International Journal of Research

p-ISSN: 2348-6848
e-ISSN: 2348-795X
Volume 07 Issue 10
October 2020

Secure Information consume in Distributed Computing Utilizing Revocable Capacity Uniformity Based Encryption

Mallepogu Madhupriya[1], Dr. M. Jahir Pasha[2]
[1]M.Tech Student, [2]Associate Professor,
[1,2] Department of CSE,
[1,2] Dr.K.V.Subba Reddy College of Engineering for Women, Kurnool

Abstract:

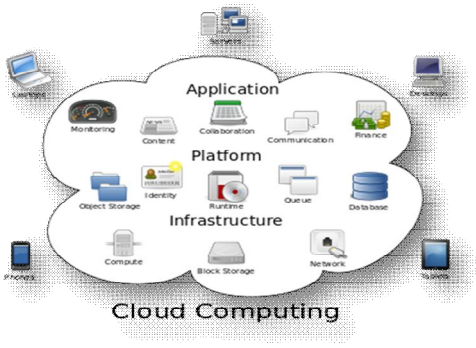
Cloud computing provides a flexible and way that is convenient data sharing, which brings various benefits for the society and people. But there is certainly a resistance that is natural users to directly outsource the shared data into the cloud server considering that the data often contain valuable information. Thus, it is crucial to position access that is cryptographically enhanced from the shared data. Identity-based encryption is a promising cryptographical primitive to construct a practical data system that is sharing. However, access control is certainly not static. This is certainly, when some user's authorization is expired, there ought to be a mechanism that will remove him/her through the system. Consequently, the user that is revoked access both the previously and subsequently shared data.

To the end, we propose an idea called revocable-storage encryption that is identity-based(RS-IBE), that could offer the forward/backward security of ciphertext by introducing the functionalities of user revocation and ciphertext update simultaneously. Furthermore, we present a concrete construction of RS-IBE, and prove its security when you look at the security model that is defined. The performance comparisons indicate that the proposed RS-IBE scheme has advantages with regards to functionality and efficiency, and so is simple for a practical and data-sharing system that is cost-effective. Finally, we provide implementation outcomes of the proposed scheme to show its practicability.

Keywords:- Cloud Computing, Ciphertext, Cryptographical, identity-based encryption (IBE)

What is cloud computing?

Cloud computing could be the utilization of computing resources (hardware and software) which can be ongoing service over a network the online world). The name arises from the typical usage of a symbol that is cloud-shaped an abstraction when it comes to complex infrastructure it includes in system diagrams. Cloud entrusts that are computing services with a person's data, software and computation. Cloud computing is made from hardware and software resources made available on the net as managed services that are third-party. These types of services typically provide usage of software that is advanced and high-end networks of server computers.



How Cloud Computing Works?

The purpose of cloud computing is always to apply supercomputing that is traditional or high-performance computing power, normally employed by military and research facilities, to execute tens of trillions of computations per second, in consumer-oriented applications such as for example financial portfolios, to produce personalized information, to give you data storage or even power large, immersive on-line games. The cloud computing uses networks of large categories of servers typically running consumer that is low-cost technology with specialized connections to spread data-processing chores across them. This shared IT infrastructure contains large pools of systems which can be linked together. Often, virtualization techniques are widely used to charged power of cloud computing.

Characteristics and Services Models:

The salient characteristics of cloud computing on the basis of the definitions given by the National Institute of Standards and Terminology (NIST) are outlined below:

- On-demand self-service: A consumer can unilaterally provision computing capabilities, such as for example server some time network storage, as required automatically without requiring interaction that is human each service's provider.
- Broad network access: Capabilities can be obtained throughout the network and accessed through standard mechanisms that promote use by heterogeneous thin or client that is thick (e.g., smart phones, laptops, and PDAs).
- Resource pooling: The provider's computing resources are pooled to serve multiple consumers using a model that is multi-tenant with various physical and virtual resources dynamically assigned and reassigned relating to consumer demand. There clearly was a feeling of location-independence for the reason that the consumer generally does not have any control or knowledge throughout location that is exact of provided resources but could possibly specify location at an increased standard of abstraction (e.g., country, state, or data center). Samples of resources include storage, processing, memory, network bandwidth, and machines that are virtual.
- Rapid elasticity: Capabilities can elastically be rapidly and provisioned, in many cases automatically, to quickly scale out and rapidly released to quickly scale in. Into the consumer, the capabilities available for provisioning often appear to be unlimited and can be purchased in any quantity at any time to the consumer.
- Measured service: Cloud systems automatically control and optimize resource use by leveraging a metering capability at some standard of abstraction appropriate into the types of service (e.g., storage, processing, bandwidth, and active user accounts). Resource usage may be managed, controlled, and reported providing transparency for the provider and consumer regarding the service that is utilized

LITERATURE SURVEY

In accordance with Lee, Kwangsu (2020) Cloud computing can offer a way that is flexible effectively share data among multiple users as it can overcome the full time and location constraints of computing resource usage. However, the users of cloud computing will always be reluctant to fairly share sensitive data to a cloud server considering that the cloud server should always be treated as an entity that is untrusted. So that you can support secure and efficient data sharing in cloud environment that is computing Wei et al. recently extended the thought of identity-based encryption (IBE) to aid key revocation and ciphertext update functionalities, and proposed a revocable-storage identity-based encryption (RS-IBE)

scheme. In this paper, we show that the Scheme that is RS-IBE of et al. will not fulfill the correctness property of RS-IBE. We also propose a strategy to modify the current scheme that is RS-IBE.

Depending on Pathare, Kedar G., and P. M. Chouragade(2017) Security has long been concern in terms of data sharing in cloud computing. Cloud computing provides computation that is high and memory. Cloud computing is way that is convenient data sharing. But users may sometime has to outsourced the shared data to cloud server though it includes valuable and information that is sensitive. Thus it's important to give you cryptographically enhanced access control for data system that is sharing. This paper discuss in regards to the promising access control for data sharing in cloud that will be encryption that is identity-based. We introduce the efficient revocation scheme when it comes to system that will be revocable-storage encryption scheme that is identity-based. It gives both forward and backward security of ciphertext. Then we shall have go through the architecture and steps tangled up in identity-based encryption. Finally we propose system that offer secure file sharing system using encryption scheme that is identity-based.

Depending on Saeid Rezaei, Mohammad Ali Doostari, and Majid Bayat(2018) Cloud storage is a service that is useful of computing makes it possible for users to upload their data when you look at the cloud and share it with other people. Although, this service that is new affordable and practical, however it is connected with several privacy and security challenges. Nowadays, Attribute Based Encryption (ABE) is widely used to present secure data sharing when you look at the environment that is distributed as cloud computing. Unfortunately, almost all of the existing ABE schemes are not suited to resource constraint cloud systems, since they use expensive bilinear pairing operation and they cause a very high encryption and decryption computation overhead because they use expensive bilinear pairing operation and thus. In this paper, we propose an no-pairing that is efficient revocable ABE data sharing scheme predicated on Elliptic Curve Cryptography (ECC) for cloud storage systems. Moreover, a security that is comprehensive performance analysis shows that our scheme is both secure and efficient

Relating to Xu, Shengmin, et al(2018) Cloud computing is an computing that is emerging that enables users to keep their data in a cloud server to take pleasure from scalable and on-demand services. Nevertheless, in addition it brings security that is many, since cloud service providers (CSPs) are not in identical trusted domain as users. To guard data privacy against untrusted CSPs, existing solutions apply cryptographic methods (e.g., encryption mechanisms) and supply decryption keys simply to users that are authorized. However, sharing cloud data among authorized users at a fine-grained level continues to be a challenging issue, specially when coping with dynamic user groups. In this paper, we propose a protected and efficient access that is fine-grained and data sharing scheme for dynamic user groups by: 1) defining and enforcing access policies on the basis of the attributes associated with data; 2) permitting one of the keys generation center to efficiently update user credentials for dynamic user groups; and 3) allowing some expensive computation tasks to be performed by untrusted CSPs without requiring any delegation key. Specifically, we first design a simple yet effective revocable encryption that is attribute-based (ABE) scheme using the property of ciphertext delegation by exploiting and uniquely combining techniques of identity-based encryption, ABE, subset-cover

framework, and ciphertext encoding mechanism. We then present a access that is fine-grained and data sharing system for on-demand services with dynamic user groups when you look at the cloud. The data that are experimental that our proposed scheme is much more efficient and scalable compared to the state-of-the-art solution.

Relating to Lee, Kwangsu(2019) Cloud computing can offer a way that is flexible effectively share data among multiple users as it can overcome the full time and location constraints of computing resource usage. However, the users of cloud computing will always be reluctant to fairly share sensitive data to a cloud server considering that the cloud server should always be treated as an entity that is untrusted. So that you can support secure and efficient data sharing in cloud environment that is computing Wei et al. recently extended the thought of identity-based encryption (IBE) to aid key revocation and cipher text update functionalities, and proposed a revocable-storage identity-based encryption (RS-IBE) scheme. In this paper, we show that the scheme that is RS-IBE of et al. will not match the correctness property of RS-IBE. In addition, we propose a strategy to modify the current RS-IBE scheme to be the correct and scheme that is secure.

Relating to Ingole, Monika.(2019) Information get upgraded to regulate by cryptographically. Cryptology is the investigation and training of methods for secure correspondence within the sight of outsiders called enemies. Distributed computing could be the conveyance of registering administrations—servers, stockpiling, databases, organizing, programming, investigation, knowledge and then some—over the world-wide-web ("the cloud") to supply quicker development, adaptable assets and economies of scale. Be that as it can, there is certainly a opposition that is characteristic clients to straightforwardly redistribute the typical information into the cloud server considering that the information frequently contain important data. Along these lines, it is essential to put cryptographically improved access control from the information that is common. Personality based encryption is a promising cryptographical crude to manufacture a information sharing framework[3] that is reasonable. Be that as control to the final end, propose an idea called revocable-capacity personality based encryption (RS-IBE)[11], that will be not static. This is certainly, the true point from which some client's approval is lapsed, there component that will expel him/her from the framework. In this manner, the denied customer can't get to both the previously and right now data can give the forward/backward security of cipher text by introducing the functionalities of customer disavowal and cipher text update simultaneously in this manner.

Relating to Wei, Jianghong, et al(2019) Personal health that is Electronic (EHR) enable medical workers to conveniently and quickly access each patient's medical background through general public cloud, which greatly facilitates patients' visits and makes telemedicine feasible. Additionally, since EHR involve patients' personal privacy information, EHR holders would think twice directly hesitate to outsource their data to cloud servers. A normal and favorite method of conquering this dilemma will be encrypt these EHR that is outsourced that only authorized medical workers have access to them. Particularly, the ciphertext-policy attribute-based encryption (CP-ABE) supports fine-grained access over encrypted data and it is regarded as being an amazing solution of securely sharing EHR when you look at the cloud that is public. In this paper, to bolster the device security and meet with the dependence on specific applications, we add new functionalities, namely, user revocation, secret key delegation and

ciphertext update into the original ABE, and propose a revocable-storage hierarchical attribute-based encryption (RS-HABE) scheme. The proposed Scheme that is RS-HABE of forward security and backward security simultaneously, and is proved to be selectively secure. The analysis this is theoretical that the proposed scheme surpasses existing similar works with regards to functionality and security, during the acceptable price of computation overhead. Moreover, we implement the proposed scheme and experiments that are present demonstrate its practicability.

Relating to Zhang, Yinghui, et al(2014) Attribute-based encryption (ABE) is a promising cryptographic primitive for implementing fine-grained data sharing in cloud computing. However, before ABE can be widely deployed in practical cloud storage systems, a issue that is challenging regard to attributes and user revocation has to be addressed. To your knowledge, almost all of the ABE that is existing are not able to support flexible and direct revocation due to the burdensome update of attribute secret keys and all sorts of the ciphertexts. Aiming at tackling the challenge above, we formalize the thought of ciphertext-policy ABE supporting flexible and direct revocation (FDR-CP-ABE), and present a construction that is concrete. The proposed plot underpins characteristic that is immediate client repudiation. To get this going objective, we present a capacity that is helper decide the ciphertexts messed up in repudiation functions, and afterward just update these included ciphertexts by receiving the methods for broadcast encryption. Moreover, our development is demonstrated secure when you take a gander at the model that is standard. Hypothetical investigation and test results show that FDR-CP-ABE beats the previous techniques which can be disavowal rodselated.

Existing System

- Boneh and Franklin previously proposed a repudiation that is normal for IBE. They added the existing time span into the cipher text, and non-repudiated users intermittently got private keys for each and every time period through the power that is critical.
- Boldyreva, Goyal and Kumar acquainted a novel methodology with acknowledge repudiation that is proficient. They utilized a tree that is parallel oversee identity such that their RIBE plot diminishes the unpredictability of key disavowal to logarithmic (in the spot of straight) when you take a gander at the most extreme wide scope of system users.
- Subsequently, using the denial that is previously mentioned, Libert and Vergnaud proposed an adaptively secure RIBE plot predicated on a variation ofWater's IBE conspire.
- Chen et al. built a plan that is RIBE grids.

DISSERVICES OF EXISTING SYSTEM:

1. Unfortunately, existing alternative would be not adaptable, as it requires one of the keys power to execute straight work in the sheer number of non-denied users. Also, a channel that is secure fundamental for one of the keys authority and non-repudiated users to send new keys.
2. However, existing plan just accomplishes security that is specific.
3. This kind of denial technique can't avoid the agreement of renounced users and pernicious non-repudiated users as vindictive non-disavowed users can share the key that is update those renounced users.
4. Furthermore, to refresh the ciphertext, the power that is key their plan needs to keep up a table for each and every client to make the re-encryption key for each

and every time period, which fundamentally helps the key position's remaining burden.

PROPOSED SYSTEM

- This shows that the idea of revocable encryption that is identity-based (RIBE) could be a promising methodology that satisfies the previously mentioned security prerequisites for information sharing.
- RIBE highlights a system that allows a sender to attach the current time that is current into the ciphertext such that the recipient can unscramble the ciphertext just underneath the condition that he/she is positively not renounced at that point period.

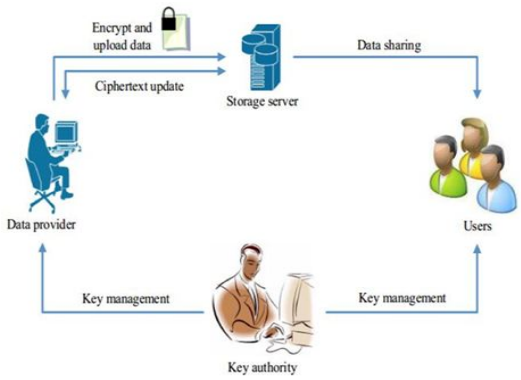
A RIBE-based information system that is sharing as follows:

Stage 1: The data supplier (e.g., David) first chooses the users (e.g., Alice and Bob) who can share the information. At that point, David encodes the infobeneath the characters Alice and Bob, and transfers the ciphertext with respect to the mutual information into thex cloud worker.
Stage 2: When either Alice or Bob might want to get the common information, the person in question can download and unscramble the ciphertext that is comparing. Nonetheless, for a client that is unapproved the cloud worker, the plaintext with respect to the common data isn't accessible.
Stage 3: at times, e.g., Alice's approval gets terminated, David can download the ciphertext with respect to the mutual information, and unscramble then-re-scramble the common then information such that Alice is kept from getting to the plaintext in regards to the mutual information, and afterward transfer the re-encoded information into the cloud worker once more.

HIGHLIGHTS OF PROPOSED SYSTEM:

- We give formal definitions to RS-IBE and its own security that is comparing model.
- We present a development that is concrete of RS-IBE.
- The proposed plan can offer privacy and in reverse/forward2 mystery all the while we demonstrate the security related with proposed plot when you take a gander at the model that is standard underneath the decisional ℓ-Bilinear Diffie-Hellman Exponent (ℓ-BDHE) presumption. What's more, the proposed plan can withstand decoding introduction that is critical.
- The strategy of ciphertext update just needs data that is public. Remember that no past encryption that is identity-based when you take a gander at the writing can offer this specific viewpoint;
- The calculation that is extra storage multifaceted nature, that are presented in by the mystery, is maybe all upper limited by O(log(T)2), where T could be the last number of the time-frames.
-

SYSTEM ARCHITECTURE



Modules with Description

MODULES:

- System Construction Module
- Data Provider
- Cloud User

Key Authority Authority that is key
MODULES DESCSRIPTION:

System Construction Module

At the point when you take a gander at the module that is first we build up the proposed system utilizing the necessary substances with regards to assessment in regards to the proposed model. The data supplier (e.g., David) first chooses the users (e.g., Alice and Bob) who can share the information. At that point, David scrambles the information underneath the characters Alice and Bob, and transfers the ciphertext with respect to the mutual data into the cloud worker. When either Alice or Bob might want to acquire the common data, the individual in question can download and unscramble the ciphertext that is relating. Notwithstanding, for a user that is unapproved the cloud worker, the plaintext with respect to the mutual data isn't accessible.

Data Provider

In this module, the Data is created by us Provider module. The data supplier module is created such that the users that are new Signup at first and afterward Login for confirmation. The data supplier module gives the choice of transferring the document into the Cloud Server. The whole cycle of File Uploading into the cloud Server is gone through with Identity-based encryption design. Data Provider will take a gander at the advancement status related with the document transfer by him/her. Data Provider provided with the famous highlights of Revocation and Ciphertext update the document. Once after fruition with respect to the cycle, the information Provider logouts the meeting.

Cloud User

In this module, the Cloud is created by us User module. The Cloud user module is created such that the users that are new Signup at first and afterward Login for validation. The Cloud user will get the choice of document search. At that point user that is cloud is included for send the Request to Auditor with regards to File access. Subsequent to getting key that is unscramble the Auditor, he/she approach into the File. The cloud user can be empowered to download the File. The user logout the meeting after culmination of the cycle.

Key Authority (Auditor)

Auditor Will Login from the Auditor's page. He/she will take a gander at the forthcoming solicitations of each with respect to the individual that is above. In the wake of tolerating the solicitation through the individual that is above he/she will produce ace key for encode and Secret key for unscramble. Following the total cycle, the Auditor logout the meeting following the total cycle.

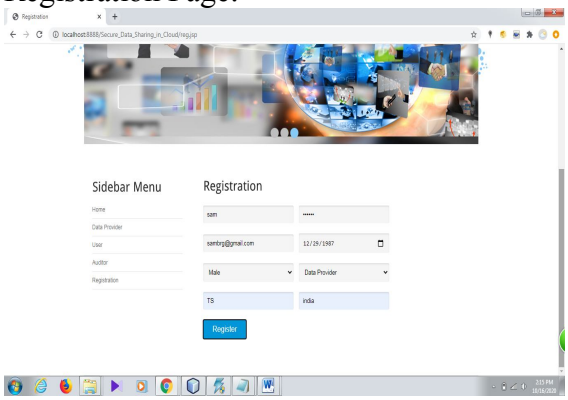
SCREEN SHOTS

Home Page:

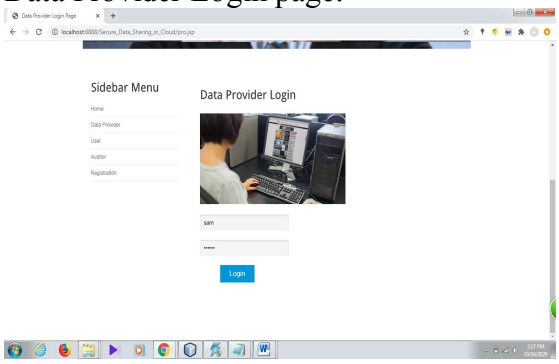
International Journal of Research

p-ISSN: 2348-6848
e-ISSN: 2348-795X
Volume 07 Issue 10
October 2020

Registration Page:

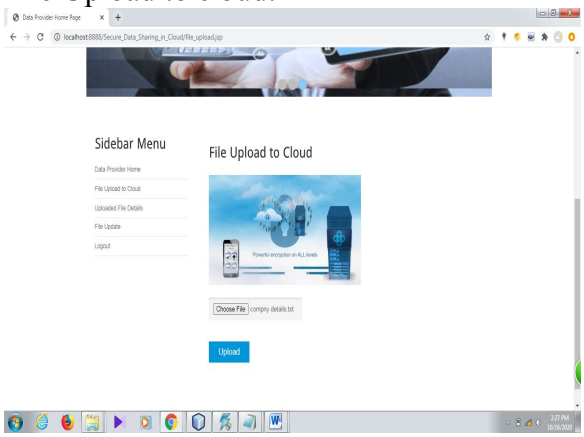


Data Provider Login page:

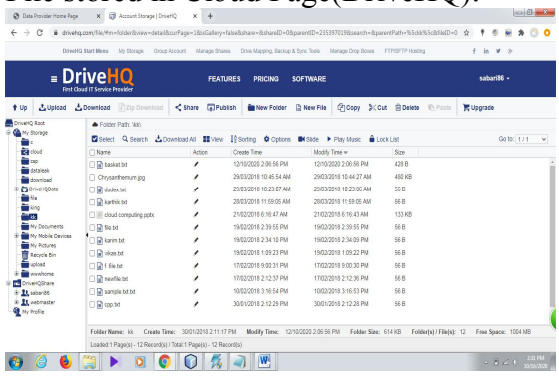


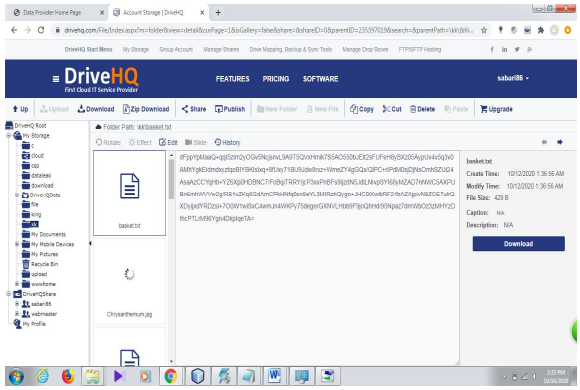
Data Provider Home:

File Upload to cloud:



File stored in Cloud Page(DriveHQ):





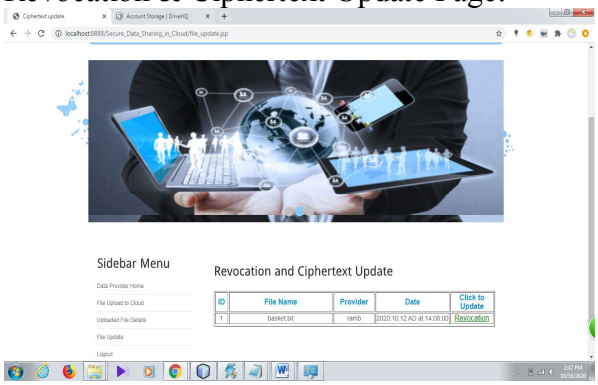
Uploaded File Details Page:

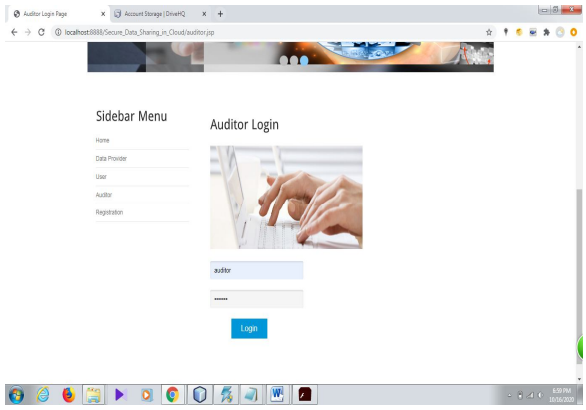
View File uploaded Data Page:

International Journal of Research

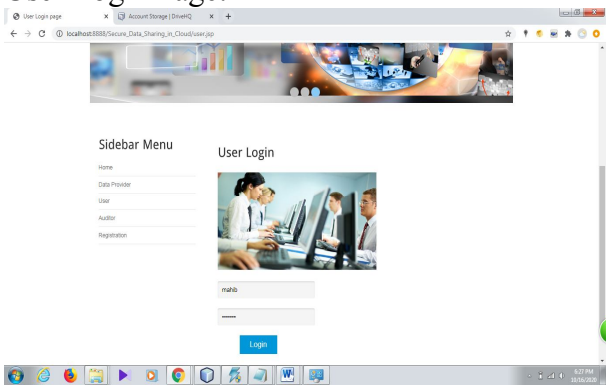
p-ISSN: 2348-6848
e-ISSN: 2348-795X
Volume 07 Issue 10
October 2020

Revocation & Ciphertext Update Page:





User Login Page:

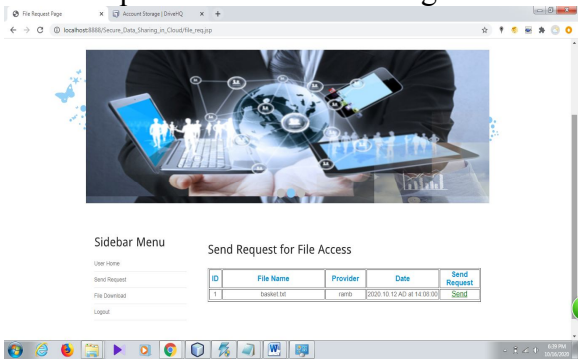


Auditor Home Page:

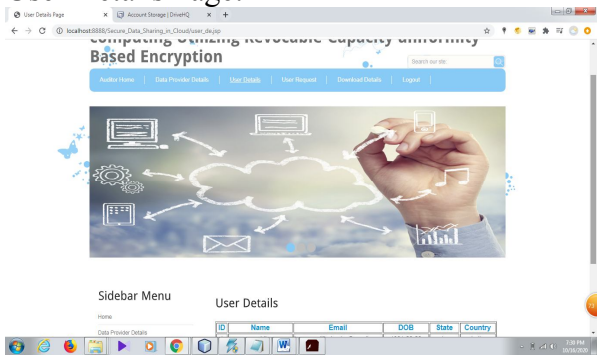
User Home Page:

Data Provider Details Page:

Send Request for File Access Page:



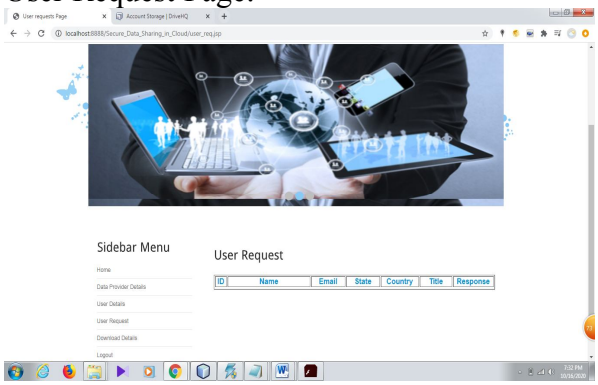
User Details Page:



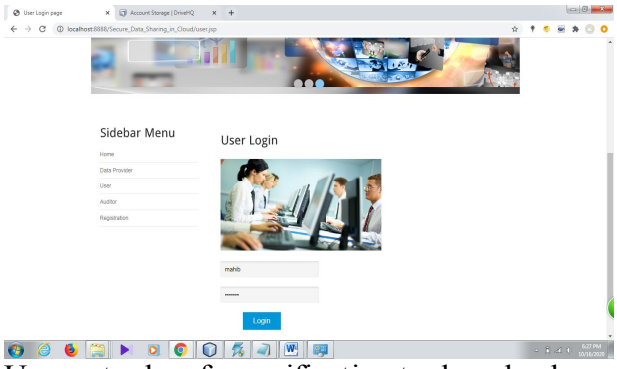
Auditor Login Page:

International Journal of Research
p-ISSN: 2348-6848
e-ISSN: 2348-795X
Volume 07 Issue 10
October 2020

User Request Page:



User Request Download File:



User enter key for verification to download

CONCLUSION

Cloud computing brings comfort this will be doubtlessly individuals that are mind blowing. Particularly, it perfectly facilitates the extended need of sharing data on the web. In this undertaking, to create a pragmatic and secure data system this is positively sharing computing that is cloud we proposed an idea called RS-IBE, which supports character forswearing and ciphertext update even while in a manner that a repudiated user is shielded from managing as of late shared data, similarly. At the same time in a way that a denied user is shielded from getting to as of late shared data, similarly as thusly shared data in this undertaking, This is decidedly concrete of RS-IBE is presented moreover, a turn of events. The proposed plot that is RS-IBE exhibited secure that is adaptable you look at the standard model, underneath the decisional doubt it is irrefutably ℓ-DBHE. The assessment results display which our arrangement has focuses that are central connection to viability and handiness, and furthermore as a result is unmistakably more essential for commonsense applications.

REFERENCES

[1] L. M. Vaquero, L. Rodero-Merino, J. Caceres, and M. Lindner, "A break in the clouds: towards a cloud definition," *ACM SIGCOMM Computer Communication Review*, vol. 39, no. 1, pp. 50–55, 2008.

[2] iCloud. (2014) Apple storage service. [Online]. Available: https://www.icloud.com/

[3] Azure. (2014) Azure storage service. [Online]. Available: http://www.windowsazure.com/

[4] Amazon. (2014) Amazon simple storage service (amazon s3).[Online]. Available: http://aws.amazon.com/s3/

[5] K. Chard, K. Bubendorfer, S. Caton, and O. F. Rana, "Social cloud computing: A vision for socially motivated resource sharing," *Services Computing, IEEE Transactions on*, vol. 5, no. 4, pp. 551–563, 2012.

[6] C. Wang, S. S. Chow, Q. Wang, K. Ren, and W. Lou, "Privacy preserving public auditing for secure cloud storage," *Computers, IEEE Transactions on*, vol. 62, no. 2, pp. 362–375, 2013.

[7] G. Anthes, "Security in the cloud," *Communications of the ACM*, vol. 53, no. 11, pp. 16–18, 2010.

[8] K. Yang and X. Jia, "An efficient and secure dynamic auditing protocol for data

storage in cloud computing," *Parallel and Distributed Systems, IEEE Transactions on*, vol. 24, no. 9, pp. 1717–1726, 2013.

[9] B. Wang, B. Li, and H. Li, "Public auditing for shared data with efficient user revocation in the cloud," in *INFOCOM, 2013 Proceedings IEEE*. IEEE, 2013, pp. 2904–2912.

[10] S. Ruj, M. Stojmenovic, and A. Nayak, "Decentralized access control with anonymous authentication of data stored in clouds," *Parallel and Distributed Systems, IEEE Transactions on*, vol. 25, no. 2, pp. 384–394, 2014.

[11] X. Huang, J. Liu, S. Tang, Y. Xiang, K. Liang, L. Xu, and J. Zhou, "Cost-effective authentic and anonymous data sharing with forward security," *Computers, IEEE Transactions on*, 2014, doi: 10.1109/TC.2014.2315619.

[12] C.-K. Chu, S. S. Chow, W.-G. Tzeng, J. Zhou, and R. H. Deng, "Key-aggregate cryptosystem for scalable data sharing in cloud storage," *Parallel and Distributed Systems, IEEE Transactions on*, vol. 25, no. 2, pp. 468–477, 2014.

[13] A. Shamir, "Identity-based cryptosystems and signature schemes," in *Advances in cryptology*. Springer, 1985, pp. 47–53.

[14] D. Boneh and M. Franklin, "Identity-based encryption from the weil pairing," *SIAM Journal on Computing*, vol. 32, no. 3, pp. 586– 615, 2003.

[15] S. Micali, "Efficient certificate revocation," Tech. Rep., 1996.

[16] W. Aiello, S. Lodha, and R. Ostrovsky, "Fast digital identity revocation," in *Advances in Cryptology–CRYPTO 1998*. Springer, 1998, pp. 137–152.

[17] D. Naor, M. Naor, and J. Lotspiech, "Revocation and tracing schemes for stateless receivers," in *Advances in Cryptology– CRYPTO 2001*. Springer, 2001, pp. 41–62.

[18] C. Gentry, "Certificate-based encryption and the certificate revocation problem," in *Advances in Cryptology–EUROCRYPT 2003*. Springer, 2003, pp. 272–293.

[19] V. Goyal, "Certificate revocation using fine grained certificate space partitioning," in *Financial Cryptography and Data Security*. Springer, 2007, pp. 247–259.

[20] A. Boldyreva, V. Goyal, and V. Kumar, "Identity-based encryption with efficient revocation," in *Proceedings of the 15th ACM conference on Computer and communications security*. ACM, 2008, pp. 417–426.

[21] B. Libert and D. Vergnaud, "Adaptive-id secure revocable identity based encryption," in *Topics in Cryptology–CT-RSA 2009*. Springer, 2009, pp. 1–15.

[22] ——, "Towards black-box accountable authority ibe with short ciphertexts and private keys," in *Public Key Cryptography–PKC 2009*. Springer, 2009, pp. 235–255.

[23] J. Chen, H. W. Lim, S. Ling, H. Wang, and K. Nguyen, "Revocable identity-based encryption from lattices," in *Information Security and Privacy*. Springer, 2012, pp. 390–403.

[24] J. H. Seo and K. Emura, "Revocable identity-based encryption revisited: Security model and construction," in *Public-Key Cryptography–PKC 2013*. Springer, 2013, pp. 216–234.

[25] ——, "Efficient delegation of key generation and revocation functionalities in identity-based encryption," in *Topics in Cryptology– CT-RSA 2013*. Springer, 2013, pp. 343–358.

[26] K. Liang, J. K. Liu, D. S. Wong, and W. Susilo, "An efficient cloud based revocable identity-based proxy re-encryption scheme for public clouds data sharing," in *Computer Security-ESORICS 2014*. Springer, 2014, pp. 257–272.

[27] D.-H. Phan, D. Pointcheval, S. F. Shahandashti, and M. Strefler, "Adaptive cca broadcast encryption with constant-

size secret keys and ciphertexts," *International journal of information security*, vol. 12, no. 4, pp. 251–265, 2013.

[28] R. Anderson, "Two remarks on public-key cryptology (invited lecture)," 1997.

[29] M. Bellare and S. K. Miner, "A forward-secure digital signature scheme," in *Advances in Cryptology–CRYPTO 1999*. Springer, 1999, pp. 431–448.

[30] M. Abdalla and L. Reyzin, "A new forward-secure digital signature scheme," in *Advances in Cryptology–ASIACRYPT 2000*. Springer, 2000, pp. 116–129.

[31] A. Kozlov and L. Reyzin, "Forward-secure signatures with fast key update," in *Security in communication Networks*. Springer, 2003, pp. 241–256.

[32] X. Boyen, H. Shacham, E. Shen, and B. Waters, "Forward-secure signatures with untrusted update," in *Proceedings of the 13th ACM conference on Computer and communications security*. ACM, 2006, pp. 191–200.

[33] J. Yu, R. Hao, F. Kong, X. Cheng, J. Fan, and Y. Chen, "Forward secure identity-based signature: security notions and construction," *Information Sciences*, vol. 181, no. 3, pp. 648–660, 2011.

[34] R. Canetti, S. Halevi, and J. Katz, "A forward-secure public-key encryption scheme," in *Advances in Cryptology–Eurocrypt 2003*. Springer, 2003, pp. 255–271.

[35] D. Yao, N. Fazio, Y. Dodis, and A. Lysyanskaya, "Id-based encryption for complex hierarchies with applications to forward security and broadcast encryption," in *Proceedings of the 11th ACM conference on Computer and communications security*. ACM, 2004, pp. 354–363.

[36] J. M. G. Nieto, M. Manulis, and D. Sun, "Forward-secure hierarchical predicate encryption," in *Pairing-Based Cryptography–Pairing 2012*. Springer, 2013, pp. 83–101.

[37] A. Sahai, H. Seyalioglu, and B. Waters, "Dynamic credentials and ciphertext delegation for attribute-based encryption," in *Advances in Cryptology–CRYPTO 2012*. Springer, 2012, pp. 199–217.

[38] B. Waters, "Efficient identity-based encryption without random oracles," in *Advances in Cryptology–EUROCRYPT 2005*. Springer, 2005, pp. 114–127.

[39] B. Lynn. (2014) Pbc library: The pairing-based cryptography library. [Online]. Available: http://crypto.stanford.edu/pbc/