IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

Design and Analysis of Scalable and Secure Big Data Internet of Things System Based on Lightweight Cryptography and Multifactor Authentication

SANDHYA GANDI [#1], CHALAPAKA SRILEKHA [#2]

[#1] Assistant Professor, Department of Computer Science and Engineering,
Sanketika Vidhya Parishad Engineering College, P.M. Palem,
Visakhapatnam, Andhra Pradesh.

[#2] MCA Student, Department of Computer Science and Application,
Sanketika Vidhya Parishad Engineering College, P.M. Palem,
Visakhapatnam, Andhra Pradesh.

ABSTRACT

Almost every organisation now strives to raise awareness of their interest in cloud computing for Internet of Things (IoT) applications. The large volume of data produced by diverse devices may be stored and managed effectively by integrating IoT devices with cloud computing technologies. The IoT-cloud architecture is complicated by these firms' large data security, though. We suggest a cloud-enabled IoT ecosystem backed by multifactor authentication and lightweight cryptography encryption approaches to safeguard large data systems in order to address security concerns. The suggested Hybrid Cloud Environment aims to provide data protection for enterprises. The Hybrid Cloud Environment combines public and private clouds. Here, we attempt data encryption using AES and after which data security will be provided by the cloud. And those who request the file need decryption key from Trusted Authority (TA). As a result, the performance of the suggested architecture using metrics like computational time, security strength, encryption time, and decryption time can only be evaluated for those who obtain keys from TA.

KEYWORDS:

Trusted Authority, Encryption, Decryption, Data Security, Multifactor Authentication.

1. INTRODUCTION

Cloud computing technology has undergone a complete commercialization in the last ten years. It can cut expenses while increasing service effectiveness. As adevelopment, administration, and maintenance tool, the cloud platform is being utilised by an increasing number of businesses. As seen in Fig. 1, this not only eases the burden of local maintenance for these businesses but also offers unified security and operation management for all services on the third-party cloud platform. Users and servers connect through a public network, despite the fact that third-party cloud platforms have more advanced technology and more standardised technical requirements to guarantee that the servers operate in a comparatively safe environment. As a result, key agreement and authentication are crucial for communication security.

Mutual authentication and key agreement (Hybrid Cloud Environment) protocols are used to stop attackers from misusing server resources as well as from pretending to be the server in order to steal user data.

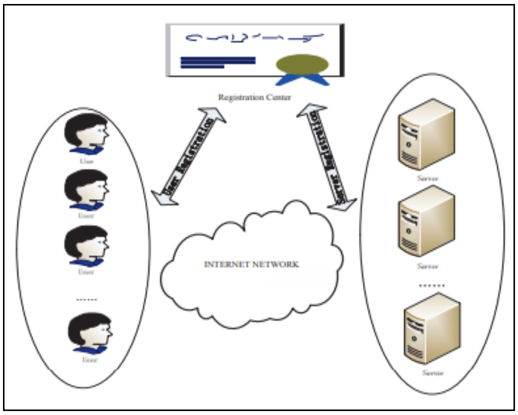


Figure 1.Represents the general cloud environment

As a result, since Lamport suggested a password-based authentication mechanism, the Hybrid Cloud Environment) protocols have undergone substantial research. For single-server architecture, earlier Hybrid Cloud Environment) protocols are created. As the number of Internet users increases tremendously, so too does the number of cloud servers offering various services. It is challenging for users to keep track of a variety of passwords for each server in a single-server design. Many academics suggest more adaptable Hybrid Cloud Environment) protocols for multi-server systems to enhance user experience. Such protocols can be used in conjunction with the cloud platform's unified management functions to be easily implemented. Users and cloud servers just need to register at the registration centre (RC) for the protocols for multi-server architectures model as shown in Fig. 2 in order to perform mutual authentication and key agreement

2. LITERATURE SURVEY

Literature survey is that the most vital step in software development process. Before developing the new application or model, it's necessary to work out the time factor, economy and company strength. Once all these factors are confirmed and got an approval then we can start building the application.

MOTIVATION

1) A Survey on Security Aspects for 3GPP 5G Networks

Authors: Lihui Xiong

The Third Generation Partnership Project (3GPP) has proposed standards for the fifth generation of mobile communication technology (5G), which officially begins the transition from the current Long Term Evolution (LTE) system to the next generation of mobile communication system, in response to the ongoing development of mobile communication technologies (5GS). This article significantly advances the security features of 3GPP 5G networks. First, we give a general overview of the 3GPP 5G networks' network architecture and security features. The support of numerous Internet of Things (IoT) devices, Device to Device (D2D) communication, Vehicle to Everything (V2X) communication, and network slicing are the new features and methods that we concentrate on since they pose significant problems to 3GPP's security measures.

2) A Chaotic Map-Based Authenticated Key Agreement in a Multi-Server Architecture that is Improved and Provably Secure.

Authors: Azeem Irshad

A subscriber may use several services from various service providers under the multi-server authentication (MSA) paradigm after registering with the registration authority. With this method, servers are freed from handling unique registrations and users just need to remember a single password for all service providers.

Many MSA-related systems have been proposed thus far, however they have a number of shortcomings. A chaotic map-based multi-server authentication technique was recently reported by Li et al.

3) A Generalized Framework for Three-Factor Authentication: Protecting Distributed Systems' Security and Privacy

Authors: Yang Xiang

Various services and resources inside distributed systems need to be secured against unauthorised usage. The most popular technique for confirming a distant client's identity is remote authentication. This study examines a methodical procedure for client authentication using a password, a smart card, and a biometric. The transition from two-factor authentication to three-factor authentication is suggested using a general and safe architecture. In distributed systems, the conversion not only greatly raises information assurance at a minimal cost but also safeguards client privacy. Additionally, we feel that our framework is of independent importance since it preserves a number of the two-factor authentication's practice-friendly characteristics.

3. EXISTING SYSTEM AND ITS LIMITATIONS

Existing cloud servers lacked both the idea of cloud data encryption and the capability of segmenting the cloud into separate regions for the safe storage of large amounts of data. The present cloud storage is essentially centralised, making it easy for the cloud server department to see all of the stored data as well as information on the data's owners and users. This is nearly a major issue for the existing cloud service providers. The existing cloud servers allow everyone with a cloud account access to view and access all of the data, meaning that the data lacks integrity and security against any alterations made by anyone.

LIMITATION OF PRIMITIVE SYSTEM

The following are the limitations of the existing system.

1) All of the current plans are only compatible with the single-owner model. Therefore, it takes a lot of time for a single owner to upload all the data to a cloud server.

2) All of the existing cloud servers offer conventional search capabilities using the plain text format, however they lack any ENRYPTED search capabilities.

3) Present-day cloud servers are virtually entirely managed centrally, allowing cloud service providers to watch and keep an eye on all access.

4. PROPOSED SYSTEM AND ITS ADVANTAGES

The proposed hybrid cloud environment aims to provide data protection for enterprises. The hybrid cloud environment combines public and private clouds. Here, we attempt to encrypt the data using AES (Advanced Encryption Standards), and cloud storage will then guarantee data security. Additionally, people making file requests require a Trusted Authority decryption key (TA). As a result, the performance of the suggested architecture using metrics like computational time, security strength, encryption time, and decryption time can only be evaluated for those who obtain keys from TA.

ADVANTAGES OF THE PROPOSED SYSTEM

1) By utilising AES to encrypt the data, we attempt to provide high security for the data in the suggested system.
2) There is an advanced degree of security since we utilise TA to give or deny user access for user permission.
3) With this suggested technique, we attempt to split the cloud into public and private storage zones, which are utilised to store and access the file, respectively.

4) We attempt to create the application in a real-time cloud environment.

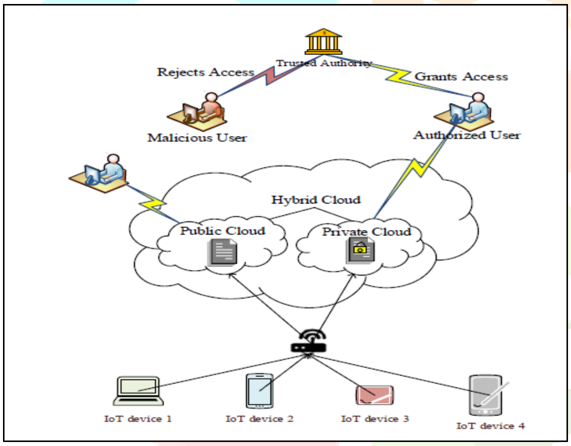


Figure 2.Represents the Proposed Architecture

5. IMPLEMENTATION PHASE

Implementation is the stage where the theoretical design is converted into programmatically manner. In this stage we will divide the application into a number of modules and then coded for deployment. The front end of the application takes Php, HTML and as a Back-End Data base we took My SQL data base. The application is divided mainly into following 4 modules. They are as follows:

1) Data Provider
2) Storage Server /Cloud Server
3) Trust Manager
4) Data User

1) Data Provider Module

The data provider is one who try to register into the application and once he gets registered he can able to login into his account and he can do following operations like :

A. He can able to upload the sensitive documents
B. He can encrypt the data by using secret key
C. He can request key from Trust Manager
D. View Key request from Data user
E. Allow or Deny key request of data user
F. See history of data users

2) Cloud Server Module

Here, the storage server is nothing other than a cloud, where it will attempt to safely store all the sensitive data. The storage server includes the following features:

A. View Files on the Storage Server
B. View the consumer Browse Owners
C. Look at Secret Keys
D. View Assailants
E. Remove Rejected Users
F. The transactions page
G. View Results using a Chart

3) Trust Manager Module

The Trust Manager in this instance is a third-party auditor used to provide keys and rights to end users and data owners. Additionally, this will have the ability to prevent unauthorised individuals from accessing cloud data. Once logged into its account, this Trust Manager can do the following operations:

A. Produce a secret key
B. View the requests made by end users
C. View Assailants

4) Data User Module

The data user is one who can able to register into the application with all his basic details and once he/she gets registered he will be able to do following operations:

A. Request Secret Key from Service Provider

B. View Secret Key that is generated by Trust Manager

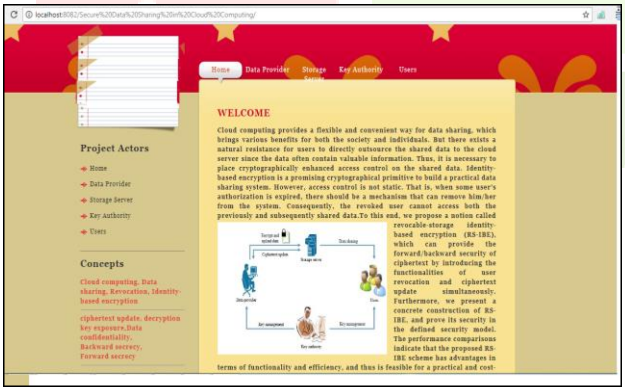
C. Download the Data in a plain text manner

D. Verify whether as genuine user or Attacker

6. EXPERIMENTAL RESULTS

In this section we try to design our current model using JSP as programming language and taking MY-SQL as storage database. Here the front end of the application is designed using JSP and HTML and back end we used My-SQL server.Now we can check the performance of our proposed application as follows:

Home Page



localhost:8082/Secure%20Data%20Sharing%20in%20Cloud%20Computing/

Project Actors

- Home
- Data Provider
- Storage Server
- Key Authority
- Users

Concepts

Cloud computing, Data sharing, Revocation, Identity-based encryption

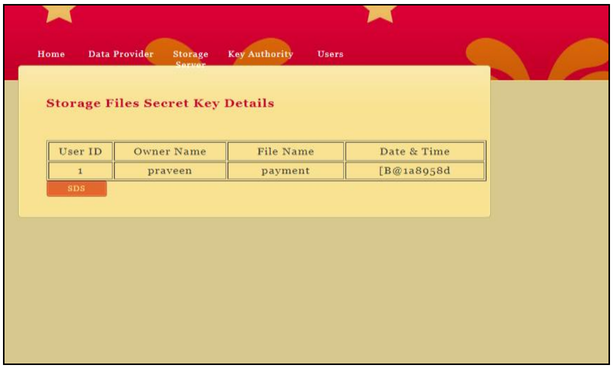
ciphertext update, decryption key exposure,Data confidentiality, Backward secrecy, Forward secrecy

WELCOME

Cloud computing provides a flexible and convenient way for data sharing, which brings various benefits for both the society and individuals. But there exists a natural resistance for users to directly outsource the shared data to the cloud server since the data often contain valuable information. Thus, it is necessary to place cryptographically enhanced access control on the shared data. Identity-based encryption is a promising cryptographical primitive to build a practical data sharing system. However, access control is not static. That is, when some user's authorization is expired, there should be a mechanism that can remove him/her from the system. Consequently, the revoked user cannot access both the previously and subsequently shared data.To this end, we propose a notion called revocable-storage identity-based encryption (RS-IBE), which can provide 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 in the defined security model. The performance comparisons indicate that the proposed RS-IBE scheme has advantages in terms of functionality and efficiency, and thus is feasible for a practical and cost-

The home page mainly contains the following links like Data provider, Storage server, Key Authority and the End users. All are connected within the same main page.

Storage Server Secret Key Details

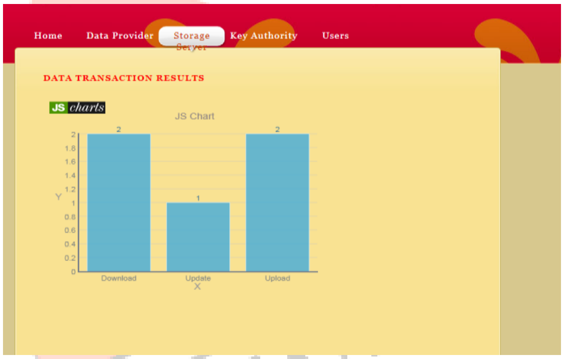


Storage Files Secret Key Details

User ID	Owner Name	File Name	Date & Time
1	praveen	payment	[B@1a8958d

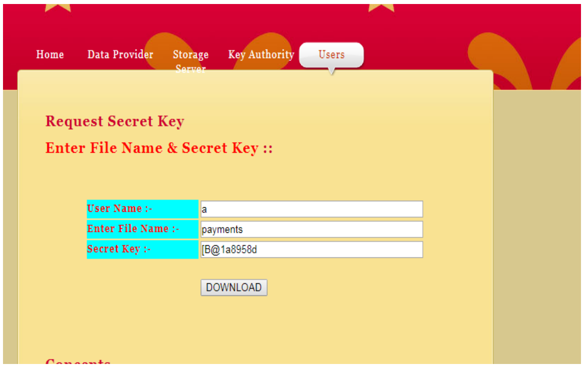
From the above window the Storage server can see the secret key details of the uploaded file.

Storage Server Can View The Results Window



From the above window we can clearly see the data transactions details in graphical manner.

User Download the File



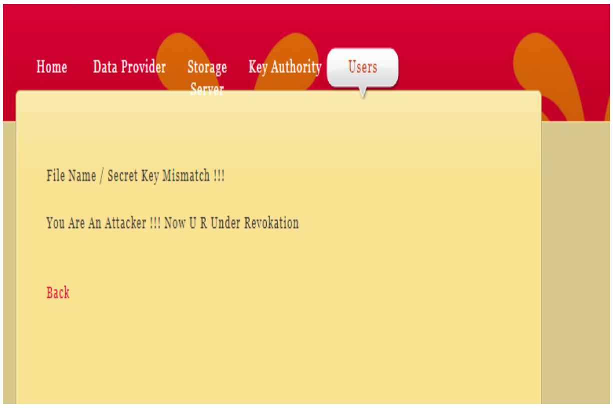
Request Secret Key

Enter File Name & Secret Key ::

User Name :-	a
Enter File Name :-	payments
Secret Key :-	[B@1a8958d

From the above window the user can see download the file by substituting all the details correctly.

User Download Failed



File Name / Secret Key Mismatch !!!

You Are An Attacker !!! Now U R Under Revokation

From the above window the user can identify that download failed and he/she is revoked because of wrong identity submission.

7. CONCLUSION

In this study, we integrate a trusted authority to provide keys to data users who want to access any file, creating for the first time a revolutionary hybrid cloud environment. Here, we attempt to encrypt the data using the AES algorithm, and the cloud will then guarantee data security. Additionally, those making file requests require a Trusted Authority decryption key (TA). As a result, the performance of the suggested architecture using metrics like computational time, security strength, encryption time, and decryption time can only be evaluated for those who obtain keys from TA.

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, “Privacypreserving 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.

About the Authors

SANDHYA GANDI is currently working as an Assistant Professor in Department of Computer Science and Engineering at Sanketika Vidhya Parishad Engineering College, P.M. Palem, Visakhapatnam, Andhra Pradesh. She has more than 10 years of teaching experience. Her research interest includes Java, Python, .Net, HTML.

CHALAPAKA SRILEKHA is currently pursuing her 2 years MCA in Department of Computer Science and Applications at Sanketika Vidhya Parishad Engineering College, P.M. Palem, Visakhapatnam, Andhra Pradesh.Her area of interest includes C, C++, Java and Python.