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.2022.11818

Hierarchical keymanagement using Elliptical Curve

Remos A[1], Vijay Kumar.M[2]

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

Assistant Professor, Department of Computer Science Engineering, CSI College of Engineering, Tamil Nadu, India[2]

Abstract: CDNs on clouds normally communicate with authenticated subscribers using HTTPS to provide privacy and data integrity. The SSL private key is the most critical component in secure communication, and it can be even more important than the protected content itself. The key challenges are a) how to provide security guarantees so that the SSL private key and the content can be stored onto untrusted public clouds and b) how to allow CDN nodes to provide autonomous and effective data transfer over HTTPS encrypted connections, with possible SSL acceleration for better performance. To solve the issues, Effective Hierarchical Key Management System caches both the data and the SSL private key onto the cloud-based CDN nodes using a hierarchical key distribution scheme and ECC algorithm that leverages the cloud distributed infrastructure with trustful fidelity and hardware assistance. The proposed method consists of a Key Distribution Center (KDC), large-range distributed Key Sub- Centers (KSCs) and Backend Caching Services, such as web content caching or in-memory data caching and also the session key establishment center. The key challenge is how to avoid the additional communication between the CDN node and the key server. A good solution is to cache the private keys in CDN nodes to comply with the elasticity principle, and at the same time, guarantee the security of the cached keys on clouds**.**

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 datacenter 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. Advance reservation concept has many advantages especially for the co-allocation for resources. It provides simple means for resource planning and reservation in the future and offers an increased expectation that resources can be allocated when demanded. Although advance 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

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.2022.11818

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:

Cryptography is the study of secure communications techniques that allow only the sender and intended recipient of a message to view its contents. The simplest method uses the symmetric or "secret key" system. Here, data is encrypted using a secret key, and then both the encoded message and secret key are sent to the recipient for decryption. Problem here is if the message is intercepted, a third party has everything they need to decrypt and read the message. To address this issue, cryptologists devised the asymmetric or "public key" system. In this case, every user has two keys: one public and one private. Senders request the public key of their intended recipient, encrypt the message and send it along. When the message arrives, only the recipient's private key will decode it. Nowadays these asymmetric cryptographic methods are used in the Cloud Computing too. The private key is the most critical component in secure communication, and it can be even more important than the protected content itself if the private key is stolen in the untrusted environment like cloud, files will also be stolen and the total trust on the cloud will be lost.

PROBLEM STATEMENT:

Standardization of problem lists in the safety concerns.

- Large networks like the internet, the centralistic approach 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 on the rather young field of pairing based crypto.

PROPOSED SYSTEM:

Content Delivery Network (CDN) on clouds normally communicates with authenticated subscribers using HTTPS to provide privacy and data integrity. The SSL private key is the most critical component in secure communication, and it can be even more important than the protected content itself. Here the key challenge is how to provide security guarantees so that the SSL private key and the content can be stored onto untrusted public clouds. To solve this issue, keys are generated in Key Distribution Centre (KDC) using Elliptic Curve Cryptographic algorithm and the private key will be hidden even to the CDN and cached or stored in the Key Sub-Centres. Only when decrypting the content or any request from the user, CDN will get the private key cached from the Key Sub-Centres. This type of key management approach in our paper is named as Effective Hierarchical Key Management System. In this systemsession keys will also be generated for further authentication. In this project a web application will be developed, with a dummy CDN(i.e. Content Delivery Network and KDC(Key Distribution Centre) in that users can be registered, registered users alone will be able to request the CDN and the private key will be secured inthe KDC. Once this key authentication gets success user can be able to manage his files in the cloud like upload files to the cloud or download file from the cloud. For storage of the files uploaded by the user cloud storage application called Dropbox is used. Dropbox is a public Software-as-a-Service (SaaS) cloud application.

Advantage of Proposed System:

- The secure data sharing between user and Cloud resources is implemented using Elliptic curve cryptography and session key management The identity signature and role are considered to identify the receivers
- Thus Our approach Effective Hierarchical Key Management System will guarantee the securityof the private key by generating keys Key Distribution Centre (KDC).
- CDN will get the private key cached from the Key Sub-Centres. Next phase, have to upload, encrypt,download and decrypt the files after the validationof the above process mentioned.

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.2022.11818

II. SYSTEM REQUIREMENT

A. *SOFTWARE REQUIEMENTS SPECIFICATION:*

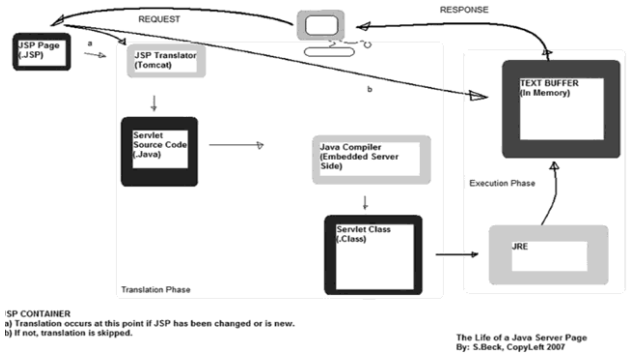
Language	:	Java, J2EE
Technologies	:	JSP, Servlet,JavaScript
Backend	:	MySQL Server
Back End Tool	:	SQL Yog
Web Server	:	Apache Tomcat
Build Tool	:	Apache Ant

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 willvisit, 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 themanner in which the application is structure to manage user interaction, handle internal processing tasks, effect navigation, and present content. Web Applicationarchitecture is defined within the context of the development environment in which the application is to be implemented.



IV. SYSTEM IMPLEMENTATION

1. Instructional Scenario
2. Request
3. Responds
4. Key

V. RESULT AND ANALYSIS

A result is the final consequence This methodology makes use of groups with efficiently computable key, and it is the key to our security proof,which we give in the generic 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 featuresexperimentally.

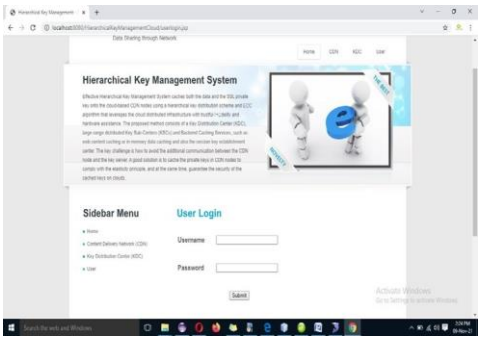
IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

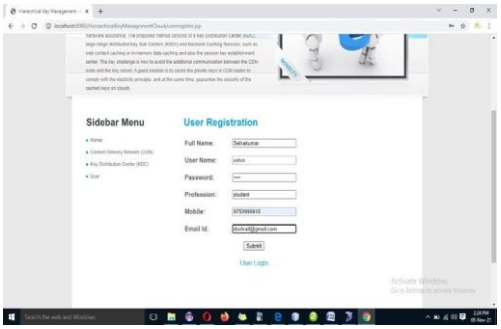
ISO 3297:2007 Certified ⁜ Impact Factor 7.39 ⁜ Vol. 11, Issue 8, August 2022

DOI: 10.17148/IJARCCE.2022.11818

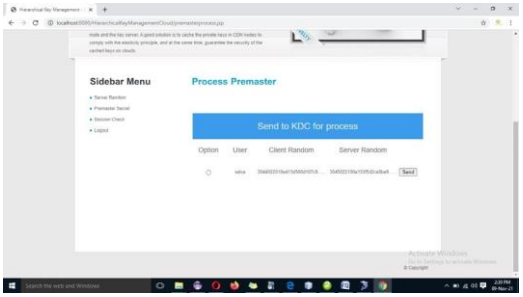
HOME PAGE:



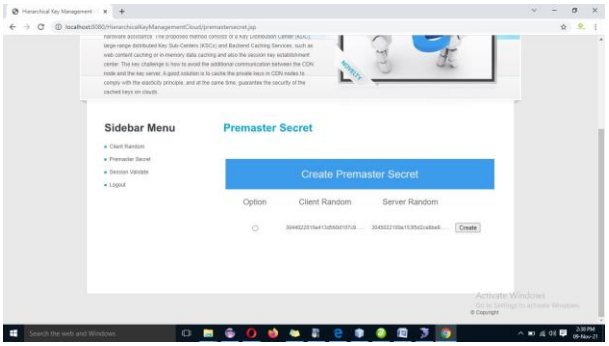
USER REGISTER :



PROCESSOR LOGIN



LOGOUT



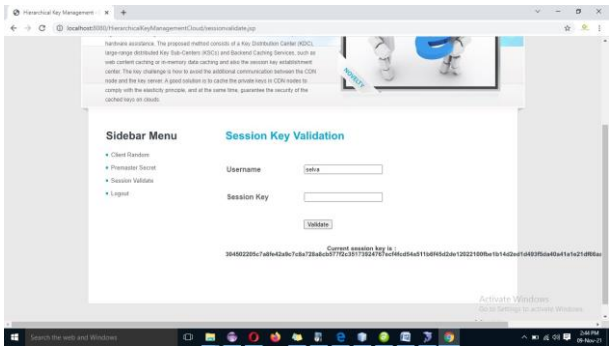
IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

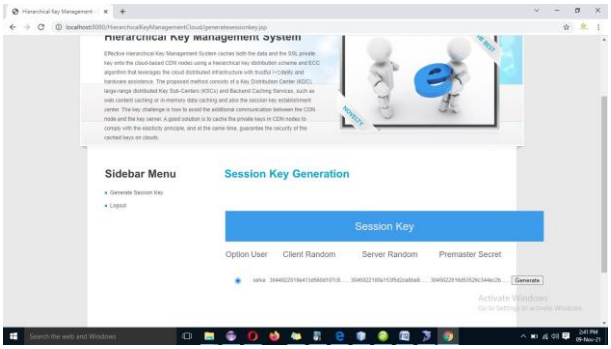
International Journal of Advanced Research in Computer and Communication Engineering

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

DOI: 10.17148/IJARCCE.2022.11818

FILE SHARING





CONCLUSION

approach Effective Hierarchical Key Management System will guarantee the security of the private key by generating keys Key Distribution Centre(KDC) using Elliptic Curve Cryptographic algorithm and the private key will be hidden even to the CDN and cached or stored in the Key Sub- Centres. Only when decrypting the content or any request from the user, CDN will get the private key cached from the Key Sub-Centres. Next phase, have to upload, encrypt, download and decrypt the files after the validation of the above process mentioned.

REFERENCES

[1] Joseph Idziorek, Mark Tannian, and Doug Jacobson. Attribution of fraudulent resource consumption in the cloud. In IEEE CLOUD 2012, pages 99–106. IEEE, 2012.

[2] Frank McKeen, Ilya Alexandrovich, Alex Berenzon, Carlos

V. Rozas, Hisham Shafi, Vedvyas Shanbhogue, and Uday R. Savagaonkar. Innovative instructions and software model for isolated execution. In HASP@ISCA 2013, page 10, 2013.

[3] Ashay Rane, Calvin Lin, and Mohit Tiwari. Raccoon: Closing digital side-channels through obfuscated execution. In 24th USENIX Security Symposium, USENIX Security 2015, pages 431–446, 2015.

[4] Jianting Ning, Xiaolei Dong, Zhenfu Cao, and Lifei Wei. Accountable authority ciphertext-policy attribute-based encryption with white-box traceability and public auditing in the cloud. In Computer Security–ESORICS 2015, pages 270–289. Springer, 2015.

[5] Jinguang Han, Willy Susilo, Yi Mu, Jianying Zhou, and Man Ho Allen Au. Improving privacy and security in decentralized ciphertext-policy attribute-based encryption. IEEE transactions on information forensics and security, 10(3):665–678, 2015..

[6] Jiguo Li, Yao Wang, Yichen Zhang, and Jinguang Han. Full verifiability for outsourced decryption in attribute based encryption. IEEE Transactions on Services Computing, DOI:10.1109/TSC.2017.2710190, 2017..

[7] Jianting Ning, Zhenfu Cao, Xiaolei Dong, Kaitai Liang, Hui Ma,and Lifei Wei. Auditable σ-time outsourced attribute- based encryption for access control in cloud computing. IEEE Transactions on Information Forensics and Security, 13(1):94–105, 2018.

[8] Jianting Ning, Zhenfu Cao, Xiaolei Dong, and Lifei Wei. White-box traceable CP-ABE for cloud storage service: How to catch people leaking their access credentials effectively. IEEE Transactions on Dependable and Secure Computing, 15(5):883–897, 2018.

[9] Alexandros Bakas and Antonis Michalas. Modern family: A revocable hybrid encryption scheme based on attribute- based encryption, symmetric searchable encryption and SGX. In SecureComm 2019, pages 472–486, 2019.

[10] The secure data sharing between user and Cloud resources is implemented using Elliptic curve cryptography and session key management.