ANALYSIS AND SECURING RESOURCES IN DECENTRALIZED CLOUD

NALAM PHANI SAI KUMARI [1], P.RAGHUVEER [2]

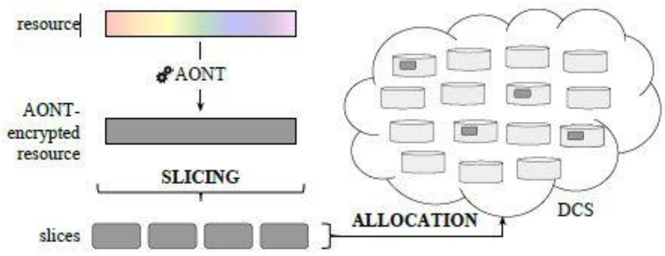
[1]Student (MCA), NRI INSTITUTE OF TECHNOLOGY, A.P., India.

[2]Assistant Professor, Dept. of MCA, NRI INSTITUTE OF TECHNOLOGY, A.P., India.

Abstract —In this paper, Decentralized Cloud Storage services represent a promising opportunity for a different cloud market, meeting the supply and demand for IT resources of an extensive community of users. The dynamic and independent nature of the resulting infrastructure introduces security concerns that can represent a slowing factor towards the realization of such an opportunity, otherwise clearly appealing and promising for the expected economic benefits. In this paper, we present an approach enabling resource owners to effectively protect and securely delete their resources while relying on decentralized cloud services for their storage. Our solution combines All-Or-Nothing-Transform for strong resource protection, and carefully designed strategies for slicing resources and for their decentralized allocation in the storage network. We address both availability and security guarantees, jointly considering them in our model and enabling resource owners to control their setting.

INTRODUCTION

In general, the procurement and management of IT resources exhibit significant scale economies, and large-scale CSPs can provide services at costs that are less than those incurred by smaller players. Still, many users have an excess of computational, storage, and network capacity in the systems they own and they would be interested in offering these resources to other users in exchange of a rent payment. In the classical behavior of markets, the existence of an infrastructure that supports the meeting of supply and demand for IT services would lead to a significant opportunity for the creation of economic value from the use of otherwise under-utilized resources.This change of landscape is witnessed by the increasing attention of the research and development community toward the realization of Decentralized Cloud Storage (DCS) services, characterized by the availability of multiple nodes that can be used to store resources in a decentralized manner. In such services, individual resources are fragmented in shards allocated (with replication to provide availability guarantees) to different nodes. Access to a resource requires retrieving all its shards. The main characteristics of a DCS is the cooperative and dynamic structure formed by independent nodes (providing a multi-authority storage network) that can join the service and offer storage space, typically in exchange of some reward. This evolution has been facilitated by blockchain-based technologies providing an effective low-friction electronic payment system supporting the remuneration for the use of the service. On platforms such as Storj [1], SAFE Network Vault [2], [3], IPFS [4], and Sia [5], users can rent out their unused storage and bandwidth to offer a service to other users of the network, who pay for this service with a network crypto-currency [6].However, if security concerns and perception of (or actual) loss of control have been an issue and slowing factor for centralized clouds, they are even more so for a decentralized cloud storage, where the dynamic and independent nature of the network may hint to a further decrease of control of the owners on where and how their resources are managed. Indeed, in centralized cloud systems, the CSP is generally assumed to be honest-but-curious and is then trusted to perform all the operations requested by authorized users (e.g., delete a file when requested by the owner) [7]. The CSP is discouraged to behave maliciously, since this would clearly impact its reputation. On the contrary, the nodes of a decentralized system may behave maliciously when their misbehavior can provide economic benefits without impacting reputation (e.g., sell the content of deleted files). Client-side encryption typically assumed in DCSs provides a first crucial layer of protection, but it leaves resources exposed to threats, especially in the long term. For instance, resources are still vulnerable in case the encryption key is exposed, or in case of malicious nodes not deleting their shards upon the owner's request to try reconstructing the resource in its entirety.



LITERATURE SURVEY

A survey on security and privacy issues of bitcoin

Bitcoin is a popular cryptocurrency that records all transactions in a distributed append-only public ledger called blockchain. The security of Bitcoin heavily relies on the incentive-compatible proof-of-work (PoW) based distributed consensus protocol, which is run by the network nodes called miners. In exchange for the incentive, the miners are expected to maintain the blockchain honestly. Since its launch in 2009, Bitcoin economy has grown at an enormous rate, and it is now worth about 150 billions of dollars. This exponential growth in the market value of bitcoins motivate adversaries to exploit weaknesses for profit, and researchers to discover new vulnerabilities in the system, propose countermeasures, and predict upcoming trends. In this paper, we present a systematic survey that covers the security and privacy aspects of Bitcoin. We start by giving an overview of the Bitcoin system and its major components along with their functionality and interactions within the system. We review the existing vulnerabilities in Bitcoin and its major underlying technologies such as blockchain and PoW-based consensus protocol. These vulnerabilities lead to the execution of various security threats to the standard functionality of Bitcoin. We then investigate the feasibility and robustness of the state-of-the-art security solutions. Additionally, we discuss the current anonymity considerations in Bitcoin and the privacy-related threats to Bitcoin users along with the analysis of the existing privacy-preserving solutions. Finally, we summarize the critical open challenges, and we suggest directions for future research towards provisioning stringent security and privacy solutions for Bitcoin.

A case for redundant arrays of inexpensive disks (RAID)

Increasing performance of CPUs and memories will be squandered if not matched by a similar performance increase in I/O. While the capacity of Single Large Expensive Disks (SLED) has grown rapidly, the performance improvement of SLED has been modest. Redundant Arrays of Inexpensive Disks (RAID), based on the magnetic disk technology developed for personal computers, offers an attractive alternative to SLED, promising improvements of an order of magnitude in performance, reliability, power consumption, and scalability. This paper introduces five levels of RAIDs, giving their relative cost/performance, and compares RAID to an IBM 3380 and a Fujitsu Super Eagle.

HAIL: A high-availability and integrity layer for cloud storage

We introduce HAIL (High-Availability and Integrity Layer), a distributed cryptographic system that allows a set of servers to prove to a client that a stored file is intact and retrievable. HAIL strengthens, formally unifies, and streamlines distinct approaches from the cryptographic and distributed-systems communities. Proofs in HAIL are efficiently computable by servers and highly compact---typically tens or hundreds of bytes, irrespective of file size. HAIL cryptographically verifies and reactively reallocates file shares. It is robust against an active, mobile adversary, i.e., one that may progressively corrupt the full set of servers.

PROPOSED SYSTEM

Protection of the encryption key is therefore not sufficient in DCS scenarios, as it remains exposed to the threats above. A general security principle is to rely on more than one layer of defense. In this paper, we propose an additional and orthogonal layer of protection, which is able to mitigate these risks.On the positive side, however, we note that the decentralized nature of DCS systems also increases the reliability of the service, as the involvement of a collection of independent parties reduces the risk that a single malfunction can limit the accessibility to the stored resources. In addition to this, the independent structure characterizing DCS systems - if coupled with effective resource protection and careful allocation to nodes in the network - makes them promising for actually strengthening security guarantees for owners relying on the decentralized network for storing their data.

The proposed solution also enables the resource owners to securely delete their resources when needed, even when some of the nodes in the DCS misbehave. Second, we investigate different strategies for slicing and distributing resources across the decentralized network, and analyze their characteristics in terms of availability and security guarantees. Third, we provide a modeling of the problem enabling owners to control the granularity of slicing and the diversification of allocation to ensure the aimed availability and security guarantees. We demonstrate the effectiveness of the proposed model by conducting several experiments on an implementation based on an available DCS system. Our solution provides an effective approach for protecting data in decentralized cloud storage and ensures both availability and protection responding to currently open problems of emerging DCS scenarios, including secure deletion. In fact, common secret sharing solutions (e.g., Shamir [8]), while considering apparently similar requirements are not applicable in scenarios where the whole resource content (and not simply the encryption key) needs protection, because of their storage and network costs (e.g., each share in Shamir's method has the same size as the whole data that has to be protected).

IMPLEMENTATION

1. **CSP**

   In this application csp is a module, csp can login directly with username and password.

   After download csp can perform some actions like view data owner and authorize, view data users and authorize and also can view all files.

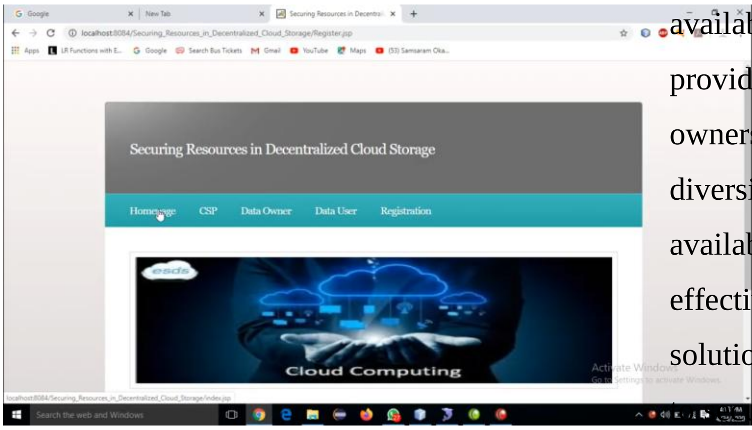
2. **DataOwner**

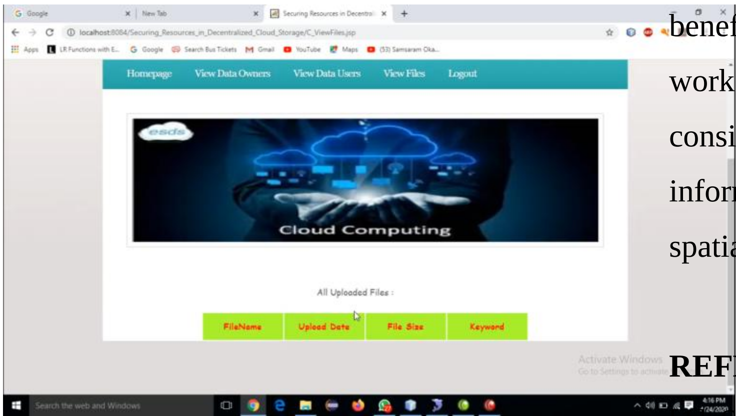
   Here data owner should register and should authorized by the cloud then only the owner can login with the application after his successful login he can perform some actions like uploadfile, view files, view file requests.

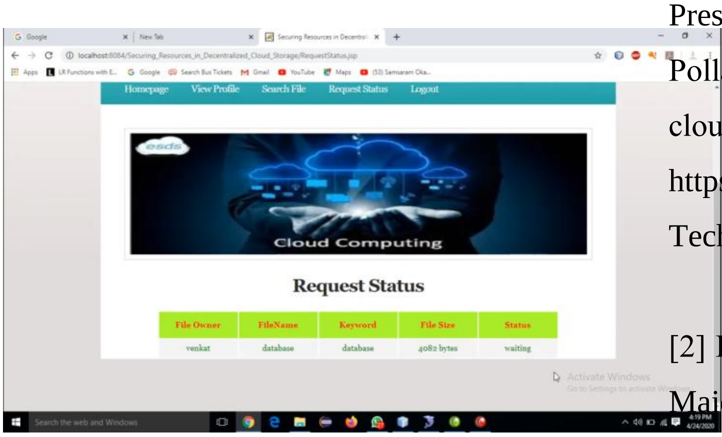
3. **Data User**

   Here data user should register and should authorized by the cloud then only the user can login with the application after his successful login he can perform some actions like view profiles, search file, request status

SAMPLE OUTPUT SCREENSHOTS







CONCLUSION

In this paper, Our approach enables resource owners to protect their resources and to control their decentralized allocation to different nodes in the network. We investigated different strategies for splitting and distributing resources, analyzing their characteristics in terms of availability and security guarantees. We also provided a modeling of the problem enabling owners to control the granularity of slicing and diversification of allocation to ensure aimed availability and security guarantees. Enabling effective control for resource owners, our solution helps in removing natural reluctance due to security concerns and moves a step forward in the realization of novel services effectively benefiting from technological evolution. Our work leaves room for extensions, such as the consideration of error correcting codes and information dispersal algorithms to reduce the spatial overhead.

REFERENCES

[1] S. Wilkinson, T. Boshevski, J. Brandoff, J. Prestwich, G. Hall, P. Gerbes,P. Hutchins, C. Pollard, and V. Buterin, “Storj: a peer-to-peer cloudstorage network (v2.0),” https://storj.io/storjv2.pdf, Storj Labs Inc., Tech.Rep., 2016.

[2] D. Irvine, “Maidsafe distributed file system,” MaidSafe, Tech. Rep.,2010.

[3] G. Paul, F. Hutchison, and J. Irvine, "Security of the maidsafe vault network," in Wireless World Research Forum Meeting 32, Marrakesh, Morocco, May 2014.

[4] J. Benet, "IPFS-content addressed, versioned, P2P file system," Protocol Labs, Tech. Rep., 2014.

[5] D. Vorick and L. Champine, "Sia: Simple decentralized storage," https: //sia.tech/sia.pdf, Nebulous Inc., Tech. Rep., 2014.

[6] C. Patterson, "Distributed content delivery and cloud storage," https: //www.smithandcrown.com/distributed-content-delivery-cloud-storage/, Smith and Crown, Tech. Rep., 2017.

[7] H. Hacig¨um¨us¸, B. Iyer, C. Li, and S. Mehrotra, "Executing SQL over encrypted data in the database-service-provider model," in Proc. of ACM SIGMOD, Madison, Wisconsin, June 2002.

[8] A. Shamir, "How to share a secret," Communications of the ACM, vol. 22, no. 11, pp. 612–613, September/December 1979.

[9] E. Bacis, S. De Capitani di Vimercati, S. Foresti, S. Paraboschi, M. Rosa, and P. Samarati, "Mix&Slice: Efficient access revocation in the cloud," in Proc. of ACM CCS, Vienna, Austria, October 2016.

[10] N. Lambert and B. Bollen, "The SAFE network - a new, decentralised internet," http://docs.maidsafe.net/Whitepapers/pdf/TheSafeNetwork.pdf, MaidSafe, Tech. Rep., 2014.

[11] M. Conti, E. S. Kumar, C. Lal, and S. Ruj, "A survey on security and privacy issues of bitcoin," IEEE Communications Surveys & Tutorials, vol. 20, no. 4, pp. 3416–3452, 2018.

[12] D. A. Patterson, G. Gibson, and R. H. Katz, "A case for redundant arrays of inexpensive disks (RAID)," ACM SIGMOD Records, vol. 17, no. 3, pp. 109–116, Jun. 1988.

[13] K. D. Bowers, A. Juels, and A. Oprea, "HAIL: A high-availability and integrity layer for cloud storage," in Proc. of ACM CCS, Chicago, IL, USA, November 2009.

[14] ——, "Proofs of retrievability: Theory and implementation," in Proc. Of ACM CCSW, Chicago, IL, USA, November 2009.

[15] M. Albanese, S. Jajodia, R. Jhawar, and V. Piuri, "Dependable and resilient cloud computing," in Proc. of IEEE SOSE, Oxford, UK, March 2016.