Volume No:4, Issue No:6 (November-2018) ISSN No : 2454-423X (Online)

International Journal of Research in Advanced Computer Science Engineering

A Peer Reviewed Open Access International Journal

www.ijracse.com

A Secured Dynamic-Hash-Table Based Public Auditing for Cloud Storage

Sk Samdani Basha
Department of Computer Science and Engineering,
Prakasam Engineering College,
O.V Road, Kandukur,
A.P -523105, India.

G.V Manikanth
Department of Computer Science and Engineering,
Prakasam Engineering College,
O.V Road, Kandukur,
A.P -523105, India.

Prof S.Sreenivasulu
Department of Computer Science and Engineering,
Prakasam Engineering College,
O.V Road, Kandukur,
A.P -523105, India.

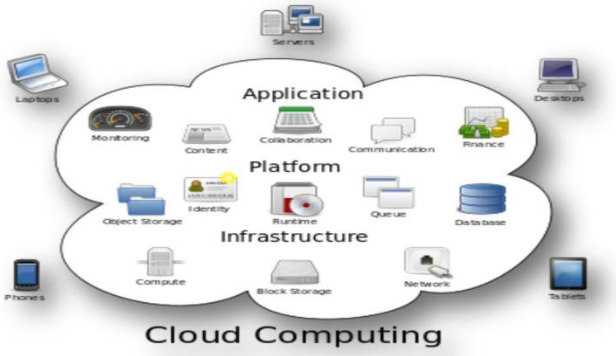
ABSTRACT

Cloud storage is an increasingly popular application of cloud computing, which can provide on-demand outsourcing data services for both organizations and individuals. However, users may not fully trust the cloud service providers (CSPs) in that it is difficult to determine whether the CSPs meet their legal expectations for data security. Therefore, it is critical to develop efficient auditing techniques to strengthen data owners' trust and confidence in cloud storage. In this paper, we present a novel public auditing scheme for secure cloud storage based on dynamic hash table (DHT), which is a new two-dimensional data structure located at a third parity auditor (TPA) to record the data property information for dynamic auditing. Differing from the existing works, the proposed scheme migrates the authorized information from the CSP to the TPA, and thereby significantly reduces the computational cost and communication overhead. Meanwhile, exploiting the structural advantages of the DHT, our scheme can also achieve higher updating efficiency than the state-of-the-art schemes. In addition, we extend our scheme to support privacy preservation by combining the homomorphic authenticator based on the public key with the random masking generated by the TPA, and achieve batch auditing by employing the aggregate BLS signature technique. We formally prove the security of the proposed scheme, and evaluate the auditing performance by detailed experiments and comparisons with the existing ones. The results demonstrate that the proposed scheme can effectively achieve secure auditing for cloud storage, and outperforms the previous schemes in computation complexity, storage costs and communication overhead.

INTRODUCTION

Cloud Computing

Cloud computing is the use of computing resources (hardware and software) that are delivered as a service over a network (typically the Internet). The name comes from the common use of a cloud-shaped symbol as an abstraction for the complex infrastructure it contains in system diagrams. Cloud computing entrusts remote services with a user's data, software and computation. Cloud computing consists of hardware and software resources made available on the Internet as managed third-party services. These services typically provide access to advanced software applications and high-end networks of server computers [1-3].



Cite this article as: Sk Samdani Basha, G.V Manikanth & Prof S.Sreenivasulu, "A Secured Dynamic-Hash-Table Based Public Auditing for Cloud Storage", International Journal of Research in Advanced Computer Science Engineering, Volume 4 Issue 6, 2018, Page 13-21.

How Cloud Computing Works?

The goal of cloud computing is to apply traditional supercomputing, or high-performance computing power, normally used by military and research facilities, to perform tens of trillions of computations per second, in consumer-oriented applications such as financial portfolios, to deliver personalized information, to provide data storage or to power large, immersive computer games.

The cloud computing uses networks of large groups of servers typically running low-cost consumer PC technology with specialized connections to spread data-processing chores across them. This shared IT infrastructure contains large pools of systems that are linked together. Often, virtualization techniques are used to maximize the power of cloud computing [4].

Characteristics

The salient characteristics of cloud computing based on the definitions provided by the National Institute of Standards and Terminology (NIST) [6] are outlined below:

On-demand self-service:

A consumer can unilaterally provision computing capabilities, such as server time and network storage, as needed automatically without requiring human interaction with each service's provider.

Broad network access:

Capabilities are available over the network and accessed through standard mechanisms that promote use by heterogeneous thin or thick client platforms (e.g., mobile phones, laptops, and PDAs) [8].

Resource pooling:

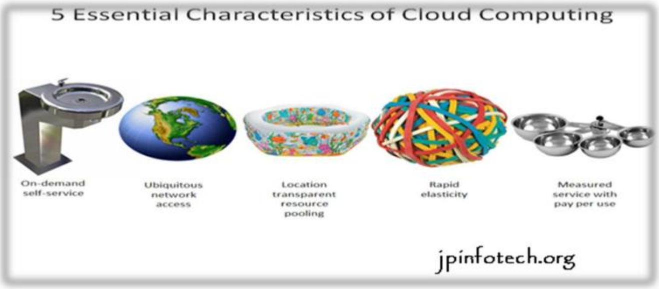
The provider's computing resources are pooled to serve multiple consumers using a multi-tenant model, with different physical and virtual resources dynamically assigned and reassigned according to consumer demand. There is a sense of location-independence in that the Customer generally has no control or knowledge over the exact location of the provided resources but may be able to specify location at a higher level of abstraction (e.g., country, state, or data center). Examples of resources include storage, processing, memory, network bandwidth, and virtual machines.

Rapid elasticity:

Capabilities can be rapidly and elastically provisioned, in some cases automatically, to quickly scale out and rapidly released to quickly scale in. To the consumer, the capabilities available for provisioning often appear to be unlimited and can be purchased in any quantity at any time.

Measured service:

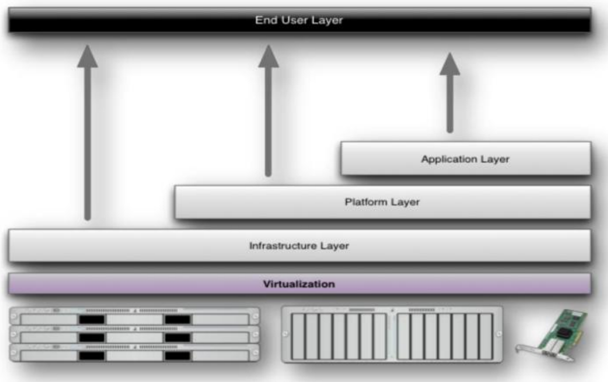
Cloud systems automatically control and optimize resource use by leveraging a metering capability at some level of abstraction appropriate to the type of service (e.g., storage, processing, bandwidth, and active user accounts). Resource usage can be managed, controlled, and reported providing transparency for both the provider and consumer of the utilized service.


5 Essential Characteristics of Cloud Computing
On-demand self-service
Ubiquitous network access
Location transparent resource pooling
Rapid elasticity
Measured service with pay per use
jpinfotech.org

Characteristics of cloud computing

Service Models

Cloud Computing comprises three different service models, namely Infrastructure-as-a-Service (IaaS), Platform-as-a-Service (PaaS), and Software-as-a-Service (SaaS) [10]. The three service models or layer are completed by an end user layer that encapsulates the end user perspective on cloud services. The model is shown in figure below. If a cloud user accesses services on the infrastructure layer, for instance, she can run her own applications on the resources of a cloud infrastructure and remain responsible for the support, maintenance, and security of these applications herself. If she accesses a service on the application layer, these tasks are normally taken care of by the cloud service provider.



Structure of service models

Benefits of Cloud Computing

1. Achieve economies of scale – increase volume output or productivity with fewer people. Your cost per unit, project or product plummets.
2. Reduce spending on technology infrastructure. Maintain easy access to your information with minimal upfront spending. Pay as you go (weekly, quarterly or yearly), based on demand.
3. Globalize your workforce on the cheap. People worldwide can access the cloud, provided they have an Internet connection.
4. Streamline processes. Get more work done in less time with less people.
5. Reduce capital costs. There’s no need to spend big money on hardware, software or licensing fees.
6. Improve accessibility. You have access anytime, anywhere, making your life so much easier!
7. Monitor projects more effectively. Stay within budget and ahead of completion cycle times.
8. Less personnel training is needed. It takes fewer people to do more work on a cloud, with a minimal learning curve on hardware and software issues.
9. Minimize licensing new software. Stretch and grow without the need to buy expensive software licenses or programs [12].
10. Improve flexibility. You can change direction without serious “people” or “financial” issues at stake.

Existing System

- Erway et al. first presented a dynamic provable data possession (DPDP) scheme, which extends the original PDP model by introducing a rank-based authenticated skip list.
- Wang et al. presented a public auditing scheme based on Merkle Hash Tree (MHT) [3], which can achieve the above auditing requirements.
- Zhu et al. proposed another public auditing scheme (IHT-PA) based on an index-hash table (IHT), which can effectively reduce both the computational costs and communication overhead by storing the data properties for auditing using the IHT in the TPA instead of the CSP [5].

Disadvantages of Existing System

- It is critical and significant to develop efficient auditing techniques to strengthen data owners′ trust and confidence in cloud storage, of which the core is how to effectively check data integrity remotely.
- The existing schemes would incur heavy computational costs of the TPA and large communication overhead during the updating and verification processes.
- The IHT is the key of IHT-PA to support data dynamics, but it is inefficient in updating operations, especially insertion and deletion operations [7].
- The existing systems would induce extra computational costs to the user and unnecessary communication overhead.

Proposed System

- This paper presents a public auditing scheme (DHT-PA) using a new data structure called dynamic hash table (DHT). Exploiting the DHT, our scheme can achieve dynamic auditing [9].
- Moreover, because DHT-PA migrates the authorized information from the CSP to the TPA, its computational costs and

Volume No:4, Issue No:6 (November-2018) ISSN No : 2454-423X (Online)

International Journal of Research in Advanced Computer Science Engineering

A Peer Reviewed Open Access International Journal

www.ijracse.com

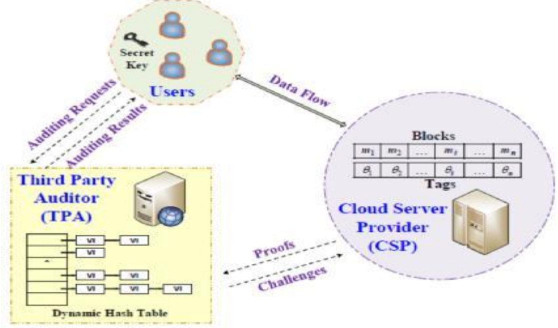
communication overhead are significantly smaller than the scheme based on skip list and the one based on MHT.

- DHT-PA also outperforms IHTPA in updating, as the times of updating operations on the DHT are much fewer than that on the IHT.
- In addition, we extend DHT-PA to achieve privacy preserving by combining the homomorphic authenticator based on the public key with random masking generated by the TPA.
- Furthermore, we employ the well-known BLS (Boneh-Lynn-Shacham) signature and bilinear maps to achieve batch auditing.

Advantages of Proposed System

- We present a novel public auditing scheme, which can completely support three vital functions, i.e., dynamic data auditing, privacy protection and batch auditing.
- We design a new data structure named DHT to record data properties for auditing in the TPA, and by virtue of it, achieve rapid auditing and efficient data updating.
- We formally prove the security of the proposed scheme, and evaluate its auditing performance by concrete experiments and comparisons with the state-of-the-art schemes.
- The results demonstrate that the proposed scheme can effectively achieve secure auditing in clouds, and outperforms the previous ones in computation complexity, storage costs and communication overhead.

System Architecture



Third Party Auditor (TPA):

TPA can verify the reliability of the cloud storage services (CSS) credibly and dependably on behalf of the users upon request. TPA is involved to check the integrity of the users data stored in the cloud. However, in the whole verification process, the TPA is not expected to be able to learn the actual content of the user’s data for privacy protection. We assume the TPA is credible but curious. In other words, the TPA can perform the audit reliably, but may be curious about the users data [11].

Dynamic Hash Table (DHT):

A hash table is a dynamic set data structure. It has three basic functions: to store data (SET/INSERT); to retrieve data (SEARCH/RETRIEVE), and to remove data that has previously been stored in the set (DELETE). In this way it is not different from other dynamic set data structure such as linked lists or trees.

The interesting about hash tables is their performance characteristics with respect to the store/retrieve/remove operations. In this regard, hash tables offer average constant time to perform any combination of the basic operations. This makes them extremely useful in many scenarios where quickly searching for an element is required, especially if multiple queries must be performed [13].

IMPLEMENTATION

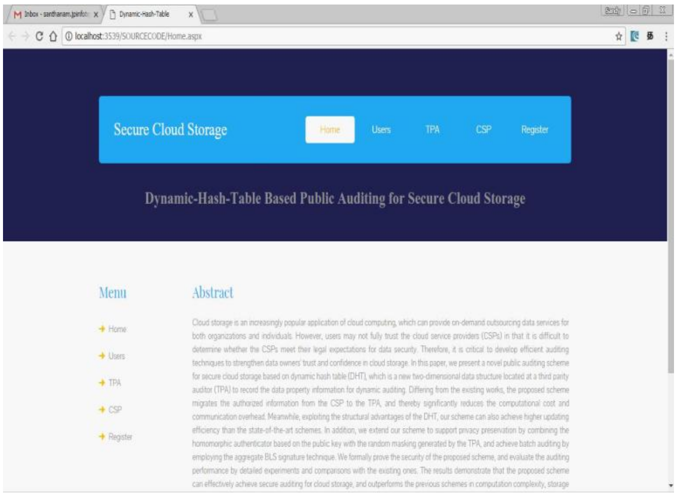
Algorithm

- This paper presents a public auditing scheme (DHT-PA) using a new data structure called dynamic hash table (DHT). Exploiting the DHT, our scheme can achieve dynamic auditing.
- Moreover, because DHT-PA migrates the authorized information from the CSP to the TPA, its computational costs and communication overhead are significantly smaller than the scheme based on skip list and the one based on MHT.

- DHT-PA also outperforms IHTPA in updating, as the times of updating operations on the DHT are much fewer than that on the IHT [6].
- In addition, we extend DHT-PA to achieve privacy preserving by combining the homomorphic authenticator based on the public key with random masking generated by the TPA.
- Furthermore, we employ the well-known BLS (Boneh-Lynn-Shacham) signature and bilinear maps to achieve batch auditing.
- We present a novel public auditing scheme, which can completely support three vital functions, i.e., dynamic data auditing, privacy protection and batch auditing.
- We design a new data structure named DHT to record data properties for auditing in the TPA, and by virtue of it, achieve rapid auditing and efficient data updating 4].
- We formally prove the security of the proposed scheme, and evaluate its auditing performance by concrete experiments and comparisons with the state-of-the-art schemes.

The results demonstrate that the proposed scheme can effectively achieve secure auditing in clouds, and outperforms the previous ones in computation complexity, storage costs and communication overhead.

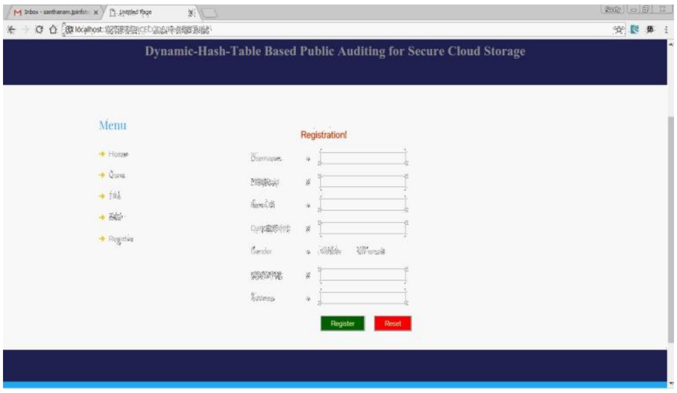
SCREEN SHOTS

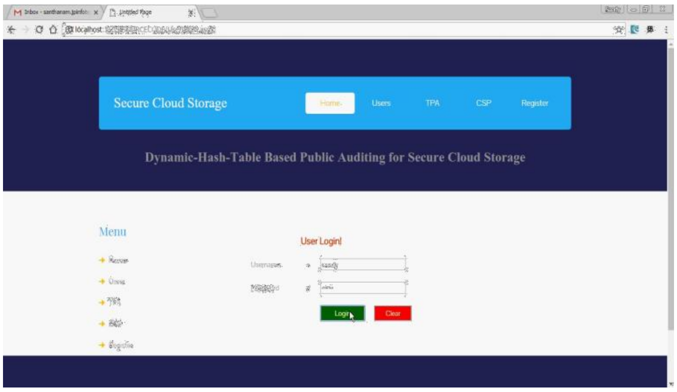


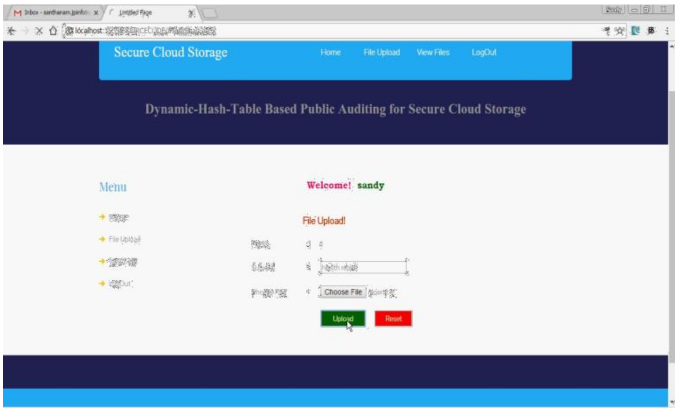
Dynamic-Hash-Table Based Public Auditing for Secure Cloud Storage

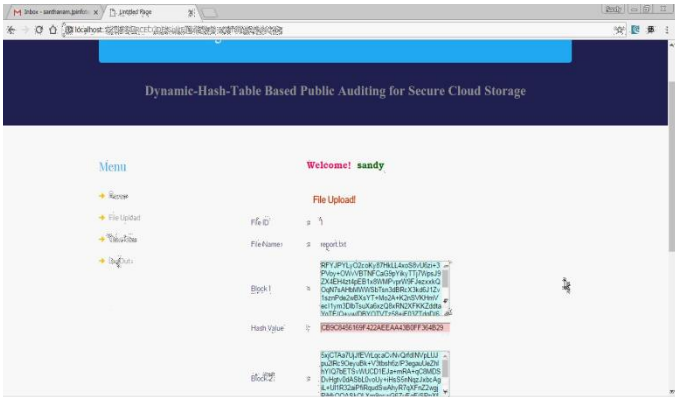
Abstract

Cloud storage is an increasingly popular application of cloud computing, which can provide on-demand outsourcing data services for both organizations and individuals. However, users may not fully trust the cloud service providers (CSPs) in that it is difficult to determine whether the CSPs meet their legal expectations for data security. Therefore, it is critical to develop efficient auditing techniques to strengthen data owners' trust and confidence in cloud storage. In this paper, we present a novel public auditing scheme for secure cloud storage based on dynamic hash table (DHT), which is a new two-dimensional data structure located at a third party auditor (TPA) to record the data property information for dynamic auditing. Differing from the existing works, the proposed scheme migrates the authorized information from the CSP to the TPA, and thereby significantly reduces the computational cost and communication overhead. Meanwhile, exploiting the structural advantages of the DHT, our scheme can also achieve higher updating efficiency than the state-of-the-art schemes. In addition, we extend our scheme to support privacy preservation by combining the homomorphic authenticator based on the public key with the random masking generated by the TPA, and achieve batch auditing by employing the aggregate BLS signature technique. We formally prove the security of the proposed scheme, and evaluate the auditing performance by detailed experiments and comparisons with the existing ones. The results demonstrate that the proposed scheme can effectively achieve secure auditing for cloud storage, and outperforms the previous schemes in computation complexity, storage


Dynamic-Hash-Table Based Public Auditing for Secure Cloud Storage
Menu
Home
Registration!
Gender
Register
Reset






Dynamic-Hash-Table Based Public Auditing for Secure Cloud Storage
Menu
File Upload
Welcome! sandy
File Upload!

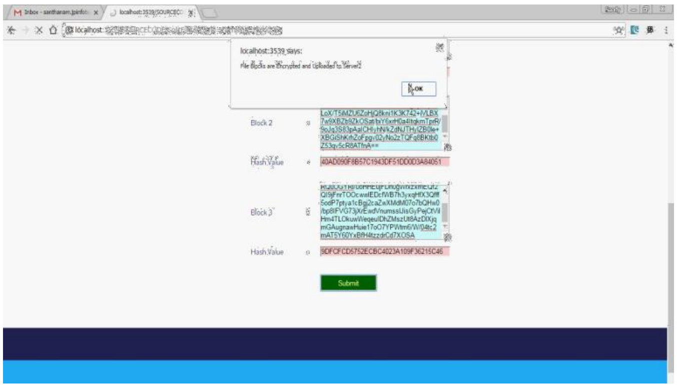
File ID : 1

File Name : report.txt

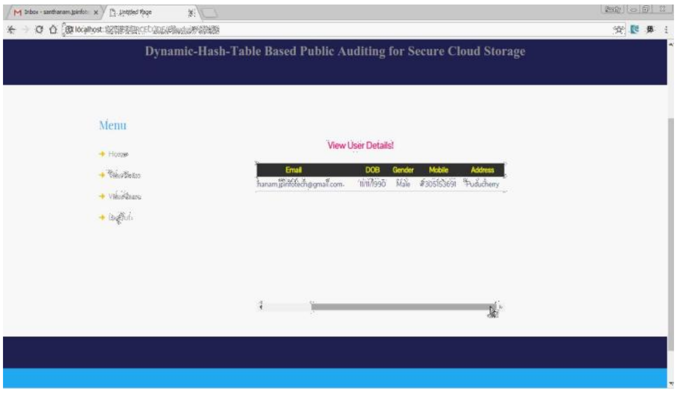
Block 1 : RFYJPYLyO2coKy87HkLL4xoS8vU6zi+3 PVoy+OWVBTNFCaG9pYikyTTj7WpsJ9 ZX4EH4zt4pEB1x8WMPvprW9FJezxxkQ OqN7sAHbMWWSbTsn3dBRcX3kd6J1Zv 1sznPde2wBXsYT+Mo2A+K2nSVKHmV ec11ym3DlbTsuXa6xzQ8xRN2XFKKZddta

Hash Value : CB9C8456169F422AEEAA43B0FF364B29

Block 2 : 5xjCTAa7UjJfEVrLqcaCvNvQrfdINVpLUJ pu2lRc9OeyuBk+V3tbsh6z/P3egauUeZhl hYIQ7bETSvWUCD1EJa+mRA+qC8MDS DvHgtv0dASbL0voUy+iHsS5nNqzJxbcAg iL+Ul1R32aiPfiRqudSwAhyR7qXFnZ2wgj

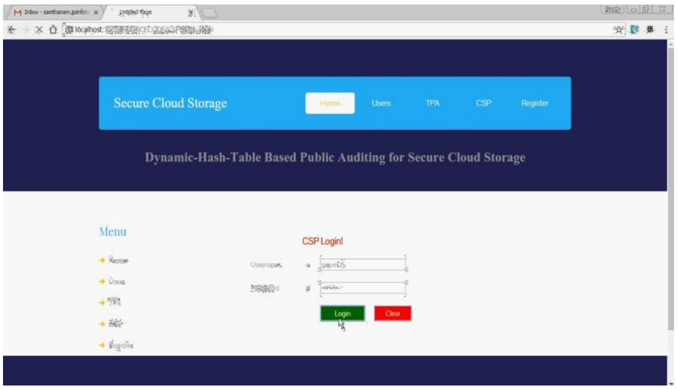

localhost:3539 says:
File Blocks are Encrypted and Uploaded to Server2

Block 2	:	LoX/T5iMZU6ZoHjQ8kni1K3K742+lVLBX 7w9XBZb9ZkOSat/biY6xrH0a4ltqkmTprR/ 9oJq3S83pAaICHIyhN/kZdNJTHyIZB0le+ XBGiShKrhZoFpgv02yNo2zTQFq8BKtb0 Z53qv5cR8ATfnA==
Hash Value	:	40AD090F8B57C1943DF51DD0D3A84051
Block 3	:	QI9jFnrTOOcwwIEDcfWB7h3yxqHfX3Qff 5odP7ptya1cBgj2caZwXMdM07o7bQHw0 /bp8lFVG73jXrEwdVnumssUisGyPejCtVl Hm4TLOkuwWeqeuIDhZMszUt8AzDIXjq mGAugnawHuie17oO7YPWtm6/W/04tc2 mAT5Y60YxBfH4tzzdrCd7XOSA
Hash Value	:	9DFCFCD6752ECBC4023A109F36215C46

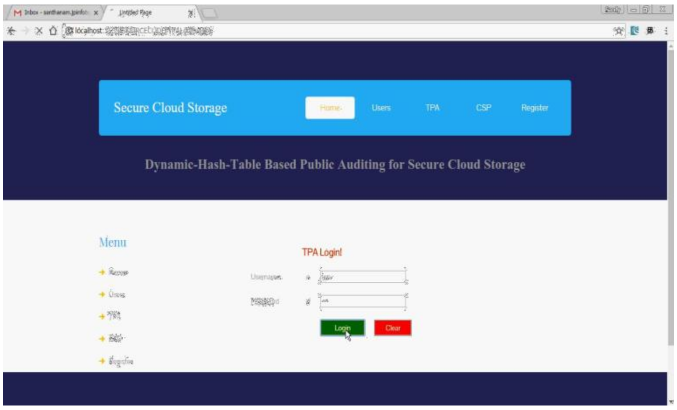

Dynamic-Hash-Table Based Public Auditing for Secure Cloud Storage

View User Details!

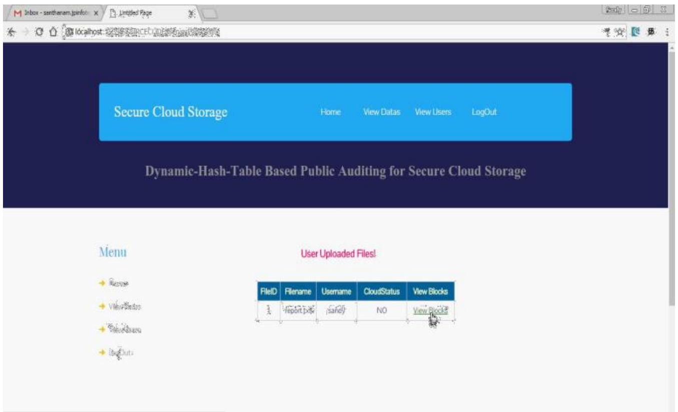
Email	DOB	Gender	Mobile	Address
hanam.jpinfotech@gmail.com	11/11/1990	Male	#305153691	Puducherry


Dynamic-Hash-Table Based Public Auditing for Secure Cloud Storage

CSP Login!

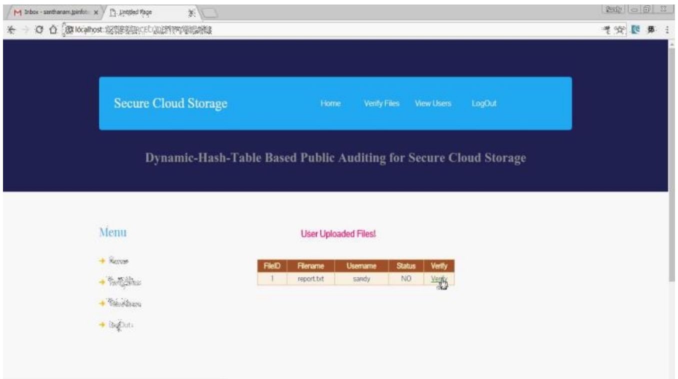

Dynamic-Hash-Table Based Public Auditing for Secure Cloud Storage

TPA Login!


Dynamic-Hash-Table Based Public Auditing for Secure Cloud Storage

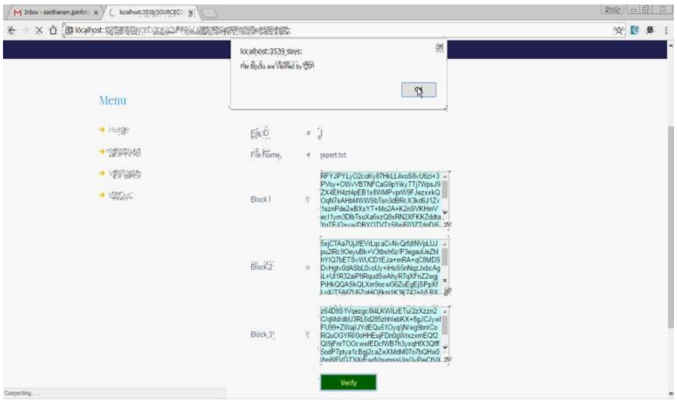
User Uploaded Files!

FileID	Filename	Username	CloudStatus	View Blocks
1	report.txt	sandy	NO	View Blocks

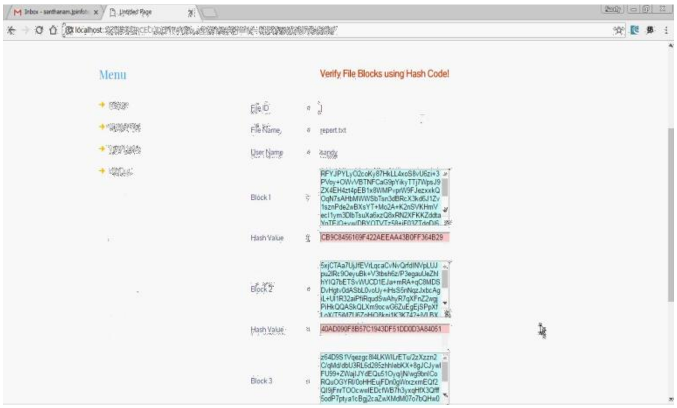

Dynamic-Hash-Table Based Public Auditing for Secure Cloud Storage

User Uploaded Files!

FileID	Filename	Username	Status	Verify
1	report.txt	sandy	NO	Verify


localhost:3539 says:
File Blocks are Verified by CSP

File ID	:	1
File Name	:	report.txt
Block 1	:	RFYJPYLyO2coKy87HkLL4xoS8vU6zi+3 PVoy+OWVBTNFCaG9pYikyTTj7WpsJ9 ZX4EH4zt4pEB1x8WMPvprW9FJezxxkQ OqN7sAHbMWWSbTsn3dBRcX3kd6J1Zv 1sznPde2wBXsYT+Mo2A+K2nSVKHmV ec11ym3DlbTsuXa6xzQ8xRN2XFKKZddta
Block 2	:	5xjCTAa7UjJfEVrLqcaCvNvQrfdINVpLUJ pu2IRc9OeyuBk+V3tbsh6z/P3egauUeZhl hYIQ7bETSvWUCD1EJa+mRA+qC8MDS DvHgtv0dASbL0voUy+iHsS5nNqzJxbcAg iL+Ul1R32aiPfiRqudSwAhyR7qXFnZ2wgj PiHkQQASkQLXm9ocwG6ZuEgEjSPpXf
Block 3	:	z64D9S1Vqezgc8l4LKWILrETu/2zXzzn2 C/qMd/dbU3RL6d285zhhIebKX+8gJCJywl FU99+ZWajIJYdEQu51Oyq/jN/wg9bnICo RQuOGYRI/0oHHEujFDn0gWrxzmEQf2 QI9jFnrTOOcwwIEDcfWB7h3yxqHfX3Qff 5odP7ptya1cBgj2caZwXMdM07o7bQHw0


Verify File Blocks using Hash Code!

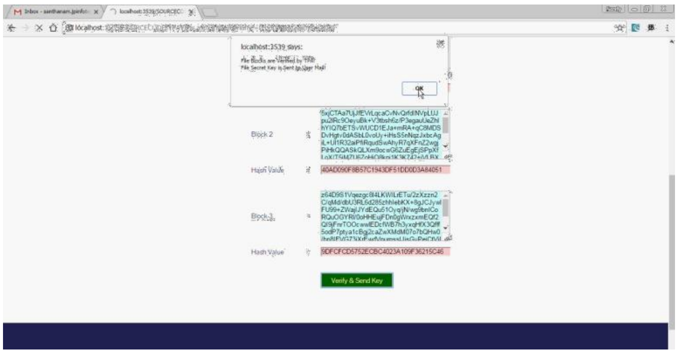
File ID	:	1
File Name	:	report.txt
User Name	:	sandy
Block 1	:	RFYJPYLyO2coKy87HkLL4xoS8vU6zi+3 PVoy+OWVBTNFCaG9pYikyTTj7WpsJ9 ZX4EH4zt4pEB1x8WMPvprW9FJezxxkQ OqN7sAHbMWWSbTsn3dBRcX3kd6J1Zv 1sznPde2wBXsYT+Mo2A+K2nSVKHmV ec11ym3DlbTsuXa6xzQ8xRN2XFKKZddta
Hash Value	:	CB9C8456169F422AEEAA43B0FF364B29
Block 2	:	5xjCTAa7UjJfEVrLqcaCvNvQrfdINVpLUJ pu2IRc9OeyuBk+V3tbsh6z/P3egauUeZhl hYIQ7bETSvWUCD1EJa+mRA+qC8MDS DvHgtv0dASbL0voUy+iHsS5nNqzJxbcAg iL+Ul1R32aiPfiRqudSwAhyR7qXFnZ2wgj PiHkQQASkQLXm9ocwG6ZuEgEjSPpXf
Hash Value	:	40AD090F8B57C1943DF51DD0D3A84051
Block 3	:	z64D9S1Vqezgc8l4LKWILrETu/2zXzzn2 C/qMd/dbU3RL6d285zhhIebKX+8gJCJywl FU99+ZWajIJYdEQu51Oyq/jN/wg9bnICo RQuOGYRI/0oHHEujFDn0gWrxzmEQf2 QI9jFnrTOOcwwIEDcfWB7h3yxqHfX3Qff 5odP7ptya1cBgj2caZwXMdM07o7bQHw0

Volume No:4, Issue No:6 (November-2018) ISSN No : 2454-423X (Online)

International Journal of Research in Advanced Computer Science Engineering

A Peer Reviewed Open Access International Journal

www.ijracse.com


localhost:3539 says:

File Blocks are Verified by TPA!
File Secret Key is Sent to User Mail

OK

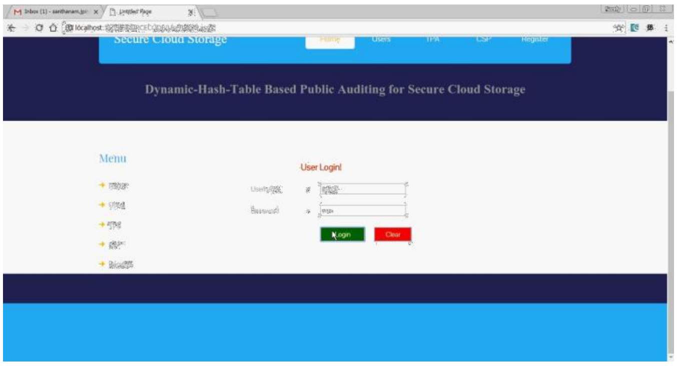
Block 2 : 5xjCTAa7UjJfEVrLqcaCvNvQrfdINVpLUJ pu2lRc9OeyuBk+V3tbsh6z/P3egauUeZhl hYIQ7bETSvWUCD1EJa+mRA+qC8MDS DvHgtv0dASbL0voUy+iHsS5nNqzJxbcAg iL+Ul1R32aiPfiRqudSwAhyR7qXFnZ2wgj PiHkQQASkQLXm9ocwG6ZuEgEjSPpXf

Hash Value : 40AD090F8B57C1943DF51DD0D3A84051

Block 3 : z64D9S1Vqezgc8l4LKWlLrETu/2zXzzn2 C/qMd/dbU3RL6d285zhhlebKX+8gJCJywl FU99+ZWajlJYdEQu51Oyq/jN/wg9bnlCo RQuOGYRl/0oHHEujFDn0gWnxzxmEQf2 Ql9jFnrTOOcwwlEDcfWB7h3yxqHfX3Qff 5odP7ptya1cBgj2caZwXMdM07o7bQHw0

Hash Value : 9DFCFCD5752ECBC4023A109F36215C46

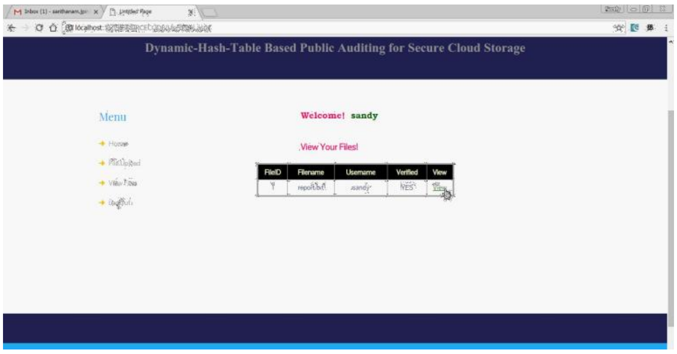
Verify & Send Key



Dynamic-Hash-Table Based Public Auditing for Secure Cloud Storage

User Login!

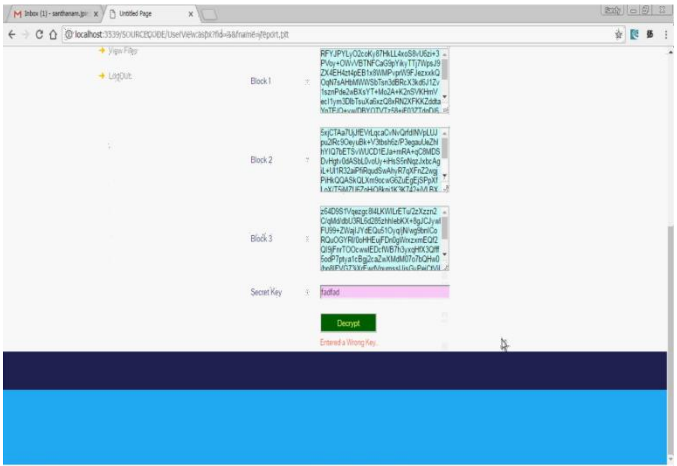
Login Clear


Dynamic-Hash-Table Based Public Auditing for Secure Cloud Storage

Welcome! sandy

View Your Files!

FileID	Filename	Username	Verified	View
1	report.txt	sandy	YES	View


localhost:3539/SOURCECODE/UserView.aspx?fid=&fname=report.txt

Block 1 : RFYJPYLyO2coKy87HkLL4xoS8vU6zi+3 PVoy+OWVBTNFCaG9pYikyTTj7WpsJ9 ZX4EH4zt4pEB1x8WMPvprW9FJezxxkQ OqN7sAHbMWWSbTsn3dBRcX3kd6J1Zv 1sznPde2wBXsYT+Mo2A+K2nSVKHmV ecl1ym3DlbTsuXa6xzQ8xRN2XFKKZddta

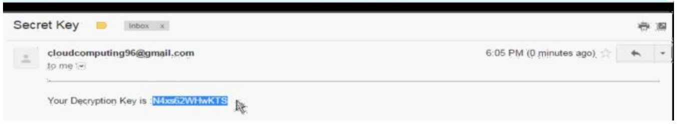
Block 2 : 5xjCTAa7UjJfEVrLqcaCvNvQrfdINVpLUJ pu2lRc9OeyuBk+V3tbsh6z/P3egauUeZhl hYIQ7bETSvWUCD1EJa+mRA+qC8MDS DvHgtv0dASbL0voUy+iHsS5nNqzJxbcAg iL+Ul1R32aiPfiRqudSwAhyR7qXFnZ2wgj PiHkQQASkQLXm9ocwG6ZuEgEjSPpXf

Block 3 : z64D9S1Vqezgc8l4LKWlLrETu/2zXzzn2 C/qMd/dbU3RL6d285zhhlebKX+8gJCJywl FU99+ZWajlJYdEQu51Oyq/jN/wg9bnlCo RQuOGYRl/0oHHEujFDn0gWnxzxmEQf2 Ql9jFnrTOOcwwlEDcfWB7h3yxqHfX3Qff 5odP7ptya1cBgj2caZwXMdM07o7bQHw0

Secret Key : fadfad

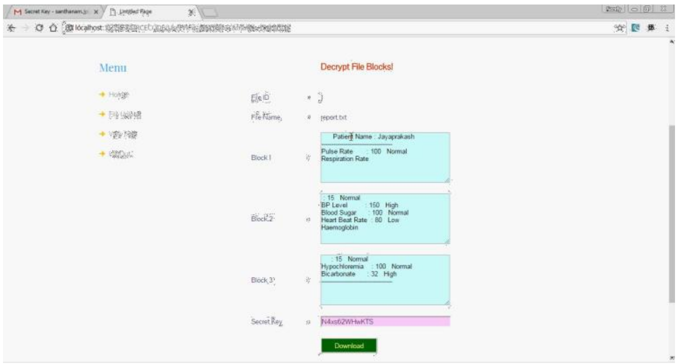
Decrypt

Entered a Wrong Key..


Secret Key Inbox

cloudcomputing96@gmail.com 6:05 PM (0 minutes ago)
to me

Your Decryption Key is :N4xs62WHwKTS



Decrypt File Blocks!

File ID : 3

File Name : report.txt

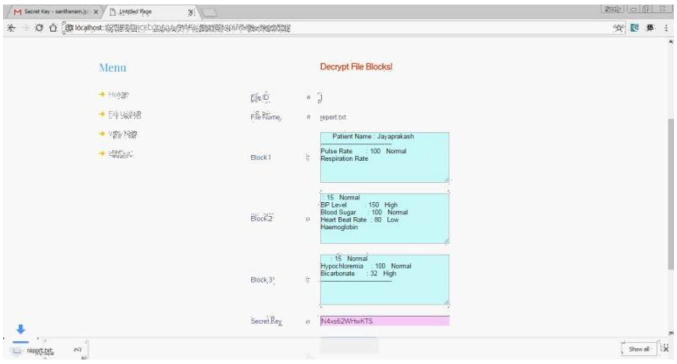
Block 1 :
Patient Name : Jayaprakash
Pulse Rate : 100 Normal
Respiration Rate

Block 2 :
: 15 Normal
BP Level : 150 High
Blood Sugar : 100 Normal
Heart Beat Rate : 80 Low
Haemoglobin

Block 3 :
: 15 Normal
Hypochloremia : 100 Normal
Bicarbonate : 32 High

Secret Key : N4xs62WHwKTS

Download



Decrypt File Blocks!

File ID : 3

File Name : report.txt

Block 1 :
Patient Name : Jayaprakash
Pulse Rate : 100 Normal
Respiration Rate

Block 2 :
: 15 Normal
BP Level : 150 High
Blood Sugar : 100 Normal
Heart Beat Rate : 80 Low
Haemoglobin

Block 3 :
: 15 Normal
Hypochloremia : 100 Normal
Bicarbonate : 32 High

Secret Key : N4xs62WHwKTS

CONCLUSION

Nowadays, cloud storage, which can offer on-demand outsourcing data services for both organizations and individuals, has been attracting more and more attention. However, one of the most serious obstacles to its development is that users may not fully trust the CSPs in that it is difficult to determine whether the CSPs meet their legal expectations for data security. Therefore, it is critical and significant to develop efficient auditing techniques to strengthen data owners' trust and confidence in cloud storage. In this paper, we are motivated to present a novel public auditing scheme for secure cloud storage using dynamic hash table (DHT), which is a new two dimensional data structure used to record the data property information for dynamic auditing. Differing from the existing works, our scheme migrates the auditing metadata excerpt the block tags from the CSP to the TPA, and thereby significantly reduces the computational cost and communication overhead. Meanwhile, exploiting the structural advantages of the DHT, our scheme can also achieve better performance than the state-of-the-art schemes in the updating phase. In addition, for privacy preservation, our scheme introduces a random masking provided by the TPA into the process of generating proof to blind the data information. Moreover, our scheme further exploits the aggregate BLS signature technique from bilinear maps to perform multiple auditing tasks simultaneously, of which the principle is to aggregate all the signatures by different users on various data blocks into a single short one and verify it for only one time to reduce the communication cost in the verification process. We formally prove the security of our scheme, and evaluate the auditing performance by detailed experiments and comparisons with the existing ones. The results demonstrate that our scheme can effectively achieve secure auditing in clouds, and induce significantly fewer costs of storage, communication and computation than the previous schemes. Moreover, we would like to point out that no single method can achieve perfect audits for all types of cloud data, just as no standard has a universal validity. Thus, it may be a new trend to design a more effective scheme, including different audit strategies for various types of cloud data, which is also the direction for our future work.

REFERENCES

[1] H. Dewan and R. C. Hansdah. ″A Survey of Cloud Storage Facilities ″, Proc. 7th IEEE World Congress on Services, pp. 224-231, July 2011.

[2] C. Wang, Q. Wang, K. Ren, N. Cao and W. Lou. ″Toward Secure and Dependable Storage Services in Cloud Computing″, IEEE Trans. Service Computing, vol. 5, no. 2, pp. 220-232, 2012.

[3] K. Ren, C. Wang and Q. Wang. “Security Challenges for the Public Cloud,” IEEE Internet Computing, vol. 16, no. 1, pp. 69– 73, 2012.

[4] J. Ryoo, S. Rizvi, W. Aiken and J. Kissell. ″Cloud Security Auditing: Challenges and Emerging Approaches″, IEEE Security & Privacy, vol. 12, no. 6, pp. 68-74, 2014.

[5] C. Wang, K. Ren, W. Lou and J. Li. ″Toward Publicly Auditable Secure Cloud Data Storage Services″, IEEE network, vol. 24, no. 4, pp. 19-24, 2010.

[6] Q. Wang, C. Wang, K. Ren, W. Lou and J. Li. ‘‘Enabling Public Auditability and Data Dynamics for Storage Security in Cloud Computing,’’ IEEE Trans. on Parallel and Distributed Systems, vol. 22, no. 5, pp. 847-859, 2011.

[7] F. Sebé, J. Domingo-Ferrer, A. Martínez-Ballesté, Y. Deswarte and J.-J. Quisquater, “Efficient Remote Data Possession Checking in Critical Information Infrastructures,” IEEE Trans. Knowledge Data Eng., vol. 20, no. 8, pp. 1034-1038, 2008.

[8] A. Juels and B.S. Kaliski Jr., “PoRs: Proofs of Retrievability for Large Files,” Proc. ACM Conf. Computer and Communications Security (CCS ’07), pp. 584-597, 2007.

[9] G. Ateniese, R.B. Johns, R. Curtmola, J. Herring, L. Kissner, Z. Peterson and D. Song, ‘‘Provable Data Possession at Untrusted Stores,’’ Proc. 14th ACM Conf. on Comput. and Commun. Security (CCS), pp. 598-609, 2007.

[10] K. Yang and X. Jia. ″Data Storage Auditing Service in Cloud Computing: Challenges, Methods and Opportunities″. World Wide Web, vol. 15, no. 4, pp. 409-428, 2012

[11] C. Wang, Q. Wang, K. Ren and W. Lou, ‘‘Privacy-Preserving Public Auditing for Data Storage Security in Cloud Computing,’’ Proc. IEEE INFOCOM, pp. 1-9, 2010.

[12] C. Wang, S. M. Chow, Q. Wang, K. Ren and W. Lou, ″Privacy- Preserving Public Auditing for Secure Cloud Storage,″ IEEE Trans. on Computers, vol. 62, no. 2, pp. 362-375, 2013.

[13] Y. Zhu, H. Hu, G. Ahn, and M. Yu, “Cooperative Provable Data Possession for Integrity Verification in Multi-Cloud Storage,” IEEE Trans. Parallel and Distributed Systems, vol. 23, no. 12, pp. 2231-2244, 2012.