Review on A Novel Protection Scheme for Cloud Environment

[1] Rajashri G. Deshmukh,[2] Prof. V. B. Bhagat,[3] Prof. K. K. Chhajed
[1]ME CSE IInd yr, [2]Assistant Professor, [3]Assistant Professor
[1],P. R. Pote College of Engineering, Amravati, India

Abstract— The aim of Cloud Computing environment is to provide low cost, reliable, rapid, on-demand services to the users anywhere and anytime. But with its rapid development the security challenges are numerous. The evolution of Cloud computing makes the major changes in computing world as with the assistance of basic cloud computing service models like SaaS, PaaS, and IaaS an organization achieves their business goal with minimum effort as compared to traditional computing environment. On the other hand security of the data in the cloud database server is the key area of concern in the acceptance of cloud. It requires a very high degree of privacy and authentication. Unsecure practices by cloud service providers (CSP), dependency on web based service delivery and cloud technology related vulnerabilities could lead to application and data compromise. These threat scenarios require cloud customer to look for more transparency and controls. The core component for hosting web applications is the web application server, but to produce secure, reliable, high performance architecture. This system will design cloud based hosting in which file manager will process web content. The web data will be protected by using encryption. The security control used in this system is IP grabber in which it keeps track of IP addresses of all users system. It also provides another technique for scanning a bugs and vulnerabilities in web application

Keywords—Cloud Computing, Security, Web Hosting, Encryption, IP Grabber, Vulnerabilities.

I. INTRODUCTION

Cloud computing is an innovation methodology for giving pay per utilize access to a gathering of shared resources for specific systems, stockpiling, servers, administration and applications, without physically getting them. Cloud computing is a totally web based innovation where customer information is put away and kept in the server farm of a cloud supplier like Google, Amazon, Salesforce.com and Microsoft and so on. Constrained control over the information may acquire different security issues and threats which incorporate data breach, unreliable connectivity, sharing of resources, data accessibility and inside attacks. A breach of security may lead to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored or otherwise processed [10]. Data security has consistently been a major issue in information technology. In the cloud computing environment, it becomes particularly serious because the data is located in different places even in the entire globe. Data security and privacy protection are the two main factors of user's concerns about the cloud technology. Though many techniques on the topics in cloud computing have been investigated in both academics and industries, data security and privacy protection are becoming more important for the future development of cloud computing technology in government, industry, and business[2]. The Effective Privacy Protection Scheme is proposed to provide the appropriate privacy in cloud environment by using some techniques. This will provide data security by using encryption and other techniques like IP grabber and vulnerability scanner.

II. CLOUD COMPUTING OVERVIEW

Cloud Computing is a rising field in the history of computing. It is a way to maximize the capacity and capabilities without spending a lot to buy a new infrastructure and software. When users are online, they can get faster access to their data due to the massive storage. Although Cloud computing has many advantages due to large number of organizations moving towards it, it comes up with lots of security issues and breaches faced by both cloud service providers and users[11] .Cloud Computing is a set of IT Services that are provided to a customer over a network and these services are delivered by third party provider who owns the infrastructure. It is often provided "as a service" over the Internet, typically in the form of infrastructure as a service (IaaS), platform as a service (PaaS) and software as a service (SaaS) [8].

In the cloud computing environment, both applications and resources are delivered on demand over the Internet as services. Cloud is an environment of the hardware and software resources in the data centers that provide diverse services over the network or the Internet to satisfy user's requirements. The explanation of "cloud computing" from the National Institute of Standards and Technology (NIST)[6] is that cloud computing enables ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. Thus, cloud computing provides a convenient on-demand network access to a shared pool of configurable computing resources [2].

Security Issues:

Security issues are the most concerned challenges in cloud computing [9]. This is very important because the cloud service provider must ensure that the users is not facing any serious problem like data loss and data theft which may cause a great loss

depending on the sensitivity of the data stored in cloud. A malicious user may pretend to be the legitimate users and infecting the cloud.
-Identification and Authentication
-Access control
-Data integrity
-Encryption /Decryption
-Availability
-Resource Allocation

Security Challenges:
Cloud Computing represents one of the most significant shifts in information technology many of us are likely to see in our lifetimes. Basically the major challenge for employing any efficient security scheme in CC is created by the tasks expected from the clouds. Security schemes look like a defense tool which every organization needs [15]. However there are some challenges the organizations face while deploying a security system in Cloud computing. Some of them are:
-Abuse and Vicious Use of Cloud Services
-Data Loss
-Malicious Activities
-Insecure API's

III. EXISTING SYSTEM

In cloud computing services, customers are worried about moving their sensitive data and applications from their own private computing environments to a cloud environment which is shared by different users and which is usually accessible via a public network. Data stored in the cloud can be retrieved at any time from any place as long as there is network access. By partaking storage and networks with many other users it is also possible for other unauthorized users to access the data. This may lead to felonious act. To solve the problem of leverage encryption technology is traditional Public Key Encryption (PKE).The resulting work ciphertext can be decrypted by a valid receiver with secret key and security device. To support revocability, employ re-encryption technology such that the part of cipher-text for an old security device can be updated for a new device if the old device is revoked. Meanwhile, need to generate a special key for the above cipher-text conversion. Also guarantee that the cloud server cannot achieve any knowledge of message by accessing the special key, the old ciphertext, and the updated ciphertext. Further use hash-signature method to "sign" ciphertext such that once a component of cipher-text is tempered by the adversary, the cloud and ciphertext receiver can tell.

Comparison factor/paper	**Greveler et al.**	**H.Liu et al.**	**J.K Liu et al.**
Access Control	Fine grained	Attribute based	Fine grained
Encryption	XML Encryption	Proxy Encryption	Yes
Policy	XACML policy	No	Two Factor Authentication

Table 1: Comparison of protection schemes

Data place the major role in the concerned cloud arena. Security issues are arise because of lack in providing secure storage service. Some researchers define and derive some models to preserve the privacy of cloud data storage. The models are as follows:
Greveler et al. designed a Privacy preservation model to protect cloud data [16]. The machine readable rights and expressions are needed for accessing the data. That is a database is created with set of controls such as roles for users, are defined at the time of application launch. It is unchangeable author found that a work is to secure the hard disk with set of decryption keys. Keys are to be stored at some space in the system. Xtensible Access Control Markup Language (XACML) is an Xtensible Markup Language (XML) based language used to define a fine grained access control policy. The author found that these techniques are not safeguarding against attacks as impersonation. The author work is based on some of the methods XML signatures, XML Encryption, and Encryption proxies. Cloud database is stored with user credentials and metadata table information. Users can access the cloud data through the encryption proxy. If user wants to access the data, he/she need to follow encryption proxy. If the user doesn't have control on existing rule, then access is restricted. This work is combined with several mechanisms. This leads to performance overheads. Each time there is a need for re calculation or redefining such rules. It gives confusion on huge requests. Entire control is on the encryption proxy. Compromising the proxy leads the system failure.
H. Liu et al. reviewed that the existing solutions focus on the illegal access of data not on privacy issues when data sharing to others [17]. Author proposed a Shared Authority based Privacy preserving Authentication protocol (SAPA). This protocol achieved the shared access authority by anonymous access matching mechanisms with privacy and security considerations. An attribute based access control is used to prove that the user can only access own data fields. Proxy re-encryption is applied to

prove data sharing among multiple users. A universal composability model, is established for multiuser applications. Anonymous ID based data sharing algorithm for the systems under distributed computing and multi party oriented. This gives an integer data sharing algorithm gives a unlimited number of anonymous assignment. Multi owner data sharing scheme is derived for dynamic groups in cloud applications. It assures the user can share the data securely to dynamic user groups through a untrusted cloud server. A granted user is able to decrypt the files. No interaction required for accessing the data from its owner.

J.K Liu et al. designed a fine grained two factor authentication access control system for the computing services based on web [18]. Attribute based access control scheme is designed by taking secret key and a device. Both are required to get access i.e. the same computer is required for every access. Personal usage system like e-Banking services is an suitable application. The device used must support algorithm functions and tamper proof. This scheme supports a fine grained attribute based access control. Mediated cryptography was designed for the immediate revocation of public keys . A Security Mediator (SEM) model is designed based on this cryptography. In this system, user has secret key, public key, identity, and signing algorithm. Secret key and SEM model are also needed. It solves the revocation problems. User is anonymous to this model. So it leads to a security issue. Key insulated cryptography is used to store long term keys in a secured device and short term signatures in unsecured device. All users are needed to update the key for every time and the device is requested to do this task.

Limitations of Existing System:

1. Basic encryption techniques are used. Key management and backup services not effective.
2. Cipher-text based security may not provide the best solution to all time.
3. Security issues are not efficient into account like authentication and confidentiality
4. High computation overload. Provides very low throughput.

IV. PROPOSED SYSTEM

The core component of protection system is centralized server. The architecture of centralized control server includes security module. Centralized Server is a management portal with web interface and security module. Administrator will monitor web portal and other related operations and user interact with API to access web application. The proposed system consists of peer to peer encryption in which it will encrypt data using private key and data will be stored on to cloud server. The web data will be encrypted by using reliable and highly secured algorithm such that data will get secured. The system will also include file manager to perform various operations on a data. It will provide editing tool for user so that data will be manipulated and updated data will be stored on a server.

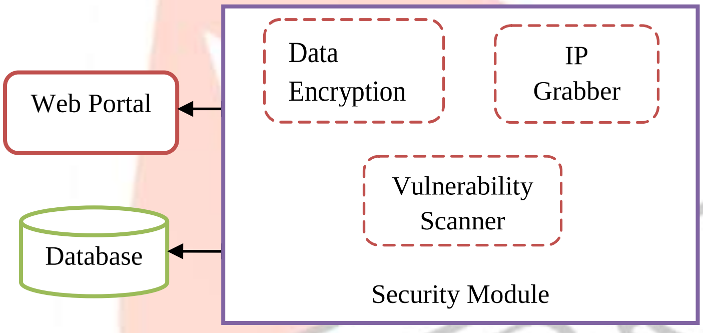

Figure 1: Structure of security module

V. APPLICATIONS

1. The proposed system may used in any applications on cloud environment.
2. This may used as security tool to any cloud based application.
3. This is used a security as a service (SECaaS) which may use in business continuity and disaster recovery systems.
4. This system may used in information security and data storage services.

VI. ACKNOWLEDGEMENT

I would first like to thank my guide Prof. Vaishali B. Bhagat of the P. R. Pote College of engineering. My Co-guide Prof. Krutika K. Chhajed was always willing to answer of any query about my research or writing. She consistently allowed this paper to be my own work, but steered me in the right the direction whenever she thought I needed it. I would also like to thank the experts who were involved in the validation survey for this research project. Without their passionate participation and input, the validation survey could not have been successfully conducted.

REFERENCES

[1] Wei-Fa Liao, Hung-Min Sun, Wei Wu, "A Distributed and Autonomous Guard System Based on Cloud Environments", *IEEE 14th Intl Conf on Dependable, Autonomic and Secure Computing, 2016*,ISBN**:** 978-1-5090-4065-0

[2] Yunchuan Sun, Junsheng Zhang, Yongping Xiong,and Guangyu Zhu,"Data Security and Privacy in Cloud Computing" *In: Hindawi Publishing Corporation*
International Journal of Distributed Sensor Networks , Article ID 190903, 9 pages, http://dx.doi.org/10.1155/2014/190903, Volume 2014

[3] Mannem Sindhuja, Punugoti Pavan Kumar,"A Trusted Framework for Data Security in Cloud Environment",*In: Journal of network and computer applications,2011*, ISSN: 2319-7064.

[4] Nitin Singh Chauhan, Ashutosh Saxena." Cryptography and Cloud Security Challenges" *Senior Member IEEE, and JVR Murthy, Infosys Labs, Infosys Limited, Hyderabad, India,2014*

[5] Deyan Chen,Hong Zhao."Data Security and Privacy Protection Issues in Cloud Computing". *International Conference on Computer Science and Electronics Engineering, Neusoft Corporation,Shenyang, China, 2012,* ISBN: 978-0-7695-4647-6

[6] P.Mell and T. Grance. "The nist definition of cloud computing," *National Institute of Standards and Technology, vol. 53, no. 6, article 50, 2009.*

[7] Varun Mahajan,Sateesh K Peddoju."Deployment of Intrusion Detection System in Cloud: A Performance-based Study" *IEEE Trustcom/BigDataSE/ICESS, 2017,* ISSN**:** 2324-9013

[8] R. H. Sakr, F. Omara, O. Nomir "An Optimized Technique for Secure Data Over Cloud OS" International Journal of Emerging Trends & Technology in Computer Science (IJETTCS) Volume 3, Issue 3, May-June 2014 ISSN 2278-6856

[9] ZiyuanWang , ―Security and privacy issues within the Cloud Computing‖ ,International Conference on Computational and Information Sciences , 2011, ISBN: 978-0-7695-4501-1

[10] A survey on data breach challenges in cloud computing security: Issues and threat R.Barona,E.A.mary anita 2017 international conference on circuit,power and computing technoloies,IEEE, ISBN: 978-1-5090-4967-7

[11] Akshita Bhandari,Ashutosh Gupta, Debasis das" A framework for data security and storage in Cloud Computing" Computational techniques in information and communication technologies, 2016 international conference , IEEE
https://www.researchgate.net/publication/299338639

[16] U. Greveler, B. Justus, D. Loehr, A Privacy Preserving System for Cloud Computing, ICCIT, IEEE, pp- 648 - 653, 2011.

[17] H. Liu, H. Ning, Q. Xiong, L.T. Yang, "Shared Authority Based Privacy-Preserving Authentication Protocol in Cloud Computing," Transactions on Parallel and Distributed Systems, Vol. 26, No. 1, pp-241-251, January, 2015.

[18] J. K. Liu, M. H. Au, X. Huang, R. Lu, J. Li, "Fine-Grained Two-Factor Access Control for Web-Based Cloud Computing Services,"Transactions on Information Forensics and Security, Vol. 11, No. 3, pp. 484-497, March, 2016