SYSTEMATIC SURVEY ON ISSUES AND CHALLENGES ON CLOUD STORAGE

[1]Pooja Singh, [2]Deepika Parihar, [3]Yogesh Kadam
[1]Student Bharati Vidyapeeth college of Engineering, [2] Student Bharati Vidyapeeth college of Engineering Lavale, [3]Professor Bharati Vidyapeeth college of Engineering
[1]Computeer Engineering
Pune,India

Abstract—Storing data securely on cloud is issue as off network attack is major challenging task. Existing techniques lack network attack handling capability. This article a systematic survey has been provided on cloud storage with effective techniques to handle network attacks . network coding strategy with data chunking has been are of interest. Encryption techniques and shortcoming have been studied. A simple problem statement has been devised for project implementataion.

Index Terms—Cloud Storage, Encryption Algorithm, Network coding, Data chunking.

I. INTRODUCTION

Need of Cloud Computing:-

Cloud computing is computing based on the internet. Where in the past, people would run applications or programs from software downloaded on a physical computer or server in their building, cloud computing allows people access to the same kinds of applications through the internet. From a customer perspective, the public cloud offers a way to gain new capabilities on demand without investing in new hardware or software. Instead, customers pay their cloud provider a subscription fee or pay for only the resources they use. Simply by filling in web forms, users can set up accounts and spin up virtual machines or provision new applications. More users or computing resources can be added on the fly—the latter in real time as workloads demand those resources thanks to a feature known as auto-scaling.

Cloud Computing

In the simplest terms, cloud computing means storing and accessing data and programs over the Internet instead of your computer's hard drive. The cloud is just a metaphor for the Internet. It goes back to the days of flowcharts and presentations that would represent the gigantic server-farm infrastructure of the Internet as nothing but a puffy, white cumulus cloud, accepting connections and doling out information as it floats.

Cloud problems:-

In PaaS,the provider might give some control to the people to build applications on top of the platform. Any security below the application level as host and network intrusion prevention will still be in the scope of the provider. Security the eat sre related with security hole in virtualization OS security issues also alive in IaaS.

Network Coding :-

Network codes designed specifically for distributed storage systems have the potential to provide dramatically higher storage efficiency for the same availability. One main challenge in the design of such codes is the exact repair problem: if a node storing encoded information fails, in order to maintain the same level of reliability we need to create encoded information at a new node. One of the main open problems in this emerging area has been the design of simple coding schemes that allow exact and low cost repair of failed nodes and have high data rates. In particular, all prior known explicit constructions have data rates bounded by 1/2 .

II. LITERATURE SURVEY

[1]In cloud data is stored on multiple vendors it cosses data loss and data redundancy. We present a proxy-based storage system for fault-tolerant multiple-cloud storage called NCCloud. NCCLoud is built on top of a network coding based storage scheme. Proof-of-Concept FMSR(functional minimum storage regenerating) EMSR(exact minimum storage regenerating). "A transient failure is expected to be short-term, such that the “failed” cloud will return
to normal after some time and no outsourced data is lost. Data centered outage in disasters. AFCOM found that many data centers are ill-prepared for disasters." Generalization of FMSR codes. In future work, we also plan to conduct further reliability analysis using more effective metrics.

[2] For an erasure coded system, a common practice to repair from a node failure is for a new node to download subsets of data stored at a number of surviving nodes, reconstruct a lost coded block using the downloaded data, and store it at the new node. We show that this procedure is sub-optimal. We introduce the notion of regenerating codes, which allow a new node to download functions of the stored data from the surviving nodes. Erasure code Maximum Distance Separable(MDS). General theoretic framework that can determine the information that must be communicated to repair failures in encoded systems and identified a tradeoff between storage and repair bandwidth. Interest involve how CPU processing and disk I/O will influence the system performance, as well as integrity and security for the linear combination packets. for any finite information flow graph, there exists regenerating code that can achieve any point on the minimum storage/bandwidth feasible region we computed.

We plan to investigate deterministic designs of regenerating codes over small finite fields, the existence of systematic regenerating codes, designs that minimize the overhead storage of the coefficients, as well as the impact of node dynamics in reliability.

[3] It works under the simple assumption of thin-cloud storage and allows different parameters to be fine-tuned for a performance-security trade-off. We implement and evaluate the overhead of our DIP scheme in a real cloud storage testbed under different parameter choices. We further analyze the security strengths of our DIP scheme via mathematical models. We demonstrate that remote integrity checking can be feasibly integrated into regenerating codes in practical deployment. FMSR(Funcctional minimum storage regenerating),Cryptographic primitives. They are designed for a single-server setting. Consider regenerating-coded storage, there are key differences with our work. First, their design extends the single-server compact POR scheme by Shacham and Waters.However, such direct adaptation inherits some shortcomings of the single-server scheme such as a large storage overhead, as the amount of data stored increases with a more flexible checking granularity in the scheme. We pose the study of different possible corruption approaches as future work.

[4]"Cooperative Security for Network Coding File Distribution".Christos Gkantsidis and Pablo Rodriguez Rodriguez. In this scheme, users not only cooperate to distribute the content,but (well-behaved) users also cooperate to protect themselves against malicious users by informing affected nodes when a malicious block is found.It also protect from DoS attact. 1)Peer 2)Cryptography,limitations such techniques do not work well with recent network coding techniques that promise to improve the resilience and throughput of content distribution.In future Currently they have an implementation of a P2P content distribution system based on network coding similar to the one described in this paper which supports security against entropy as well as jamming attacks. We plan on reporting our experiences with such live system in future work.

[5] An Efficient and Secure Dynamic Auditing Protocol for Data Storage in Cloud Computing by Kan Yang, Student Member, IEEE, Xiaohua Jia, Senior Member, IEEE.In this paper we extend our auditing protocol to support the data dynamic operations, which is efficient and provably secure in the random oracle model. We further extend our auditing protocol to support batch auditing for both multiple owners and multiple clouds, without using any trusted organizer. The analysis and simulation results show that our proposed auditing protocols are secure and efficient, especially it reduce the computation cost of the auditor.By using Confidentiality,Dynamic Auditing ,Batch Auditing ,Datafragment technique. It is easy to find that our schemincurs less computation cost of the auditor than Zhu's IPDP scheme, especially when there are a large number of clouds in the large scale cloud storage systems.Protocol cannot perform block insertions anywhere(only append-type insertions are allowed).Schemes incur heavy computation cost of the auditor, which makes the auditing system inefficient.In future In this scheme batch auditing can be used for multiple owners.

[6] Storing Shared Data on the Cloud via Security-Mediator by author Boyang Wang , Sherman S.M. Chow , Ming Li , and Hui Li. We propose a simple and efficient publicly verifiable approach to ensure cloud data integrity without sacrificing the anonymity of data owners nor requiring significant verification metadata. Specifically, we introduce(SEM), which is able to generate verification metadata (i.e., signatures) on outsourced data for data owners.By implementing Provable Data Possession (PDP) ,Securitymediator (SEM),Public Key Infrastructure (PKI)

The limitation these three schemes are not able to preserve the identities of data owners.

[7] DEPSKY: Dependable and Secure Storage in a Cloud-of-Clouds by Alysson Bessani Miguel Correia Bruno Quaresma Fernando Andr´e Paulo Sousa. We observed that our protocols improved the perceived availability and, in most cases, the access latency when compared with cloud providers individually. Moreover, the monetary costs of using DEPSKY on this scenario is twice the cost of using a single cloud, which is optimal and seems to be a reasonable cost, given the benefits. DEPSKY ,AES ,HTTPS, REST APIs. The limitation is lke that 1) Cloud computing has limitations related to security and privacy, which should be accounted for, especially in the context of critical applications. 2) Data unit of size S consumes n S storage capacity of the system and costs on average n times more than if it was stored in a single cloud.In future Many applications are moving to the cloud, so, it is possible to think of new applications that would use the storage cloud as a back-end storage layer. Systems like databases, file systems, objects stores and keyvalue databases can use the cloud as storage layer as long as caching and weak consistency models are used to avoid paying the price of cloud access on every operation.

[8] Privacy-Preserving Public Auditing for Secure Cloud Storage by Cong Wang, Student Member, IEEE, Sherman S.-M. Chow, Qian Wang, Student Member, IEEE,Kui Ren, Member, IEEE, and Wenjing Lou, Member, IEEE. We propose a secure cloud storage system supporting privacy-preserving public auditing. We further extend our result to enable the TPA to perform audits for multiple users simultaneously and efficiently. Extensive security and performance analysis show the proposed schemes are provably secure and highly efficient. by implementing KeyGen ,SigGen ,GenProof,VerifyProof, the limitattions are Without a properly designed auditing protocol, encryption itself cannot prevent data from "flowing away" towards external parties during the auditing process. It can only support static data, and cannot efficiently deal with dynamic data at all and With random masking, the TPA no longer has all the necessary information to build up a correct group of linearequations and therefore cannot derive the user's data content, no matter how many linear combinations of the same set of file blocks can be collected.The future In addition to help users to evaluate the risk of their subscribed cloud data services, the audit result from TPA would also be beneficial for the cloud service providers to improve their cloud based service platform, and even serve for independent arbitration purposes.

[9] Provable Data Possession at Untrusted Stores by Giuseppe Ateniese† Randal Burns† Reza Curtmola† Joseph Herring Lea Kissner Zachary Peterson† Dawn Song . We present two provably-secure PDP schemes that are more efficient than previous solutions, even when compared with schemes that achieve weaker guarantees. In particular, the overhead at the server is low (or even constant), as opposed to linear in the size of the data. Experiments using our implementation verify the practicality of PDP and reveal that the performance of PDP is bounded by disk I/O and not by cryptographic computation. Remote ,Provable Data Possession (PDP),KeyGen,TagBlock,GenProof,CheckProof

The limitation of the algorithm lies in the computational complexity at the server, which must exponentiate the entire file, accessing all of the file's blocks.In future In contrast, our PDP schemes can be applied to (large) public databases(e.g., digital libraries,astronomy/medical/legal repositories,archives, etc.) other than encrypted ones and put no restriction on the number of challenges that can be executed.The variant of the protocol described above that does not rely on KEA1-r can be further modified in order to offer the public verifiability property, which allows anyone, not just the data owner, to challenge the server for data possession.

[10] Privacy-Preserving Audit and Extraction of Digital Contents by Mehul A. Shah, Ram Swaminathan, Mary Baker

To make storage services accountable for data loss, we present protocols that allow a thirdparty auditor to periodically verify the data stored by a service and assist inreturning the data intact to the customer. Most importantly, our protocols are privacy-preserving, in that they never reveal the data contents to the auditor. Our solution removes the burden of verification from the customer, alleviates both the customer's and storage service's fear of data leakage, and provides a method for independent arbitration of data retention contracts.by implementing symmetric-key encryption,Provable data possession"(PDP),Peer-to-Peer (P2P),Proof of retrievability (POR),Public-key infrastructure (PKI). the limitation The customer, however, cannot tell which challenge (xi,1 or xi,2) the service generated and which the auditor generated since

they are drawn from the same distribution.The customer offers no additional information and the auditor cannot recover either K or z.The auditor ensures both the service and customer agree on contents of the encrypted data and encryption key; otherwise, the auditor cannot resolve future disputes. For future work, we should consider modifying previous schemes [1, 2, 11, 23] to allow privacypreserving audit and extraction. Certainly a hybrid as mentioned above is simple, but it still imposes the encryption and decryption overheads that the storage service and customer experience with our protocols. It may be possible to eliminate the encryption key altogether. To do so, we must first extend the formal definitions of proofs of possession or proofs of retrievability to include a notion of privacy from the auditor.

[11] Data Security, Privacy, Availability and Integrity in Cloud Computing: Issues and Current Solutions by Sultan Aldossary,William Allen. We present those issues that are preventing people from adopting the cloud and give a survey on solutions that have been done to minimize risks of these issues. For example, the data stored in the cloud needs to be confidential, preserving integrity and available.Moreover, sharing the data stored in the cloud among many users is still an issue since the cloud service provider is untrustworthy to manage authentication and authorization. In this paper, we list issues related to data stored in cloud storage and solutions to those issues which differ from other papers which focus on cloud as general by implementing Meadia Access Control (MAC). the Limitation are Key management issue and the need to get fine grained access to file, such part of it.Also, this solution is not flexible and scalable because encryption and decryption is needed when a user leave the group in order.There are many security issues coming with this technology as happens when every technology matures. Those issues include issues related to the previous issues of the internet, network issues, application issues, and storage issues.The future Cloud computing is an emerging technology that will receive more attention in the future from industry and academia.

[12] Ensuring Data Storage Security in Cloud Computing by Cong Wang ,Qian Wang , Kui Ren , and Wenjing Louy. the identification of misbehaving server(s). Unlike most prior works, the new scheme further supports secure and efficient dynamic operations on data blocks, including: data update, delete and append. Extensive security and performance analysis shows that the proposed scheme is highly efficient and resilient against Byzantine failure, malicious data modification attack, and even server colluding attacks.By implementing Simple Storage Service (S3),Elastic Compute Cloud (EC2),Third Party Auditor (TPA).the limitations are like Traditional cryptographic primitives for the purpose of data security protection can not be directly adopted due to the users' loss control of data under Cloud Computing.Cloud Computing is not just a third party data warehouse. The data stored in the cloud may be frequently updated by the users, including insertion, deleting, modification, appending, reordering, etc.

In future An efficient insert operation is difficult to support and thus we leave it for our future work.

III. Problem Definition

To design a secure cloud storage system using network encoding system developed using AES DES Algorithm procedure powered with hash verification functionality.

IV. Conclusion And Future Scope

This survey paper has highlighted the need of secure cloud storage mechanism and present issues in existing techniques. The technique have certain shortcoming and need to improve in terms of secure encryption algorithms .There are numerous encryption techniques exists which have shortcomings. Future project would be proposing technique to overcome this shotcomings.

V. Acknowledgment

I do acknowledge my guide for approving this project topic and providing proper technique and guidance

References

[1] G. Eason, B. Noble, and I. N. Sneddon, "On certain integrals of Lipschitz-Hankel type involving products of Bessel functions," Phil. Trans. Roy. Soc. London, vol. A247, pp. 529–551, April 1955. *(references)*

[2] J. Clerk Maxwell, A Treatise on Electricity and Magnetism, 3rd ed., vol. 2. Oxford: Clarendon, 1892, pp.68–73.

[3] S. Jacobs and C. P. Bean, "Fine particles, thin films and exchange anisotropy," in Magnetism, vol. III, G. T. Rado and H. Suhl, Eds. New York: Academic, 1963, pp. 271–350.

[4] K. Elissa, "Title of paper if known," unpublished.

[5] R. Nicole, "Title of paper with only first word capitalized," J. Name Stand. Abbrev., in press.

[6] Y. Yorozu, M. Hirano, K. Oka, and Y. Tagawa, "Electron spectroscopy studies on magneto-optical media and plastic substrate interface," IEEE Transl. J. Magn. Japan, vol. 2, pp. 740–741, August 1987 [Digests 9th Annual Conf. Magnetics Japan, p. 301, 1982].

[7] M. Young, The Technical Writer's Handbook. Mill Valley, CA: University Science, 1989.