IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

SHARED DYNAMIC SECURED DATA WITH INTEGRATED USER IDENTITY

Edwin. P[1], Jeejo Vetharaj J[2]
[1]PG Scholar, Marthandam College of Engineering & Technology
[2]Assistant Professor, Marthandam College of Engineering & Technology

Abstract

Cloud computing is a model for enabling ubiquitous network access to a shared pool of configurable computing resources. Cloud computing and storage solutions provide users and enterprises with various capabilities to store and process their data in third-party data centers. It relies on sharing of resources to achieve coherence and economies of scale, similar to a utility (like the electricity grid) over a network. At the foundation of cloud computing is the broader concept of converged infrastructure and shared services. In Real time the issue we are discussing about is patent (ownership) misuse. The seller buys the ownership of a document or a streaming resource and it is being shared with other partners in the same business stream. This in turn causes great financial loss to the seller. The seller or the owner of the entity should be aware of file is being shared. We overcome this issue using security access protocol. The idea is we add limited access time to the file. The file or screening resource is controlled from owner side even if the resource is shared. If an unauthorized user tries to access the file, he will be promoted for access code; the owner can decide to grant access permission for the request user. A payload will be generated from the client side and sent to the origin user. The Payload contains the client details such as IP address, filename etc. with the help of payload, original user can check whether he have permission for the file he is trying to access.

Keywords - Cloud computing, payload, movie.

I. INTRODUCTION

This paper seeks to overcome patent miss use of a product like movie by providing the use of access code and payload through a website. Today's greatest problem related to the movie is patent miss use. In some cases, the actual owner cannot get expected profit of his hard work for his movie. Several theatres or like other persons sell the copy of original movie to various other parties or hosting the copy of the movie to the website without permission of the owner. This will cause great financial loss to the owner. This will lead to several directors may confuse to obtain his field. Several films cannot obtain expected profit because of this reason. All these problems are

overcome by using this website. Through this project, the registered user can able to see trailer of coming film and can able to pay early. And the existing user can play movie in two ways such as unlimited and limited payment system. Unlimited payment provides lifelong movie play while limited payment provides access time related movie play.

The project is based on cloud computing. Cloud computing is an information technology paradigm that enables ubiquitous access to Shared pool of configurable system resources that and higher-level services that can be rapidly provisioned with minimal management effort, often over the internet. Cloud storage is a model of data storage in which the digital data is stored in logical pools. Physical storage spans multiple servers (and often locations) and physical environment is typically own and managed by a hosting organization. These cloud storage providers are responsible for keeping the data available. Cloud provide load balancing of data, File management and storage, pay for what you consumed. The movie sells to the customer into a particular access time after payment.

II. LITERATURE REVIEW

CLOUD STORAGE MODEL

In the cloud storage model, there are three entities, namely the cloud storage server, group users and a Third Part Auditor (TPA). Group users consist of a data owner and a number of users who are authorized to access and modify the data by the data owner. The cloud storage server is semi-trusted, who provides data storage services for the group users. TPA could be any entity in the cloud, which will be able to conduct the data integrity of the shared data stored in the cloud server. In our system, the data owner could encrypt and upload its data to the remote cloud storage server. Also, he/she shares the privilege such as access and modify (compile and execute if necessary) to several group users.

THREAT MODEL AND SECURITY GOALS

Our threat model considers two types of attack:

1) An attacker outside the group (include the revoked group user cloud storage server) may obtain some knowledge of the plaintext of the data. This kind of attacker must at least break the security of the adopted group data encryption scheme.

2) The cloud storage server colludes with the revoked group users, and they want to provide an illegal data without being detected. In cloud environment, we assume that the cloud storage server is semi-trusted. Thus, it is reasonable that a revoked user will collude with the cloud server and share its secret group key to the cloud storage server. In this case, although the server proxy group user revocation way brings much communication and computation cost saving, it will make the scheme insecure against a

malicious cloud storage server who can get the secret key of revoked users during the user revocation phase. Thus, a malicious cloud server will be able to make data m, last modified by a user that needed to be revoked, into a malicious data m′. In the user revocation process, the cloud could make the malicious data m′ become valid.

To overcome the problems above, we aim to achieve the following security goals in our paper: 1) Security. A scheme is secure if for any database and any probabilistic polynomial time adversary, the adversary cannot convince a verifier to accept an invalid output. 2) Correctness. A scheme is correct if for any database and for any updated data m by a valid group user, the output of the verification by an honest cloud storage server is always the value m. Here, m is a ciphertext if the scheme could efficiently support encrypted database. 3) Efficiency. A scheme is efficient if for any data, the computation and storage overhead invested by any client user must be independent of the size of the shared data.

VECTOR COMMITMENT

Commitment is a fundamental primitive in cryptography, and it plays an important role in security protocols such as voting, identification, zero-knowledge proof, etc. The hiding property of commitment requires that it should not reveal information of the committed message, and the binding property requires that the committing mechanism should not allow a sender to change his/her mind about the committed message. Recently, Catalano and Fiore put forward a new primitive called Vector Commitment. Vector Commitment satisfies position binding that an adversary should not be able to open a commitment to two different values at the same position, and the Vector Commitment is concise, which means that the size of the commitment string and its openings must be independent of the vector length.

PERFORMANCE EVALUATION

In this section, we provide both the numerical and the experimental analysis of our scheme and conduct the computation time cost comparison.

We provide the time cost simulation for our scheme in different phases and the numerical analysis of computation of our scheme and two other schemes related. For the convenience of analysis, we denote by Mul a multiplication in G (G1, G2 and GT), Exp an exponentiation in G, Pair a computation of the pairing, and Hash a regular hashing operation. We omit other operations such as addition in G for all the schemes.

EXISTING SYSTEM

By the existing system the owner of the product cannot get expected profit. The owner creates his own product. He is the seller of the product. The seller buys the ownership of product and It is being shared with other partners in the same

business stream. This cause less benefit to the owner or the seller and cause great financial loss to the seller. But may have benefits to others in the same business stream. Through the existing system there is no way to control ownership misuse of movie. Several directors are confused due to this reason. Many third parties or hackers are trying to obtain the original copy and then they may misuse the situation.

Drawbacks of the Existing system:

- Third party can easy to obtain original copy just copying the movie.
- Anybody can play movie any time without permission of the owner.
- Owner cannot get expected profit.
- Cannot know movie details before they launch.
- Movie play on any device without permission of owner.
- Global access is not possible.
- The existing system is very time consuming.
- Frequent updating is not possible

PROPOSED SYSTEM

The main objective of the new system is to overcome the difficulties and demerits of the existing system or the manual system. Our system is to overcome patent or ownership misuse. The seller buys the ownership of the product. The seller or owner of the entity aware of the file is being shared. We overcome the issue by using security access protocol. The idea is we added limited access time to the file. The file or screening resource is controlled from owner side. If the unauthorized user tries to access the permission, he will be promoted for access code. The owner can decide to grant the access permission for the request. With the payload original user can check whether he has permission for the file he is trying to access.

- The system contains advanced booking before launch the product.
- The system provides File analysis. In this feature file hit, usability, file analytics are analyzed in a graphical representation.
- The system provides two type of access types:
- Unlimited access: Provide lifelong access for the product.
- Limited access: Provide rented time for access the product based on payment.
- System provides location related tracking accessibility for the product.
- Provide RestIP service.
- Provide discount to the existing customer.
- View trailers to the existing customers.
- Indore search engine is used for fast searching capability.
- Request file that is not available in the repository.
- Provide single device accessibility handler.ie, if the currently working system

has any fault, transfer the ownership to another new device and delete old device.

CONCLUSION

The application titled "Shared Dynamic Secured Data with Integrated User Identity "developed is designed in such a way that any further enhancement can be done with ease. The system has the capability for easy integration with other systems. New modules can be added to the existing system with less effort. I have put as much as my effort to develop this system based application titled "Shared Dynamic Secured Data with Integrated User Identity" that is easily accessible, informative and helpful. It has been designed in such a way that it is easy to modify, can be updated efficiently and accurately. On realizing the importance of systematic documentation all the processes are implemented using a software engineering approach. We have gained a lot of practical knowledge from this project, which we think, shall make us stand in a good state in the future.

FUTURE ENHANCEMENT

This paper can be extended by providing offline support. i.e., in the absence of internet system send payload through SMS. Current products in our system contain the extensions like pdf, text file and doc files. In the future, we try to access products without any extensions.

REFERENCES

1. Ateniese G., Burns R., Curtmola R. , Herring J., Kissner L., Peterson.Z, and Song.D, (2007)"Provable data possession at untrusted stores," in Proc. of ACM CCS, Virginia, USA, pp. 598–609.
2. Boneh D. and Boye.X(2004) "Collision-free accumulators and fail stop signature schemes without trees," in Proc. of EUROCRYPT, Interlaken, Switzerland.
3. Chaum.D and Van Heyst E.(1991), "Group signatures," in Proc. of EUROCRYPT 1991, Brighton, UK, pp. 257–265.
4. Dodis. Y(2009) "Proofs of retrievability via hardness amplification," in Proc. of TCC.
5. Gentry.C(2009) "Fully homomorphic encryption using ideal lattices," in Proc. of ACM STOC".
6. Juels.A and Kaliski B.S,(2007) "Pors: Proofs of retrievability for large files," in Proc. of ACM CCS, Virginia, USA, pp. 584–597.
7. Wang.B, Baochun L(2013) "Public auditing for shared data with efficient user revocation in the cloud," in Proc. of IEEE INFOCOM.