As per UGC guidelines an electronic bar code is provided to seure your paper

International Journal for Modern Trends in Science and Technology, 8(08): 92-99, 2022
Copyright © 2022 International Journal for Modern Trends in Science and Technology
ISSN: 2455-3778 online
DOI: https://doi.org/10.46501/IJMTST0808014
Available online at: http://www.ijmtst.com/vol8issue08.html

Two Level Authentication Based Secure Data Transmission Over Cloud

N.Priyanka[1] | Ch. Kodanda Ramu[2]

[1]PG Scholar, student Miracle Educational Group of institutions, Vizianagaram, Andhra Pradesh, India.
[2]Associate professor, Department of CSE, Miracle Educational Group of institutions, Vizianagaram, Andhra Pradesh, India

To Cite this Article
N.Priyanka and Ch. Kodanda Ramu. Two Level Authentication Based Secure Data Transmission Over Cloud. International Journal for Modern Trends in Science and Technology 2022, 8(08), pp. 92-99. https://doi.org/10.46501/IJMTST0808014

Article Info
Received: 06 July 2022; Accepted: 02 August 2022; Published: 09 August 2022.

ABSTRACT

Cloud computing research continues to focus on secure data transmission and multi-owner data exchange, both of which are critical today. Information capacity utilizing a productive gathering key convention and an original procedure of adding another information proprietor without imperiling the uprightness of current information are both proposed to give secure information transmission between numerous proprietors. Currently In Place: Multiple researchers have proposed various approaches to the problem in the traditional approach, which divides files into blocks and applies cryptographic mechanisms to each block. This is a very time-consuming process, and when a new owner is added, the key needs to be updated and accepted by all data owners. Previous approaches have divided files into multiple blocks and applied cryptographic mechanisms to each block. Complex cryptographic procedures are necessary to provide the greatest degree of security. If the key is sent over the network, it becomes susceptible. The old technique does not include data owner authentication. Problems with multi-owner data sharing were recognised, and a protocol and cryptographic mechanism were suggested to alleviate the shortcomings of the conventional approach. Group key generation using LaGrange's polynomial-based equation is introduced, and data owners may be confirmed before the key creation. The AES technique may be used to encrypt data once the key has been generated.

Keywords : cloud computing, secure data, multi owner, crypto graphic, AES

INTRODUCTION

1. Cloud Introduction

The phrase "cloud computing" refers to a relatively new computer concept centred on the concept of utility and resource usage. Distributed computing, which utilizes a few far off servers and programming organizations, considers incorporated information capacity and online admittance to PC administrations and assets. Mists might be named either open, private, or a mixture of the three. Computing resources (hardware and software) are made available through a wide area network (WAN) by cloud computing platform providers (typically the Internet). In system diagrams, a cloud-shaped symbol is used to represent the complex infrastructure that is included inside the cloud. The data, software, and processing of a user are entrusted to distant services through cloud computing. Software and physical resources are made accessible online as managed services provided by a third party under the cloud computing model. Software applications and high-performance networks of servers are available via several of these services.

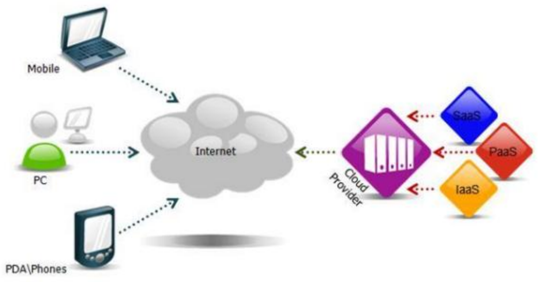


Fig 1.1 Architecture of cloud computing

1.2 Cloud Computing services are classified like below

i. IaaS A service that provides a platform virtualization environment as a computer infrastructure. It's feasible to pay a specialist organization as opposed to buying servers and programming, server farm space, and organization hardware.

ii. PaaS provide the developers the ability to build their own apps on the platform.

iii. SaaS in which the consumers are supplied with apps as a service rather than owning them outright

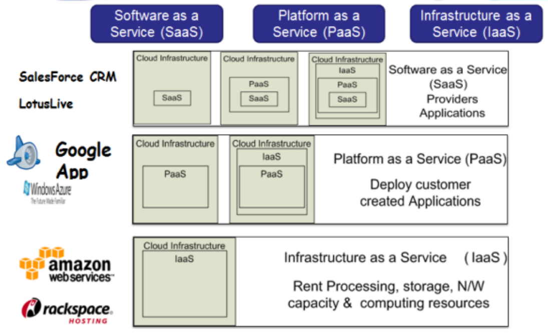

Software as a Service (SaaS)
Platform as a Service (PaaS)
Infrastructure as a Service (IaaS)
SalesForce CRM
LotusLive
Google App
WindowsAzure
amazon webservices
rackspace HOSTING
Cloud Infrastructure
SaaS
PaaS
IaaS
Software as a Service (SaaS) Providers Applications
Platform as a Service (PaaS)
Deploy customer created Applications
Infrastructure as a Service (IaaS)
Rent Processing, storage, N/W capacity & computing resources

Fig 1.2Service Models of cloud computing

1.3 Characteristics

A number of important aspects of cloud computing have been identified by NIST.

Whenever-needed self-service: An end user may offer computer resources, like as server time and organization stockpiling, without having to contact each specialist co-op by and by.

Broad network access: Standard techniques enable diverse thin and thick client systems to make advantage of available capabilities via the network (e.g., mobile phones, laptops, and PDAs).

Resource pooling: An solution that utilises both physical and virtual resources is known as a "multi-tenant" model because it allows the service provider to offer a greater number of clients by pooling its computing resources. Cloud computing is the term for this. in other words, the client has no say in where their resources are placed, in any case, they might determine area at a higher deliberation level, on the off chance that they like (e.g., nation, state, or server farm). Assets incorporate, however are not restricted to, circle space, figuring power, memory, network data transmission, and virtual machines.

Rapid elasticity: Automatic provisioning and release of capabilities may be possible in certain cases, allowing for quick scaling up and down as needed. The number of capabilities that may be provided at any one time seems to be endless in the perspective of the customer.

Measured service: To govern and optimise the usage of resources, cloud systems utilise metres at an abstraction level appropriate for the kind of service (e.g., capacity, handling, transfer speed, and dynamic client accounts). For both the provider of the service as well as the end-user, it is possible to track how resources are being utilised.

1.4 Deployment Models

It is possible to use three different service models in the cloud: infrastructure-based, platform-based, and software-based (SaaS). In order to complete the three service models or layers, the end client layer exemplifies the end client's point of view on the cloud administrations. The model may be seen in the following image. You may run your own apps on the infrastructure of a cloud and be in charge of their support, maintenance, and security if you employ the infrastructure layer services that a cloud provider offers. The cloud service provider often handles these responsibilities if she uses an application-layer service.

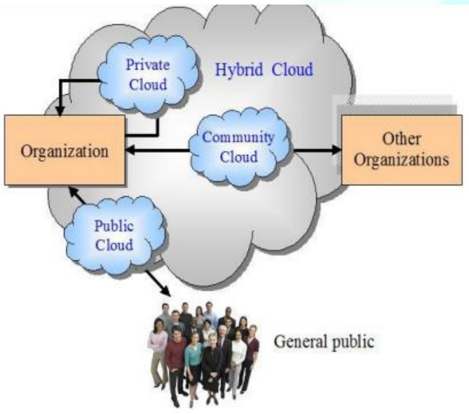


Fig 1.3 Deployment Models of Cloud

1.5 Benefits of cloud computing

1. Realize scale economies – With a smaller workforce, enhance production or productivity. Your costs per unit, project, or product are dramatically reduced.

2. Reduce the amount of money spent on technical infrastructure. Invest a little amount of money up front

to keep your data easily accessible. According to demand, you may pay in increments (weekly, quarterly, or annually).

3. Expand your workforce to different nations at a low cost. The cloud may be accessed from anywhere in the world with an Internet connection.

4. Process simplification. To accomplish more significantly quicker, utilize less individuals.

5. Reduce the cost of capital. Costs associated with hardware, software, and licences may be kept to a minimum.

6. Improve the usability of the system. It may be accessed at any time, from any place, making your life easier.

7. Improve your ability to keep track of your tasks. Keep your costs in check and your completion schedule on track.

8. More people can be trained with less effort. In the cloud, more work can be done with fewer people, and hardware and software problems have a low learning curve.

9. A minimum number of licences should be issued for every new programme. In order to grow and prosper, you don't have to purchase costly programming licenses or projects.

10. Improve flexibility. It is possible to shift course without risking severe "people" or "money" concerns.

11. Uptime: Multiple servers are used to ensure optimum uptime. An instance may be generated on another server in the event of a server failure.

12. Control: From anywhere, you may access your account. With a server snapshot and software library, you may quickly and easily create new instances of your server.

13. Traffic: Quickly deploys extra instances to accommodate the strain as traffic spikes.

2. LITERATURE SURVEY

A vast number of IT benefits, including on-demand service, geographical independence, resource pooling, and flexibility, have made cloud computing the next generation of IT design. As a result of clouding, both people and organisations may benefit from the following advantages: lessening the burden of data storage management, gaining access to data from anywhere in the world, and avoiding big expenditures on hardware and human maintenances, among other things.

Cloud services are becoming more popular because of their efficiency as both a resource area and a data storage area. You may create a programme, a cloud virtual machine, and many other advantages by using cloud service technology. There is a pay-per-use model for cloud service providers and data owners. He or she has no idea where the actual data is kept, but he or she may use their login credentials to browse the cloud as necessary.

Data Owner: An owner or user of data is someone who has more data on a server than the service provider or who provides the service provider with data or data components. Without having to worry about storage or maintenance, a user may upload their data onto the cloud. A service provider's services and privileges will be available to the user. When storing data on the cloud, it is crucial to ensure that the data is accurate and reliable.

Third Party Auditor: Third-party auditors serve as verifiers, verifying that the data requested by the user is stored accurately and reliably. Using the Cloud Service Provider as a conduit, this auditor keeps tabs on all of the data that the data owner uploads.

Using cloud storage, It is possible for data owners to migrate their files to the cloud from their local computer systems, which is a key function provided by cloud computing. Cloud storage is becoming more popular among business owners. Data deployment services using this new concept offer a new set of security concerns. Owners would be concerned about losing their data on the cloud. No matter how much care cloud service companies take to ensure their systems are reliable, data loss is always a possibility. Cloud service providers might be corrupt in certain instances. To preserve storage space, they might delete material that has not been accessed for a long time or has only been accessed a few times. Data must be stored in a systematic way in the cloud for owners to be happy.

Confidentiality is a significant concern for cloud service providers while transferring or receiving data components from or to Cloud service providers in numerous circumstances. We'll go through everything in great depth in this article.

Multiple researchers have proposed various approaches to the problem in the traditional approach, which divides files into blocks and applies cryptographic mechanisms to each block. This is a very time-consuming process, and when a new owner is added, the key needs to be updated and accepted by all data owners. Previous approaches have divided files into multiple blocks and applied cryptographic mechanisms to each block.

You don't have to worry about maintaining your own infrastructure if you utilise cloud-based software for development or other services. Data confidentiality is the most important consideration when uploading data to the server, since consumers do not know where the data is truly kept. When migrating servers, it's critical to protect data privacy and integrity.

Digital certificates, authentication, and cryptographic processes are all accessible for safe storage thanks to a variety of newly developed systems for maintaining data authenticity, secrecy, and integrity.

To ensure data security, we're introducing the concept of several data owners sharing their data, which may be encrypted using a key derived from the Shamir method and transformed to unformatted text using the AES technique.

2.1 Cloud Computing's Data Security and Privacy Protection Issues

Authors:Deyan Chen, Hong Zhao

Cloud computing is well-known for its potential benefits, and many company applications and data are moving to public or hybrid cloud. Large corporations in particular will not, however, migrate certain mission-critical programmes to the cloud. Cloud computing's market share is still a lot less than anticipated. Data security and privacy protection concerns remain the key barrier to cloud computing adoption from the standpoint of customers. All aspects of cloud computing's data security and privacy protection are examined in this article, which gives a succinct yet comprehensive overview. Afterwards, this article explores a few of the most recent options. Finally, this study outlines future research on cloud-based data security and privacy concerns.

2.2 An analysis of cloud computing security issues

Author(s): Behl A, Behl K.

When it comes to implementing IT and associated activities and elements, a non-traditional computing model like cloud computing may save companies money in the long run by reducing their Total Cost of Ownership (TCO). Among the many advantages of distributed computing is the capacity to scale figuring assets on request, as well as unique stockpiling and the capacity to satisfy handling needs on request. Security of an unconditional and free asset is still being referred to, which affects cloud reception regardless of the advantages of distributed computing. As additional aspects of the issue linked to architecture, multi-tenancy, layer dependence, and elasticity enter the problem scope, the security challenge is increased under the cloud model. The subject of cloud security is examined in depth in this study. Stakeholders, architecture, cloud features, and delivery model are all considered in this study while examining how to best secure the cloud. There are several obstacles in developing cloud-based security solutions that can keep pace with the ever-changing and dynamic nature of cloud computing. This paper gives an exhaustive examination of the cloud security predicament and the significant highlights that ought to be tended to by any proposed distributed computing security arrangement.

2.3 Secure cloud computing: Benefits, risks and controls

Author(s): Carroll M,vanderMerwe A, Kotze P.

Self-service, on-demand, elastic, and dynamically scaleable access to pools of frequently virtualized resources is the characteristic of cloud computing. For businesses and IT departments, cloud computing offers the potential to improve productivity and efficiency by enabling fast start-up times and scalability, as well as cost savings. Despite the fact that cloud computing offers appealing advantages and cost-effective IT hosting and growth choices, it also introduces new security concerns and chances for exploiting security. The importance of standards, rules, and controls in protecting and securing systems and data cannot be overstated. Cloud computing risks must be understood and analysed by management in order to keep systems and data safe. To provide safe cloud computing environments, this study focuses on mitigating cloud computing security threats.

2.4 Encrypted Cloud Data with Privacy-Preserving Multi-Keyword Ranked Search

Author: Ning Cao

With cloud computing, organisations and individuals may reap the advantages of shifting their data management systems from on-premise servers to commercial public clouds without sacrificing the security and efficiency of their data. Because sensitive data must be encrypted before being outsourced to preserve privacy, plaintext keyword search is out of date. As a result, it is critical to have an encrypted cloud data search service. Since there are so many people accessing data in the cloud, it is vital to accept numerous keywords and return documents based on relevancy to these keywords. A single term or a Boolean keyword search is all that is often utilised in investigations of searchable encryption. This article is quick to blueprint and resolve the issue of doing a multi-catchphrase positioning pursuit on encoded information in the cloud (MRSE). For such a safe method of using cloud data, we established very specific privacy standards. A measure of how closely data documents match a search query is called "coordinate matching," and it is the most efficient way to determine how closely data documents match a search query. In addition, we employ "inner product similarity" to objectively analyse this measure of similarity. Two considerably enhanced techniques are shown to meet varied rigorous privacy criteria in two separate threat models based on MRSE's core notion of safe inner product computation. We've added additional search semantics to these two methods to make the data search service better for users. The suggested systems' privacy and efficiency guarantees are thoroughly analysed. Experimental results using real-world data reveal that the suggested approaches do, in fact, reduce compute and transmission overhead to a minimal level.

2.5 Cloud Computing Security: Current Trends and Future Research

Author:Sengupta, S.

As more and more business applications and data migrate to cloud platforms, cloud computing is growing in popularity. There is, however, an inherent and perceived lack of security when it comes to cloud computing. Virtualization, programming stage, character the board and access control, information respectability and classification and protection, and physical and procedural security in distributed computing are evaluated in this article from a wide assortment of perspectives. Our discoveries incorporate cloud specialist co-ops, cloud clients, and outsider associations including the public authority. Topics like Trusted Computing, Information Centric Security, and Privacy Preserving Models research are also covered in detail. Finally, we provide a high-level process for evaluating a business application's security readiness before moving it to the cloud.

3. PROBLEM STATEMENT

Cloud computing research continues to focus on secure data transmission and multi-owner data exchange, both of which are critical today. As a result of the complexity of handling multi-owner data sharing in the traditional approach, various researchers have proposed a variety of solutions, including dividing the files into blocks and applying cryptographic mechanisms to each block, which is a time-consuming process and must be accepted by all data owners.

Disadvantages of Existing System

Cloud-based data cannot be shared with a new data owner. If a new data owner is added, it's possible that disclosing the secret key may compromise the data's security. An very labor-intensive procedure, updating the key every time a new owner is added requires consensus among all the data's existing owners. There is no guarantee that a trustworthy user will be able to access the cloud in question. Complex cryptographic procedures are needed to provide the maximum degree of security. If the key is sent across the network, it is susceptible.

4. PROPOSED SYSTEM

Multi-owner data sharing has been noted as a difficulty by the suggested system, which offered an efficient protocol and cryptographic mechanism to address these issues. Group key generation using LaGrange's polynomial-based equation is introduced, and data owners may be confirmed before the key creation. The AES cryptographic technique may be used to encrypt data once the key has been generated.

Authentication: When a user is registered at a key generation centre (KGC), the KGC generates and sends a secret share in the format of (xi,yj) to all registered users, which the data owners compute XOR(Yj, R) and forward to KGC, KGC verifies with the reverse XOR operation and checks authentication, and the key is generated.

Advantages of Proposed System

New data owners may be added to the cloud's storage space. Trusted user access to the cloud is guaranteed by us. As long as the key is sent across the network, it is safe

5. ARCHITECTURE

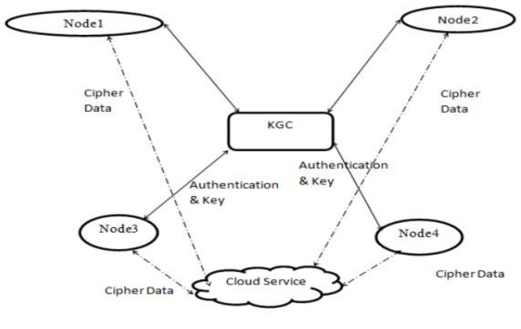


Fig 3.1 Architecture of KGC

6. IMPLEMENTATION

6.1 KGC Authentication

When a user is registered at a key generation centre (KGC), the KGC generates and sends a secret share in the format of (xi,yj) to all registered users, which the data owners compute XOR(Yj, R) and forward to KGC, KGC verifies with the reverse XOR operation and checks authentication, and the key is generated.

6.2 Secure Data

A data owner may encrypt a document and save it in the cloud using the AES technique provided by the Key Generation Center. The Shamir secret-sharing method is used to generate a key for the AES algorithm, which is used to encrypt data. Encrypted plain data components are sent back and forth between client computers and the server using this key.

6.3 Algorithm used : Key Generation

Data D (such as the safe combination) in such a way that any k or more of these D pieces may be used to easily calculate D. This is the goal.

D remains a mystery until all k -1 components are known (in the sense that it is equally likely to have any of its potential values).

The (k,n) threshold scheme is the name given to this method. This means that all players must work together in order to solve the puzzle.

The (k,n) threshold approach may be used to divulge our secret S if k is less than or equal to n.

Let S be the (k-1) random coefficients S1, S2, S3, S4...ak-1.

f(x)=a0 + a1x + a2x2 + ……….+ak-1k-1

Create n points I f(i)) with i=1, 2,... n.

Example:

Let S be the number 1234.

n is six and k is three random numbers 166 and 94 are generated f(x)=1234+166x+94x2.a1

There are a total of five secret sharing points: (1,1494), (2,1942), (3,2598)(4,3402)(5,4414) (6,5614)

Each participant is awarded a single, special point. (x and f(x)) in the experiment.

Re-construction:

If just three points are available, it will be enough to solve the puzzle.

Let us examine (x0,y0)=(2,1924), (x1,y1)=(4,3402), and (x2,y2)=(2,1924) as examples (5,4414)

Using lagrangeous polynomials

L0=x-x1/x0-x1*x-x2/x0-x2=x-4/2-4*x-5/2-5=(1/6)x2-(3/2)x+10/3

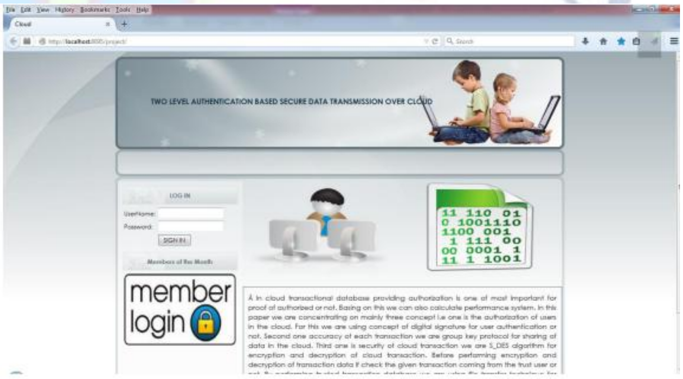
L1=x-x0/x1-x0*x-x2/x1-x2=x-2/4-2*x-5/4-5=-(1/2)x2-(7/2)x -5

L2=x-x0/x2-x0*x-x1/x2-x1=x-2/5-2*x-4/5-4=(1/3)x2-2x+8/3

f(x)= ∑ y 2 j=0 jlj(x)=1942((1/6)x2-(3/2)x+10/3)+3402(-(1/2)x2-(7/2)x-)+4414((1/3)x2- 2x+8/3)

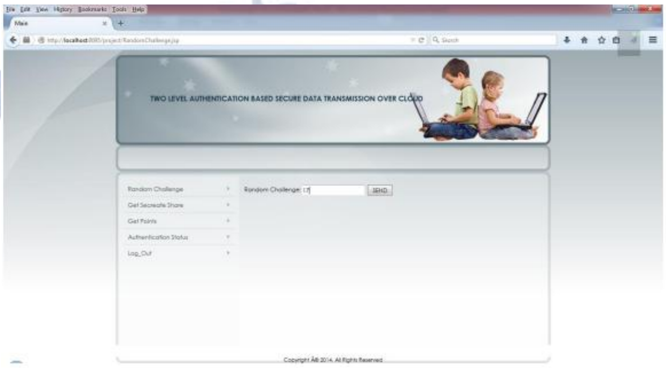
f(x)=1234+166x+94x2 Remember that the free coefficient is the key, hence S=1234 is the answer.

7. RESULTS


File Edit View History Bookmarks Tools Help
Cloud
http://localhost:8085/project/
Search
TWO LEVEL AUTHENTICATION BASED SECURE DATA TRANSMISSION OVER CLOUD
LOG IN
UserName:
Password:
SIGN IN
Members of the Month
member login
11 110 01
0 1001110
1100 001
1 111 00
00 0001 1
11 1 1001

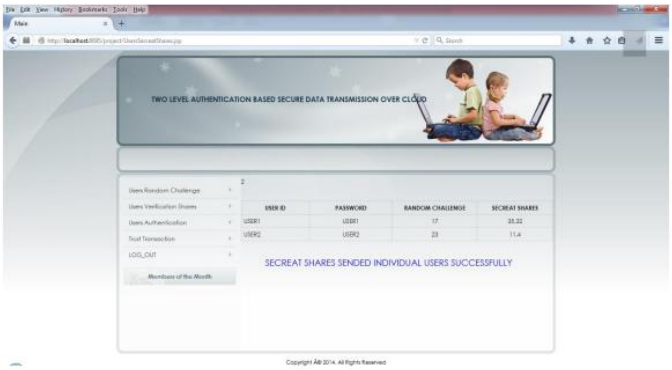
A In cloud transactional database providing authorization is one of most important for proof of authorized or not. Basing on this we can also calculate performance system. In this paper we are concentrating on mainly three concept i.e one is the authorization of users in the cloud. For this we are using concept of digital signature for user authentication or not. Second one accuracy of each transaction we are group key protocol for sharing of data in the cloud. Third one is security of cloud transaction we are S_DES algorithm for encryption and decryption of cloud transaction. Before performing encryption and decryption of transaction data it check the given transaction coming from the trust user or

Home page


File Edit View History Bookmarks Tools Help
Main
http://localhost:8085/project/RandomChallenge.jsp
Search
TWO LEVEL AUTHENTICATION BASED SECURE DATA TRANSMISSION OVER CLOUD
Random Challenge
Get Secreate Share
Get Points
Authentication Status
Log_Out
SEND
Copyright Â© 2014. All Rights Reserved

Random Challenge: 17

Random Challenge Page

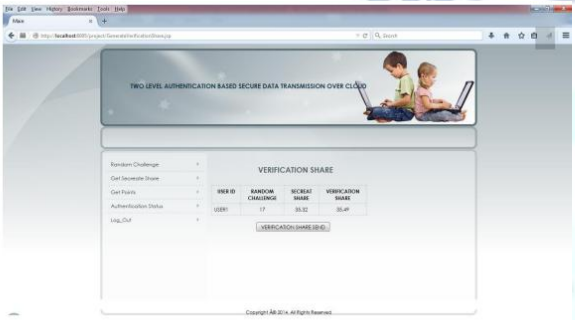

TWO LEVEL AUTHENTICATION BASED SECURE DATA TRANSMISSION OVER CLOUD
Users Random Challenge
Users Verification Shares
Users Authentication
Trust Transaction
LOG_OUT
Members of the Month
Copyright Â© 2014. All Rights Reserved

2

USER ID	PASSWORD	RANDOM CHALLENGE	SECREAT SHARES
USER1	USER1	17	35.32
USER2	USER2	23	11.4

SECREAT SHARES SENDED INDIVIDUAL USERS SUCCESSFULLY

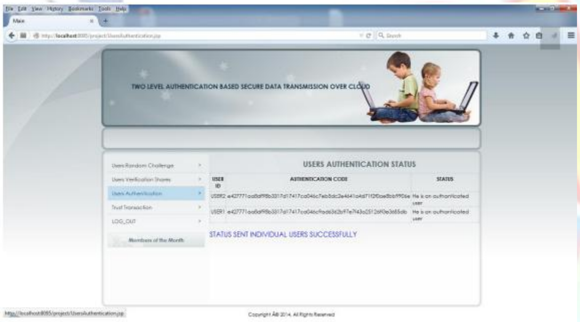
Secrete Share Page


TWO LEVEL AUTHENTICATION BASED SECURE DATA TRANSMISSION OVER CLOUD
Random Challenge
Get Secreate Share
Get Points
Authentication Status
Log_Out
VERIFICATION SHARE SEND
Copyright Â© 2014. All Rights Reserved

VERIFICATION SHARE

USER ID	RANDOM CHALLENGE	SECREAT SHARE	VERIFICATION SHARE
USER1	17	35.32	35.49

Verification Share Page

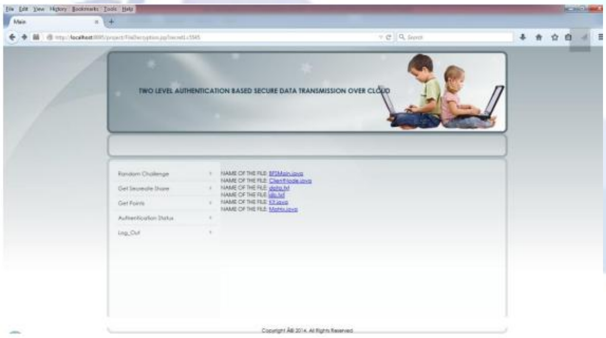

TWO LEVEL AUTHENTICATION BASED SECURE DATA TRANSMISSION OVER CLOUD
Users Random Challenge
Users Verification Shares
Users Authentication
Trust Transaction
LOG_OUT
Members of the Month
http://localhost:8085/project/UsersAuthentication.jsp
Copyright Â© 2014. All Rights Reserved

USERS AUTHENTICATION STATUS

USER ID	AUTHENTICATION CODE	STATUS
USER2	e427771aa8af98b3317a17417ca046c7eb5dc2e4641a4d71f2f0ae8bb9906e	He is an authenticated user
USER1	e427771aa8af98b3317a17417ca046c9ad63d2b97e7f43a2512693e3685db	He is an authenticated user

STATUS SENT INDIVIDUAL USERS SUCCESSFULLY

Authentication Code Status Page


TWO LEVEL AUTHENTICATION BASED SECURE DATA TRANSMISSION OVER CLOUD
Random Challenge
Get Secreate Share
Get Points
Authentication Status
Log_Out
Copyright Â© 2014. All Rights Reserved

NAME OF THE FILE: BFSMain.java
NAME OF THE FILE: ClientNode.java
NAME OF THE FILE: data.txt
NAME OF THE FILE: ab.txt
NAME OF THE FILE: KF.java
NAME OF THE FILE: Matrix.java

Decrypt Page

8. CONCLUSION AND FUTURE SCOPE

In this study, I presented a system that highlighted the issues that arise when data is shared among several owners and offered an efficient protocol and cryptographic mechanism for addressing the shortcomings of the old approach. LaGrange's polynomial-based formula is used to provide a safe and efficient key protocol for group key creation prior to key generation. The AES cryptographic technique may be used to encrypt data once the key has been generated. New data owners may be added to the cloud's storage space. Trusted user access to the cloud is guaranteed by us. If the key is sent directly over the network, it is not susceptible.

Conflict of interest statement

Authors declare that they do not have any conflict of interest.

REFERENCES

[1] M. Armbrust, A. Fox, R. Griffith, A. D. Joseph, R. H.Katz, A. Konwinski,G. Lee, D. A. Patterson, A. Rabkin, I.Stoica, and M. Zaharia,"Above the clouds: A berkeley view of cloud computing," University ofCalifornia,Berkeley, Tech. Rep. USB-EECS2009-28, Feb 2009.

[2] Amazon Web Services (AWS), Online at http://aws.amazon.com.

[3] Google App Engine, Online athttp://code.google.com/appengine/.

[4] Microsoft Azure, http://www.microsoft.com/azure/.

[5] 104th United States Congress, "Health InsurancePortability and Accountability Act of 1996 (HIPPA)," Online athttp://aspe.hhs.gov/admnsimp/pl104191.htm, 1996.

[6] H. Harney, A. Colgrove, and P. D. McDaniel,"Principles of policy insecure groups," in Proc. OfNDSS'01, 2001.

[7] P. D. McDaniel and A. Prakash, "Methods andlimitations of securitypolicy reconciliation," in Proc. OfSP'02, 2002.

[8] T. Yu and M. Winslett, "A unified scheme for resourceprotection inautomated trust negotiation," in Proc. OfSP'03, 2003.

[9] J. Li, N. Li, and W. H. Winsborough, "Automated trust negotiationusing cryptographic credentials,"

[10] R. Buyyaet al., "Cloud computing and emerging it platforms: Vision, hype, and reality for delivering computing as the 5th utility," Future Gener. Comput. Syst., vol. 25, pp. 599–616, June 2009.

[11] X. Menget al., "Efficient resource provisioning in compute clouds via vm multiplexing," in Proceedings of the 7th international conference on Autonomic computing, ser. ICAC '10. New York, NY, USA: ACM, 2010, pp. 11–20.

[12] H. Liu et al., "Live virtual machine migration via asynchronous replication and state synchronization," Parallel and Distributed Systems, IEEE Transactions on, vol. 22, no. 12, pp. 1986 –1999, dec. 2011.

[13] B. Rochwergeret al., "Reservoir - when one cloud is not enough," Computer, vol. 44, no. 3, pp. 44 –51, march 2011.

[14] R. Buyya, R. Ranjan, and R. Calheiros, "Modeling and simulation of scalable cloud computing environments and the cloudsim toolkit: Challenges and opportunities," in High Performance Computing Simulation, 2009. HPCS '09. International Conference on, june 2009, pp. 1 –11.

[15] A. Iosup, N. Yigitbasi, and D. Epema, "On the performance variability of production cloud services," in Cluster, Cloud and Grid Computing (CCGrid), 2011 11th IEEE/ACM International Symposium on, may 2011, pp. 104 –113.

[16] A. V. Do et al., “Profiling applications for virtual machine placement in clouds,” in Cloud Computing (CLOUD), 2011 IEEE International Conference on, july 2011, pp. 660 –667.

[17] A. Vermaet al., “Server workload analysis for power minimization using consolidation,” in Proceedings of the USENIX Annual technical conference, Berkeley, CA, USA, 2009, pp. 28–28.

[18] G. Balbo et al., Modelling with Generalized Stochastic Petri Nets. John Wiley and Sons, 1995.

[19] R. Sahner, K. S. Trivedi, and A. Puliafito, Performance and reliability analysis of computer systems: an example based approach using the SHARPE software package. Kluwer Academic Publishers, 1995.