International Journal for Research in Applied Science & Engineering Technology (IJRASET)

Distributed Verifiable Data Control in Cloud Storage

D.Maryleela[1], M.S.Vijayakumar[2]
[1]PG scholar, [2]Assistant Professor,
[1,2]Department of CSE, Tejaa Shakthi Institute of Technology for Women, Coimbatore

Abstract: Data integrity, Data Confidentiality is the main vital role in cloud storage. It allows the users to verify the outsourced data is kept intact without downloading the whole data. In Most of the area the clients have to store their data on multi cloud servers. At the same time, the integrity checking protocol must be efficient in order to save the verifier's cost. From the two points, we propose a novel remote data integrity checking model: ID-DPDP (identity-based distributed provable data possession) in multicloud storage. The formal system model and security model are given. Based on the bilinear pairings, a concrete ID-DPDP protocol is designed. The proposed ID-DPDP protocol is provably secure under the hardness assumption of the standard CDH (computational Diffie-Hellman) problem. In addition to the structural advantage of elimination of certificate management, our ID-DPDP protocol is also efficient and flexible. Based on the client's authorization, the proposed ID-DPDP protocol can realize private verification, delegated verification, and public verification.

I. INTRODUCTION

Cloud computing has been envisioned as the next generation architecture of the IT enterprise due to its long list of unprecedented advantages in IT: on demand self-service, ubiquitous network access, location-independent resource pooling, rapid resource elasticity, usage-based pricing, and transference of risk.

One fundamental aspect of this new computing model is that data is being centralized or outsourced into the cloud. From the data owners' perspective, including both individuals and IT enterprises, storing data remotely in a cloud in a flexible on-demand manner brings appealing benefits: relief of the burden of storage management, universal data access with independent geographical locations, an

Avoidance of capital expenditure on hardware, software, personnel maintenance, and so on.While cloud computing makes these advantages more appealing than ever, it also brings new and challenging security threats to the outsourced data. Since cloud service providers (CSP) are separate administrative entities, data outsourcing actually relinquishes the owner's ultimate control over the fate of their data. As a result, the correctness of the data in the cloud is put at risk due to the following reasons.First of all, although the infrastructures under the cloud are much more powerful and reliable than personal computing devices, they still face a broad range of both internal and external threats to data integrity. Outages and security breaches of noteworthy cloud services appear from time to time.

Amazon S3's recent downtime, Gmail's mass email deletion incident, and Apple Mobile Me's post-launch downtime are all such examples. Second, for benefits of their own, there are various motivations for CSPs to behave unfaithfully toward cloud customers regarding the status of their outsourced data. Examples include CSPs, for monetary reasons, reclaiming storage by discarding data that has not been or is rarely accessed, or even hiding data loss incidents to maintain a reputation.In short, although outsourcing data into the cloud is economically attractive for the cost and complexity of long-term largescale data storage, it does not offer any guarantee on data integrity and availability. This problem, if not properly addressed, may impede successful deployment of the cloud architecture.As data owners no longer physically possess the storage of their data, traditional cryptographic primitives for the purpose of data security protection cannot be directly adopted. In particular, simply downloading the data for its integrity verification is not a practical solution due to the high cost of input/output (I/O) and transmission across the network. Besides, it is often insufficient to detect data corruption only when accessing the data, as it does not give correctness assurance for un accessed data and might be too late to recover the data loss or damage. Considering the large size of the outsourced data and the owner's constrained resource capability, the tasks of auditing the data correctness in a cloud environment can be formidable and expensive for data owners. Moreover, from the system usability point of view, data owners should be able to just use cloud storage as if it is local, without worrying about the need to verify its integrity. Hence, to fully ensure data security and save data owners' computation resources, I propose to enable publicly auditable cloud storage services, where data owners can resort to an external third party

auditor (TPA) to verify the outsourced data when needed.

Third party auditing provides a transparent yet cost-effective method for establishing trust between data owner and cloud server. In fact, based on the audit result from a TPA, the released audit report would not only help owners to evaluate the risk of their subscribed cloud data services, but also be beneficial for the cloud service provider to improve their cloud based service platform. In a word, enabling public risk auditing protocols will play an important role for this nascent cloud economy to become fully established; where data owners will need ways to assess risk and gain trust in the cloud.

II. LITERATURE REVIEW

cloud storage has become an attractive and cost effective alternative for enterprises to outsource their valuable business data. however, there are security concerns pertaining to the integrity of data as the cloud server is treated as "untrusted". To overcome this problem many security schemes came into existence. recently zhuetal presented a technique known as provable data possession (pdp) for data integrity in cloud with distributed storage mechanisms. they considered multiple cloud service providers to store data in cooperative fashion. their solution makes use of homomorphic verifiable response indeed and multi-prover zero-knowledge system for ensuring data integrity. in this paper we practically implement the pdp scheme proposed by zhu et al. and build a prototype application to demonstrate the proof of concept. the empirical results reveal that the pdp scheme is very effective and can be used in real time multi-cloud environments.

provable data possession (PDP) that allows a client that has stored data at an untrusted server to verify that the server possesses the original data without retrieving it. The model generates probabilistic proofs of possession by sampling random sets of blocks from the server, which drastically reduces I/O costs. The client maintains a constant amount of metadata to verify the proof. The challenge/response protocol transmits a small, constant amount of data, which minimizes network communication. Thus, the PDP model for remote data checking supports large data sets in widely-distributed storage systems. 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 Data possession (RDP) is a technique for ensuring the data integrity in storage outsourcing. In this paper, based on authentication cloud service providers request customers to store the information in the cloud. RDP scheme is used for cloud storage to support the scalability of service and data migration. Cloud security is applied to protect data, applications and infrastructure associated with in the cloud. Remote data integrity checking is of crucial importance in cloud storage. It can make the clients verify whether their outsourced data is kept intact without downloading the whole data. In some application scenarios, the clients have to store their data on multi-cloud servers. At the same time, the integrity checking protocol must be efficient in order to save the verifier's cost. From the two points, we propose a novel remote data integrity checking model: Authentication-based Remote data possession in multi-cloud storage.

Identity-Based Provable data possession (PDP) is a technique for ensuring the integrity of data in storage outsourcing construction of an efficient scheme for distributed cloud storage to support the scalability of service and data migration, in which of multiple cloud service providers to cooperatively store and maintain the clients' data. Cloud computing has become an important thing in computer field. Cloud computing takes information processing as a service, such as storage and computing. Data integrity is important thing in cloud storage. In certain situations, clients should store their data such as image or text in multi cloud. When the client stores his/her data on multicloud servers, the distributed storage and integrity checking is very important. Here we propose an Identity Based Distributed Provable Data Possession (ID-DPDP) protocol for multi-cloud storage. Remote data integrity checking is important in cloud storage. It can make the clients verify whether their data is kept as it is without downloading the entire data. In some application scenarios, the clients have to store their data on multi-cloud servers. At the same time, the integrity checking protocol must be efficient in order to save the verifier's cost.

Cloud storage provides a convenient means of storing and retrieval of hug amount of data. With this facility, organizations and individuals can outsource their data to cloud. Though cloud storage gives significant benefits to users, there are security concerns as well. Since the cloud users store their valuable business data in cloud, the security is an utmost concern. Moreover the cloud server has to be untrusted since it is accessed through a public network such as Internet. Many techniques came into existence to address the storage security problem in cloud. However, providing data audit with low communication and computation cost is important. Recently Wang et al. presented a distributed storage integrity auditing mechanism. This mechanism is based on security approaches

such as erasure-coded data and homomorphic tokens. In this paper we practically implement the security mechanism using a prototype application that demonstrates the proof of concept. The empirical results revealed that the prototype is capable of preventing various attacks such as server colluding attacks, malicious data modification attack besides protecting byzantine failures

III. STRUCTURE AND TECHNIQUES

The infrastructures under the cloud are much more powerful and reliable than personal computing devices, they still face a broad range of both internal and external threats to data integrity. Outages and security breaches of noteworthy cloud services appear from time to time. Amazon S3's recent downtime, Gmail's mass email deletion incident, and Apple Mobile Me's post-launch downtime are all such examples. Second, for benefits of their own, there are various motivations for CSPs to behave unfaithfully toward cloud customers regarding the status of their outsourced data. Examples include CSPs, for monetary reasons, reclaiming storage by discarding data that has not been or is rarely accessed, or even hiding data loss incidents to maintain a reputation.

In short, although outsourcing data into the cloud is economically attractive for the cost and complexity of long-term largescale data storage, it does not offer any guarantee on data integrity and availability. This problem, if not properly addressed, may impede successful deployment of the cloud architecture.

As data owners no longer physically possess the storage of their data, traditional cryptographic primitives for the purpose of data security protection cannot be directly adopted. In particular, simply downloading the data for its integrity verification is not a practical solution due to the high cost of input/output (I/O) and transmission across the network.

Besides, it is often insufficient to detect data corruption only when accessing the data, as it does not give correctness assurance for unaccessed data and might be too late to recover the data loss or damage. Considering the large size of the outsourced data and the owner's constrained resource capability, the tasks of auditing the data correctness in a cloud environment can be formidable and expensive for data owners. Moreover, from the system usability point of view, data owners should be able to just use cloud storage as if it is local, without worrying about the need to verify its integrity. Hence, to fully ensure data security and save data owners' computation resources, we propose to enable publicly auditable cloud storage services, where data owners can resort to an external third party auditor (TPA) to verify the outsourced data when needed.

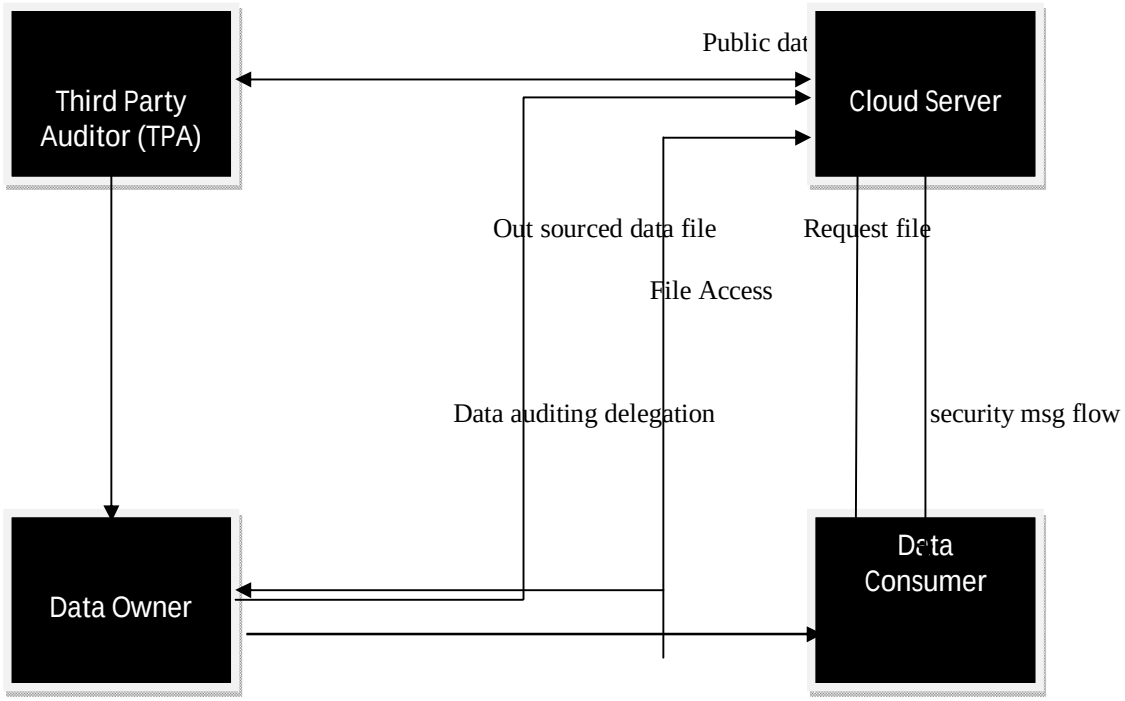

FIG 1. Architecture Diagram of ID-DPDP

A data flow diagram (DFD) is a graphical representation of the "flow" of data through an information system, modeling its process aspects. It does not show information about the timing of processes, or information about whether processes will operate

in sequecnce or in parallel. DFDs can also be used for the visualization of data processing (structured design).

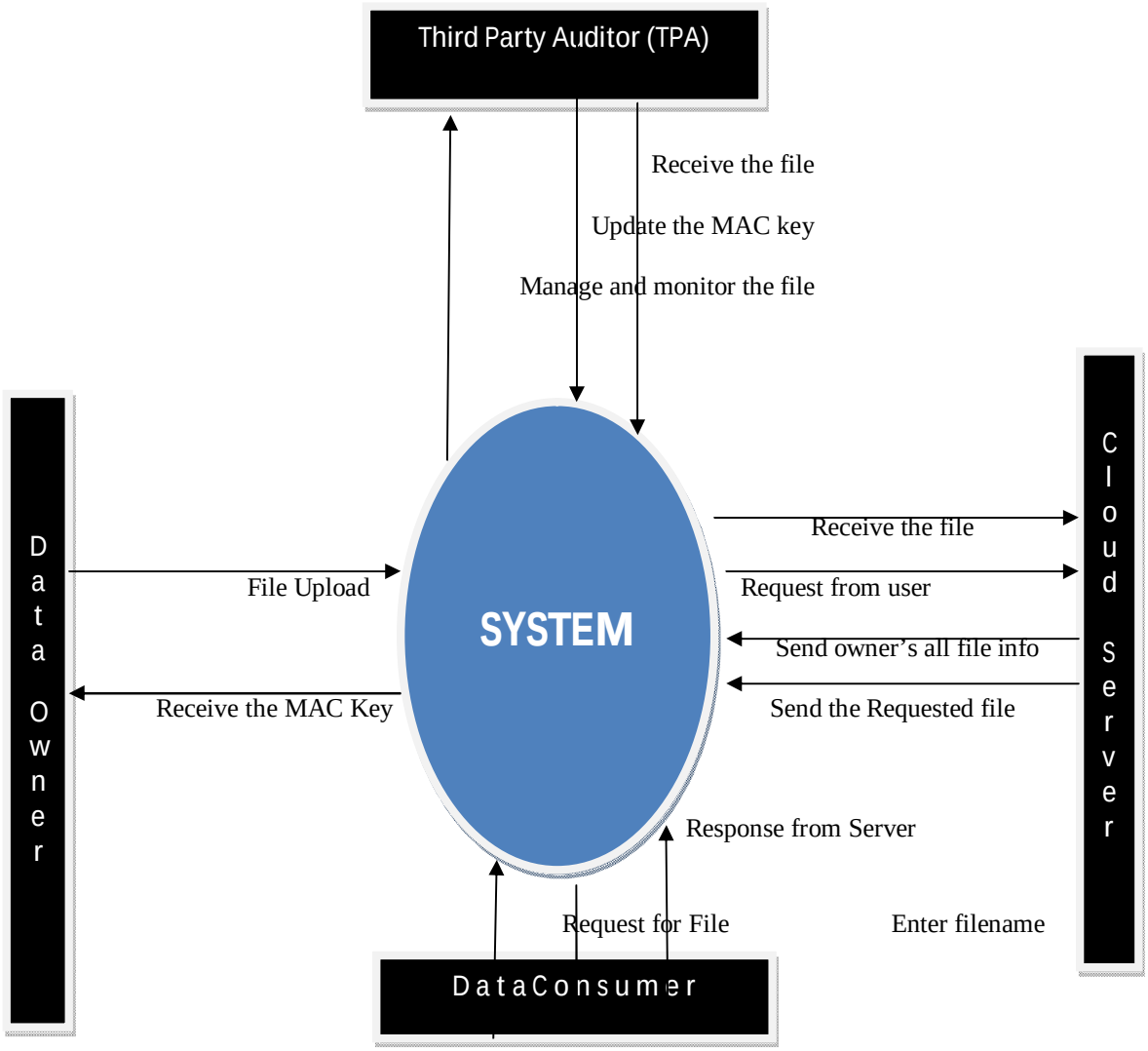

FIG 2. Context Diagram

Context diagram is a 0^{th} level of dataflow diagram, Request send to system then the request has been processed by third party auditor, then the response is send to the consumer.

Volume 4 Issue IV, April 2016
ISSN: 2321-9653
International Journal for Research in Applied Science & Engineering Technology (IJRASET)

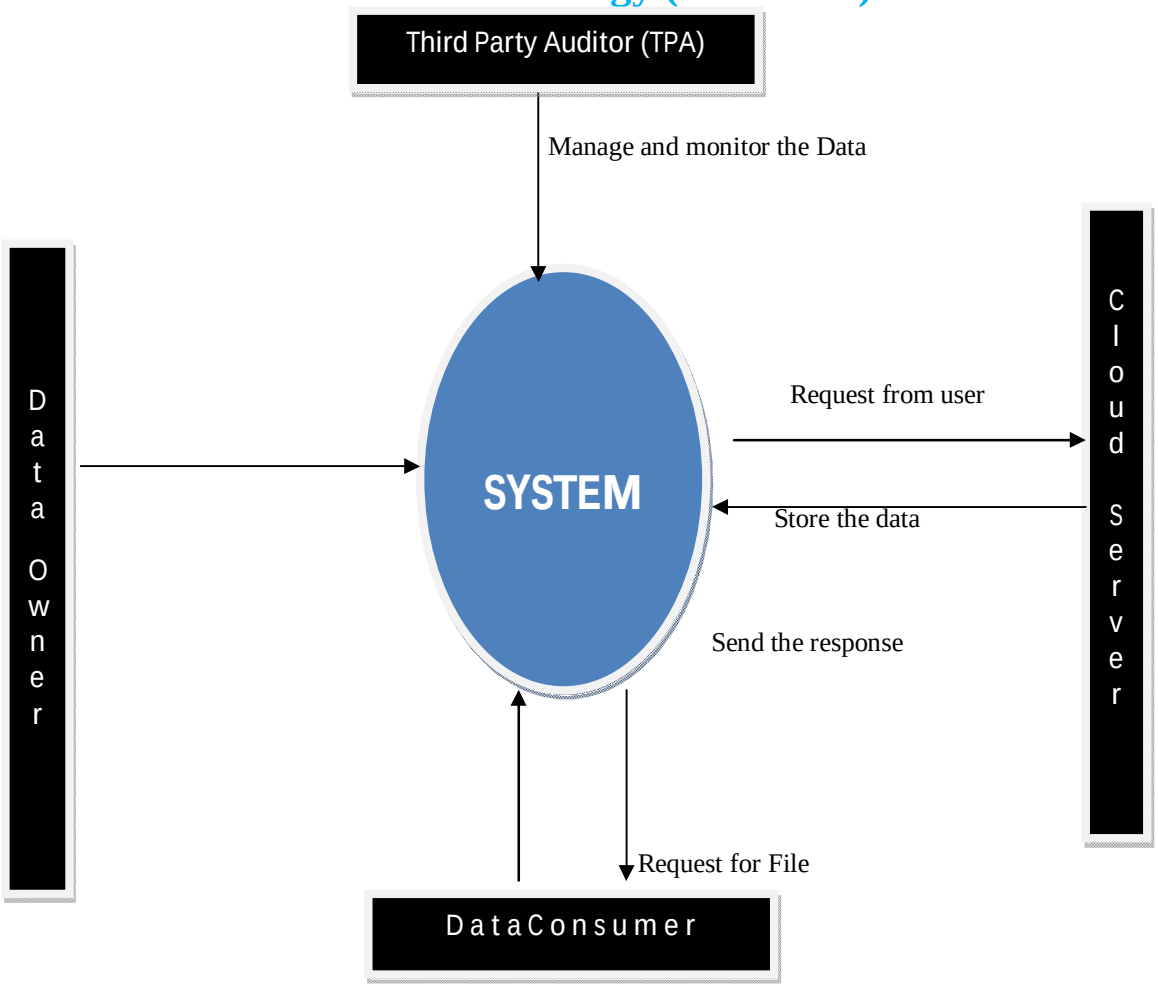

FIG 3. Level 1-DFD

Third party auditor fix a time frame for check the original data which is stored in cloud storage, and its replace the file which will be corrupted.

IV. RESULTS AND DISCUSSION

A. File Upload

Cloud storage is a service where data is remotely maintained, managed, and backed up., which is The service is available to users over a network usually the internet. It allows the users to store files online so that the user can access them from any location via internet. The provider company makes them available to the user online by keeping the uploaded files on an external server. This gives companies using cloud storage services ease and convenience, but can potentially be costly. Users should also be aware that backing up their data is still required when using cloud storage services, because recovering data from cloud storage is much slower than local backup

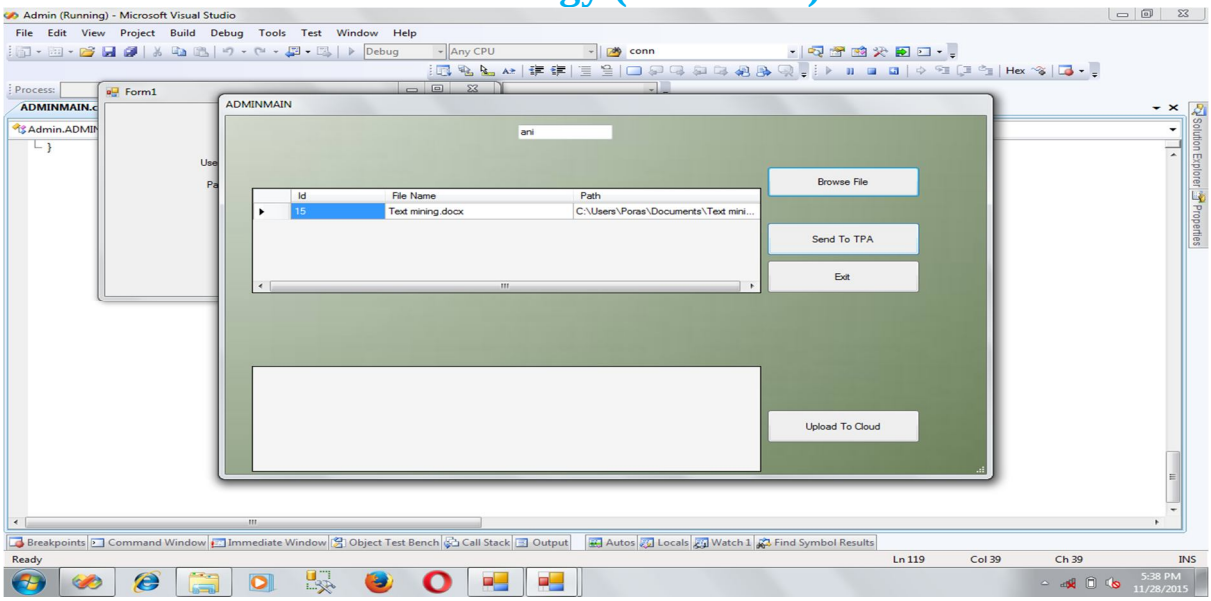

FIG 4. File Upload Using Security Keys

User can upload any file with some security keys, this key will generated by the system.

B. Cloud Server

Cloud service provider (CSP) to provide data storage service and has significant storage space and computation resources (we will not differentiate CS and CSP hereafter.).cloud servers work in the same way as physical servers but the functions they provide can be very different .When opting for cloud hosting, clients are renting virtual server space rather than renting or purchasing physical servers. They are often paid for by the depending on the capacity required at any particular time.

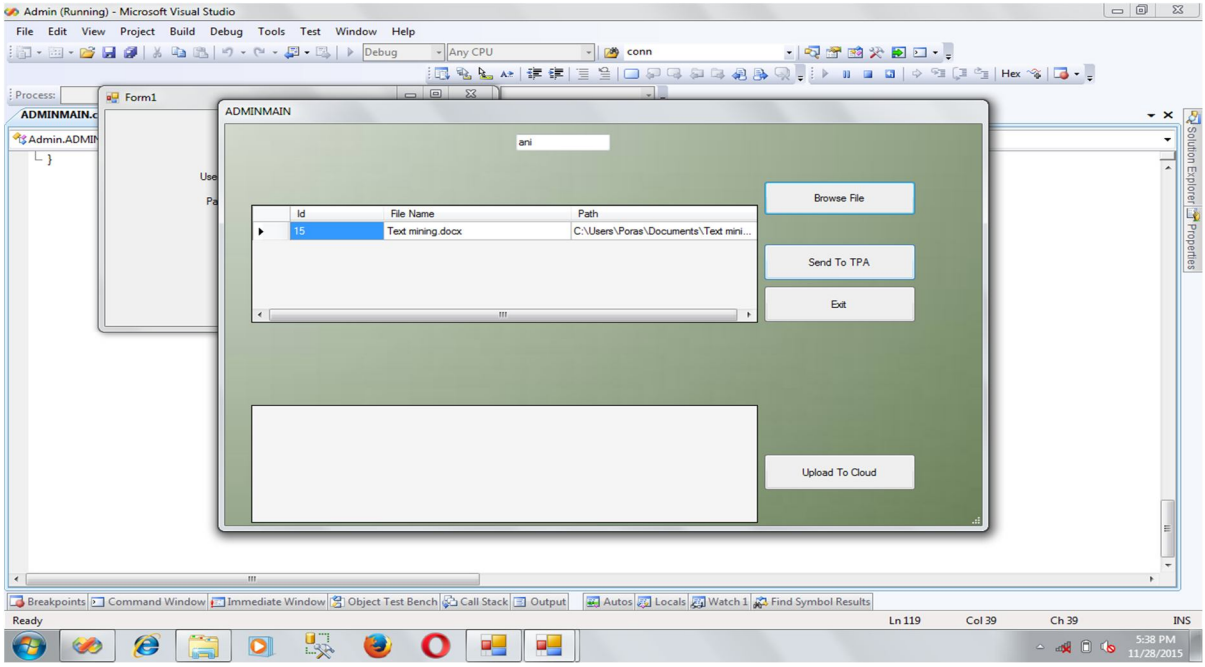

FIG 5. Cloud Server Access The File

C. TPA Request

An optional TPA, who has expertise and capabilities that users may not have, is trusted to assess and expose risk of cloud storage services on behalf of the users upon request.TPA is a kind of inspector .There are two categories: Private auditability and Public

auditability. Although Private auditability can achieve higher scheme efficiency, public auditability allows anyone, not just the client; to challenge the cloud server for the correctness of data of the data owner.TPA will audit the data of the client. It eliminates the involvement of the client by auditing that whether his data stored in the cloud are intact ,which can be important in achieving economics of scale for cloud computing.

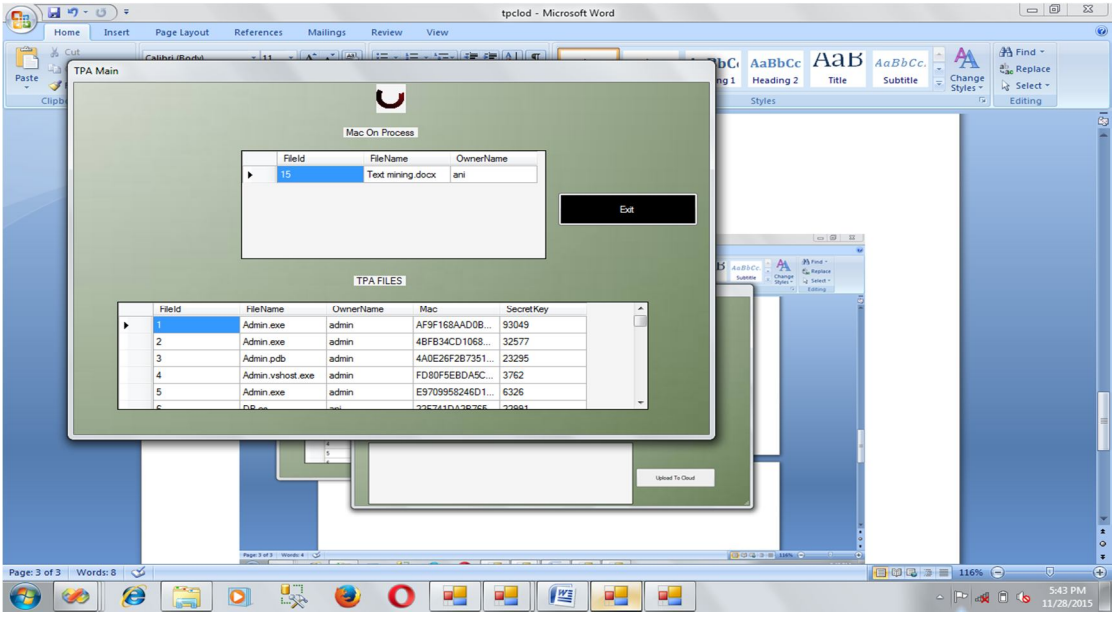

FIG 6. TPA Audit the Data of the Client

D. MAC Request

In cryptography, a **message authentication code** (often **MAC**) is a short piece of information used to authenticate a message. A MAC algorithm, sometimes called a **keyed** (**cryptographic**) **hash function**, accepts as input a secret key and an arbitrary-length message to be authenticated, and outputs a MAC (sometimes known as a *tag*). The MAC value protects both a message's data integrity as well as its authenticity, by allowing verifiers (who also possess the secret key) to detect any changes to the message content.

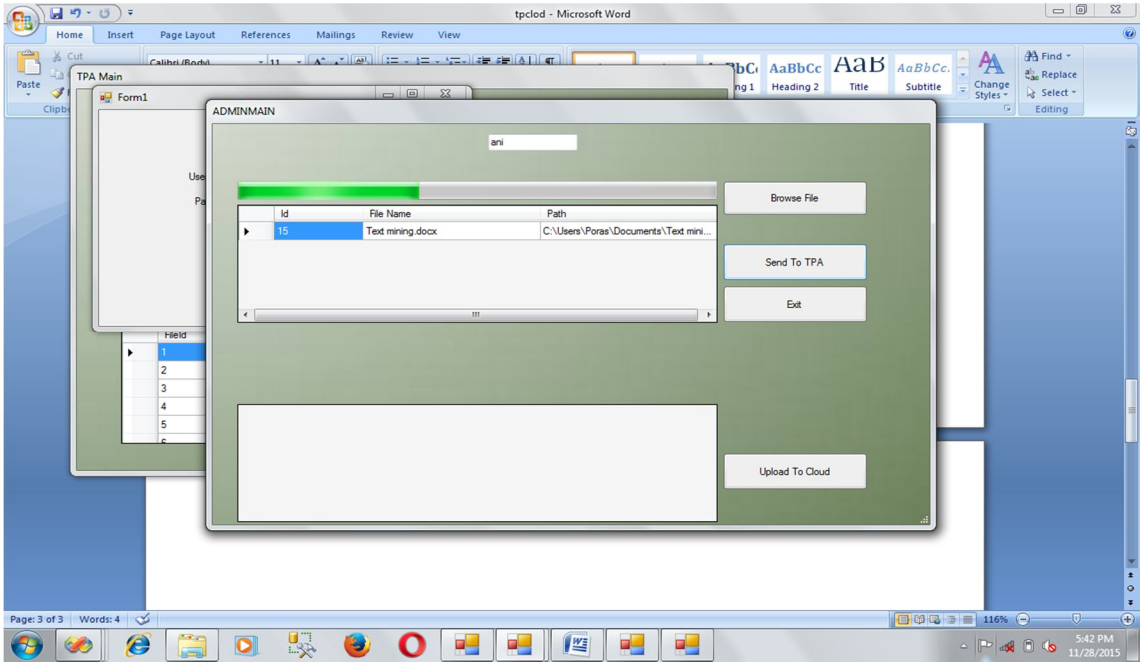

FIG 7. MAC is Ready to Generate the Secret Key

V. CONCLUSION

Cloud computing has been envisioned as the next-generation architecture of enterprise IT. In contrast to traditional enterprise IT solutions, where the IT services are under proper physical, logical, and personnel controls, cloud computing moves the application software and databases to servers in large data centers on the Internet, where the management of the data and services are not fully trustworthy. This unique attribute raises many new security challenges in areas such as software and data security, recovery, and privacy, as well as legal issues in areas such as regulatory compliance and auditing, all of which have not been well understood. In this project we focus on cloud data storage security. We first present network architecture for effectively describing, developing, and evaluating secure data storage problems

REFERENCES

[1] Scalable and Efficient Provable Data Possession Hadassa Katta1 Vivek Kolla2 P Raja Rao3 Department of Computer Science,Department of Computer Science M Tech Student, Dept., of CSE, QIS College of Engg., & Technology, Ongole, Prakasamdt, Assistant Professor, Dept., of CSE, QIS College of Engg., & TechnologyInternational Journal of Advanced Research in Computer and Communication Engineering Vol. 2, Issue 9, September 2013.

[2] Provable Data Possession at Untrusted Stores,Giuseppe Ateniese, Randal Burns, Reza Curtmola, Joseph Herring, Lea Kissner,Zachary Peterson, Dawn Song &14th ACM Conference on Computer and Communications Security(CCS 2007) [3].

[3] Authentication based remote data possession in multicloud storage Venkata Pallavi B, E.Padma Student, Asst.Professor, Dept.of CSE, SCSVMV University, Enathur, Kancheepuram (India),International Journal of Science, Technology & Management Volume No 04, Special Issue No. 01, March 2015.

[4] Distributed Provable Data Possession in Multi-Cloud Storage through Client Authentication,N.A Gayatri M.Th(CSE) Sankethika Vidya Parishad Engineering College,G.Kalyan Chakravarthi, M.Tech Assistant Professor Sankethika VidyaParishad Engineering . International Journal & Magazine of, Engineering,Technology,Management and Research,Volume 2, Issue 12,December 2015 ,ISSN: 2348 4845

[5] A Distributed Storage Integrity Auditing for Secure Cloud Storage Services Anuradha.R* , Dr. Y. Vijayalatha Department of CSE & JNTUH India, International Journal of Advanced Research in Computer Science and Software Engineering,Volume 3, Issue 8, August 2013 ISSN: 2277 128X

[6] Y. Zhu, H. Hu, G.J. Ahn, and M. Yu, ‘‘Cooperative Provable Data Possession for Integrity Verification in Multicloud Storage,’’ IEEE Trans. Parallel Distrib. Syst.,vol. 23, no. 12, pp. 2231-2244, Dec. 2012.

[7] Y. Zhu, H. Wang, Z. Hu, G.J. Ahn, H. Hu, and S.S. Yau, ‘‘Efficient Provable Data Possession for Hybrid Clouds,’’ in Proc. CCS,2010, pp. 756-758.

[8] R. Curtmola, O. Khan, R. Burns, and G. Ateniese, ‘‘MR-PDP: Multiple-Replica Provable Data Possession,’’ in Proc. ICDCS, 2008, pp. 411-420.

[9] A.F. Barsoum and M.A. Hasan, ‘‘Provable possession and replication of data over cloud servers,’’ Centre Appl. Cryptogr. Res., Univ. Waterloo, Waterloo, ON, Canada, Rep. 2010/32. [Online]. Available: http://www.cacr.math.uwaterloo.ca/ techreports/2010/cacr2010-32.pdf.

[10] Z. Hao and N. Yu, ‘‘A Multiple-Replica Remote Data Possession Checking Protocol with Public Verifiability,’’ in Proc. 2nd Int. Symp. Data, Privacy, E-Comm., 2010, pp. 84-89.

[11] A.F. Barsoum and M.A. Hasan, ‘‘On verifying dynamic multiple data copies over cloud servers,’’ Int. Assoc. Cryptol. Res., New York, NY, USA, IACR eprint Rep. 447, 2011. [Online]. Available: http://eprint.iacr.org/2011/447.pdf.