IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

ISO 3297:2007 Certified ⁜ Impact Factor 7.39 ⁜ Vol. 11, Issue 8, August 2022

DOI: 10.17148/IJARCCE.2022.11820

FILE SECURITY USING RING SIGNATURE BASED ROLE ACCESS CONTROL MECHANISM

Revathi.L[1], Vijay Kumar.M[2]

Department.of Computer Science Engineering, CSI College of Engineering, Tamil Nadu, India[1]

Assitant Professor Department of Computer Science Engineering, CSI College of Engineering,

Tamil Nadu, India[2]

Abstract: The key feature of cloud computing is one can access information any place, anywhere, at any time. So basically, cloud computing is subscription-based service where one can obtain network storage space and computer resources for data storage as well as data sharing. Due to high fame of cloud for data storage and sharing, large number of participants gets attracted to it but it leads to issue related to efficiency, Data integrity, privacy and authentication. To overcome these issues, concept of ring signature has been introduced for data sharing amongst large number of users. Ring signatures are used to provide user's anonymity and signer's privacy. It allows a data owner to anonymously authenticate the data which can be stored into the cloud or analysis purpose. Yet the most cost consuming certificate verification for public key infrastructure (PKI) setting becomes a bottleneck for this solution to be scalable. Session based ID with ring mechanism helps to implement session based key and access files within a session. Use of ID-based ring signature, removes the need of certificate verification which was done using public key infrastructure, hence reduce cost as well as introduction of forward security, further strengthen this system more. Use of weil pairing, keeps even shorter keys secure and it also requires less processing power. So the motivation of this paper is to propose a secure data reading and sharing scheme using above mentioned scheme.

Keywords: Public Key Infrastructure

I. INTRODUCTION

According to Over the past few years, cloud computing has rapidly emerged as a successful paradigm for providing IT infrastructure, resources and services on a pay- per-use basis. The wider adoption of Cloud and virtualization technologies has led to the establishment of large scale data centers that provide cloud services. This evolution induces a tremendous rise of electricity consumption, escalating data center ownership costs and increasing carbon footprints. For these reasons, energy efficiency is becoming increasingly important for data centers and Cloud. The fact that electricity consumption is set to rise 76% from 2007 to 2030 with data centers contributing an important portion of this increase emphasizes the importance of reducing energy consumption in Clouds. According to the Gartner report, the average data center is estimated to consume as much energy as 25000 households, and according to McKinsey report,"The total estimated energy bill for data centers in 2010 is 11.5 billion and energy costs in a typical data center double every five years". Face to this electronic waste and to these huge amount of energy used to power data centers, energy efficient data center solutions have become one of the greatest challenges.

Provided solutions should scale in multiple dimensions and Cloud providers must also deal with the users' requirements which are being more and more complex. Requested services are more sophisticated and complete since users need to deploy their own applications with the topology they choose and with having the control on both infrastructure and programs. This means combining the flexibility of IaaS and the ease of use of PaaS within a single environment. As a result, the classic three layer model is changing and the convergence of IaaS and PaaS is considered as natural evolutionary step in cloud computing. Cloud resource allocation solutions should be flexible enough to adapt to the evolving Cloud landscape and to deal with users requirements.

Another important dimension we consider is the type of the virtualization. In addition to traditional VM based technology, Cloud providers are also adopting new container-based virtualization technologies like LXC and Dockers that enable the deployment of applications into containers. Hence, this resource variety aspect should be taken into account when modeling the problem of resource allocation to scale with the Cloud evolution and with new users requirements. One last important dimension at which we are interested in this work is the resource provisioning plan. Cloud providers could offer two types of resource provisioning: on-demand and advance or long-term reservation.

International Journal of Advanced Research in Computer and Communication Engineering

ISO 3297:2007 Certified ⁜ Impact Factor 7.39 ⁜ Vol. 11, Issue 8, August 2022

DOI: 10.17148/IJARCCE.2022.11820

Advance reservation concept has many advantages especially for the co-allocation for resources. It provides simple means for resource planning andreservation in the future and offers an increased expectation that resources can be allocated when demanded. Althoughadvance reservation of resources in cloud is very advantageous, the focus has been mostly on the on-demand plan. Solving the problem of resource allocation in Cloud while maximizing energy efficiency and adopting the previously cited dimensions, is a very challenging issue. In this thesis, we address the problem with its multiple facets and levels to provide not only a specific solution, but also a generic and complete approach.

EXISTING SYSTEM:

The above PRE schemes only allows the re- encryption procedure is executed in an all-or-nothingmanner. The proxy can either re-encrypt all the initial ciphertexts or none of them. This coarse-gained control over cipher texts to be re-encrypted may limit the application of PRE systems. To fill this gap, a refined concept referred toas conditional PRE (CPRE) has been proposed. In CPRE schemes, a sender can enforce fine-grained re-encryption control over his initial cipher texts. The sender achieves this goal by associating a condition with a encryption Key.

Only the cipher texts meeting the specified condition can be re-encrypted by the proxy holding the corresponding re-encryption key.A recent conditional proxy broadcast re-encryption

Scheme allows the senders to control the time to encrypt their initial cipher texts. When a sender generates a re-encryption key to re-encrypt an initial cipher text, the sender needs to take the original receivers' identities of the initial cipher text as input. In practice, it means that the sender must locally remember the receivers' identities of all initial cipher texts. This requirement makes this scheme constrained for the memory-limited or mobile senders and efficient only for special applications.

PROBLEM STATEMENT:

Standardization of problem lists in the safety concerns.

- Large networks like the internet, the centralisticapproach of IBE becomes problematic. Of course, one could adapt the existing CA system so that parameters for multiple PKGs are automatically deployed with common software packages.
- Although some bureaucrats would surely like this idea, history has shown that systems designed to ensure privacy with secret backdoors are not accepted as they take the actual goal ad absurdum.
- Another completely different topic is that the mathematics behind IBE (considering for instance the presented scheme) are in many cases far more complicated than those for RSA, ElGamal or DSA
- This makes implementation difficult, especially since less experience and resources are available onthe rather young field of pairing based crypto.

PROPOSED SYSTEM:

1) The proposed system is a signature based role access control mechanism, also known as role-orientedring signature. In this scheme, only the person who belongs to the designated role can verify the validity of the ring signature.
2) In a PKI authentication frame, each person should have his own key pair.
3) So the core issue of role-oriented signature is how to design a scheme in which each role member is allowed to verify the signature independently. As we have mentioned above, a ring signature with limited verification range is necessary in some instances.
4) The receiver identity is mainly considered while receiving the file and also during re-encryption.

Advantage of Proposed System:

- The receiver identity is mainly considered while receiving the file and also during re-encryption.
- The identity signature and role are considered to identify the receivers
- High secure to the system by generating unique signature for each users.
- Three factors combination will give the high securefor the users data transmission.
- High secure to the system by generating unique signature for each users. Three factors combination will give

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

ISO 3297:2007 Certified ⁜ Impact Factor 7.39 ⁜ Vol. 11, Issue 8, August 2022

DOI: 10.17148/IJARCCE.2022.11820

the high secure for the users data transmission

II. SYSTEM REQUIREMENT

A. SOFTWARE REQUIEMENTS SPECIFICATION:

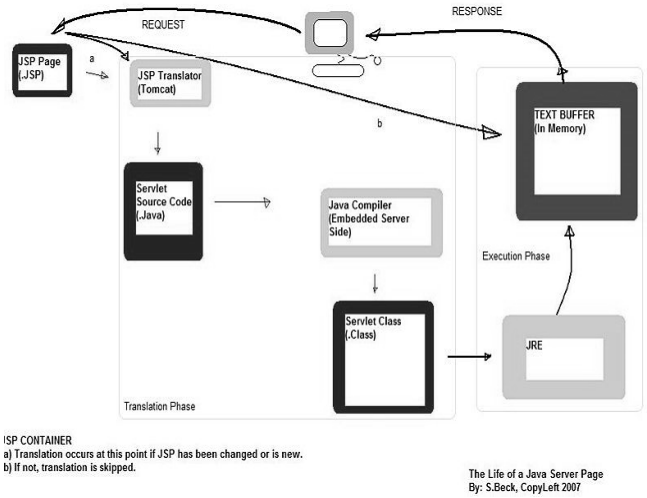
Operating System:		Windows 2000 or Higher
Language	:	Java, J2EE
Technologies	:	JSP, Servlet, JavaScript
Backend	:	MySQL Server
Back End Tool	:	SQL Yog
Web Server	:	Apache Tomcat
Build Tool	:	Apache Ant

B. HARDWARE REQUIEMENTS SPECIFICATION:

Processor	:	PIV
Ram	:	512 Mb
Hard Disk	:	10 GB Space
Monitor	:	VGA Color (256)

III. SYSTEM ARCHITECHURE

System Architecture design-identifies the overall hypermedia structure for the Web Application. Architecture design is tied to the goals establish for a Web Application, the content to be presented, the users who will visit, and the navigation philosophy that has been established. Content architecture, focuses on the manner in which content objects and structured for presentation and navigation. Web Application architecture, addresses the manner in which the application is structure to manage user interaction, handle internal processing tasks, effect navigation, and present content. Web Application architecture is defined within the context of the development environment in which the application is to be implemented.



IV. SYSTEM IMPLEMENTATION

1. Instructional Scenario
2. Data Collection And Preprocessing
3. Data Analysis
4. Data Prediction

V. RESULT AND ANALYSIS

A result is the final consequence This methodology makes use of groups with efficiently computablebilinear maps, and

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

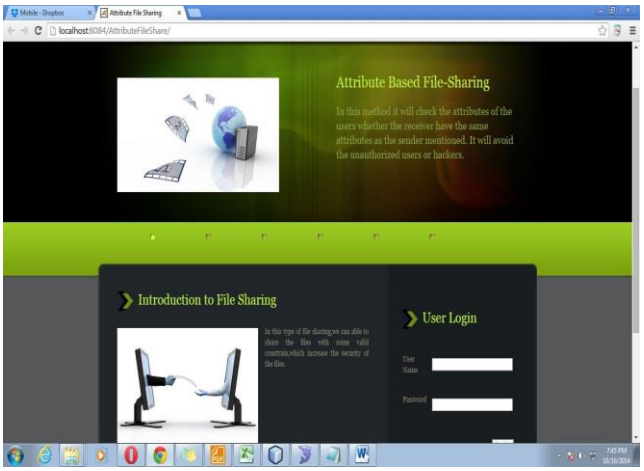
International Journal of Advanced Research in Computer and Communication Engineering

ISO 3297:2007 Certified ⁜ Impact Factor 7.39 ⁜ Vol. 11, Issue 8, August 2022

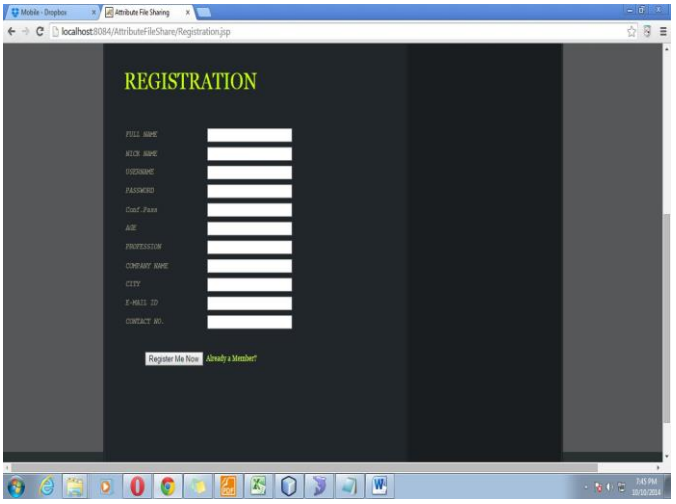
DOI: 10.17148/IJARCCE.2022.11820

it is the key to our security proof, which we give in the generic bilinear group model. Finally, we provide an implementation of our system to show that our system performs well in practice. We provide a description of both our API and the structure of our implementation. In addition, we provide several techniques for optimizing decryption performance and measure our performance features experimentally.

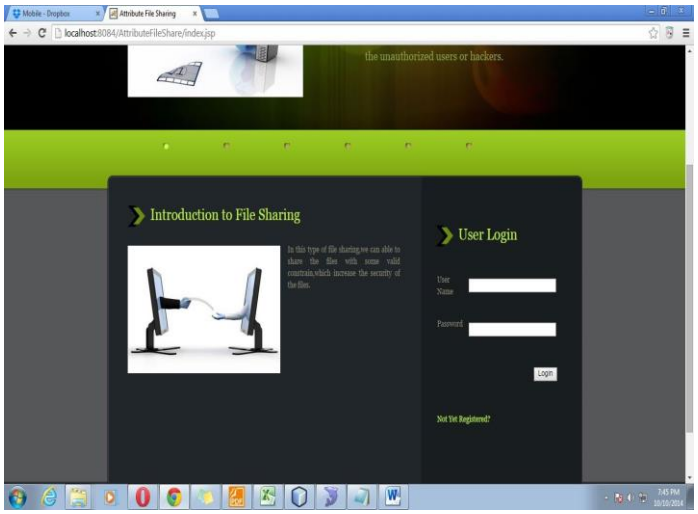
HOME PAGE:



User Register



PROCESSOR LOGIN



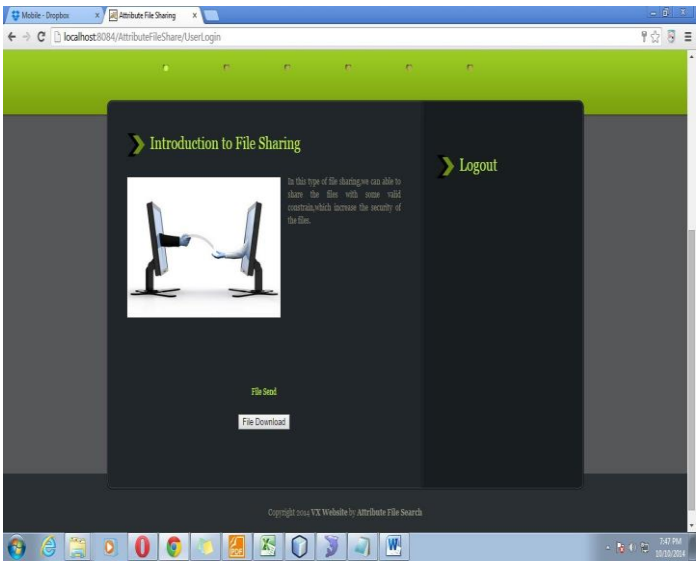
IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

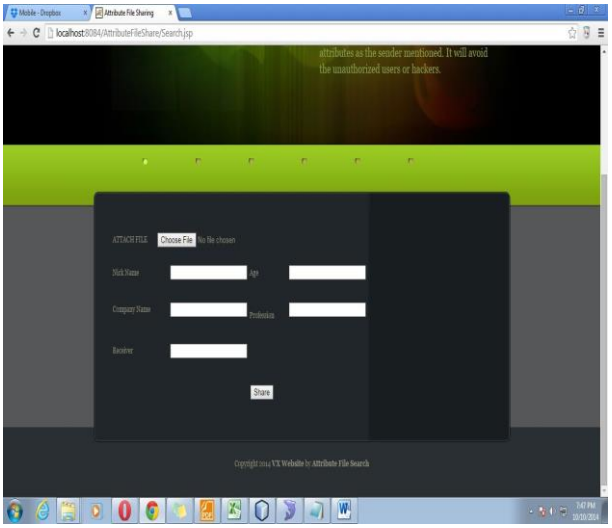
ISO 3297:2007 Certified ⁜ Impact Factor 7.39 ⁜ Vol. 11, Issue 8, August 2022

DOI: 10.17148/IJARCCE.2022.11820

LOGOUT



FILE SHARING



CONCLUSION

In the work, collusion resistance is insured by using a secret-sharing scheme and embedding independently chosen secret shares into each private key. Because of the independence of the randomness used in each invocation of the secret sharing scheme, collusion- resistance follows. In our scenario, users' private keys are associated with sets of attributes instead of access structuresover them, and so secret sharing schemes do not apply. Instead, we devise a novel private key randomization technique that uses a new two-level random masking methodology. This methodology makes use of groups with efficiently computable bilinear maps, and it is the key to our security proof, which we give in the generic bilinear group model. Finally, we provide an implementation of our system to show that our system performs well in practice. We provide a description of both our API and the structure of our implementation. In addition, we provide several techniques for optimizing decryption performance and measure our performance features experimentally.

REFERENCES

[1] P. Mell and T. Grance, ''The NIST Definition of Cloud Computing,'' National Institute of Standards and Technology,Gaithersburg, MD, USA, Tech. Rep., 2009.

[2] J. Bethencourt, A. Sahai, and B. Waters, ''Ciphertext-Policy Attribute-Based Encryption,'' in Proc. IEEE Symp.

International Journal of Advanced Research in Computer and Communication Engineering

ISO 3297:2007 Certified ⁜ Impact Factor 7.39 ⁜ Vol. 11, Issue 8, August 2022

DOI: 10.17148/IJARCCE.2022.11820

Security and privacy (S&P'07), 2007, pp. 321-334.

[3] B. Waters, ''Ciphertext-Policy Attribute-Based Encryption: An Expressive, Efficient, and Provably Secure Realization,'' in Proc. 4th Int'l Conf. Practice and Theory in Public Key Cryptography (PKC'11), 2011, pp. 53-70.

[4] V. Goyal, A. Jain, O. Pandey, and A. Sahai, ''Bounded Ciphertext Policy Attribute Based Encryption,'' in Proc. 35th Int'l Colloquium on Automata, Languages, and Programming (ICALP'08), 2008, pp. 579-591.

[5] A.B. Lewko, T. Okamoto, A. Sahai, K. Takashima, and B. Waters, ''Fully Secure Functional Encryption: Attribute- Based Encryption and (Hierarchical) Inner Product Encryption,'' in Proc. Advances in Cryptology-EUROCRYPT'10, 2010, pp. 62-91.

[6] S. Yu, C. Wang, K. Ren, and W. Lou, ''Attribute Based Data Sharing with Attribute Revocation,'' in Proc. 5th ACM Symp.Information, Computer and Comm. Security (ASIACCS'10), 2010, pp. 261-270.

[7] M. Li, S. Yu, Y. Zheng, K. Ren, and W. Lou, ''Scalable and Secure Sharing of Personal Health Records in Cloud Computing Using Attribute-Based Encryption,'' IEEE Trans. Parallel Distributed Systems, vol. 24, no. 1, pp. 131-143, Jan. 2013.

[8] S. Jahid, P. Mittal, and N. Borisov, ''Easier: Encryption- Based Access Control in Social Networks with Efficient Revocation,'' in Proc. 6th ACM Symp. Information, Computer and Comm. Security (ASIACCS'11), 2011, pp. 411-415.