IOSR Journal of Engineering (IOSR JEN) **www.iosrjen.org**
ISSN (e): 2250-3021, ISSN (p): 2278-8719
PP 34-39

Data Security Model in Cloud Computing for Privacy and Risk Management

Mr. H. D. Kale [1], Dr. V. M. Thakare [2]
Department of Computer Science and Engineering, SGBAU,Amravati,Maharashtra,India

Abstract: *Cloud storage technology has been paid additional and additional attention as an rising network storage technology that is extended and developed by cloud computing concepts. Cloud computing setting depends on user services like high-speed storage and retrieval provided by cloud ADP system. Meanwhile, knowledge security is a crucial drawback to resolve desperately for cloud storage technology. knowledge security is taken into account because the constant issue leading towards a hitch within the adoption of cloud computing. knowledge privacy, Integrity and trust problems area unit few severe security considerations resulting in wide adoption of cloud computing. the appearance of the projected model has comfortable functionalities and capabilities that ensures the info security and integrity. the aim of this paper is to attain knowledge security of cloud storage and to formulate corresponding cloud storage security policy. Those were combined with the results of existing educational analysis by analyzing the safety risks of user knowledge in cloud storage and approach a theme of the relevant security technology, that supported the structural characteristics of cloud storage system.*

Keywords: *Cloud Computing, Cloud storage technology, Data security, Security Assessment Model.*

I. Introduction

Cloud computing has been unreal because the next generation info technology (IT) design for enterprises, because of its long list of unprecedented benefits within the IT history: on-demand self-service, present network access, location freelance resource pooling, speedy resource physical property, usage-based rating and transference of risk [1]. A cloud computing realizes the vision of computing as a utility, suppliers area unit developing a shared pool of configurable computing resources, that customers will dynamically provision and unleash in keeping with their dynamical wants.1 Thus, each teams benefit: suppliers will recycle computing resources, and users scale back prices through on demand resource provisioning [2]. Cloud computing provides completely different layers of computing utilities, from storage and networking to tools and applications, through 3 main service models: code as a service (SaaS), platform as a service (PaaS), and infrastructure as a service (IaaS). The models trust existing technologies for support—in specific, virtualization provides on-demand resource provisioning and multitenancy. Access management is one amongst the foremost vital measures to confirm the protection of cloud computing. Early access management technology can't solely guarantee traditional access necessities of valid users, stop invasions of unauthorized users, however it may also solve security issues caused by valid users' misoperation. Cloud computing surroundings may be a typical distributed environment; thus the distribution, dynamism, and namelessness of knowledge resources and services area exceptional options of cloud computing surroundings [3].

Cloud computing surroundings could be a typical distributed environment; thence the distribution, dynamism, and obscurity of knowledge resources and services are exceptional options of cloud computing setting . Therefore, the standard centralized access management model has apparently cannot satisfy the safety needs of cloud computing. The implementation of access management in cloud computing setting can face a series of challenges [4]. because the development and progress of engineering, the net has been changing into associate integral a part of one's life. The user-demands of net use haven't solely restricted to browse the portal however additionally to the event of web application services leading to explosive growth of net knowledge [5]. Facing huge knowledge, the ISPs desires a lot of process units and storage devices to confirm the regular operation of the corresponding system functions. However, it's still associate pressing issue to unravel for ISPs that the high price of memory devices, personnel management, and instrumentality maintenance.

II. Background

At present, as Associate in Nursing rising network storage technology extended and developed by cloud computing ideas, cloud storage technology is important with the widespread popularization of Cloud Computing. Cloud storage technology uses cluster applications, network technology or distributed file systems, etc. Cloud storage technology makes full use of the present completely different storage devices within the system to produce users with information storage, information retrieval, information backup and different functions through application software system ran by a user terminal [1]. to attain a sensible understanding of the "delta" that cloud computing adds with relevance security problems, we have a tendency to should analyze however cloud computing influences established security problems. A key issue here is security vulnerabilities: cloud computing makes sure well-understood vulnerabilities additional important yet as adds new ones to the combination [2]. The cryptography and secret writing approach facilitating the cloud user with information security assurance. The projected resolution solely talks concerning the raised security however doesn't mention the performance. the answer additionally includes the functioning of rhetorical virtual machine, malware detection and real time watching of the system. a survey of various security problems and threats also are given. {ainformation|aknowledge|an information} security framework additionally provides the transparency to each the cloud service supplier and also the cloud user thereby reducing data security threats in cloud setting.

A privacy protective auditing protocol for cloud systems. The protocol supports dynamic operations on knowledge and batch auditing for multi-cloud setting [3]. It uses additive pairing to get an encrypted proof. The verification of the proof correctness is then executed by the information auditor. during this protocol, the procedure overhead of the auditor is affected to the cloud server. but it fails to produce knowledge confidentiality and user authorization. Cloud-Trust—that estimates high level security metrics to quantify the degree of confidentiality and integrity offered by a CCS or cloud service supplier (CSP). Cloud-Trust is employed to assess the protection level of 4 multi-tenant IaaS cloud architectures equipped with various cloud security controls. Results show the likelihood of CCS penetration (high worth knowledge compromise) is high if a borderline set of security controls are enforced [4]. Multi-authority ciphertext-policy attribute-based encryption-based knowledge access management for cloud storage, during which the authors claimed that the mechanism in handling attribute revocation may accomplish each forward security and backward security [5]. Compared to the standard computing model, the cloud computing model distributes computing tasks on an outsized range of computers because of the explosive growth of net knowledge these days. This model permits users to apportion resources to the desired on demand and access the pc and storage systems on demand, providing quick, efficient, and cheap computing power that maximizes users' storage service desires.
These are organizes as follows.
Section I Introduction. **Section II** discusses Background. **Section III** discusses previous work. **Section IV** discusses existing methodologies. **Section V**discusses attributes and parameters.**Section VI** proposed method and outcome result possible. Finally **section VII** Conclude this review paper.

III. Previous Work Done

Bernd Grobauer et al (2011) [1] have designed a privacy conserving auditing protocol for cloud systems. The protocol supports dynamic operations on information and batch auditing for multi-cloud setting. It uses additive pairing to get an encrypted proof. The verification of the proof correctness is then dead by the info auditor. during this protocol, the procedure overhead of the auditor is affected to the cloud server. but it fails to supply information confidentiality and user authorization.

Yuan Zhangin et al (2015) [2] propose SCLPV is that the 1st work that at the same time supports certificate less public verification and resistance against malicious auditors to verify the integrity of outsourced information in CPSS. a proper security proof proves the correctness and security of our theme. Propose a secure certificate less public integrity verification theme (SCLPV). The SCLPV is that the 1st work that at the same time supports certificate less public verification and resistance against malicious auditors to verify the integrity of outsourced information in CPSS. a proper security proof proves the correctness and security of our theme. additionally, an elaborate performance analysis demonstrates that the SCLPV is economical and sensible. Compared with the sole existing certificate less public verification theme (CLPV), the SCLPV provides stronger security guarantees in terms of remedying the safety vulnerability of the CLPV and resistance against malicious auditors.

LIN Guoyuan et al (2013) [3] the author talked regarding RACS technique this can be redundant array of cloud storage technique to avoid vender lock-in and additionally scale back the price. The author of the paper given the privacy manager for shielding information theinfo|the information} being purloined or ill-used and additionally helping the cloud computing supplier to evolve the privacy law by describing the privacy design to shield non-public data. The on top of approaches ar smart for providing the safety to the info however somewhere the performance is compromised.

Cong Wang et al (2017) [4] Cloud storage is of important importance so users will resort to a third-party auditor (TPA) to envision the integrity of outsourced knowledge and be worry free. To firmly introduce a good TPA, the auditing method ought to herald no new vulnerabilities toward user knowledge privacy, and introduce no further on-line burden to user. during this paper, we tend to propose a secure cloud storage system supporting privacy-preserving public auditing. we tend to additional extend our result to change the TPA to perform audits for multiple users at the same time and with efficiency.

Jianan Hong et al (2015) [5] have projected analyze the defect of DAC-MACS in handling attribute revocation, though the most construction of that employment is verified secure. the safety vulnerability exists as a result of DAC-MACS wrong uses a duplex re-encryption theme within the cipher text change procedure.

IV. Existing Methodologies

A. Vulnerabilities in cloud computing

Vulnerability [1] is that the chance that an quality are unable to resist the actions of a threat agent. Vulnerability exists once there's a distinction between the force being applied by the threat agent, associated an object's ability to resist that force. A key issue here is security vulnerabilities: cloud computing makes bound well-understood vulnerabilities additional vital further as adds new ones to the combination.

B. Secure Certificate less Public Verification (SCLPV)

The SCLPV [2] is that the initial work that at the same time supports certificate less public verification and resistance against malicious auditors to verify the integrity of outsourced knowledge in CPSS. a proper security proof proves the correctness and security of our theme. Propose a secure certificate less public integrity verification theme (SCLPV). The SCLPV is that the initial work that at the same time supports certificate less public verification and resistance against malicious auditors to verify the integrity of outsourced knowledge in CPSS. a proper security proof proves the correctness and security of our theme. additionally, associate elaborate performance analysis demonstrates that the SCLPV is economical and sensible. Compared with the sole existing certificate less public verification theme (CLPV), the SCLPV provides stronger security guarantees in terms of remedying the protection vulnerability of the CLPV and resistance against maliciousauditors.

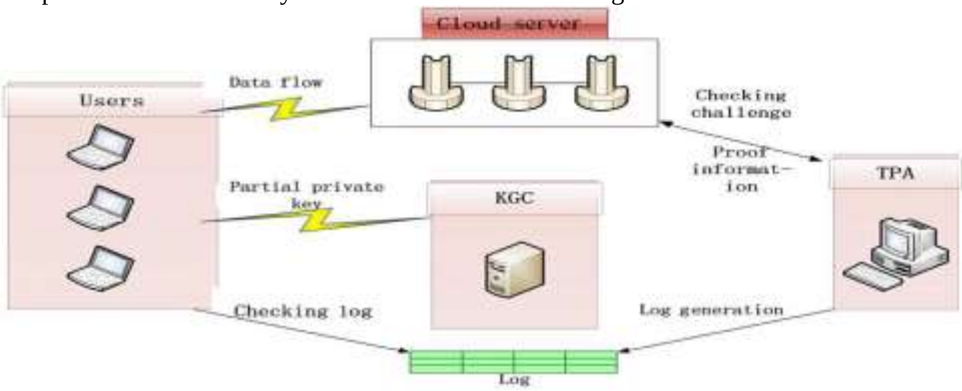

Fig1. *System model*

C. A Mutual Trust based Access control Model in Cloud Computing (MTBAC)

Combining with Trust Management (TM) , a mutual trust primarily based access management (MTBAC) [3] model is projected during this paper. MTBAC model take each user's behavior trust and cloud services node's believability into thought. Trust relationships between users and cloud service nodes ar established by mutual trust mechanism. Security issues of access management ar resolved by implementing MTBAC model into cloud computing setting. Simulation experiments show that MTBAC model will guarantee the interaction between users and cloud service nodes.

D. Cloud-Trust—a Security Assessment Model

Presenting a cloud design reference model that includes a large vary of security controls and best practices, and a cloud security assessment model—Cloud-Trust—that estimates high level security metrics to quantify the degree of confidentiality and integrity offered by a CCS or cloud service supplier (CSP) [4]. Cloud-Trust is employed to assess the protection level of 4 multi-tenant IaaS cloud architectures equipped with different cloud security controls. Results show the chance of CCS penetration (high worth knowledge compromise) is high if a lowest set of security controls ar enforced. CCS penetration likelihood drops well if a cloud defense full security design is adopted that protects virtual machine (VM) pictures at rest, strengthens CSP and cloud tenant supervisor access controls, and that employs alternative network security controls to attenuate cloud network surveillance and discovery of live VMs.

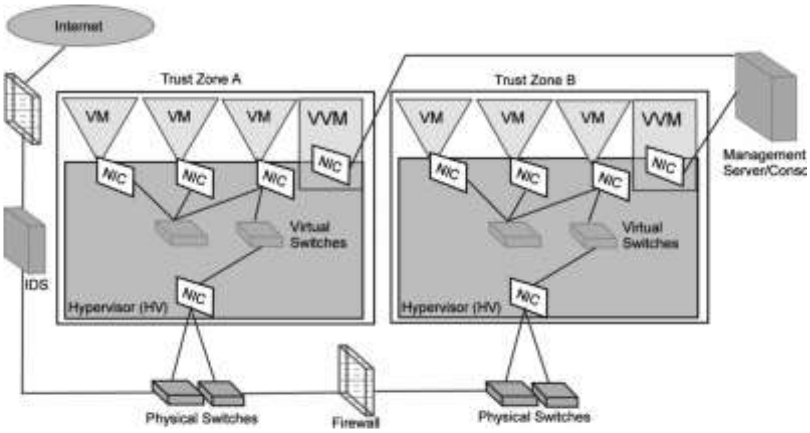

Fig2. *CCS network segmentation scheme*

E. Cloud-Based Utility Service Framework

Utility primarily based cloud services will with efficiency offer varied verifyi services to totally different service suppliers [5]. Trust negotiations with united identity management square measure important for conserving privacy in open systems like distributed cooperative systems. However, because of the big amounts of server primarily based communications concerned in trust negotiations quantifiability problems encourage be less cumbersome once offloaded on to the cloud as a utility service. during this read, we have a tendency to propose trust {based|basedmostly|primarily primarily based} united identity management as a cloud based utility service. the most part of this model is that the trust institution between the cloud service supplier and therefore the identity suppliers. In propose novel trust metrics supported the potential vulnerability to be attacked, the out there security enforcements and a unique price metric supported policy dependencies to rank the tractableness of identity suppliers.

V. Analysis And Discussion

Cloud storage has become one among the hotspots of knowledge storage recently with the increase of cloud computing. Cloud storage refers to a system that gives information storage and service access functions for users through cluster application, network technology and distributed filing system, that collects an outsized range of various kinds of storage devices within the network through application software system to figure along [1].

Users will use selection types of terminals to get application services no matter no matter his location is and don't got to care concerning wherever the applying runs. In information security privacy, Integrity and Trust area unit a number of the bench marks that facilitate within the analysis of the secured system [2]. The projected model is useful in building the well extremely secured information security system. The projected model is expounded specific to the info security altogether the 3 layers of the cloud services that area unit offered to the cloud user by the cloud supplier [3]. The art movement issue of information security in cloud computes opens new challenges like information locks by cloud supplier, fault tolerance and disaster recovery mechanisms in cloud computing [4]. Vulnerabilities that area unit relevant for all cloud computing parts generally concern the provider—or rather users' inability to manage cloud infrastructure as they are doing their own infrastructure. Among the management challenges are skimpy security audit prospects, and also the indisputable fact that certification schemes and security metrics aren't adopted to cloud computing [5].

Table 1: Pros And Cons of Various Cloud computing security models

Cloud Computing Security Models	Pros	Cons
The Cloud MultipleTenancy Model of NIST	Isolate fault, virus, and intrusion of one from other virtual machines and hardware, and reduce the damage of malicious applications.	The technology difficulties like data isolation, architecture extension, configuration selfdefinition, and performance customization
The Cloud Risk Accumulation Model of CSA	The layer dependency of cloud service models help to analyze the security risks of cloud computing.	Lower service layer that a cloud service provider lies in, the more management duties and security capabilities that a customer is in charge of, more risk of security breach.

JericoFormu's Cloud Cube Model	Selecting cloud formations for secure collaboration	When closing down an agreement with a provider, care should be taken to ensure that the data is appropriately deleted from the cloud service provider's infrastructure (including backups), otherwise a data leak risk will remain.
Multi-Clouds Database Model	Lowers the risk of malicious insider in the cloud and avoid failing of cloud services	More time and cost consumption

VI. Proposed Methodology

In this section a replacement model for knowledge security in cloud computing surroundings exploitation the data declared within the previous section is obtainable. This paper enhances ancient knowledge security model for cloud computing. The projected knowledge security model use a 3 layer system structure within which these layers square measure used for guaranteeing knowledge security. In projected model, all the techniques and mechanism helpful for implementing a extremely protected atmosphere is developed. the tip user can access the cloud through net and for that sturdy log in access is provided to the user. The high security login feature within the model can stop the user with malicious intent to use the info hold on on the cloud. The code encrypts and protects knowledge at numerous levels by mistreatment varied security techniques and security algorithms. The projected model ensures that protection of the user counselling by guaranteeing quicker retrieval of {the knowledge|theinfo|the information} mistreatment counterintelligence and advanced security data protection.

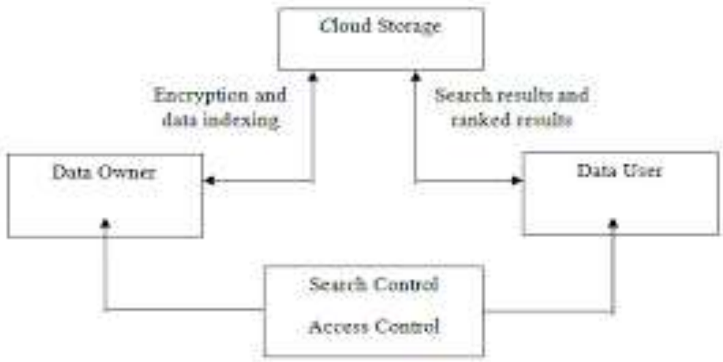

Fig3. *Secured Cloud Storage Process*

VII. Outcome And Possible Result

Cloud computing is that the up stormy technology that is wide interesting whole of the data business. The four models are surveyed and compared. it's been ended that JericoFormu's Cloud Cube Model and Multi-Clouds information Model are safer compared to The Cloud Multiple-Tenancy Model of agency and also the Cloud Risk Accumulation Model of CSA. it's been analyzed that Multi-Clouds information Model has less malicious insiders among the opposite compared models. because the future purpose of read work will be carried on to supply safer cloud computing security model to boost the technology used, authorization, security and malicious insiders.

VIII. Conclusion

Cloud computing is common recently and additional and additional users area unit adding to the cloud surroundings leading towards security problems associated with the info. This paper presents an summary on the info security downside related to the cloud computing. This paper talked regarding numerous threats related to knowledge security in cloud computing describing concisely knowledge integrity, knowledge privacy and knowledge trust associated. The model is projected talks regarding 3 level authentication mechanisms for rising security to the information as compared to the previous ancient system. though the extra responsibilities are additional to the supplier in implementation of extremely secured knowledge access network however the projected model can minimize the problems mentioned within the previous section.

IX. Future Scope

From the comparison and performance analysis, quick recovery of knowledge achieved to the user. These appear within the planned information security model third section. From the comparison and performance analysis, cloud computing depend upon some condition, but it's advanced security technologies instead of traditional desktop.

References

[1]. Bernd Grobauer, Tobias Walloschek, and ElmarStöcker, "Understanding Cloud Computing Vulnerabilities," *Copublished By The Ieee Computer And Reliability Societies ,MARCH/APRIL 2011.*

[2]. Yuan Zhang ,Chunxiang Xu ,Shui Yu, Hongwei Li, "SCLPV: Secure Certificateless Public Verification for Cloud-Based Cyber-Physical-Social Systems Against Malicious Auditors," *IEEE Transactions On Computational Social Systems,* VOL. 2, NO. 4, DECEMBER 2015.

[3]. LIN Guoyuan, WANG Danrul, BIE Yuyul, LEI Min," MTBAC: A Mutual Trust Based Access Control Model in Cloud Computing",*China Communications·* April 2014.

[4]. Dan Gonzales,Jeremy M. Kaplan, Evan Saltzman, Zev Winkelman, and Dulani Woods "Cloud-Trust—a Security Assessment Model for Infrastructure as a Service (IaaS) Clouds",*IEEE Transactions On Cloud Computing,* VOL. 5, NO. 3, July-September 2017.

[5]. Jianan Hong, KaipingXue,"DAC-MACS: Effective Data Access Control for Multiauthority Cloud Storage Systems"/Security Analysis of Attribute Revocation in Multiauthority Data Access Control for Cloud Storage Systems," *IEEE Transactions On Information Forensics And Security*, Vol. 10, No. 6, June 2015.