International Journal of Combined Research & Development (IJCRD)
eISSN:2321-225X; pISSN:2321-2241 Volume: 14; Issue: 8; August- 2025

NC101 IDENTITY BASED DATA OUTSOURING WITH COMPERSIVE AUDITING IN CLOUDS

Vijay Sagar
PG, Student
Dept. of MCA
The Oxford College of Engineering,
Bommanahalli, Bengaluru- 560068
vijaysagar903@gmail.com

Sowmya J
Assistant Professor
Dept. of MCA
The Oxford College of Engineering,
Bommanahalli, Bengaluru- 560068
sowmyaj@theoxford.edu

ABSTRACT

The use of clouds can save us a great amount of money yet makes us breathless as to who can see and maybe edit our information being stored on the servers we do not have much confidence in it. This is been overcome by the Identity-Based Data Outsourcing (IBDO) system which uses a model with known identities e.g. email addresses or professions instead of certificates to regulate access to data.

The system uses a technique in which files which are uploaded to the owner by trusted assistants can be verified as being correct without downloading them. It uses a mixture of crypto mechanisms: AES to safely encry the data in bulk CP-ABE to decide which bits you can input, and RSA to safely store your keys whilst SHA-256 will ensure your information stays the way it should be. To address integrity, controllable outsourcing, and origin auditing concerns on outsourced files. IDBO ensures secure, scalable, and efficient cloud storage through encryption, proxy support, and transparent verification.

Keywords: *Identity-Based Data Outsourcing (IBDO), cloud storage, proxy authorization, data integrity, auditing, identity-based cryptography, secure data sharing, origin verification, access control, efficiency*

INTRODUCTION

Identity-Based Data Outsourcing (IDBO) enhances cloud security by integrating encryption, proxy support, and verification for scalable, efficient, reliable data management. However, sharing sensitive information with third-party cloud servers comes under the risks of privacy invasion, unauthorized access and integrity. Conventional cryptography processes are prone to operating in a certificate manner and complex key administration; hence it is difficult to manage and less convenient the multi-user systems. This paper proposes Identity-Based Data Outsourcing (IBDO) system to mitigate these challenges by streamlining security so that user authentication occurs using their unique attributes, such as email ID or roless, as opposed to certificates. It includes the support of proxy based delegation, in which files are uploaded by trusted proxies acting on behalf of owners,

and an open audit architecture to verify integrity without downloading the entire files Services like Amazon Web Services, Microsoft Azure, and Google Cloud Platform have big setups around the world. Infrastructure as a Service (renting servers), Platform as a Service (tools for building apps), and Software as a Service (apps on the web).

LITERATURE SURVEY

The value of cloud computing with regards to data storage has transformed the field of data storage through the provision of flexibility, expandability and at a moderate price. However, the question of no confidentiality, right of access and integrity arises since sensitive information may be relayed through the third-party servers. To address such issues, a number of models and cryptographical schemes are proposed.

The initial attested ways were that of symmetric encryption such as AES to encrypt outsourced files. The inconvenience of having a complex distribution of key and being very efficient, such solutions were inappropriate to be used in a multi-user scenario. Asymmetric encryption like RSA ensured there was no key management problem, but had huge computation overheads and therefore was not viable to encrypt larger datasets.

An improvement was the fine-grained access control through the introduction of Attribute-Based Encryption (ABE). And unlike Key-Policy ABE (KP-ABE), with Ciphertext-Policy ABE (CP-ABE) the user keys carried the policies ciphertexts and described access structures. The advantage was that CP-ABE was more feasible in that data owners were allowed to define flexible data privacy. policies. But ABE schemes had some limitations including high overheads and impossibility to revoke user attributes.

In regards to the data integrity, features that are specifically implemented are Provable Data Possession (PDP) and Proofs of Retrievability (PoR) which are implemented to address this issue and enable the claims of file integrity to be verified without downloading it. These also were the sources of integrity but in most instances they will required the data owner to be a verifier hence will be highly burdensome.

The proxy based outsources service which are offered with the opportunity to download, operate and position files in a controlled manner and the trusted proxies kept in order to take up the data burden of their owners. Proxy Re-Encryption (PRE) helps in securing data by allowing delegation, but it doesn't provide much flexibility when setting access rules.

EXISTING WORK

Thus, the cloud server needs to compute at most $\xi(2|I|+1)$ bilinear pairings when ξ users require the outsourced decryption services. While the cloud server merely needs to compute $2|I|$ bilinear pairings for the total overhead of all outsourced decryption for our method via simply comparing their transformation keys. These methods are effective but they are inefficient in the use of energies and not scaleable as well as they do not have good measures against the middlemen. This demands the need of having an integrated system .

PROPOSED SYSTEM

The proposed system aims the platform Due to the speed at which cloud technology has grown the transfer of data to the other party servers has become a common procedure among the individuals and organizations that are keen on expanding and saving on financial costs. The easy way out however has in itself had tremendous concerns of the data confidentiality, secure access and verification of data veracity. Conventional mechanisms of data locking offer an certain degree of security which is marred by the handicapping key management, poor access control and the inability to large user configuration. Attribute-Based Encryption (ABE) overcomes a part of this but its slow and not particularly effective at handling change to attributes Along with those, there have been other data verification approaches proposed such as Provable Data Possession (PDP) and Proofs of Retrievability (POR), which too verify the correctness of the data in question but may require the data owner to be involved as it involves additional overhead and reduces scalability. Shifting of the responsibility on other people via the existing arrangements, has permeable controls. A novel light system with the capability of outsourcing data which is resistant, runs actively and is reliable in cloud systems is thus required. All these make up the research topic and inform us of why the new system is required.

In the real world individuals will require things that are not only secure but are also convenient to operate as well as those things that are able to evolve in order to meet their various requirements. The excessive use of the certificates in this mechanisms which are utilized in the past results other problematic stages which acts as a Disturbance which is inconveniently utilized by the users. Besides it, an Substandard provision of user support and un-proofing presents The information might yet be misused or interfered with later, even when it is shared with others The methods used today do not allow producing good safety and speed of the systems jointly, and thus they are not able to be quick enough to react for upcoming dangers or simply stop being efficient. Thus, not only data storage is hidden, but configured to ensure that the data is out of the way, unsuitable and inconvenient to use which makes data secret, suitable and convenient not to use. It encodes, shares proxies and verifies them in a manner that does not put a strain on it, and is compatible to everyone. It is thus not just a matter of how one can make outsourced data secure. It is how to devise a system by which data can be made confidential that makes people accountable is friendly and at the same time can be built to a larger scale without making it too complex to the users or causing too much of extra work to be done. This solution will mix encryption, proxy management and public checks in an efficient and tight cloud security setting. It is how to create a mechanism not only keeping information very confidential but also makes people responsible.

METHODOLOGY

The Identity-Based Data-Outsourcing (IBDO) system proposed is developed to establish a secure, efficient and convenient access to cloud data services, through the integration of an identity-based mathematics and proxy assistance and public verification. The strategy is comprised of a clear plan, and has certain major steps. First, the users enroll and get their IDs authenticated through a server. Unlike tradition methods where certificates are used, IBDO employs user IDs, e.g. Use of key creation tools (JCE/JCER/JCEM and others) and management of keys can be easily achieved.

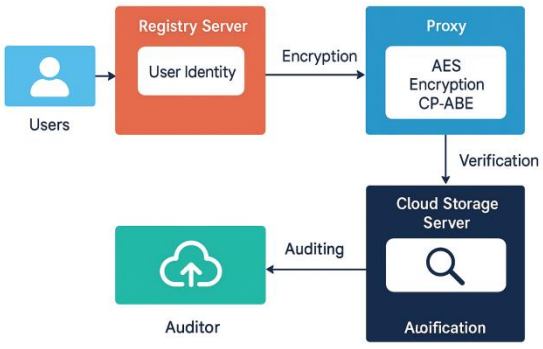

Fig1 Block Diagram

less multiple labours Scheduled Feasibility deals with the time concern and how long can be consumed in developing it. Temporary files are encrypted using the Advanced Encryption Standard (AES) and Ciphertext-Policy Attribute-Based Encryption (CP-ABE) performs the access control part of who can see what. The secure sharing of keys is done via the RSA process and the verification of truths is by the use of SHA-256. File uploading and the storage Files can be uploaded and saved by file owners using assistants that are provided. The activities of a proxies are recorded to keep them answerable. Finally a public verification will be confirmed by external verifiers and will not require any burden of having all information and it will be transparent based on the following process. The Java Database Connectivity was developed by Sun Microsystems in this regard we can consider of having a fair ratio of security, size control and simplicity of the IBDO system. The system should have all the capabilities of accommodating all of the data files uploaded.

Task	Task Name	Status
1	Requirement Analysis & Literature Survey	Done
2	Problem Statement & Feasibility Study	Done
3	Implementation of Encryption & Proxy Delegation	Done
4	Integration with Cloud Storage & Auditor Module	Done
5	Final Deployment & Documentation	Done

EXPERIMENTAL RESULTS

At First We have loaded and evaluated a new cloud architecture referred to as the Identity-Based Data Outsourcing (IBDO) founded on Java/J2EE, MySQL, and a local server. We tested it many times to understand how good it is in terms of security, efficiency, and ease of use.

We started our tests with the locking and unlocking speed of its named files between 1 MB to 100MB. The tests are categorized in very rapid and less hang up AES locking. The use of the CP-ABE allowed us to specify a significant part of the access rules without additional effort. Moreover, the RSA algorithm was good enough in performing key exchanges while SHA-256 was good enough in keeping the files secure and the system was fast.

Then we tried out the proxy assist option. Authorized proxies had the capability to lock the files of their owners and could upload files on their behalf and they were good at keeping records of the activities of the proxies then we tried out the proxy assist option. This eliminated access that was not supposed to be granted hence it could regulate access by the rightful persons in the right manner.

Then we checked how it was performing as far as checking with the populace goes. Files in order to verify the files safety. Even when fake attack was conducted in order to make sure that the safety checks do not know about the attack the data was presented as accurate.

Fig 2. File Proprietor Login Page

Fig 3. Proxies list of processed file

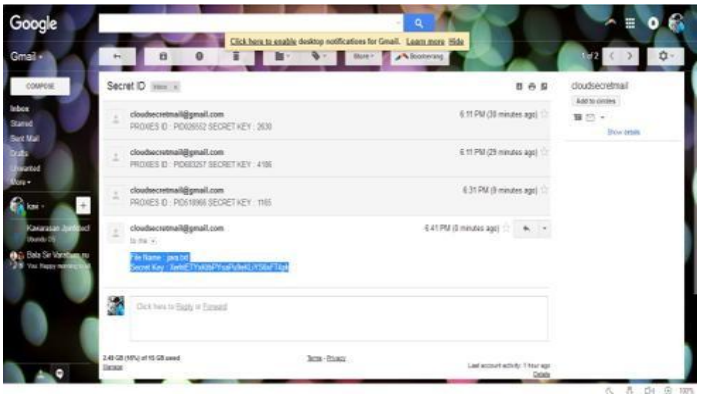

Fig 4. Access key Details

CONCLUSION

A new stratagem, ID-Based Data Outsourcing (IBDO) offers a straightforward, end to end approach to ensuring data security on the cloud. Problems like a private, unbroken, scalable and accountable cloud storage are huge issues to great cloud storage, yet with ID-based coding, proxy support and open examination are solutions to these issues in cloud storage except the big ones. Compared to old certificate usage, IBDO makes use of ID attributes hence is easy to compute against the user and is user friendly.

These standards indicate that the encryption model hybrid network that enjoys at least some time locking data in AES to provide fast data locking but the CP-ABE used to provide high access controls, RSA used in secure key support and the SHA-256 used to check the whole data dossier is helpful to data security without affecting the speed. The proxy element makes it Achievable since the trusted users can add files but the logs will ensure the responsibility. Additionally, the open check part assures data wholesomeness without files being added and lowering the amount of data to be moved and making it user-friendly. This study brings a step forward toward safer utilisation of cloud data and suggests means of its improvement the three most common being the withdrawal of features change of regulation to indicate files are Intact.

REFERENCES

[1] G. Ateniese, R. Burns, R. Curtmola, J. Herring, O. Khan, L. Kissner, Z. Peterson, and D. Song, “Provable data possession at untrusted stores,” in Proc. 14th ACM Conf. Computer and Communications Security (CCS), 2007, pp. 598–609.

[2] A. Juels and B. Kaliski, “PORs: Proofs of retrievability for large files,” in Proc. 14th ACM Conf. Computer and Communications Security (CCS), 2007, pp. 584–597.

[3] V. Goyal, O. Pandey, A. Sahai, and B. Waters, “Attribute-based encryption for fine-grained access control of encrypted data,” in Proc. 13th ACM Conf. Computer and Communications Security (CCS), 2006, pp. 89–98.

[4] J. Daemen and V. Rijmen, The Design of Rijndael: AES – The Advanced Encryption Standard. Berlin, Germany: Springer, 2002

[5] D. Boneh, B. Lynn, and H. Shacham, “Short signatures from the Weil pairing,” J. Cryptology, vol. 17, no. 4, pp. 297–319, 2004.