy Y, to prove her authenticity and signs the message.

A. Creation of KDC (Key Distribution Centre)

To create a different number of KDC's given a input as KDC name, KDC id and KDC password it will save in a database and to register a user details given an input as user name and user-id.

B. User Enrolment

After KDC given a user id to a user, the user will enrolled the personal details to KDC's given an input as user-name user-id, password etc. The KDC will be verifying the user details and it will insert it in a Database.

C. Trustee and User Accessibility

User can login with their credentials and request the token from trustee for the file upload using the user id. After the user id received by the trustee, trustee will be create token using user id, key and user signature (SHA). Then the trustee will issue a token to the particular user and then trustee can view the logs.

D. Creation of Access Policy

After trustee token issuance for the users, the users produce the token to the KDC then the token verify by the KDC if it is valid then KDC will provide the public and Private key to the user. After users received the keys the files are encrypt with the public keys and set their Access policies (privileges).

E. File Accessing Using their access policies the users can download their files by the help of KDC's to issue the private keys for the particular users.

F. Hash algorithm.

SHA-1 is one of several cryptographic hash functions, most often used to verify that a file has been unaltered. SHA is short for Secure Hash Algorithm. File verification using SHA-1 is accomplished by comparing the checksums created after running the algorithm on the two files you want to compare. SHA-1 is the second iteration of this cryptographic hash function, replacing the previous SHA-0.SHA-2 cryptographic hash function is also available and SHA-3 is being developed. One iteration within the SHA-1 compression function. A, B, C, D and E are 32bit words of the state. F is a nonlinear function that varies. N denotes a left bit rotation by n places. N varies for each operation. Wt is the expanded message word of round t. Kt is the round constant of round t. denotes addition modulo 232.

G. Paillier Algorithm

The Paillier cryptosystem, named after and invented by Pascal Paillier is a probabilistic asymmetric algorithm for public key cryptography.

1. Key generation Choose two large prime number p and q randomly and independently of each other such that gcd (pq,(p-1)(q- 1))=1. This property is assured if both primes are of equivalent length, i.e p,q {0,1 }s-1 for security parameter S . Compute n=pq and λ=lcm (p-1, q-1.Select random integer g where gZ*n2. Ensure n divides the order of g by checking the existence of the following modular multiplicative inverse. μ= (L (gλ mod n2))-1mod n, where function L is defined as The public (encryption) key is (n,g).. The private (decryption) key is (λ,μ).

2. Encryption Let m be a message to be encrypted where m Zn. Select random r where r Z*n. Compute cipher text as: c= gm .rn mod n2

3. Decryption Cipher text: cZ*n2.Compute message: m =L (cλ mod n2). M modn

VI.CONCLUSION

In this paper, we propose a shared authority based privacy-preserving authentication protocol (SAPA) to address above privacy issue for cloud storage. In the SAPA, 1) shared access authority is achieved by anonymous access request matching mechanism with security and privacy considerations (e.g., authentication, data anonymity, user privacy, and forward security); 2) attribute based access control is adopted to realize that the user can only access its own data fields; 3) proxy re-encryption is applied by the cloud server to provide data sharing among the multiple users. Meanwhile, universal composability (UC) model is established to prove that the SAPA theoretically has the design correctness. It indicates that the proposed protocol realizing computing to achieve privacy-preserving access authority sharing. Authentication is established privacy-preserving data access authority sharing is attractive for multi-user collaborative cloud applications.In this work, we have identified a new privacy challenge during data accessing in the cloud to guarantee data confidentiality and data integrity. Data anonymity is achieved since the wrapped values are exchanged during transmission. User privacy is enhanced by anonymous access requests to privately inform the cloud server about the users' access desires. Forward security is realized by the session identifiers to prevent the session correlation. It indicates that the proposed scheme is possibly applied for enhanced privacy preservation in cloud applications.

VII. REFERENCES

[1] P. Mell and T. Grance, "Draft NIST Working Definition of Cloud Computing," National Institute of Standards and Technology, USA, 2009.

[2] K. Hwang and D. Li, "Trusted Cloud Computing with Secure Resources and Data Coloring," IEEE Internet Computing, vol. 14, no. 5, pp. 14-22, 2010.

[3] C. Wang, K. Ren, W. Lou, J, Lou,"Toward Publicly Auditable Secure Cloud Data Storage Services," IEEE Network, vol. 24, no. 4, pp. 19-24, 2010.

[4] S. Grzonkowski and P. M. Corcoran, "Sharing Cloud Services: User Authentication for Social Enhancement of Home Networking," IEEE Transactions on Consumer Electronics, vol. 57, no. 3, pp. 1424-1432, 2011.

[5] A. Mishra, R. Jain, and A. Durresi, "Cloud Computing: Networking and Communication

Challenges," IEEE Communications Magazine, vol. 50, no. 9, pp, 24-25, 2012.
[6] J. Chen, Y. Wang, and X. Wang, "On-Demand Security Architecture for Cloud Computing," Computer, vol. 45, no. 7, pp. 73-78, 2012.
[7] Y. Zhu, H. Hu, G. Ahn, and M. Yu, "Cooperative Provable Data Possession for Integrity Verification in Multi-cloud Storage".
[8] H. Wang, "Proxy Provable Data Possession in Public Clouds," IEEE Transactions on Services Computing, [online] ieeexplore. ieee.org/stamp/stamp.jsp?tp=&arnumber=6357181, 2012.
[9] X. Liu, Y. Zhang, B. Wang, and J. Yan, "Mona: Secure Multi- Owner Data Sharing for Dynamic Groups in the Cloud," IEEE Transactions on Parallel and Distributed Systems, [online] ieeexplore. ieee.org/stamp/stamp.jsp?tp=&arnumber=6374615, 2012.
[10] C. Wang, Q. Wang, K. Ren, N. Cao, and W. Lou, "Toward Secure and Dependable Storage Services in Cloud Computing," IEEE Transactions on Services Computing, vol. 5, no. 2, pp. 220-232, 2012.
[11] S. Sundareswaran, A. C. Squicciarini, and D. Lin, "Ensuring Distributed Accountability for Data Sharing in the Cloud," IEEE Transactions on Dependable and Secure Computing, vol. 9, no. 4, pp. 556-568, 2012.
[12] L. A. Dunning and R. Kresman, "Privacy Preserving Data Sharing With Anonymous ID Assignment," IEEE Transactions on Information Forensics and Security, vol. 8, no. 2, pp. 402-413, 2013.

AUTHORS

Mr. Saisaran Anumalasetty received B.Tech degree in Computer Science and Engineering from Ramireddy Subbarami Reddy Engineering College affiliated to the JNT University Anantapur in 2013 and pursing M.Tech in Computer Science and Engineering from Visvodaya Engineering College affiliated to JNT University Anantapur in 2013.

Mrs.I.Sapthami working as an Assistant Professor in VEC affiliated to JNT University Anatapur. She received B.Tech degree in Computer Science and Engineering from PBR VITS affiliated to JNT University Anantapur and M.Tech in Computer Science and Engineering from PBR VITS affiliated to JNT University Anantapur.