Authenticate Data Distribution Based On User Identity

M.Manipriya , C.Yalini

Abstract— In Cloud Computing and data sharing has been never easier, an accurate analysis on the shared data's provided an array of benefits to both their society and individuals. Data sharing is a large number of participants, must take into an account several issues, including efficiency's data integrity and privacy of data owner. It allows a data owner to anonymously authenticating this data which can be put into the clouds for storage or analysis purpose. Identity based ring signature, which eliminates the process of certificate verifications, can be used in instead. To further enhance the securities of ID based ring signatures by providing forward securities. The forward securing is an essential tool for building cost effective authenticating and anonymous of data sharing system. This property is especially important to any large scale of data sharing systems, data even if a secret keys of an one single user has been compromised. To access analyze, and responds too much more precise and detailed data from all levels of the electric grids is critical to efficient energy usage.

Keywords: Cloud Computing, Data sharing, *cloud storage, cloud service provider, Access control.*

I. INTRODUCTION

Cloud computing is a recently developed computing terminologies is based on the utilities and consumptions of computing resources. Cloud computing involved for deploying groups of remote servers and software networks that allows centralized data storage and online access to computer service and resources of cloud can be classified as pirating cloud, public clouds and hybrid clouds. Cloud computing rely on sharing of resources to achieves coherence and economy of scales [1].

User's access cloud computing using networks client devices such as desktop, laptops, and smart phones etc. some of these devices clouds clients rely on cloud computing for all or majorities of their applications so as to be basically useless without it. Browser based chrome book is the examples of thin clients. Many cloud applications do not requires specific software on the clients and use a browser to interact with cloud application. There are three models of cloud computing, deployment models and service models. Public clouds, private cloud and hybrid clouds are come under the deployment models. Platform as services, infrastructure as a service, and application as a service is come under the service models [2, 3].

Privating clouds are operated only for a single organizations; it can be managed by third parties and hosted either's internally or externally. When the services are rendered over networks that are opened for public use is called as public clouds. Public cloud resources may be offered on a pay per usage models. The hybrid cloud is combinations of two or more clouds it may be public or community privates. The important issues and cloud computing are securities and privacy. Cloud computing posses privacy concerns because the service provider can access the resources that is on the cloud at any times. A solution to privacy contains policy and legislation as well as end users for how data is stored [4].

While sharing IT infrastructures in cloud computing is more than efficient and provides flexibility for the clients [5]. In recent systems adding and removing a user's and to prevents forward secrecy and backward secrecy. The keys collaborates with attributes must be changed and the files must be encrypted also the new keys must be re distributed [6].

Now IT infrastructure is under the controlling of the cloud providers, the user has not only to trusting the securities mechanisms and also configuration of the cloud providers, but also the cloud service provider itself. Secure outsourcing of arbitrary computations and data storage is especially difficulties to fulfilling if a cloud client does not trust the cloud provider at all. There are the proposals for cryptographic methods. It has allows to perform particular computations on encrypted data's [7].

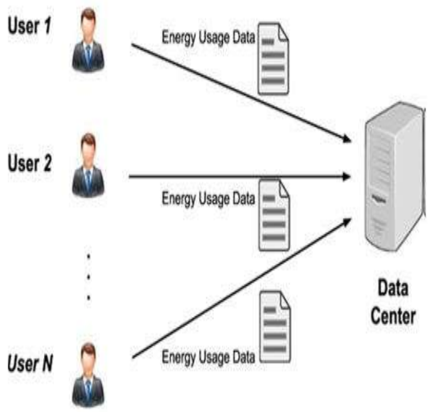


Fig.1 System Architecture

M.Manipriya, PG Scholar , Department of CSE ,Kongunadu College of Engineering and Technology, Trichy, Tamilnadu .
(Email : priyachandra@gmail.com.)
C.Yalini , Assistant Professor, Department of CSE ,Kongunadu College of Engineering and Technology, Trichy, Tamilnadu .

There are three types of access controls: user based access controls (UBAC), role based access controls (RBAC) and attribute based access controls (ABAC). The access controls list which contained the list of users who are the authorized to access data's is called user based access control It is not feasible to clouds be causing there are many users. In role based on access control Users are classified to base on their own roles [8].

User who has matching roles can be able to access the data's. The system defined as the role attributes based on access control in which users are given attributes and there data has been attached access policies. The user can access the data that having valid set of attributes and also satisfying the access policies. Records are encrypted under some access policy, such as attribute based encryption and stored in the cloud [9].

Trusted platforms module (TPM) cannot perform arbitrary secure computation on data; it has protected cryptographic keys and performs the pre defined cryptographic operations like encryptions, decryption [5]. Cloud storage system enables to users storing their data remotely and enjoy the on demand high quality cloud applications without the burden of hardware and software management [10].

Cipher text attribute based encryption(CP-ABE) is the attributes based crypto systems offers a way to encrypts a file for multiple user according to their privileges [11]. Data owner's is the user who wants to outsource their data's into the cloud and also responsible for encrypting the files and generating access structures and policies [12].

II. MODULES

A. Assumptions:

a. Users can have either's read or write or both accesses to a file stored in the cloud.
b. All communications between user's clouds are secured by the securing shell protocol technique, SSH.

B. Formats of Access Policies:

a. Boolean functions of attributes,
b. Linear secret sharing schemes (LSSS) matrix of the data [1],
c. Monotone span programs.

III. PROPOSED METHOD

The system develops new notions called forward secure ID based ring signatures, which is an essential tool for building cost effective authentic and anonymous data sharing system. For the first time, it provides formal definitions on forward securing ID-based ring signature. We present a concrete design of forward secure ID based ring signature. No previous ID-based ring signature schemes in the literature have the property of forward securities, and it provides this feature. It proved the security of the proposed schemes in the random oracle model, under the standard RSA Assumptions.

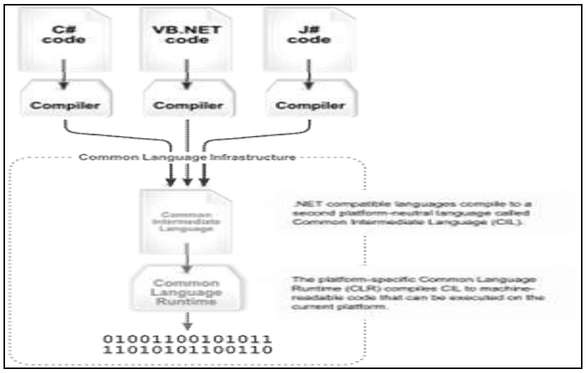

C# code
VB.NET code
J# code
Compiler
Compiler
Compiler
Common Language Infrastructure
Common Intermediate Language
.NET compatible languages compile to a second platform-neutral language called Common Intermediate Language (CIL).
Common Language Runtime
The platform-specific Common Language Runtime (CLR) compiles CIL to machine-readable code that can be executed on the current platform.
01001100101011
11010101100110

Fig.2 Common Language Infrastructure

A database is a structured collection of data. Data refers to the characteristics of people's things and event. SQL Servers stored each data items in its own field. In SQL Server's, the field relates to a particular persons, thing or event are bundled together to form a single completes unit of data, called a record. Each record is made up of number of fields. Now two fields in a record can have the same field names. The importance can be stated with a single word "Quality". Design is the place where quality is fostered in software developments. Design provides us with representations of software that can assess for quality. Design is the only way that we can accurately translate a employee's view into an finished software product or systems. Software design serves as a foundation for all the software engineering steps that follows'. Without strong designs, we risk building an unstable system one that will be difficult to tests one whose quality cannot be assessed until the last stages.

During design, progressive refinement of data structure, program structure, and procedural details are developed reviewed and documented. System design can be viewed from either technical or project management perspective.

IV. IDENTITY-BASED RING SIGNATURE

Identity-based (ID-based) crypto system, eliminated the need for verifying the validity of public key certificates, the management of which is both time and cost consuming. In an ID based cryptosystem, the public key of each user is easily computable from a string corresponding to this user's publicly known identity (e.g., an email address, a residential address, etc.). A private key generator (PKG) then computes private keys from its master secret for users. This property avoids the need of certificates (which are necessary in traditional public-key infrastructure) and associates an implicit public key (user identity) to each user within the system. In order to verify an ID-based signature, different from the traditional public key based signature, one does not need to verify the certificate first. The elimination of the certificate validation makes the whole verification process more efficient, which will lead to a significant save in communication and computation when a large number of users are involved (say, energy usage data sharing in smart-grid). Ring signature is a group-oriented signature with privacy protection on signature producer.

V. KEY EXPOSURE IN BIG DATA SHARING SYSTEM

The issue of key exposure is more severe in a ring signature scheme: if a ring member's secret key is exposed, the adversary can produce valid ring signatures of any documents on behalf of that group. Even worse, the "group" can be defined by the adversary at will due to the spontaneity property of ring signature: The adversary only needs to include the compromised user in the "group" of his choice. As a result, the exposure of one user's secret key renders all previously obtained ring signatures invalid (if that user is one of the ring members), since one cannot distinguish whether a ring signature is generated prior to the key exposure or by which user. Therefore, forward security is a necessary requirement that a big data sharing system must meet. Otherwise, it will lead to a huge waste of time and resource.

VI. SQL SERVER

A database management, or DBMS, gives the user access to their data and helps them transform the data into information. Such database management systems include dBase, paradox, IMS, SQL Server and SQL Server. These systems allow users to create, update and extract information from their database.

A database is a structured collection of data. Data refers to the characteristics of people, things and events. SQL Server stores each data item in its own fields. In SQL Server, the fields relating to a particular person, thing or event are bundled together to form a single complete unit of data, called a record. Each record is made up of a number of fields. No two fields in a record can have the same field name.

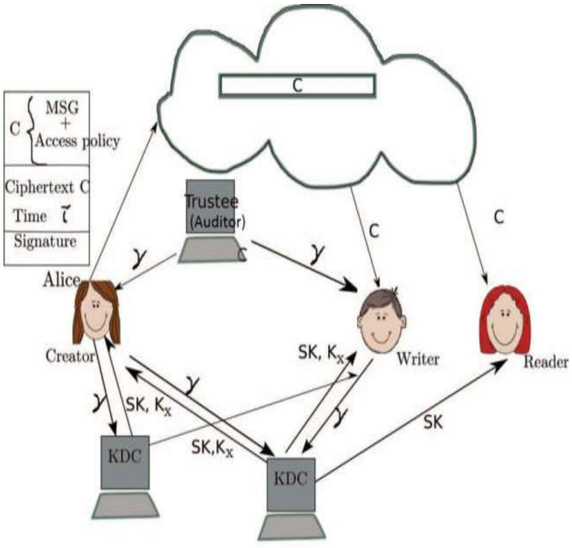


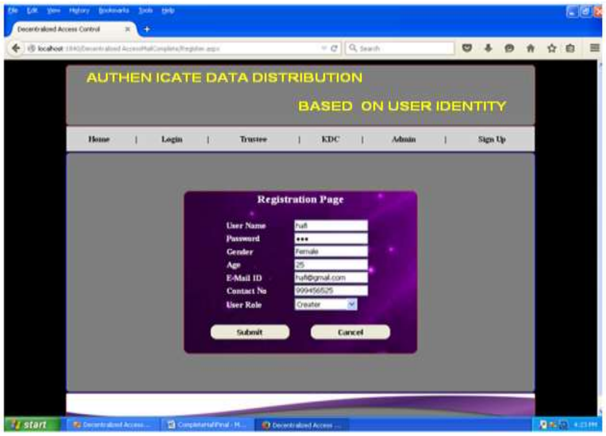
Fig 3: Our secure and authenticated cloud storage model

VII. RESULTS AND DISCUSSIONS

Implement the Smart Grid examples, and evaluate the performance of an IDFSRS scheme with respects to three entities: the private key generator (PKG), the energy data owners (user), and the service provider (data center). In the experiments, the programs for three entities are implemented by using the public cryptographic library MIRACL, programmed in C++. All experiments were repeated in 100 times to obtain average results, and all experiments were conducted in the cases of jNj = 1024 bits and jNj = 2048 bits respectively.

The average times for the PKG to setup the systems is shown in Table, where the test bed for the PKG is a DELL T5500 workstation equipped with 2.13 GHz Intel Xeon dual core dual processor with 12GB RAM and running Windows 7 Professional 64bit operating systems. It took 151 ms and 2198 ms for the PKG to setup the whole system for jNj = 1024 bits and jNj = 2048 bits respectively.

The average time of the data owner (user) to sign energy usage data with different choice of n and T are shown in Fig.3 and fig.4, for jNj = 1024 bits and jNj = 2048 bits respectively. The test bed for the users is a laptop personal computer to equip with 2.10 GHz Intel CPU with 4GB RAM and running Windows 7 operating systems.


File Edit View History Bookmarks Tools Help
Decentralized Access Control
localhost
Search
Home | Login | Trustee | KDC | Admin | Sign Up
Submit
Cancel
start

AUTHEN ICATE DATA DISTRIBUTION

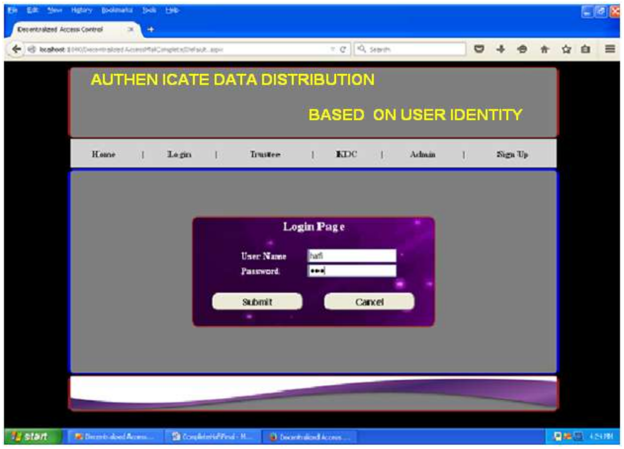
BASED ON USER IDENTITY

Registration Page

User Name	hafi
Password	•••
Gender	Female
Age	25
E-Mail ID	hafi@gmail.com
Contact No	9994456525
User Role	Creater

Fig.4 Registration page

Login to the user based on the customer details the algorithm generates the ring signatures. The signature sends to the user email id.


AUTHEN ICATE DATA DISTRIBUTION

BASED ON USER IDENTITY

Login Page

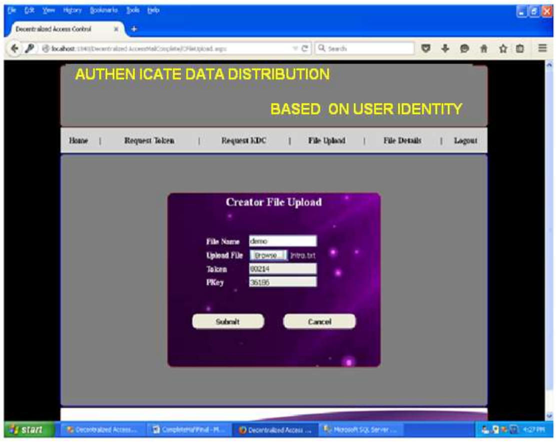
User Name: hafi

Password: •••

Decentralized Access Control
Home | Login | Trustee | KDC | Admin | Sign Up
Submit
Cancel
start

Fig.5 Login page

Login the user based on the customer details the algorithm generates the ring signature. The signature sends to the user email id.


AUTHEN ICATE DATA DISTRIBUTION

BASED ON USER IDENTITY

Creator File Upload

File Name: demo

Upload File: Browse... intro.txt

Token: 00214

PKey: 36186

Decentralized Access Control
Home | Request Token | Request KDC | File Upload | File Details | Logout
Submit
Cancel
start

Fig.6 Cloud File Upload

After getting a siganature ,they can upload our files. The file can be stored in the data center.

VIII. CONCLUSION

The objective of the systems was to developing the practical needs in data sharing, proposed new notions called Forward Secure ID Based Ring Signatures. It allows an ID-based ring signatures scheme to have forward security. It is the first in the literature to have this feature for ring signatures in ID-based setting. This scheme provided unconditional anonymity and can be proven forward secure unforgivable in the random oracle models, assuming RSA problem is hard. The scheme is very efficient to do not require any pairing operations. The size of user secret key is just one integer, while the key update process only requires an exponentiation.

We believe our schemes will be very useful in many other practical applications, especially to those requires user privacy and authentication, such as Adhoc network, e-commerce activities and smart grids. The current schemes rely on the random oracle assumption to prove its security.

REFERENCES

[1] G. N. Garcia, “Direct brain-computer communication through scalp recorded EEG signals,” Doctor’s thesis, Department of Electricity, techniques Federalae de Lausanne, Swiz, 2004.

[2] J. d. R. Milan, Brain Computer Interfaces, Handbook of Brain Theory and Neural Networks, 2nd ed., Cambridge, MA, The MIT Press, 2002.

[3] J. R. Wolpaw, D. J. McFarland, T. M. Vaughan, “Brain Computer Interface Research at the Wads worth Center,” IEEE Transactions on Neural Systems, Eng, vol. 8, 2000.

[4] N. Birbaumer, “A spelling device for the paralyzed,” Nature, vol. 398, 1999.

[5] J. Kalcher, “Graz brain-computer interface II,” Med. & Biol. Eng. & Comput., vol. 34, 1996.

[6] B. Obermaier, C. Neuper, C. Guger, G. Pfurtscheller, “Information Transfer Rate in a Five-Classes Brain Computer Interface,” IEEE Transactions on Neural Systems and Rehabilitation Engineering, vol. 9, no. 3, 2001.

[7] J. R. Wolpaw, D. J. McFarland, “Multichannel EEG based brain computer communication,” Electro enceph. Neuro physiol. vol. 90, 1994.

[8] C. W. Anderson, “Effects of variations in neural networks topology and output averaging on the discriminations of mental task from spontaneous EEG,” Journal of Intelligent System, vol. 7, pp. 165–190, 1997.

[9] J. d. R. Milan, Brain Computer Interfaces, Handbook of Brain Theory and Neural Networks, Second editions, Cambridge, MA, The MIT Press, 2002.

[10] J. D. Bayliss, “Use of the Evoked Potential P3 Components for Control in a Virtual Apartment,” IEEE Transactions Rehabilitation Engineering, vol. 11, no. 2, 2003.

[11] B. Obermaier, G. Müller, G. Pfurtscheller, “‘Virtual Keyboard’ controlled by spontaneous EEG activity,” Proc. of the Int. Conference on Artificial Neural Networks, Heidelberg: Springer-Verlag, 2001.

[12] J. del R. Millán and J. Mourino, “Asynchronous BCI and local neural classifiers: an overview of the adaptive brain interface project,” IEEE Transactions on Neural Systems and Rehabilitation Engineering, vol. 11, no. 2, pp. 159–161, 2003