Volume 3, Issue 5, May 2013 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

An Application for Preserving Privacy of data in Cloud Computing

Ramya.G* *SITE,VIT University, Vellore* , India.

Priya. G *SCSE,VIT University, Vellore*, India.

Jaisankar.N *SCSE,VIT University, Vellore*, India.

Abstract— Digital Rights Management(DRM) is an advanced strategy for preserving data in a secured manner for long time developed as an user friendly application. We propose an application using Digital Rights Management technique using privacy preserving algorithm in it to make small bytes of data stored securely.According to our proposed mechanism user and provider should be accountable for any misuse with authorized data or elements which is purchased with complete license to use it. In DRM systems, the distributors and users must be accountable for any misuse of their purchased contents/licenses. To achieve the accountability of users, content providers perform usage tracking and monitoring via license acquisition transactions and user authentication mechanisms. However, accountability affects the user's privacy as it reveals the link between users and their usage patterns. User data gathered in this process can be later used to generate detailed profiles of the users and their activities. The resulting profiles of the entities can be misused by the content providers. We propose privacy enabled digital rights management mechanism without using the trusted third party assumption. The proposed mechanism supports both accountability and privacy simultaneously.

The system can also be extended for mobile cloud computing e- learning, business purpose etc. and the application can be further enhanced for using greater size files. The growing use of the internet can help in successfully use the developed proposal in real time.

Keywords— Encryption, Decryption, Anonymous Authentication, Trusted Third Party, Blind Decryption

I. INTRODUCTION

Digital rights management (DRM) technologies have been developed to protect the intellectual property rights of the entities involved User data gathered in this process can be later used to generate detailed profiles of the users and their activities. The resulting profiles of the entities can be misused by the content providers. The proposed mechanism supports both accountability and privacy of the data as well as stores it in the data base simultaneously. We use simple cryptographic primitives such as blind decryption and hash chain to construct the proposed system. We also provide a privacy preserving revocation mechanism which preserves a user's anonymity even after that user has been blocked for its misbehaviour. This mechanism can be successfully deployed in the cloud. Initially the data are stored in the database in the back end but after the complete deployment it will be deployed in the cloud database i.e. cloud storage. This is a novel way of securing and storing data using the proposed mechanism. Now these are some important features on what we are working upon in this application which acts as an add on services which is one of the noble ideas. In existing system simultaneous consideration of accountability and privacy has not been addressed well yet. Some schemes that take care of the accountability and privacy need the user to trust a third party. Whereas, other schemes which use complex cryptographic mechanisms to avoid trusted third parties fail to satisfy many of the desirable properties of DRM. Trusted third parties (TTP) are undesirable in DRM because users can never be assured that their privacy will be secured by these entities. The algorithm used in previous application was encryption of contents and the most disadvantages are that it became very complex issue to avoid third party interruption on the stored data and sometimes even database.

A. Integration

In our application we are working upon the two features of the cloud i.e. security and storage along with the user's feature to be accountable. We will be trying to integrate all these features in one application which can be used as a software as a service in cloud. This application would provide the features to secure and store data through hash encryption and private key generation technique with anonymous token generation for each data and Digital Right Management.

B.Automation

Our application depends on the fast and quick service of storing and purchasing the contents with full authorized license. Further the data and elements are saved and stored for long run of time till the application is in use. We will assume when this application is hosted on cloud it will be very dynamic application for use in industries and for

government sales and purchase scheme. Each one can get access to the resources, check according to their need and buy it for their use. The automation defines that the application will be fully automated with all the present features overcoming from all the previous issues of storage and security as well as other weaknesses.

II. RELATED WORK

In DRM systems, the distributors and users must be accountable for any misuse of their purchased contents/licenses. To achieve the accountability of users, content providers perform usage tracking and monitoring via license acquisition transactions and user authentication mechanisms. However, accountability affects the user‟s privacy as it reveals the link between users and their usage patterns. User data gathered in this process can be later used to generate detailed profiles of the users and their activities. The resulting profiles of the entities can be misused by the content providers [1]. K - times anonymous authentication (k-TAA) schemes allow members of a group to be authenticated anonymously by application providers for a bounded number of times. Dynamic k-TAA allows application providers to independently grant or revoke users from their own access group so as to provide better control over their clients [2].

Most real-life systems delegate responsibilities to different authorities. We apply this model to a digital rights management system, to achieve security. In our model a hierarchy of authorities issues certificates that are linked by cryptographic means. This linkage establishes a chain of control, identity-attribute-rights, and allows e rights control over content. Typical security objectives, such as identification, authentication, authorization and access control can be realized. Content keys are personalized to detect illegal super distribution.[3].

Cloud computing moves the application software and databases to the large data centers, where the management of the data and services may not be fully trustworthy. This unique attribute, however, poses many new security challenges which have not been well understood. In this article, we focus on cloud data storage security, which has always been an important aspect of quality of service. To ensure the correctness of users' data in the cloud, we propose an effective and flexible distributed scheme with two salient features, opposing to its predecessors. By utilizing the homomorphism token with distributed verification of erasure-coded data, our scheme achieves the integration of storage correctness insurance and data error localization, i.e., the identification of misbehaving server (s). Unlike most prior works, the new scheme further supports secure and efficient dynamic operations on data blocks, including: data update, delete and append.[4]

III. PROPOSED SYSTEM

We propose privacy enabled digital rights management mechanism without using the trusted third party assumption. The proposed mechanism supports both accountability and privacy simultaneously. We use simple cryptographic primitives such as blind decryption and hash chain to construct the proposed system. The advantage of using the proposed system is that it is very effective and it considers the accountability and responsibility of the provider and owner for the security of the data in it. The proposed algorithm is privacy preserving revocation of users.

A. Detailed Architecture

The use and advancement of internet which is increasing like web net has made the work easy to great extent. The replication and distribution of digital contents without any loss of quality to the contents is the major issue to be taken care in this proposed system in which work is done. This has resulted in violation of illegal copy rights. DRM technique helped to protect the intellectual property rights of the entities involved. Our mechanism has the major role of the administrator of the application who can generate anonymous token randomly and digital signature for the token and assigns the generated keys to any particular file which he wants to get stored in the cloud database for the use of the customers. Each item data stored will be given some private keys to be securely stored in the system in a complete package with its detail of time of uploading. The users can view the data items and then can buy the item using secured transaction service along with the complete decrypted package which was kept encrypted initially. They can download the package and use it for according to their requirement with full copy right. The administrator will have the complete details of what is uploaded and what has been sold along with their token table and signature values in some secured form. The details of the encrypted forms for any items are given to the legal users only.

This mechanism can be deployed in cloud as a storage of the secured data items which can be further enhanced with several other features and file size of bigger bits can also be used in future after the advancement of the mechanism. The mechanism uses the DRM technology as base design and privacy preserving algorithm for securing the data. The technology has already been existing but we worked upon with slight changes and separate way of presentation mechanism.

B. Algorithm Used

There are basically three modules of this application. One is owner, the other is provider/distributor and the third one is user. Owner is an admin for this application and he log in using his admin login account and then he generates an anonymous token along with the valid digital signature and then assigns its expiry date using a column of date and time and this date must be less than 30 days from the generation. Then these are packaged as one file and keys are generated and then he can upload any document or data to which the previously generated key file is assigned and saved in the data base. After this there is a role of the user. The new user can create his new user id and password and then for both existing and new user there is the user login. The user can login and view the data or elements such as paintings and choose to buy it so that he can be authenticated. He has to pay for the particular file what he has to buy and he gets authenticated for the product. The product is still in encrypted form as the owner has saved it. Now to get the original

content package user has to go through the decryption process in the mdule of decrypting package. User will get all the packages and he has to fill with the correct digital signature and randomly generated token in the given place so as to decrypt the content. Finally after decryption the original content will be downloaded to the same destination where it was saved. And the user can get the original content with full copy right.

Here there is no role of third party to save the document and sell it. Sometimes third party is not trusted and also it takes a longer process. User can buy the authenticated element without the interruption of any trusted third party just like an online shopping through online payment. And the last module is for the provider/distributor who can see and has the full details of what are the digital signatures assigned to what element to protect it from being corrupted and who paid for what element i.e. who bought which element or file. Also one element uploaded can be bought by many users with same signatures and privacy.

*1)Privacy preserving algorithm:*Privacy Preserving Revocation of Users

The Owner generates a collection of Anonymous Token Sets for the Users.

ATS1,ATS2……..ATSi

A user Ui can get a token setATSi from the Owner anonymously and use it for content purchase.

TID (i,j)= Epub(TID(i,j), K(p,b))

Denotes the encryption of TID(i,j) with the public key K(p,b)of the owner. Let Texpdenotes the expiry time of all the tokens and

TID(i,j) = Sign(TID(i,j) || Texp, K(p,r))

ATSi = Esym({T(i,1),T(i,2)……T(i,l)},Ki)

Owner can add now anonymous token set ATSi to revocation list. Now owner update revocation list to all content provider.

2)Database Design Description: Database design is the process of producing a detailed data model of a database. This logical data model contains all the needed Logical and physical design choices and physical storage parameters needed to generate a design in a Data Definition Language, which can then be used to create a database. A fully attributed data model contains detailed attributes for each entity. There are three tables in the database i.e. content table, new user table and anonymous token set package tables with proper values.

IV. **RESULTS AND DISCUSSIONS**

A. Create Anonymous Token Package

In the below Fig.1 and 2 owner generate anonymous token and encrypt that token and create anonymous token package it consist of encryption key and encrypted anonymous token and create signature for that package

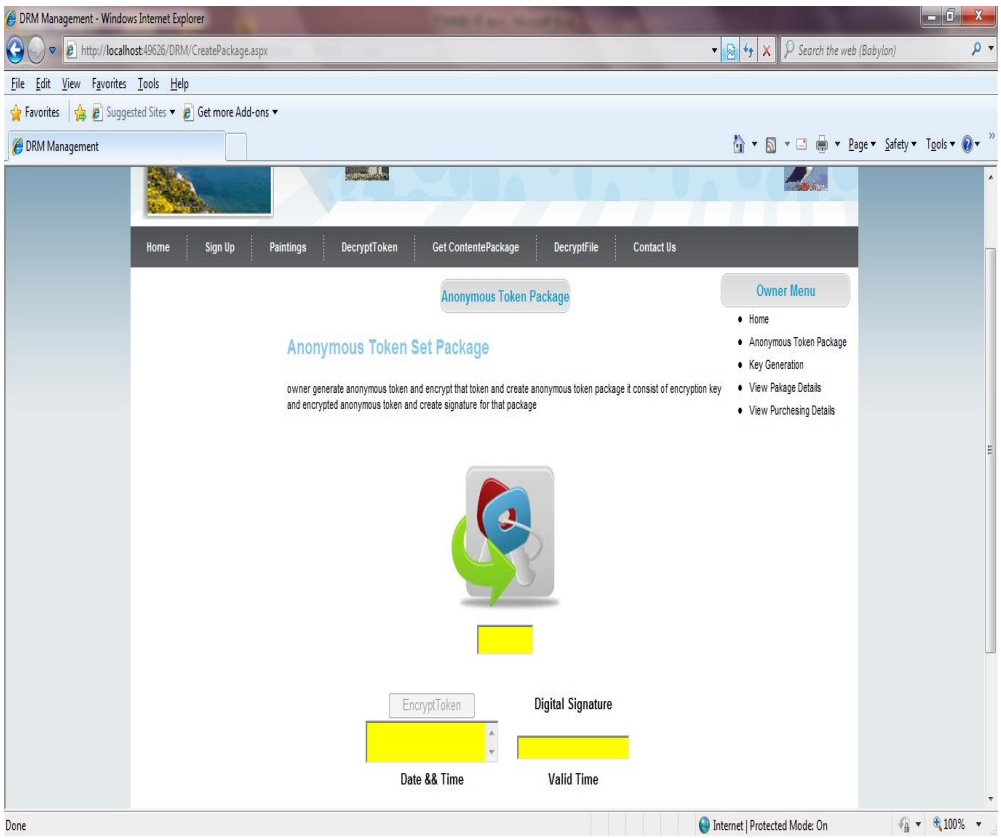


Fig .1 Anonymous Token Packages

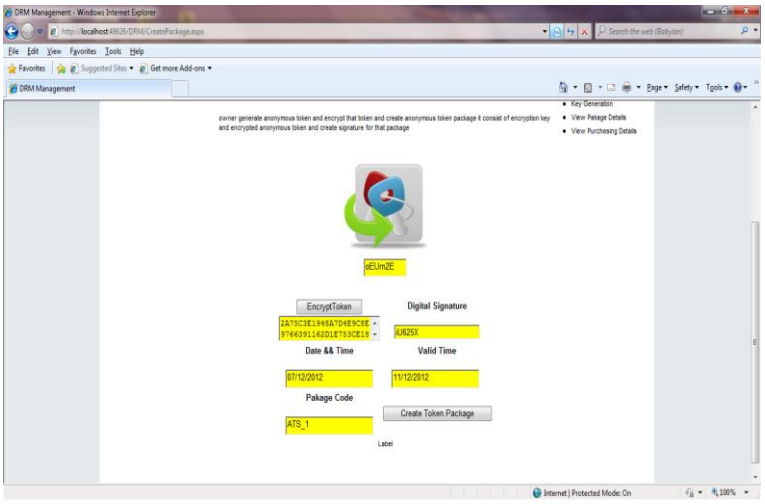
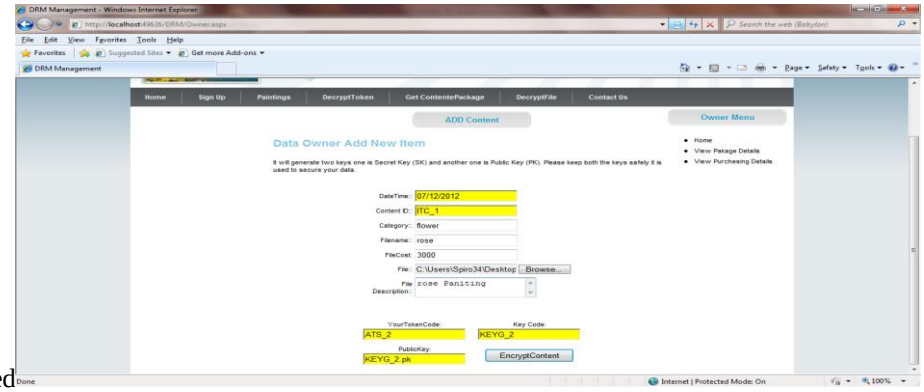


Fig .2 Anonymous Encrypted Token Package

B.Create Encrypted Content

In this Fig.3, after creating anonymous token package owner add our content encrypted and provide to Content provider.



encrypted

C. Decryption of Element

Using an algorithm of privacy preserving, we decrypt the content which is bought using the encrypted token set and key which further helps to get the original package of data which is required.

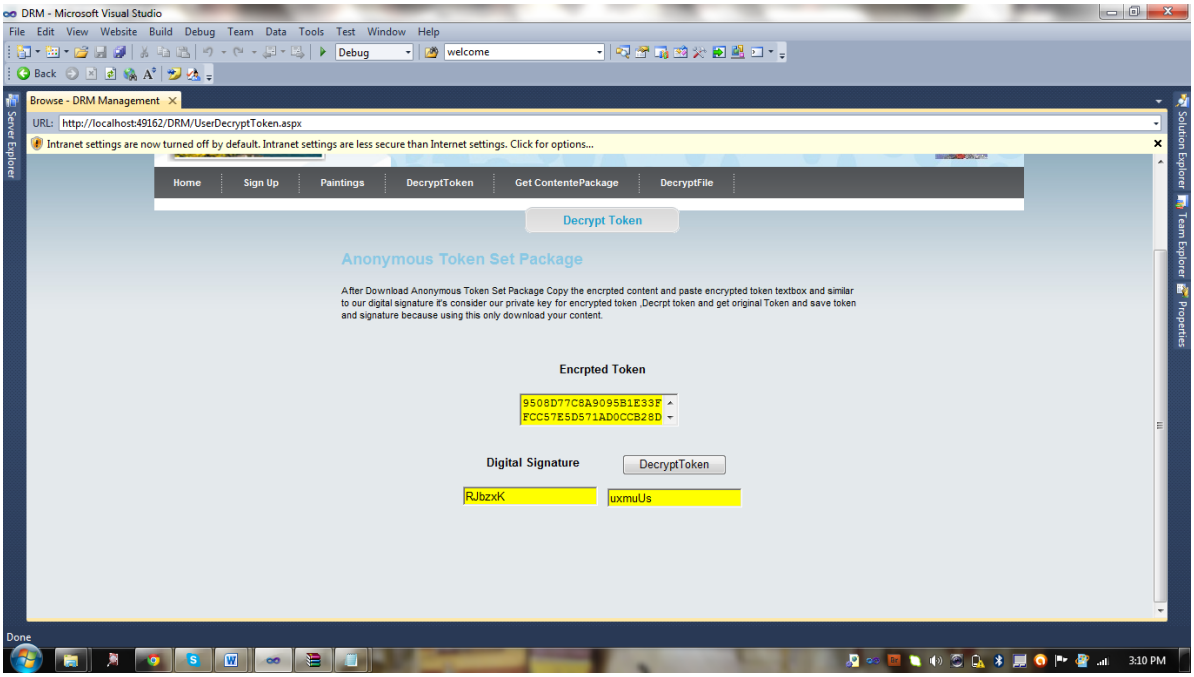


Fig 4 Decrypting of element

C. Getting the decrypted content

This is the final step of getting the original file or data.

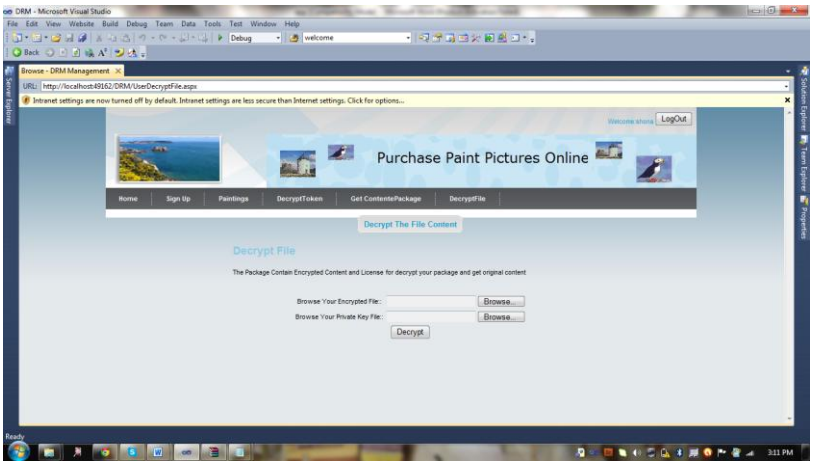


Fig 5 Getting the decrypted content

V. CONCLUSIONS

The proposed scheme satisfies the conflicting requirements of accountability and privacy in digital content distribution. Further, the proposed scheme supports access control without degrading user's privacy as well as allows revocation of even malicious users without violating their privacy.

ACKNOWLEDGMENT

We would like to give our thanks to Mani Shankar Gupta (B.tech IT)RoshniKumari (B.tech IT),School of Information Technology and Engineering, VIT University, Vellore) who have contributed towards the implementation part of an application. According to our guidance they have done an excellent work.

REFERENCES

1. Lei lei win, tony thomas, sabuemmanuel , "secure domain architecture for interoperable content distribution" singapore, in ieee transaction, june 2012 , vol 14.
2. Cong Wang, Kui Ren, Qian Wang, Wenjing Lou, Ensuring Data Storage Security in Cloud Computing,2008.
3. Man Ho Au, Willy Sosilu and Yi Mu , "Constant- size dynamic k-TAA " from university of Wollongong Australia. 2006.
4. Jan camenisch and susuan hohenberger and Anna lysynanskaya from USA, "Balancing Accountability and privacy using e-cash er SCN06 Proceeding of the 5th International Coonference on on Securv and Cryptography for Networks ,2006.
5. Chong, Chuen Ngen and van Buuren, R. and Hartel, P.H. and Kleinhuis, G. "security attributes based digital rights Management" , feruary 3, 2002.

