ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirset.com

Vol. 6, Issue 6, June 2017

A Review on Confidential Data Classify Based Authentication Tactic for Cloud Computing Security

Ankita Awasthi [1], Pragati Gautam [2]

P.G. Student, Department of Computer Engineering, JNCT Engineering College, Ratahara, Rewa(M.P), India[1]

Assistant Professor, Department of Computer Engineering, JNCT Engineering College, Ratahara , Rewa(M.P), India[2]

ABSTRACT: Security is a main concern of cloud computing as long as data increase over cloud, number of user access also increase, now a days users put data over cloud and then access by every one but who modify our data and by whom it alter it's our main concern. In this paper we study about cloud or its security application at the end we proposed an authentication based security which is based on AES or MD5 hashing technique for providing security over cloud.

KEYWORDS: CC, PDF, DB, IDBPS

I. INTRODUCTION

Cloud computing is a revolutionary machinery which is likely to dominate and reshape the information technology industry in the near future. This emerging computing machinery provides highly scalable computing resources (e.g. information, applications, and transactions) in a method which is accessible, flexible, on-demand, and at a low cost it provides unique opportunities for organizations to run business with efficiency and efficiency through allowing businesses to run their applications on a shared data center thus eliminating the require for servers, storage, processing power, upgrades, and technical teams. Furthermore; in cloud computing replica, business organizations don't require to purchase any s/w services or products to run business because they can merely subscribe to the applications in the cloud; those applications normally are reliable and scalable ultimately allow business leaders to attend on their core company functions to enhance profitability and increase performance . Several associations have happen to interested in the cloud computing idea due to several compelling advantages presented through this rising computing model. Cloud computing seller are offering scalable services and applications by centralized data centers using thousands of server computers that provide easy access to computing resources anytime and anywhere ; the capability of cloud computing to fast scale and provide access to computing services and resources anytime and anywhere, allowing business to fast react to modify business requirements without the expenditures of space, money, personnel, time and another assets requires for traditional substructures, for instance, New York newspaper organization were capable to convert 11 million scanned and archived hard copies into portable document format (PDF) files in 24 hours by renting 100 servers from Amazon's cloud services at a cost to the organization was approximately $250. Alternative methods for the conversion would have required cost and taken weeks or even months to complete [3].while cloud computing offer huge potential for decreasing costs and increasing an organization's ability to fast scale computing resources to respond to modify needs, there are hazard linked with cloud computing. Specifically, cloud computing may represent which business hand over control, losses in data integrity and availability and resulting in exposure to breaches in confidentiality. However; as with any technology, cloud computing has its own weakness for instance releasing control of maintaining confidentiality, availability of sensitive business data, and integrity; In general, most cloud computing customers want to be certain which cloud providers have effective security policies and controls in place to comply with data protection standards and meet regulatory compliance needs prior to making a decision to migrate their data or applications to the cloud.[1]

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirset.com

Vol. 6, Issue 6, June 2017

II.PRIVACY PRESERVING IN CLOUD

Privacy issues exist for a long time in the computing literature. Data storage in the Cloud Computing device that is located in multi regions to create the system more tolerant may also raise the privacy problems. Such research contributions are given below.

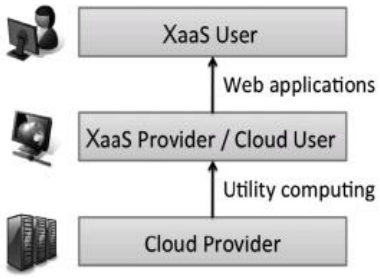

Figure 1: Users and Providers of Cloud Computing

III.SECURITY AND PRIVACY IN CLOUD

This paper [1] discusses the which arise in famous salesforce.com, and epic.com, Google docs, due to cloud security limit. Cloud computing is protected if customers can based on them to behave like customers expect, fulfilling 5 goals, say availability, confidentiality, control ,inspection and data integrity.
The relationship between the users and providers in cloud computing devices is discussed in stipulations of 3 roles say Cloud provider, Xaas provider/Cloud user and Xaas user as illustrate in Figure 1, where X could be D (Data), S (Software). P (Platform), I (Infrastructure), and so on illustrate in Figure 1.[2]

IV. PRACTICES FOR CLOUD SECURITY

A. Secure access
Usually users access the cloud using client web browser. Ensure browsers are correctly renew and protected from browser exploits. Through utilizing this, data can be prevented from threat to a few extent.
B. Backups and restoration
There should be suitable device that grant via the service giver so that customer is able to have backups of the cloud deepened on resources and data. Some services like Amazon S3, Amazon Dynamo DB provide automatic data restoration.
C. Data Integrity
To makes sure data integrity, restrictions the district of utilizing of resources for customers. This can prevent the change of data and therefore data integrity is maintained. In case of data, integrity is compulsory reinstate the data from backup with the aid of backup services give.
D. Encryption of data
Data encryption grants protection to the data. Encryption should be done before the data is moved to the cloud [4]. If an unknown customer wants to access the dangerous data, encrypting the data create it much harder for unknown customer to do anything with incorrect start.
E. Evaluation
Evaluate applications, company procedure and data according to their value and hazard linked with them then create cloud with precautions and tools to create the cloud [3].

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirset.com

Vol. 6, Issue 6, June 2017

V. CLOUD SECURITY CATEGORIES AND ISSUES

Table:1 Cloud Security categories:[4]

S.N	Category	Description
1	Security Standards	Identify the normal require to obtain deterrent measures in the cloud computing so as to prevent attacks. It straight the strategy of cloud computing for security without compromising performance and reliability.
2	Network	Consist of networking attacks such as DoS (Denial of Service), Connection Availability, internet protocol vulnerabilities, DoS, flooding attack, *etc*.
3	Access Control	Access control and Authentication and It capture the problems which affect the privacy of customer information and data storage.
4	Cloud Infrastructure	Attacks which are severe to the cloud substructure (PaaS and SaaS, IaaS,) as privileged insiders and tampered binaries
5	Data	Data related security problems, contain integrity, data migration, confidentiality, and data warehousing.

Table2: Cloud Security Issues and Classifications

S.N	Category	Issues
1	Security Standards	nonappearance of lawful feature (Service level agreement) nonappearance of security standards observance risk Trust nonappearance of inspection
2	Network	Network security configurations suitable installation of network firewalls Internet Dependence Internet protocol vulnerabilities
3	Access	Malicious insiders Account and Service hijack Privileged customer access Browser Security Authentication machinery
4	Cloud Infrastructure	Quality of service (QoS) Sharing technical fault Insecure interface of API Multi-tenancy Reliability of supplier Server area and Backup Security Misconfiguration
5	Data	Data locality, Data loss and leakage Data redundancy Data privacy, Data protection Data recovery, Data availability

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirset.com

Vol. 6, Issue 6, June 2017

VI. RELATED WORK

The privacy problems in the cloud access are managed and assessed through utilizing assessment methods and privacy protocols that are also addressed. The trust problems in cloud computing have been addressed with different models. An intra-cloud and inter-cloud regular of cloud interoperability has been known in sequence to emphasize the defy exist through the cloud interaction. The cloud resources are deployed over cloud atmosphere with different models also faces a problem. This paper focuses/attend on a current survey linked to the cloud interoperability, privacy, and security, trust depends on standards and guidelines have been analyzed. The overall attend of this paper is to establish an interoperability amongst dissimilar cloud service giversfor effective interaction by maximizing the QoS of cloud computing.[5]Sharma et al. The research present the latest replica through extending the TAM (Technology Acceptance Model) with three external constructs namely trust, and job opportunity and computer self-efficacy. One of the major donations of this examine is the introduction of the newest build, JO (Job Opportunity), for the first time in a machinery choosing study. Data were collected from 101 IT professional and analyzed utilizing multiple linear regression (MLR) and neural network (NN) modeling. depend on the RMSE values from the results of these models NN models were found to outperform the MLR model. [6]Gill et al. The large data centers emit carbon-dioxide which guide to global warming. So to address both of these issues, we have present a framework which tackles with security and is energy efficient. Signature and anomaly based hybrid IDPS detects, logs, prevent and alert the security Admin. The Nesting of the VMs provide easy management and IDPS can deal better as the grouping of VMs has been done on the basis of security protocols. In this paper, a comprehensive survey on existing cloud security frameworks has been done. Based upon the limitations on existing frameworks a latest framework has been present to grant security in virtual networks that is depend on Intrusion Detection and Prevention System (IDPS) and its prototype implementation has also been done.[7]*Khan et al.* present a discussion of security concerns in stipulations of security threats and their remediation's. The contribution aim at the analysis and categorization of working ways of the major security difficulty and likely solutions that available in the literature. We execute a parametric match of the threats being faced through cloud platform. Moreover, we match several prevention and intrusion detection frameworks being utilized to address security problems. The trusted cloud computing methods for regulating security compliance amid cloud service giver are also analyzed. Since the security method continues to evolve, we also present the future introduction of cloud security difficulty and their possible countermeasures.[8]Krishna et al. Cloud computing has a likely for cost savings to the enterprise but the security hazard are also huge. Company regarding into cloud computing technology since an idea to reduce on cost and enhance profitability should sincerely analyze the security hazard of cloud computing of cloud computing. The asset of cloud computing in information risk management is the facility to manage risk more effectively from a integrate point. Although Cloud computing can be seen as a latest marvel that is group to improvement the approach we utilize the Internet, there is much to be thoughtful about. There are many new technologies emerging at an express rate, each with technological developments and with the potential of making human's lives at ease.[9]Piplode et al. This paper totally discusses the cloud computing security difficulties and defies. This paper also analyzes cloud computing weakness, security threats cloud computing faces and presented the security objective that necessitates being achieved. On one hand side, the security-sensitive applications of a Cloud computing need high degree of security on the other hand side, cloud computing are intrinsically vulnerable to security attacks. Therefore, there is a require to create them extra secure and robust to adapt to the demanding needs of these networks. The future of cloud computing is really appealing, giving the vision of cheap communications.[10]

VII. SIMULATION TOOLS

The .NET structure is the major element for developing ASP. .Net web applications absolute of SAS and is obtainable since a without charge download for Windows 2000 (Professional and Server versions) as well as Windows XP. It is also an integral element of Windows Server 2003. Although the framework in itself is actually now the sub-routine library - can I call it that or am I giving away my age ? - to really get going with .NET. You require an, VS.Net (Visual Studio.Net) and Integrated Development Environment (IDE) is the primary enterprise-level IDE but Microsoft have also released a tool that is known as 'ASP.Net Web Matrix', that is available like a free download.

1. COMPONENTS OF SAS/IT

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirset.com

Vol. 6, Issue 6, June 2017

The introduction of Integration machinery with version 8.2 opens up the SAS device tool group in a method not possible in previous versions. There are a number of elements of Integration machinery, each with different purposes. The elements applicable to .NET application programming are the 'Workspace Manager' and the 'IOM - Integrated Object Model - Data Provider'. These elements open up the SAS programming language interpreter and the SAS data library architecture to the external programming language interfaces provided by ASP.Net [11]

VIII. PROBLEM FORMULATION

Cloud computing is growing area of research there are lots of research done in this area. it's an open to all and all access data from the cloud there is no restriction when data available publically, existing work provide lots of trust technique overview if we use high encrypted technique than trust value is higher, or our technique is more secure if trust value is higher. Cloud computing has been the new paradigm in distributed computing in the recent times. For cloud computing to become widely adopted several issues need to be addressed. Cloud security is one of the most important issues that has to be addressed. Trust management is one of the important components in cloud security as cloud environment will have different kinds of users, providers, and intermediaries. Proper trust management will help the users select the provider based on their requirements and trust worthiness. Also, trust management would help the providers select the clients who are trustworthy to serve.

In existing technique we only apply encryption and decryption for our data at the time of login but there is no authentication provided at the time of login. Because of only basis of trust value security is not provided.

IX. PROPOSED WORK

In our proposed work we apply authentication based data classify security technique for cloud computing

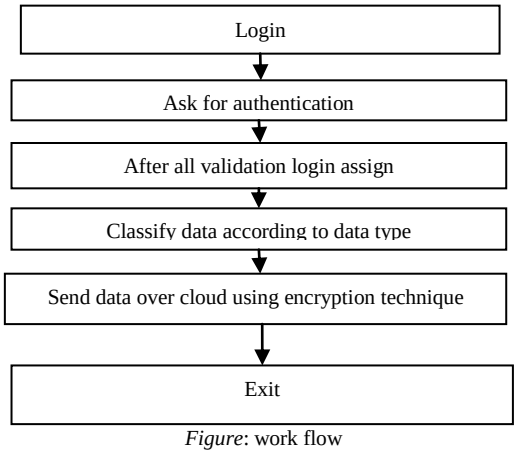

Figure: work flow

Algorithm:
Step1: login(valid)
Step2: authentication(valid)
Step3: classify data
Step4: switch data:
Case: basic data
Encrypt using RSA;
Break;
Case: confidential
Encrypt using AES
Break;

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirset.com

Vol. 6, Issue 6, June 2017

Case: highly confidential
Encrypt using AES and MD5
Break;
Default:
Encrypt using RSA
Step5: exit.

X. CONCLUSION

Cloud computing has been the new paradigm in distributed computing in the recent times. For cloud computing to become widely adopted several issues need to be addressed. Cloud security is one of the most important issues that have to be addressed. Trust management is one of the important components in cloud security as cloud environment will have different kinds of users, providers, and intermediaries. Cloud security is one of the main concern of cloud computing in this paper we provide security using authantication and data security using data classification method. In future we apply any insubstantial cryptography for cloud scenario.

REFERENCES

[1] Yasir Ahmed Hamza1, Marwan Dahar Omar1 **"Cloud Computing Security: Abuse and Nefarious Use of Cloud Computing" International Journal of Computational Engineering Research**||Vol, 03||Issue, 6
[2] R. Sumithra1 & Sujni Paul2 "**A Survey Paper On Cloud Computing Security And Outsourcing Data Mining In Cloud Platform**" International Journal of Knowledge Management & e-Learning ,Volume 3 • Number 1 • January-June 2011 • pp. 43-48
[3] Jasleen Kaur1, Ms.Anupma Sehrawat2, Ms.Neha Bishnoi3 **"Survey Paper on Basics of Cloud Computing and Data Security" International Journal of Computer Science Trends and Technology (IJCST**) – Volume 2 Issue 3, May-Jun 2014
[4]B. Rex Cyril1, DR. S. Britto Ramesh Kumar2 "**Computing Data Security Issues, Challenges, Architecture and Methods- A Survey" International Research Journal of Engineering and Technology (IRJET)** e-ISSN: 2395-0056 Volume: 02 Issue: 04 | July-2015 www.irjet.net
[5] C.Saravanakumar, and C.Arun "**Survey on Interoperability, Security, Trust, Privacy Standardization of Cloud Computing" IEEE-2014**
[6] Sujeet Kumar Sharma a, *, Ali H. Al-Badi b, Srikrishna Madhumohan Govindaluri a, Mohammed H. Al-Kharusi b "**Predicting motivators of cloud computing adoption: A developing country perspective**" (ELSEVIER-2015)
[7] Komal Singh Gill, Anju Sharma "**IDPS based Framework for Security in Green Cloud Computing and Comprehensive Review on Existing Frameworks and Security Issues**" IEEE-2015
[8] Minhaj Ahmad Khan "**A survey of security issues for cloud computing" Journal of Network and Computer Application**
[9] B. Hari Krishnaa, Dr.S. Kiranb, G. Muralia,b,* , **R. Pradeep Kumar Reddy "Security Issues In Service Model Of Cloud Computing Environment"** 2016 International Conference on Computational Science , ELSEVIER-2016.
[10] Rajesh Piplode and Umesh Kumar Singh "**An Overview and Study of Security Issues & Challenges in Cloud Computing" International Journal of Advanced Research in Computer Science and Software Engineering**
[11] Graham Murray, Independent Consultant WebMiner.co.uk, Dunfermline, Scotlan "ASP.Net and SAS® **A New Model for Developing Web-based SAS System Applications**.
[12] https://en.wikipedia.org/wiki/Cloud_computing
[13] https://en.wikipedia.org/wiki/Network_security