Data Security and Privacy using Data Partition and Centric key management in Cloud

Mr. Krunal Patel
M.Tech CSE-SCSE
Vellore Institute of Technology
Vellore, India

Prof. Sendhil Kumar K.S
Assistant Professor(Sr)- SCSE
Vellore Institute of Technology
Vellore, India

Mr. Navneet Singh, Mr.Kushang Parikh
M.Tech CSE-SCSE
Vellore Institute of Technology
Vellore, India

Dr. Jaisankar N.
Professor -SCSE
Vellore Institute of Technology
Vellore, 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 research paper 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.

I. 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 on type 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.

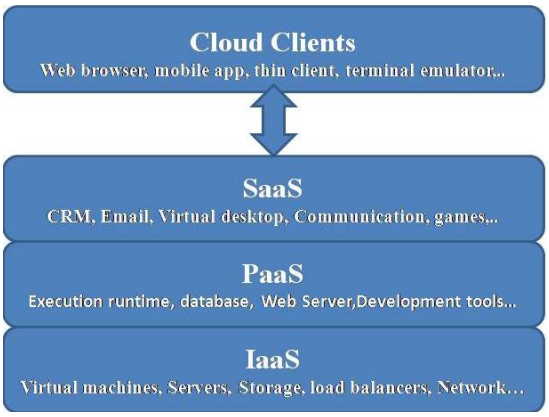

Fig.1 Service Layers of Cloud Environment

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 [4] shows further classification on the basis of service provided. These are listed below: Storage-as-a-service, 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.

II. RELATED WORK

SeongMinYoo et al [2] proposed a user-centric key management scheme which enables the user to store the key fragment and enables only user to use the encryption key since optional key fragments are stored in a dispersed

ISBN No. 978-1-4799-3834-6/14

manner. There is a problem that encryption key may be leaked by intruder who have acquired the mobile device which is lost by any user.

Wu Suyan, Li wenbo , Hu Xiangyi [3] proposed hardware in which hardware equipment has the functions of creating symmetric key by combining key seed matrix with combined symmetric key algorithm and digital signature.

Dripto Chatterjee et al.[4] proposed a new symmetric key cryptography method for encryption and decryption of any file. They have used a random key square matrix containing 65536 elements but still the hackers can find the actual key matrix. Also for a large sized file, a lot of time will be consumed.

Neeraj Khanna et al.[5] have used a bit manipulation method for symmetric key cryptographic method, which includes bit exchange, right shift and XOR-operation on the incoming bits. But they have used a key matrix of size (16x16)which can be easily intercepted by intruders and also the encryption method have not full proof.

Niraj Kumar et al.[6] proposed a new 32-bit encryption and decryption asymmetric-key algorithm, which is developed for secured data transfer in form of small &large files. However, the security concern still remains in this approach.

Thongpon Teerakanok et al [7] introduce a new asymmetric-key cryptography algorithm, which gives the system in encryption and decryption process. In addition, it strengthens the system against Brute force attack but there are few areas of concern in key agreements and limitation of the number of key, which need to be maintained in-group.

A. Selby and C. Mitchell [8] 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.

Ravi Shankar Dhakar, Prashant Sharma and Amit Kumar Gupta [9] used the Public Key cryptography. Here two different keys are used. In this, no other key can decrypt the message, not even the original key that is used at first time encryption. However, this algorithm still has not given a complete secure plan against the brute force attack. Bin Liu and Bevan M. Baas [10] proposed parallel AES encryption engine for multi-core machine. This parallel AES algorithm we can use in our proposed technique.

III. MOTIVATION

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 [11].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 [13].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.

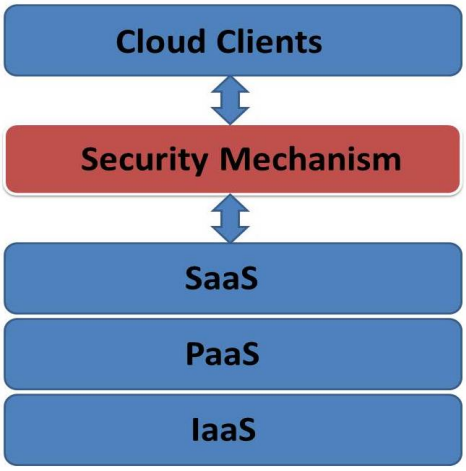

Fig.2 New Proposed Layer in cloud environment.

ISBN No. 978-1-4799-3834-6/14

IV. PROPOSED METHOD

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.

In real time scenario of cloud service, customer satisfaction about trust of data is most important thing. Whenever customer wants any type of a service by cloud providers, he always communicates via internet. To secure data our method is most appropriate. Now here problem is how customer comes to know that he communicates with only his cloud provider and vice versa.

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. 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.

Public and private keys are generated by RSA algorithm.RSA is developed by Ron Rivest, Adi Shamir and Leonard Adleman in 1978 at MIT. This algorithm is best known public key cryptosystems for key exchange and digital signature or encryption of blocks of data.RSA algorithm has a strong mathematical procedure and so far theoretically cannot be broken in acceptable time.

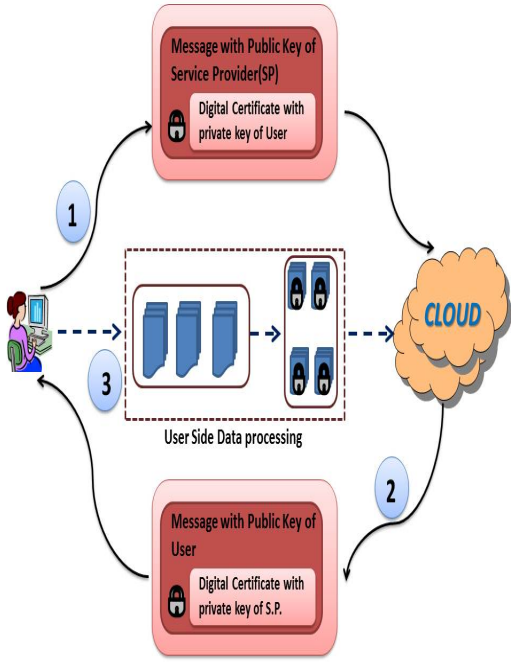

Fig.3 Proposed mechanism

A. Data Partition

Instead of encrypting large data and sending over network, first partitioned data and then sending it over communication link i.e. internet provide two layer security i.e. intruder cannot analysis whole data at time easily but can able to analysis only part of data. Other big advantage is making this new approach feasible in real world by doing encryption of the small partitioned data in parallel manner instead of a large data and this takes less time, which is a primary requirement for real time system.

ISBN No. 978-1-4799-3834-6/14

When data reaches on cloud side, it is decrypted and merged into its original form. The most common user-data are files and database. File is type of unstructured data (because it may contain pictures, text document.). Hence, it cannot be split easily. This kind of data can only be partitioned using cryptographic methods described in [14],[15],and [16] Whereas the second approach recommended by this paper is to use the tool, which performs big data analysis like hadoop (which perform on unstructured data in parallel manner and save time and efficiency). As the Database is a structured data, organized in columns and rows, there are several techniques that handle partition of database. Most common is horizontal fragmentation and vertical fragmentation of database [17]. In vertical fragmentation, the column is distributed as service provider cannot identify relationship by its own. However, for real-world applications, it is an impossible task to find such a fragmentation without user involvement. one approach is first, new relations can be learned by performing transitive combination of existing ones. Then, some relations can be deducted using external knowledge. For example, student health record, might be fragmented into two parts, e.g., (name, registration number, medication) and (registration_ number, disease), the first this mechanism learns about the relation (registration_ number, medication), it has technically still no knowledge about the patient's disease. However, with pharmaceutical background , it can derive the disease from the medication. This type of Artificial intelligence can split data vertically without user involvement. In [18] author describes Vertical partitioning of relational OLTP databases using integer programming. In [19] author shows an enhanced grouping algorithm for vertical partitioning problem in DDBs. database can be partition row wise called vertical partition. In [20] [21] and [22] author suggest some partitioned algorithm that give better performance and also used clustering technique. Finally, partitioned data is fed to the encryption algorithm, which encrypts the partitioned data in parallel mode. Hence, encryption is parallelized and saves time, which is a critical requirement in this real world.

B. Encryption

This paper used symmetric key encryption algorithm, which uses client's private key. Hence, client data is provided privacy as no one can decrypt it other than client itself. After creating an authentication link between user and service provider, service provider generate a secure key and again using the same asymmetric key encryption algorithm to sent it to user. This key is worked as private key for that client who is required in encryption algorithm to encrypt partitioned data. So no one other than service provider and client can read (decrypt) actual data. In this manner, the privacy is provided.

This is recommended that partitioned data will encrypted by Advanced Encryption Standard [10]. Reason for using AES is, partitioned user data still large in size and its take long time to encrypt it by any symmetric key encryption algorithm, but it is found that AES is parallel in nature and give better performance by encrypting data in parallel.[10] Today most of Customer's system has multi-core architecture so its time to take better use of it by performing computation in parallel.

V. CONCLUSION & FUTURE WORK

As it was known that in cloud computing, security challenges are still persistent especially in public-cloud computing. This research paper 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). This paper 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. By using this data partition approach, considerable amount of time

ISBN No. 978-1-4799-3834-6/14

is reduced because all the partitioned data is encrypted in parallel. This paper recommends the use of Advanced Encryption Standard (AES). Finally the encrypted partitioned data is sent to the service provider. This mechanism provides security to client-data. When the authentic link is created, service provider sends a key to the client by using asymmetric cryptography key technique. This key is only known to the service provider and the user itself which behaves as a private key. The encryption algorithm uses the private key, so that no user can decrypt the confidential data other than the actual user and the service provider.

The drawback of this proposed work is that 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.

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] SeongMin Yoo, Pyung Park, JinSeop Shin, JinSeok oh, HoYong Rya, JaeCheol Ryou. "User-Centric Key Management Scheme for Personal Cloud Storage" ,2013 IEEE

[3] Wu Suyan, Li wenbo and Hu Xiangyi. "Study of Digital Signature with Encryption Based on Combined Symmetric Key", 2009 IEEE.

[4] 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.

[5] Neeraj Khanna, Joyshree Nath, Joel James, Amlan Chakrabarti, Sayantan Chakraborty, Asoke Nath. "New Symmetric key Cryptographic algorithm using combined bit manipulation and MSA encryption algorithm: NJJSAA symmetric key algorithm", 2011 IEEE.

[6] Niraj Kumar, Pankaj Gupta, Monika Sahu and Dr. M A Rizvi. "Boolean algebra based Effective and Efficient Asymmetric Key Cryptography Algorithm: BAC Algorithm", 2013 IEEE.

[7] Thongpon Teerakanok and Sinchai Kamolphiwong. "Accelerating Asymmetric-Key Cryptography using Parallel-key Cryptographic Algorithm (PCA)", 2009 IEEE.

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

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

[10] Bin Liu and Bevan M. Baas. "Parallel AES Encryption Engines for Many-Core Processor Arrays". IEEE transaction on, March 2013.

[11] Farhan Bashir Shaikh, Sajjad Haider "Security Threats in Cloud Computing" Department of Computing & Technlogy SZABIST Islamabad, Pakistan Shaikh.farhan@live.com ,Sajjad Haider ITS Department NUML Islamabad. http://ieeexplore.ieee.org/xpls/icp.jsp?arnumber=6148380

[12] http://thecloudtutorial.com/cloudtypes.html

[13] Wentao Liu," Research on Cloud Computing Security Problem and Strategy "Department of Computer and Information Engineering, Wuhan Polytechnic University, Wuhan Hubei Province 430023, China. uddisoap@gmail.com.

[14] S. Kamara and K. Lauter, "Cryptographic Cloud Storage," Proc. 14th Int'l Conf. Financial Cryptography and Data Security, pp. 136-149, 2010.

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

[16] 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.

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

[18] Rasmus Resen Amossen,"Vertical partitioning of relational OLTP databases using integer programming" IT Univ. of Copenhagen, Copenhagen, Denmark. http://ieeexplore.ieee.org/xpls/icp.jsp?arnumber=5452739

[19] Marir, F. ; London Metropolitan Univ., London ; Najjar, Y. ; AlFaress, M.Y. ; Abdalla, H.I. "An enhanced grouping algorithm for vertical partitioning problem in DDBs" http://ieeexplore.ieee.org/xpl/articleDetails.jsp?arnumber=4456833

[20] Shao Xiufeng Department of Soft and Information Management BeiJing City University Beijing, China "Improved CURE Algorithm and Application of Clustering for Large-scale Data"

[21] Rehab F. Abdel-Kader ,"enetically Improved PSO Algorithm for Efficient Data Clustering" Electrical Engineering Department, Faculty of Engineering - Port-Said Suez Canal University, Port Fouad 42523, Port-Said, Egypt E-mail**:** r.abdelkader@scuegypt.edu.eg

[22] Ajit M. Tamhankar and Sudha Ram, *Member, IEEE* "Database Fragmentation and Allocation: An Integrated Methodology and Case Study"

ISBN No. 978-1-4799-3834-6/14