ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 1, January 2015

A New Cloud Paradigm: Data Protection as a Service (DPASS)

KholeSagar R. [1],Walunj Ajit S.[2],Gulave Rahul K.[3],Nikam Umesh P.[4]

Student, Department of Computer Engineering, SavitribaiPhule Pune University, Shri Chhatrapati Shivaji College of Engineering, Shrishivajinagar, India[1234].

ABSTRACT: The Paper consist of new cloud computing pattern, data protection as a service (DPASs) which is a suite of security primitives by a cloud platform, which having data security and privacy and which provide powerful proof of privacy for data owners. Despite in the presence of strongly compromised or unsecured application. Such as security of data using encryption, logging, key management. Due to this new model of security user can get the confidence that there data which store on cloud is being handle very security. The result show that user that can get notification about the security of their data which is store on the cloud platform.

KEYWORDS: AES, Logging, Key management, Cloud Computing, Auditor.

I. INTRODUCTION

As Cloud Computing has become important and simple to implement. Many multinational companies and topmost companies are coming towards for achieving the cloud features for the best management and increasing scalability of their organization. Cloud computing offers random scaling, easy to maintain and availability of services anytime anywhere. Cloud computing offers on demand, higher quality data storage services. But there is most important factor that everybody is worried about the cloud computing is the security problem. Since all the data are stored in cloud platform data owners are worried about the security

Uptil now cloud computing environment providers such as google, amazon web servers gogrid etc. had implement the cloud platform with the help of there cloud service model or cloud service stack such as Pass (Platform As a Service), Iass (Infrastructure As a Service), and Saas (Software As a Service). This are there cloud computing models which are implemented in previous cloud computing environment. But the security provided by this three models that matter the privacy issue and also the misuse of data. Also the current survey which is taken by Microsoft corporation about the cloud security has found that “58 percent of the public and 86 percent of business tikun are excited about the possibility, security and privacy of their data as it the data stored in the cloud.

Therefore to overcome this issues, we propose a new cloud computing paradigm, Data protection as a service (DPaas). Dpaas is new model of security primitives offered platform which enforce data security, privacy and offers proof of privacy to data owners. Dpaas provided fined-grained access control polices on data unit through application confinement and information flow checking. It employs cryptographic protections at rest and offers robust logging and auditing to provide accountability crusially, DPaas also directly addresses the issue of rapid development and maintenance. Therefore this DPaas security approach provides security alert message, to the user, when the data is accessed by unauthorized person which is stored on cloud environment.

II.RELATED WORK

Firstly in 2003, “The language based information flow security” proposed by Andrei Sabelfeld and Andrew C. Myers, They suggested that the conventional security mechanism such as encryption and access control do not directly address the enforcement of information flow polices. A providing new approach has been developed for specifying and enforcing information flow polices. Also they survey the pass there decades of research on information flow security.

10.15680/ijircce.2015.0301032

Particularly focusing on work that uses static program analysis of enforce information flow polices.Also in 2009, “Data protection aware design for cloud computing” which implemented by Sadie-creese and their team concluded that to begin the process of designing the data protection control into cloud from the Outset, so as to avoid the associated with bolting on security as on after through. This model to explore privacy maturity within an enterprise cloud developement & explore when, where there may be opportunity to design in data protection control as exploitation of the cloud matures. Also for security cloud environment the encryption algorithm i.e DES (Data Encryption Standard), which is used to protect the sensitive information as federal information processing standard. But the principle of the DES is that, it has three times as many round. Hence it is time consuming process therefore it is not favourable for long term use. Therefore Rijndael proposes the encryption standard that is the advanced encryption system (AES) in 2001. The AES algorithm provide more security to the cloud platform.In 2012, Dawn song & her team published the paper "Cloud Data Protection for the Masses" in IEEE computer society. They proposed that the new cloud security model i.eDPaas, which builds the cloud platform architecture that dramatically reduces per application developement effort required to data protection while still allowing rapid development&maintainance.

III. EXISTING WORK

Cloud computing is the type of computing that realise on the sharing of resources rather than having local servers or personal devices to handle the application .The cloud computing is the model to delivering information technology services in which the resources are retrieved from the internet through the hundreds of millions of application. In the previous cloud computing system platform is build with help of three cloud service models such as Paas(Platform as a service), Saas(Software as a service), Iaas (Infrastructure as a service).This three models deliver software application over the web build the infrastructure for the cloud & create the platform for the entire application developement environment, not only just the use of an application. But this models having issues related with the compatibilty with hardware & operating system, also it have to do extra work to maintain the system & to maintain the integrity of the database.

If the users data which is stored on cloud platform can be access by any unauthorised person then user can not get any immediate alertness about the misuse of data. Due to this more than 90 percent of public & business leaders are worried about security, availability, and privacy of their data as it rests in the cloud. Therefore the security becomes the major issue in this previous cloud computing platform.

IV. PROPOSED WORK

For the more security required for the cloud platform we need to build the strong security & need to protect the cloud services from large number of malicious application and avoiding unauthorised accesses.

This paper proposed the new cloud computing pattern i.e the DPaas which consists of security primitives offered by cloud platform. This platform enables the verification of the cloud environment operation, so the user can get confidence about their data that is being handle securely , also DPaas is a provision of data security & privacy, that offers proof of privacy to data owners even in the presence of malicious application ,so the system have the large number of scope such as all the users are managed by the admin of the system. The uploaded data can be viewed by the auditor & user itself. Every data requires unit data key so the encryption provided in high quality. If the user data can be change by any unauthorised person or the auditor itself then the user get the security alert message & user immediately alert about their data which is stored on cloud environment. To truly support this vision, cloud platform providers would have to offer DPaaS in addition to their existing hosting environment, which could be especially beneficial for small companies or developers who dont have much in-house security expertise, because DPaaS can guarantee the integrity of the data at rest via cryptographic authentication of the data in storage and by auditing the application code at runtime.Therefore the propose system build successfully by implementing security but not affecting performance.

V. SYSTEM DESIGN AND IMPLEMENTATION

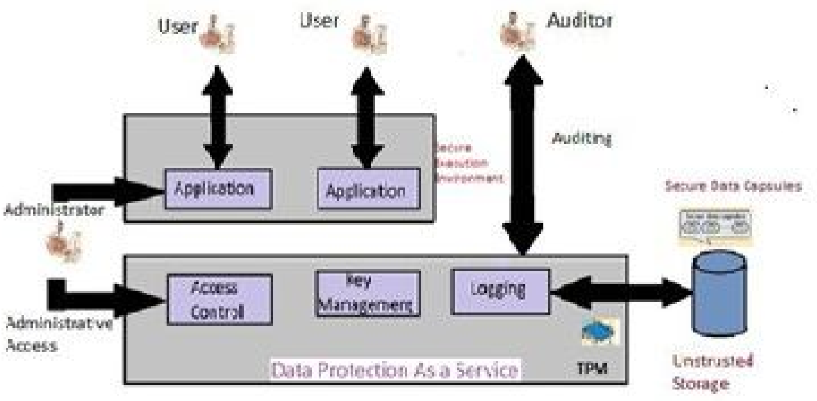

Figure : System Architecture

The figure illustrates architecture for the elaborating DPaas design implementation .Here each server has the Trusted platform module(TPM),Which acts as the cryptoprocessor which can encrypt the each of the data bit before it going to the database. Above architecture depicted that at a high Level how the system make the possible to combine the various technologies such as logging ,encryption and information flow checking to realize Dpaas .

Generally the system architecture consist of four main modules which plays an important role to maintain and handle the data over the cloud environment. The main module of our system is cloud computing which is a provision of dynamically scalable services over the internet. This cloud computing model is responsible for storing the user data also another module that is TPM which is responsible for encrypting data .There is an important module i.e. Auditor who tracking all the transaction and all the conversation Between the users so multilevel data security provided by the architecture .the user module from the user section allows the user to store the large amount of data in cloud and access data using secure key.Secure key provided by admin while encrypting the data .the above architecture exhibits the some key.

PERFORMANCE is monitor and loosely coupled architecture using web services .
SECURITY:cloud architecture improves due to centralization of data increase security focus resources.
MAINTENANCE: maintenance of cloud computing architecture is easier because they do not need to be install on each user computer and can be access from different places.
RELIABILITY: in this architecture reliability is improved if multiple redundant sites are used which makes well design cloud computing ,which is suitable for disaster recovery .
MULTITENDANCY: That enable sharing of resources and cost across large pool of users .
VERIFIABLE ARCHITECTURAL SUPPORT :It is necessary to fix the error also information is to be migrated and updated as architecture change .The computation which process of line that is valuable for data aggregation across hundreds of millions of users for pecompilationvaluale function . To reduce the risk of unauthorized backdoor access ,all the function should be subject to same authorization flows and platform level check as normal request .

VI. ENCRYPTION OVERVIEW

Encryption is the process of converting of plaintext into cipher text. Encryption is a track to keep secure data by using mathematical transformations on a secure data by using mathematical transformation on a sequence of bits. This transformation use a applied sequence of bits known as a key. There are two types of key i.e public key and private key. The public key uses for encrypt the data and private key used for decrypt the data.

In this paper provide better security on cloud by using Advanced Encryption Standard 128 bits of Rijndael algorithm because as compared to the other 64 or etc. it provide more security. The 128 bit encryption completed In the 10 encryption round. In 128 bit Rijndael algorithm different operation are used that is shift rows , mix columns, sub bytes and add round key. The AES algorithm is selected for several reason. The encryption core will need to provide a wide range of application will be based to encrypt large amount of data. The AES algorithm is based on simple mathematical transformation whose inverse are difficult to compute without the key.In above figure shows there are four transformation used for encryption that is sub bytes , shift rows, mix column and add round key. Each of these transformation are uses in each round. In this paper key size of 128 bit there are 10 rounds. In additional time in round 0. The last round 10 that is the mix column transformation round doesn't performed.

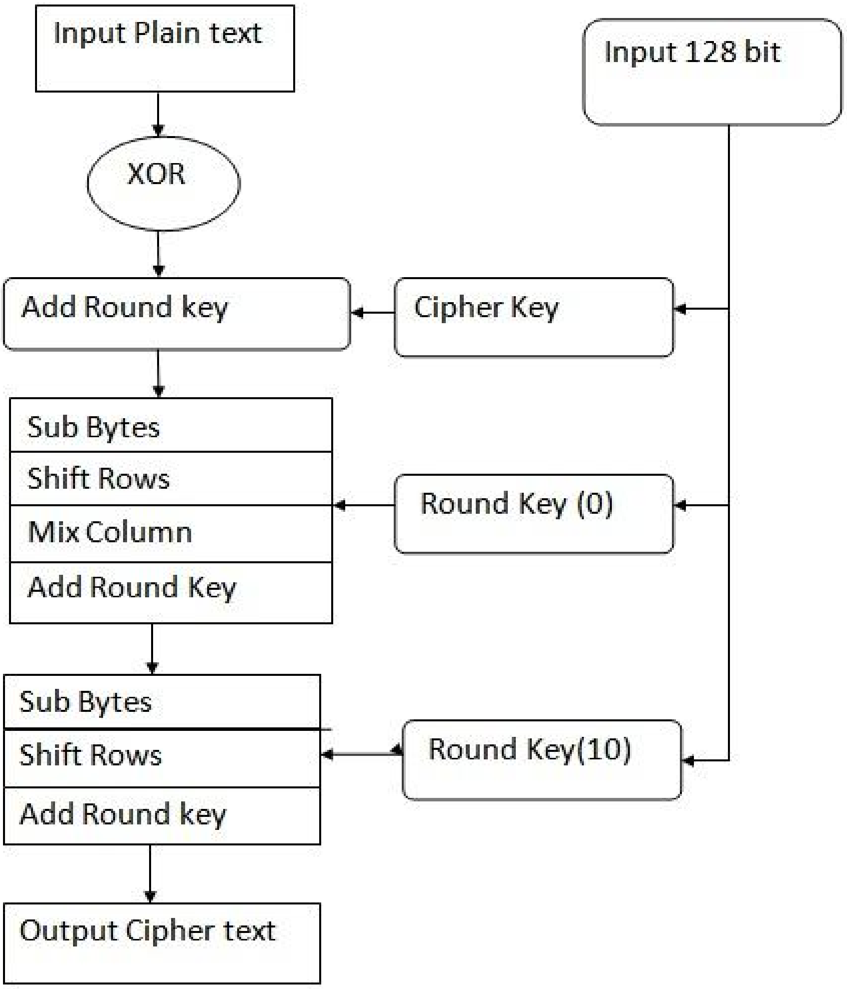

Figure:Round Structure of 128 Bit AES

VII. RESULT AND ANALYSIS

We made experimental in terms of checking the attributes of data protection as a service.which is one of the service module of cloud computing. according to this paper the security mechanism are applied to all cloud users the service model implemented in this paper is not user specific,instead it treats every user alike and provide security to data automatically as a service.

1) File encrypted.
2) Auditor change or modified the data containing in the file.
3) User view the notification of file.

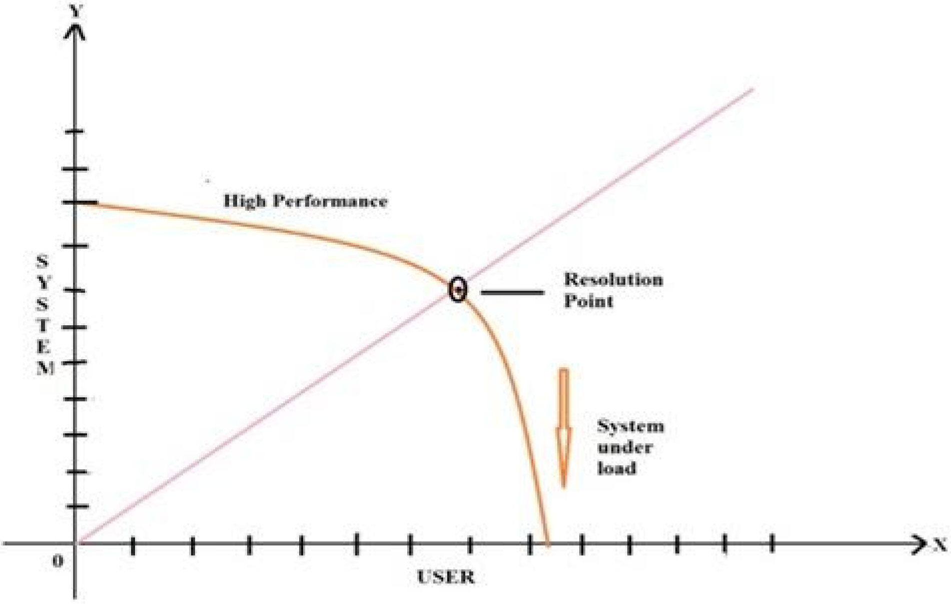

Fig : System Performanance Graph

The system graph shows the system versus user. it indicate the system performance is less or high. X –Co-ordinate line is indicate the percentage of user and the Y line co-ordinate show the performance of the system. the middle point is called as the resolution point. the resolution point means the point at which the system user meets the requirement. if the number of user increases then the system performance decreases. under the resolution point system performance decreases i.e the system under load.Above the resolution point the system performance high. In the previous system user does not get notification to the user.i.e by whom access there own data stored on the cloud.the DPAS system provide the notification the file is changed or not.

VIII. ACKNOWLEDGEMENT

We are profoundly grateful to Prof.Gade D.P. for his expert guidance and continuous encouragement throughout to see that this project rights its target since its commencement to its completion. We are also grateful to Prof. Dighe M.S. (Project Coordinator) for his support and guidance that have helped us to expand our horizons of thought and expression.We would like to express our deepest appreciation towards Dr.Sathe Y.U., Principal, SCSCOE, Shrishivajinagar, Prof.Jadhav H.B, HOD Computer Engineering Department, whose invaluable guidance supported us in completing of this project.At last we must express our sincere heartfelt gratitude to all friends and staff members of Computer Engineering Department who helped us directly or indirectly during this course of work.

IX. CONCLUSION AND FUTURE WORK

Due to increasing need for secure data storage a more safe and secure DPASS module has to be proposed.in previous paper we implemented a new data protection as a service module for provide the security to the data store on the cloud.By using the AES algorithm we provide the powerful security as compare to the previous DES algorithm.due to this new security model there is a possibilities of provision of security alert message to the user.

REFERENCES

1. Dawn Song, Elaine Shi, and Ian Fischer **“Cloud Data Protection for Masses"**,Published by the IEEE Computer Society, 0018-9162/12 ,JANUARY 2012.
2. SunumolCherian, KavithaMurukezhan\Providing Data Protection as a Service in Cloud Computing"International Journal of Scientic and Research Publications, Volume 3, Issue 6, June 2013 1 ISSN 2250-3153.
3. C.HariHar , Prof. Mrs.Varshapriya J.N. \Cloud Data Storage Protection For The Masses, ",International Journal,May- 2014 Volume 1, Issue 3.
4. P. KiranRao , V. Lakshmi Sailaja , Alfisha Khan , S. Mamatha\High level security in cloud for scalable data, *International Journal of Advanced Research in Computer and Communication Engineering ,Vol. 2, Issue 3, March 2013.*
5. Craig Gentry Stanford University and IBM Watson cgentry@cs.stanford.edu, Fully Homomorphic Encryption Using Ideal Lattices.
6. Andrei Sabelfeld and Andrew C. Myers, Language-Based Information-Flow Security, IEEE JOURNAL ON SELECTED AREAS IN COMMUNICATIONS, VOL. 21, NO. 1, JANUARY 2003.