ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 4, Issue 4, April 2015

Implementing Multiprime RSA Algorithm to Enhance the Data Security in Federated Cloud Computing

Dr.M.Srivenkatesh [1], Ms.K.Vanitha [2]

Associate Professor, GITAM Institute of Technology, GITAM University[1]

Assistant Professor, Dept.Computer Science, GITAM University[2]

Abstract: Federated Cloud computing is an internet based technology where a large amount of resources are shared as a service among several cloud service providers. Some business organizations using the federated cloud due to the organizational needs. Data Security is very important and critical factor needs to be considered .Different encryption strategies have been carried out for attaining the secure data storage and access security. In this paper, we propose Multi-prime RSA algorithm used for data extraction as requested by sender then forwarded to receiver. The data is decrypted and provided to the receiver.

Keywords: Federated Cloud computing, Multiprime RSA Algorithm.

I. INTRODUCTION

A**.** Federated Cloud Computing

They are some deifications of cloud computing namely Inherently Limited Scalability of Single-Provider Clouds, Lack of Interoperability among Cloud Providers. No Built-In Business Service Management Support .To address these issues Federated Cloud Computing was introduced. Cloud federation brings together different service providers and their offered services so that many Cloud variants can be tailored to match different sets of customer requirements. Cloud provider can provide resources to satisfy complex application request only if he holds infinite resources at his premises. Since this is not the case, so providers need to collaborate to be able to fulfill requests during peak demands and negotiate the use of idle resources with other peers. A federated cloud (also called (cloud federation) is the deployment and management of multiple external and internal cloud computing services to match business needs. A federation is the union of several smaller parts that perform a common action. Scalability-- Cloud bursting to address peak demands .The major advantages of federated cloud computing is

- Scalability-- Cloud bursting to address peak demands
- Collaboration--Sharing of infrastructure between partners
- Multi-site Deployments-- Infrastructure aggregation across distributed data centers
- Reliability--Fault tolerance architectures across sites
- Performance--Deployment of services closer to end users
- Cost--Dynamic placement to reduce the overall infrastructure cost
- Energy Consumption--Minimize energy consumption.

Federated clouds, by providing end to end quality of services, offer many advantages over traditional cloud services, which are:

Guaranteed performance: Due to limited resources, that are available with a single cloud service provider, sudden increase in workload may lead to deterioration of performance. Cloud federation overcomes this disadvantage by hiring resources from foreign cloud service providers, thereby guaranteeing the agreed Quality of Service. Also, high priority processing is guaranteed by delegating low priority processing tasks to foreign cloud service providers.

Guaranteed availability: During unexpected disasters, the cloud system will be able to recover the services by federating with other cloud service providers in unaffected areas. Availability may be guaranteed according to the priority of the service, as disaster recovery may not be an instant process.

Convenience of service cooperation: Cloud federations greatly increase the convenience by providing a one stop solution such that the consumer can see all the services together. For example, while applying for a passport, all the associated services may be integrated as one single service.

Dynamic load distribution: Geographical distribution of clients for every cloud service provider is highly uneven.

Copyright to IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 4, Issue 4, April 2015

In order to provide seamless services, dynamic load distribution is facilitated by cloud federations so that they could rise above their geographical shortcomings.

II. Security in Federated Cloud Computing

Security in Federated Cloud Computing is very important and critical Issues. Our emphasis here is data security. Data requested by user(Sender) and data may be received (Receiver)from singe cloud provider or sender and receiver may be from different cloud providers. Data that needs to be extracted either from single Cloud provider or from multiple cloud providers need to be accurate. That way data security has played very important role in federated cloud Computing.

III. State of Art-literature review

Federated Identity in the Cloud Computing Was described by[1] as about trust and security of cloud computing users, and introduced federated identity as a useful feature for user management and Single Sign-on (SSO) has also become an important part of federated identity environment. Any Misuse of the identity, identity theft, and platform trustworthiness are some of the problems in the federated identity environment. It deals with OAuth, OpenID, SAML are three main concepts in cloud authentication and federated environment. It was discussed the security issues of federated identity in the cloud authentication and highlights the proposed models to solve identity theft in the federated environment.

Another interesting investigation {2] deals with Partitioning applications over set of public and private clouds in order to meet a range of non-functional requirements including performance (for example where private cloud resources alone are insufficient), dependability(e.g. to allow the application to continue to operate even if one cloud fails) and security (for example to ensure that sensitive data is restricted to sufficiently secure clouds and networks) was described in The proposed a novel deployment planning algorithm to partition complex workflow-based applications over federated clouds, while meeting security requirements.

The issue of identity management was addressed in[3[a typical service providers' environment without the need for a trusted third party to federate the user identity for acquainted service providers. It leverage the establishment of trust between cross-domain service providers (SPs) to themselves rather than relying on a third party that brokers the trust between service providers and hence formed network of SPs is then ready to facilitate a typical identity management scenario like a single sign- on (SSO). It also proposed a graph optimization algorithm that reduces the number of edges (connections between SPs) to reduce the overall communication in the network of SPs.

Introduction of SaaS new security challenges is to provide a single sign-on environment for services through an identity provider plus sufficient authorization granularity for backend services for the client applications to access was discussed in[4]. It deals with detailed discussion of the two standards (SAML 2.0 and OAuth 2.0) and presented a study how the two standards (SAML 2.0 and OAuth 2.0) can provide a single sign-on solution for cloud computing.

Identity Access Management (lAM). Companies encounter identity management as security challenges while adopting more technologies became apparent as described in[5]. Single Sign on (SSO) and OpenID has been released to solve security and privacy problems for cloud identity. Both trusted computing based on a hardware TPM chip and trust multi tenancy are great technologies for solving the trust and security concerns in the cloud identity environment. It proposed the use of Trusted Computing, Federated Identity Management and OpenID Web SSO to solve identity theft in the cloud

The organization of the paper is as follows. Section deals with brief introduction and benefits of federated cloud computing and section two gives brief description about security in federated cloud .Section three describes about state of art (Literature review).Section four deals with security issues in federated cloud section five describes the proposed work .Methodology is described in section sex and section seven and eight deals with conclusion & future work and references

IV. Security Issues In Federated Cloud Computing

Security Mechanisms (e.g. encryption) which make it extremely difficult or uneconomical for an unauthorized person to access some information [6, 7].Data security has important and interesting issue in federated cloud computing. Only authorized person need to access the data. If any unauthorized person accesses the data which may involves the loss of data or manipulation of data. So authorized user only is allowed to access the data. In order to have accuracy of data that is be transported among the users and among the cloud service providers we are proposing Multiprime RSA algorithm.

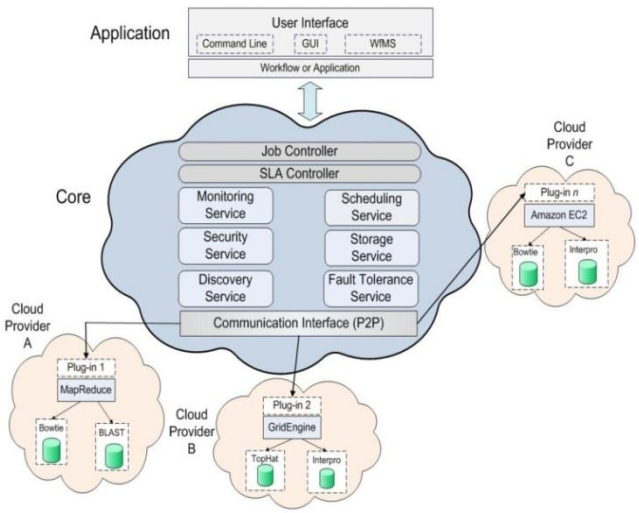


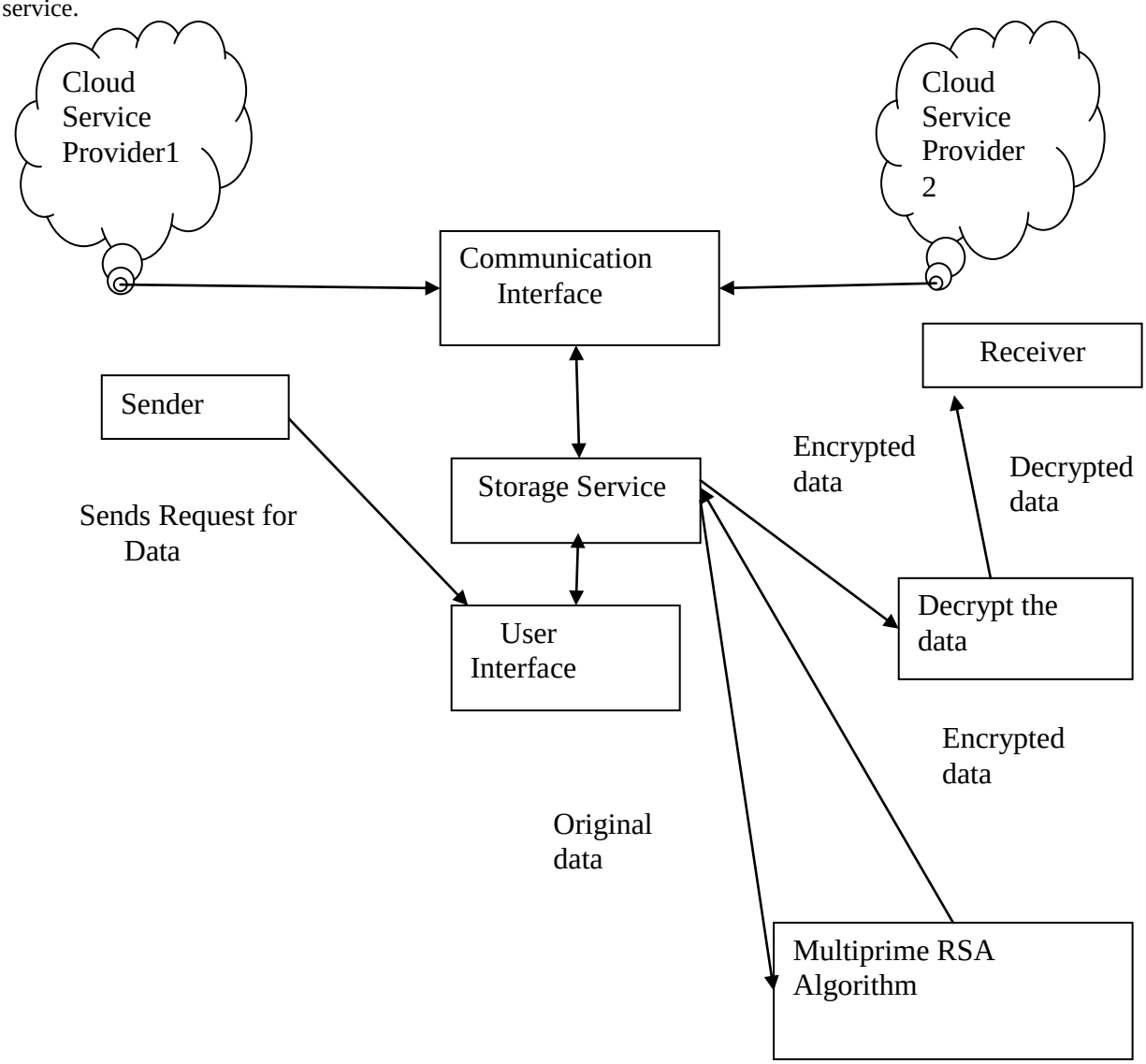
Fig1. A federated Cloud Computing Architecture

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 4, Issue 4, April 2015

V. Proposed Framework

To improve the security of the user's data Multprime RSA algorithm is implemented as a middle secure layer of storage service.



A proposed Architecture

The user who sends data is called sender. The user who receives the data is called receiver. In some cases the sender and receiver are same. In other cases they are different. In our case they are different. That means we have different users one user is sender and another user is receiver. The sender and receiver may be available through singe cloud servicer or multiple cloud service providers. In either of the cases cloud service providers interact through communication interface. It intern accessing storage service which has bidirectional interaction to user interface which is accessed by sender. The user interface accesses the requested data from storage Service through user interface. The storage service uses multi prime RSA algorithm .The multiprime RSA Algorithm generates a public and a private key with the help of randomly chosen prime numbers. The data will be encrypted by using public key and send to the storage service. The private key is kept as secret. The encrypted data is extracted from storage service and sent to the receiver. At the receiver this data is decrypted before it is available to the receiver.

MULTI PRIME RSA ALGORITHM

Multi-prime RSA is an isolated version of RSA cryptosystem. In Multi-prime the modulus consists of more than two prime numbers and the decryption will be speed-up by using Chinese remainder theorem.

Multi-prime RSA is composed of three phases
i)Key Generation
ii)Encryption
iii)Decryption

For any integer, r>= 2, r-prime RSA consists of the following three algorithms.

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 4, Issue 4, April 2015

Key Generation:
Let N be the product of r, randomly chosen distinct primes p1…..pr. Compute Euler's Totient function of $N : \phi(N) \prod_{i=1}^{r} (p_i - 1)$. Choose an integer e, 1 < e <φ(N), such that gcd(e,φ(N)) =1

The pair (N; e) is the public key.
Compute the integer d € ZN such that ed ≡ 1 mod φ(N), here d is the private key[8].

Encryption:
For any message $M \in Z_N$ the cipher text is computed as $C \equiv m^e \bmod N$ [9]

Decryption:
Decryption is done using the Chinese remainder theorem. Let di ≡d mod (pi-1). To decrypt the cipher text C, one can first computes $M_i \equiv C_I^d \bmod p_i$ for each i, 1<= i<=· r, then combines the M_I's using the CRT to obtain $M \equiv C^d \bmod N$

VI. METHODOLOGY

In completing these objectives, our work will provide the following contributions:
In sender sends the query to the storage service of Federated cloud. Depends on the query the storage service responds to the cloud service provider with the corresponding file. Before this process, the authorization of sender step is involved. In the storage service, it checks the sender name and its password for security process. If it is satisfied, the queries are received from the sender, the corresponding files are searched in the database. Finally, the corresponding file is retrieved which will be send to the receiver

In the second phase, virtual setup is configured. Since virtual machines are dynamic, they can quickly be reverted to previous instances, paused and restarted, relatively easily. Virtualization technology allows the sender to run multiple operating systems simultaneously on a single physical machine sharing the underlying resources. The sender subscribed applications are stored in the storage service of federated cloud computing

VII. Conclusion And Future Work

Security is the major concern in all the emerging technology because users often work with sensitive data. The federated cloud computing is an emerging technology, but to better use of technology we need to block the security holes. The storage service can keep their data secret only if they are having proper security policies. To achieve this we implemented this technique. Encryption plays a vital tool in preventing threats to preserve the data integrity.

In future, we will try to concentrate on more Confidentiality issues in federated cloud computing.

REFERENCES

1. Eghbal Ghazizadeh, Mazdak Zamani,jamalul-lail Ab Manan,Abolghasem Pasang," A Survey on Security Issues of Federated Identity in the Cloud Computing",IEEE 2010.
2. Zhenyu Wen, Jacek Cała, Paul Watson, "A Scalable Method for Partitioning Workflows with Security Requirements over Federated Clouds",
3. Makarand V. Bhonsle, Nayot Poolsappasit and Sanjay K. Madria," ETIS – Efficient Trust and Identity Management System for Federated Service Providers,IEEE computer society 2013.
4. Tim Reimer, Phil Abraham, and Qing Tan, "Pattern for Cloud Computing",
5. C. Saravanakumar, C. Arun, "Survey on Interoperability, Security, Trust, Privacy Standardization of Cloud Computing", IEEE 2014.
6. John Townsend ,"Beyond Boundaries Learning to Trust Again in Relationships, September 2011+.
7. Qing Zhang, Ting YU and Keith Irwin, "A Classification Scheme for Trust Functions in Reputation-Based Trust Management", japan 2004.
8. Suganya , N.Boopal , Naveena , "Implementing Multiprime RSA Algorithm to Enhance the Data Security in Cloud Computing", Vol. 4, Issue 1, January 2015.
9. Esh Narayan,Mohit Malik,Aman preet singh and Prem Narain "To Enhance the Data Security of Cloud in Cloud Computing using RSA Algorithm" International Journal of Software Engineering vol.1 No.1 sep 2012.