International Journal of Science and Engineering Applications
Volume 5 Issue 3, 2016, ISSN-2319-7560 (Online)

Empirical Study on Data Security Privacy: Data Partition for Centric Key Management Cloud

Deepika.P[1], B.V.N.Sai Kumar[1], K.Jhansi[1], K.Lavanya[1], A.V.S.Sudhakar Rao[2]

[1]Department of computer science & engineering, St. Ann's college of Engineering & Technology, Chirala, Andhra Pradesh, India.

[2]Department of Computer Science & Engineering, St.Ann's college of Engineering & Technology, Chirala, Andhra Pradesh, India.

Abstract: The Cloud Computing is a next generation platform, which provides virtualization with resource pool.There are three types of cloud service models, Infrastructure as-a-Service (IaaS), Platform-as-a-Service (PaaS) and Software-as-a-Service (SaaS).Most of the scientific research focus on IaaS model, which manage virtualization and storage. IaaS allows customer to scale based on user demand and user only pays for the resource usage. Data security plays a crucial role in cloud environment and user trust is most challenging problem of cloud services. This project proposed new methodology that secures data and provide privacy to the customer in cloud. Our technique providing security by using data partition approach and that partitioned data will be proceed further parallel for encryption mechanism. Here privacy is given by centric key management scheme.

Keywords: ***Cloud Computing, Encryption, Key Management, Service Models, Algorithm.***

1. INTRODUCTION

Cloud computing is term that describes various type of computing concepts that uses a high number of computers connected via network such as the Internet. In general Cloud computing is a type of computing that depends on sharing computing resources rather than using local servers or personal devices to perform application.

Cloud viewed as the third party, on-demand, self-service that implemented on pay-per-use mechanism and it is scalable computing resources whose services offered by the Cloud paradigm promise to reduce capital as well as operational expenditures for hardware and software.

It classified based on Location of the cloud computing and Type of services offered [1].Based on Location its types are: public cloud,private cloud, hybrid cloud, community cloud. Based ontype of services it's categorized in Infrastructure as a service(IaaS) , Platform as a Service (PaaS) , Software as a service(SaaS). Public cloud is offered by third party service provider and it involves resources that are outside the user premises. Customer has no visibility and no control over the computing infrastructure where it is hosted and this infrastructure is shared between any organizations.

If computing infrastructure is dedicated to particular organization and not shared with other than this setup is private cloud. The hybrid cloud uses hybrid approach.The above classification is well accepted in the industry. David Linthicum [2] shows further classification on the basis of service provided. These are listed below: Storage-as-aservice, Database-as-a-service, Information-as-a-service, Process-as-a-service, Application-as-a-service, Platform-as-a-service, Integration-as-a-service, Security-as-a-service,Testing-as-a-service, Infrastructure-as-a-service.

2. PROPOSED WORK

In proposed security layer, cloud-client data is not just sent to cloud directly instead data processed intelligently and sent to cloud. This mechanism ensures client data security but to provide authentication, before data processed, secure connection between client and cloud is created logically. For providing privacy to client data, we introduce a new way that deal with encryption mechanism and provide privacy to client data. User data is processed in two different passes, in first pass user data is partitioned dynamically and then partitioned encrypted using parallelism.

The limitation of cloud computing are the security issues of cloud computing. It comes to know that there are no security standards available for secure cloud computing.Users has serious concerns about confidential of sensitive information. Privacy is not provided for critical data being processed in the public accessible cloud. The main security problems involve user data privacy, data security, protection, cloud computing administration and cloud computing platform stability. Customers should have the right of the supervision and have audit of cloud computing services for fully ensure the security of customer data.

The data must be protected from virus, worms and Trojan in cloud computing platform within the network of internal and external .We introduced a new security layer between user and cloud as combined three layer (PaaS,IaaS, SaaS) that provide mechanism which deal with user data security, privacy and authentication.

To solve the problem existing we need authentication at both the side. While data sends via internet, any encryption algorithm must secure it. To address authentication we are going to use public key cryptography. Public key cryptography is most common method for authenticating a sender and receiver.

Ravi Shankar Dhakar, Prashant Sharma and Amit Kumar Gupta [3] used the Public Key cryptography. In traditional cryptography, one secret key is used for encryption and decryption at both the side. So if secret or private key is discovered by some else than message can easily be decrypted. For this reason, public key cryptography is most suitable approach on the internet. This public key system is known as asymmetric cryptography.

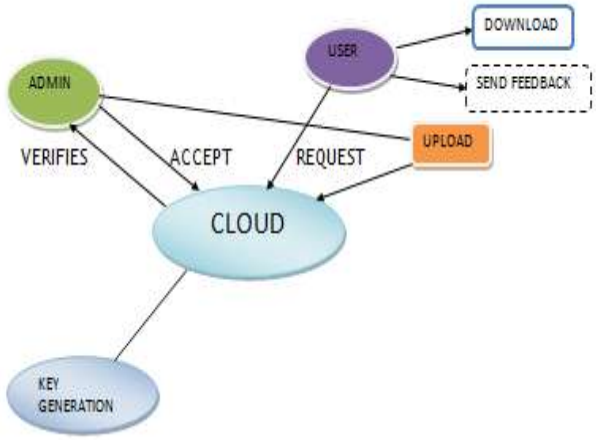
3.SYSTEM IMPLEMENTATION

To solve this problem we need authentication at both the side. While data sends via internet, any encryption algorithm must secure it. To address authentication we are going to use public key cryptography. Public key cryptography is most common method for authenticating a sender and receiver. In traditional cryptography, one secret key is used for encryption and decryption at both the side. So if secret or private key is discovered by some else than message can easily be decrypted. For this reason, public key cryptography is most suitable approach on the internet.

A. Selby and C. Mitchell [4] have proposed two algorithms that are used to implement RSA. The first algorithm performs modular reduction and the other performs modular multiplication. But when the bit size is large, the computation takes a lot of time. This public key system is known as asymmetric cryptography. In public key cryptography, private and public keys are generated simultaneously using the same algorithm by trusted certificate authority. In this system, private key is given to the requesting person means here any customer in cloud. Every customer has a unique private key, which is confidential. Public key is available publicly to everyone. In cloud, whenever customer wants any type of service from service providers he will make a request.

In this request, customer's digital signature is encrypted by private key after that encrypted message again encrypt using receiver's public key. Here cloud service provider is receiver. After receiving this encrypted message first receiver will decrypt by own private key and then decrypt encrypted digital signature by public key of sender. Here customer is sender.Digital signature contains customer name, serial number, expiry date. After decrypting message, cloud service provider easily come to know about their customer. Using this mechanism, we can provide perfect authentication and privacy in cloud environment.

4.SYSTEM ARCHITECTURE



5.CODING

```
<?php
if(isset($_GET['filename']))
{
   $var_1 ="admin/upload/".$_GET['filename'];
$file = $var_1;
 session_start();
  include 'dbconn.php';
            $k1=$_POST['key'];
 echo "<br>";
            $id=$_GET['id'];


  $q=mysql_query("select `encryptfile` from `uploadfiles` where id='$id'")or die(mysql_error());


  $q1=mysql_num_rows($q);
```

```
 $a=mysql_fetch_array($q);
            $k=$a['0'];
 if($k1==$k)
 {
  $a=$_SESSION['user'];
$dt=date('d/m/y');
$q1=mysql_query("select * from download where user='$a' and date='$dt'");
$q=mysql_fetch_array($q1);
$z=$q[2];
if($z>=5)
{
echo "<script>alert('download limit exceed');window.location='downloadfiles.php';</script>";
exit;
}
if (file_exists($file)) {
   header('Content-Description: File Transfer');
   header('Content-Type: application/octet-stream');
   header('Content-Disposition: attachment; filename='.basename($file));
   header('Expires: 0');
   header('Cache-Control: must-revalidate');
   header('Pragma: public');
   header('Content-Length: ' . filesize($file));
   ob_clean();
   flush();
   readfile($file);
$z++;

mysql_query("update download set count='$z' where user='$a' and date='$dt'")or die(mysql_error());

   exit;
}
echo "<h1>Content error</h1><p>The file does not exist!</p>";
exit;
}

}
echo "<script>alert('ENTER CORRECT KEY');window.location='downloadfiles.php';</script>";
?>
```

6.RESULTS

Fig 1: Home page

Fig 2:Registrationpage

Fig 3:Login page

Fig 4:User Download File

Fig 5:Downloading Files

Fig 6:User Feedback

Fig 7:Admin Home Page

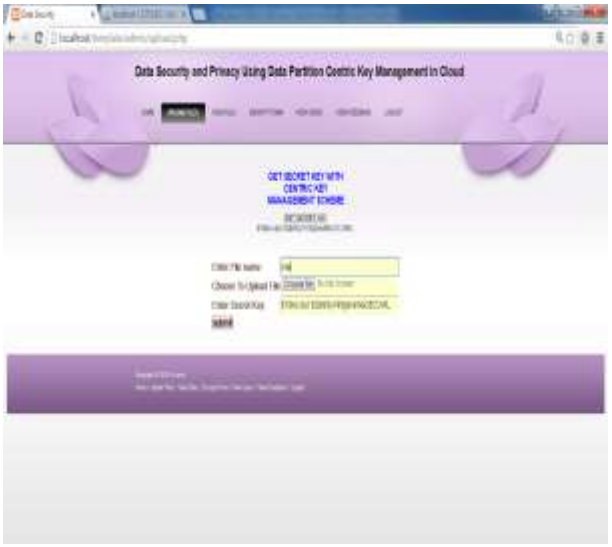


Fig 8:Upload Files

Fig 9:View Upload Files

Fig 10:Encrypt Form

Fig 11:View Users

Fig 12:View Feedback

7.CONCLUSION

This project suggests use of an "asymmetric public key cryptography" algorithm as part of the key management to ensure the authentication between client and service provider. After creating the logical authentic link between client and service provider, large client-data is partitioned and is encrypted in parallel. This project proposes a new way to provide data security, privacy & authentication on different cloud models. Especially in public-cloud model, by introducing a new layer in-between the client and the service provider (i.e. cloud) and also suggests use of an "asymmetric public key cryptography" algorithm as part of the key management to ensure the authentication between client and service provider.

8.FUTUIRE SCOPE

This mechanism provides security to client-data.The partition &encryption of user-data is done on the user side only. This approach raises the power & computational consumption at the user side which is of a great concern. In future the drawback of the project will be implemented as a advantage.

9.REFERENCES

[1]. P. Mell and T. Grance, "The NIST Definition of Cloud Computing Version 15," Nat'l Inst. of Standards and Technology, Information Technology Laboratory, vol. 53, p. 50,http://csrc.nist.gov/groups/SNS/cloud-computing/, 2010.

[2].Dripto Chatterjee, Joyshree Nath, Suvadeep Dasgupta and Asoke Nath. "A new Symmetric key Cryptography Algorithm using extended MSA method: DJSA symmetric key algorithm", 2011 IEEE.

[3] Ravi Shankar Dhakar, Prashant Sharma and Amit Kumar Gupta."Modified RSA Encryption Algorithm (MREA)", 2012 IEEE.

[4]. A. Selby and C. Mitchell. "Algorithms for software implementations of RSA", IEE PROCEEDINGS.

[5] R. Rivest, A. Shamir, and L. Adleman, A method for obtaining digital signatures and public-key cryptosystems , Commun. ACM, vol. 21, pp. 120-126, 1978.

[6] Symmetric key cryptography using random key generator, A. Nath, S. Ghosh, M.A. Mallik, Proceedings of International conference on SAM-2010 held at Las Vegas(USA) 12-15 July, 2010, Vol-2, P-239-244

[7] William Stallings, "Cryptography and Network Security", ISBN 81-7758-011-6, Pearson Education, Third Edition, pages 42-62,121-144,253-297.

[8] Atul Kahate, "Cryptography and Network Security", ISBN-10:0-07-064823-9, Tata McGraw-Hill Publishing Company Limited, India, Second Edition, pages 38-62,152-165,205-240.

[9] R. Curtmola, J. Garay, S. Kamara, and R. Ostrovsky, "Searchable Symmetric Encryption: Improved Definitions and Efficient Constructions," Proc. 13th ACM Conf. Computer and Comm. Security, pp. 79-88, 2006.

[10] M. Abdalla, M. Bellare, D. Catalano, E. Kiltz, T. Kohno, T. Lange,
J. Malone-Lee, G. Neven, P. Paillier, and H. Shi, "Searchable Encryption Revisited: Consistency Properties, Relation to Anonymous IBE, and Extensions," Proc. 25th Ann. Int'l Conf .Advances in Cryptology (CRYPTO '05), pp. 205-222, 2005.

[11] L. Wiese, "Horizontal Fragp098
7entation for Data Outsourcing with Formula-Based Confidentiality Constraints," Proc. Fifth Int'l Workshop Security (IWSEC '10), pp. 101-116, 2010.