e-ISSN: 2582-5208
International Research Journal of Modernization in Engineering Technology and Science
(Peer-Reviewed, Open Access, Fully Refereed International Journal)
Volume:04/Issue:07/July-2022 Impact Factor- 6.752 www.irjmets.com

BLOCK CHAIN BASED SECURE DATA STORAGE ON CLOUD

Kranti Warke*1, Devika Mahindre*2, Vishakha Patil*3, Vaibhavi Shinde*4, Shrutika Hapse*5, Prof. V.A. Shevade*6

*1,2,3,4,5Students, B.Tech Computer Science And Engineering SETI, Kolhapur, Maharashtra, India.

*6Assistant Professor, Dept. Of Computer Science And Engineering, Sanjeevan Engineering And Technology Institute, Kolhapur, Maharashtra, India.

ABSTRACT

In this paper, we present a security that provide to the confidential data. cloud storage is used for the storing an important data. Cloud storage has many benefits over traditional physical storage method, including more accessible data storage. Using cloud, you can easily share file and collaborate with others. A blockchain is a type of digital database that is used to store a huge amount of information. Blockchain is one of the safe growing information technologies that help in providing security to the data. Blockchain is the technology that helps the data from hacking. Once the data gets initialized by the user, it cannot be exchanged or modified, it provides more and more security to user data. Data privacy is unharmed because the user data cannot be shared with authorized and unauthorized users in the network except the current use. On the other hand, encryption and decryption techniques will also be used along with the blockchain techniques Encryption is a process which transforms the original information into an unrecognizable form. In this project, an implementation of the AES encryption and decryption algorithm is used. This will provide security to the confidential data. For more security purpose we have used blockchain technique with distributed system. This data will be securely stored on cloud.

Keywords: Cloud, Blockchain, Encryption, Decryption.

I. INTRODUCTION

Cloud computing is the recent arising technology of IT industry to solve the problems and difficulties of business database services such as storage capacity, performance, stability, security, load and many other issues. Cloud storage was used to provide the cloud-based data storage platform. The computing tasks are distributed to a large number of computer systems, so that all applications can access the calculation capability, storage space and software services. Definition of Cloud computing changes from professionals to professionals and from individual to individual. Everyone has their own way of defining cloud computing. e primary goal of cloud computing is to offer the organisation services that are both affordable and effective. Infrastructural and data management costs are decreased as a result. vast services are offered by cloud providers. How to secure, safeguard, and process data is the core objective of cloud computing. AES Algorithm is of the out sourced data in cloud environment the "effective automatic data reading protocol" and multi-server data compression algorithm. AES is an algorithm for performing encryption which is a series of well-defined steps that can be followed as a procedure. The original information is known as plaintext, and the encrypted form as cipher text. Plain text converted into the cipher text, that is not in the readable format. To convert this cipher text into plain text there is reverse technique that decryption technique it will convert cipher text into the plain text means in readable format.

Blockchain plays a key part in the decentralised peer-to-peer system that is driving the rapid development of information technology in security. Blockchain technologies like the hashing algorithm, public/private key encryption, and transaction ledgers make this possible. Every piece of data is kept in a different decentralised place. If hackers attempt to access it, they first obtain encrypted data and then only a portion of the file, not the entire thing. This protects documents stored in cloud storage powered by blockchain. Blockchain is having a good effect and making it easier, faster, and more reliable to use storage, transactions, and business operations. The way forward is to combine blockchain and cloud to benefit from increased security and decentralisation, which improves authorisation, privacy, and efficiency.

II. LITERATURE SURVEY

Cloud Computing-based Data Storage and Disaster Recovery

Author - Zhang Jian-hua and Zhang Nan. This survey paper focuses on issues related to storing and sharing huge amounts of data on the cloud over the internet by using Cloud Storage technique.

Enhanced Data Storage Security in Cloud Environment using Encryption, Compression and Splitting technique

Author - Kajal Rani1, Raj Kumar Sagar 2.

The challenges and issues related to cloud storage security were covered in was essay. By putting this proposed work into practise, we may strengthen the security of cloud storage using techniques like encryption, decryption, compression, and sharing.

Data Integrity and Security in Cloud Environment Using AES Algorithm

Author - Mr. B.Thiyagarajan, Mr. Kamalakannan.R

This paper method is quite helpful since it allows the user to keep the unauthorised individual at a distance. They gave Cloud end users file-level security by utilising the AES algorithm.

An Efficient Secure Distributed Cloud Storage for Append-only Data

Author - Binanda Sengupta, Nishant Nikam, Sushmita Ru,Srinivasan Narayanamurthy, Siddhartha Nandi

In this paper, servers can update parity blocks themselves and the client not need to download any data blocks to update the tags of the modified blocks that are present on the servers.

Blockchain-based Security Architecture for Distributed Cloud Storage

Author- Jiaxing Li, Zhusong Liu, Long Chen, Pinghua Chen,JigangWU

In this work, a distributed cloud storage security architecture based on blockchain technology is suggested. In terms of network performance and security, the suggested design has been compared to two existing conventional architectures with tolerable network transmission delay.

Redundancy Prevention and Secure Audit of Encrypted Big Data in HDFS Cloud using Cloud Guard+ System

Author – Vinit Atul Shevade, D.A. Kulkarni

From above paper we gathered information about preventing duplications of data and integrity of cloud data.

III. PROBLEM STATEMENT

Now a days blockchain is one of the most leading technologies. We aim to build a system which will overcome the problem of data security using technique of encryption decryption and block chain in cloud. There are various security concerns nowadays, including challenges with access control, scalability, virtualization, privacy, and enormous amounts of data processing. For data and applications in the cloud, traditional security techniques are no longer appropriate. Applications and data stored in the cloud have no fixed restrictions because cloud computing is scalable and location independent. When exchanging and storing data on centralised servers, difficulties with data manipulation and authentication frequently arise. By avoiding malicious users, blockchain offers a platform for data and cloud storage, boosting security.

IV. PROPOSED WORK

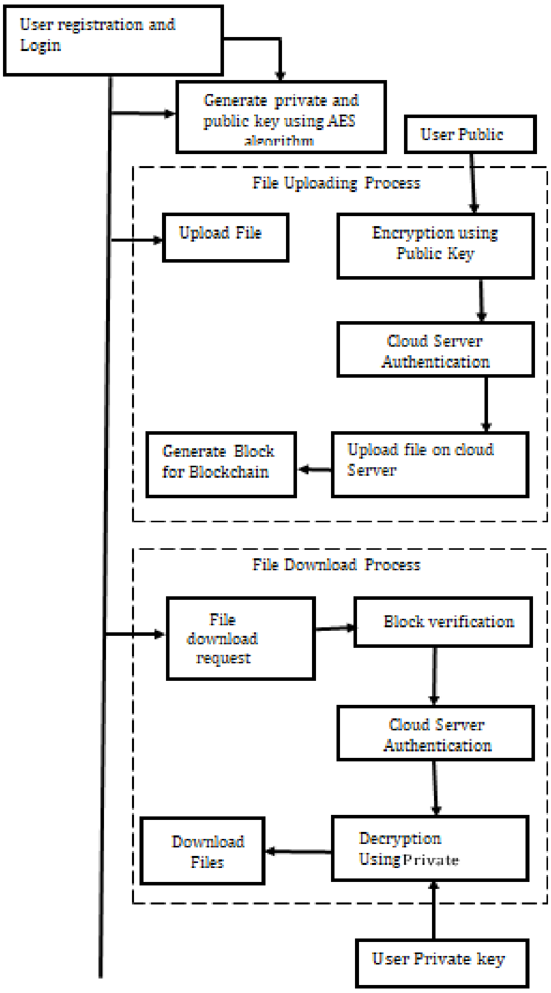
There are various security concerns nowadays, including challenges with access control, scalability, virtualization, privacy, and enormous amounts of data processing. For data and applications in the cloud, traditional security techniques are no longer appropriate. Applications and data stored in the cloud have no fixed restrictions because cloud computing is scalable and location independent. When exchanging and storing data on centralised servers, difficulties with data manipulation and authentication frequently arise. By avoiding malicious users, blockchain offers a platform for data and cloud storage, boosting security.

In this project once user is logged in by using user details like login Id and password, the home page of project is shown that has two buttons one for uploading a new file and another one for retrieving the uploaded file. When user wants to upload the data, that time AES algorithm is used for encryption purpose, after that file will be uploaded on cloud. If user wants to retrieve the data, first decryption happens then user will get the data.

Also, there is search box and view button available, with help of that user can access documents from other users and also send the request to other user by using user request option.

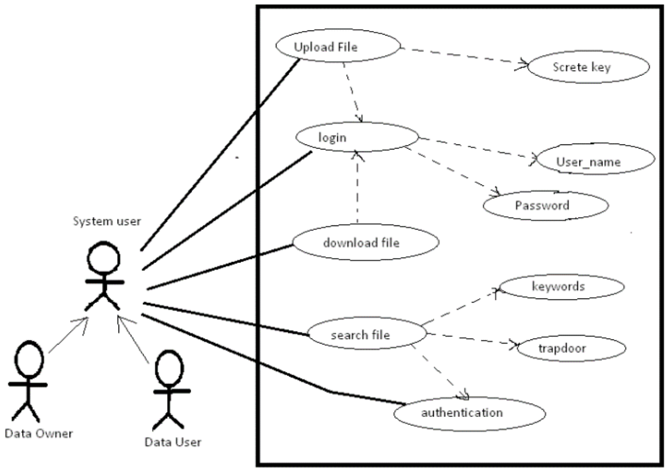
V. SYSTEM ARCHITECTURE

A. System design


User registration and Login
Generate private and public key using AES algorithm
User Public
File Uploading Process
Upload File
Encryption using Public Key
Cloud Server Authentication
Generate Block for Blockchain
Upload file on cloud Server
File Download Process
File download request
Block verification
Cloud Server Authentication
Download Files
Decryption Using Private
User Private key

In the following proposed system by using AES algorithm encryption decryption techniques is done, and with help of blockchain technology the file will be more securely store on the cloud Encryption and Decryption techniques helps to store important data securely and the blockchain will store the data in decentralized network, hance more security will provide for confidential data.

B. UML Diagram



VI. SYSTEM REQUIREMENTS

A. Blockchain

Blockchain is a system for storing data in a way that makes system changes, hacking, and cheating difficult or impossible. A permanent, open, transparent ledger system for collecting sales data, monitoring digital use, and paying content creators can be made using blockchain technology.

B. Cloud Computing

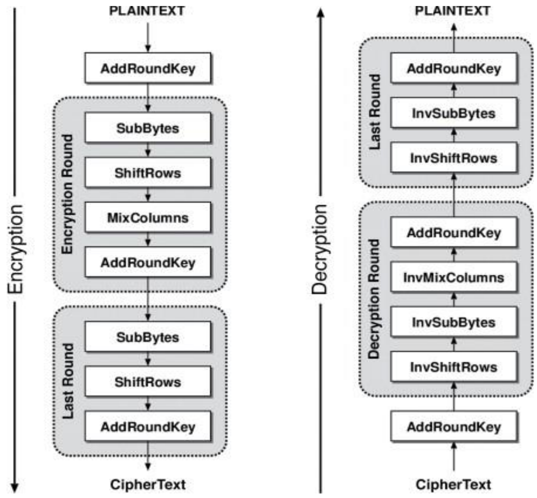
Delivering various services over the Internet is known as cloud computing. These tools and programmes comprise software, servers, databases, networking, and data storage, among other things. Google Cloud is one such instance.

C. Jelastis cloud

It is a provider of cloud platform software that offers Multi cloud Platform as a Service based on container technology to developers, telecommunications firms, and hosting service providers, among others.

D. AES Algorithm

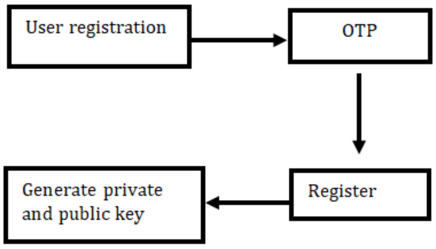
Standard for Advanced Encryption It is a block cypher technique that uses keys of 128, 192, and 256 bits to transform plain text stored in blocks of 128 bits into ciphertext. The AES algorithm is the accepted global standard because it is thought to be secure.



VII. MODULES

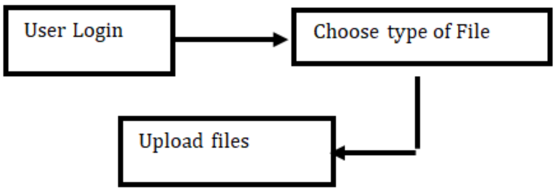
A. Registration and Login

- First user registration done, then user login their account
- generate private and public key.



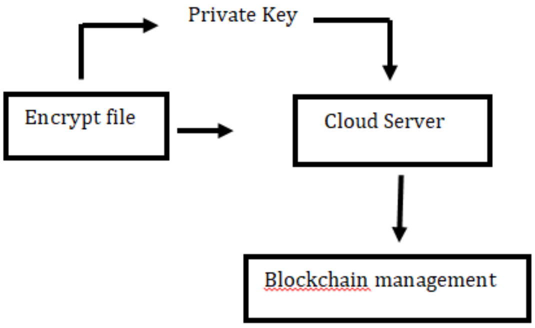
B. File Uploading

- User uploads files or data.



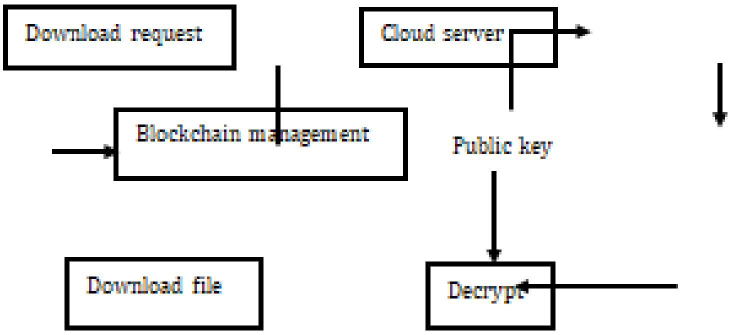
C. File Encryption

- Encryption Using Private key.
- Cloud Server Authentication.
- Upload File on Cloud Server.
- Generate Block for Blockchain management.



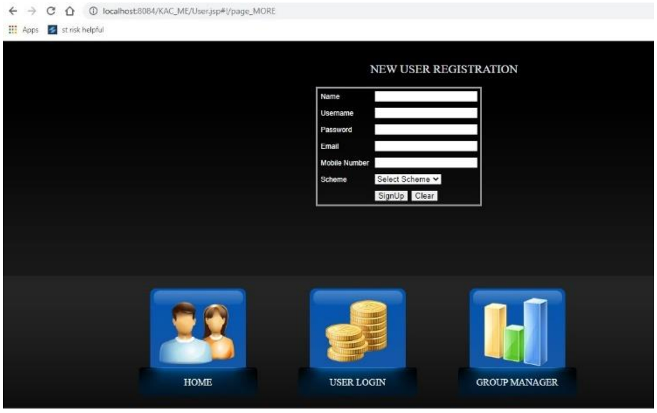
D. File Decryption

- Verification throw Blockchain management
- Cloud Server Authentication
- Decryption Using Public key
- Download File



VIII. PROJECT RESULTS

A. Registration and Login module



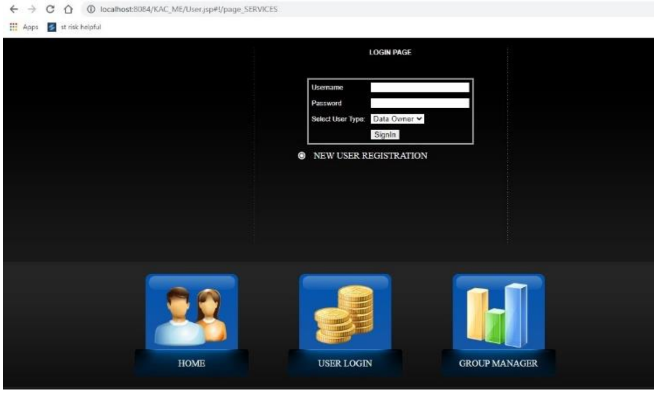
NEW USER REGISTRATION

Name
Username
Password
Email
Mobile Number
Scheme Select Scheme
SignUp Clear

First step is to register a new user account and fill this above form for registration in detail and then click on the sign-up button.

B. User Login

Second step is to login user account, on login page fill username and password, then user need to select the user type. There are two user types, first one is Data Owner means owner of data and second one is Data User means user of the data.



localhost:8084/KAC_ME/User.jsp#!/page_SERVICES

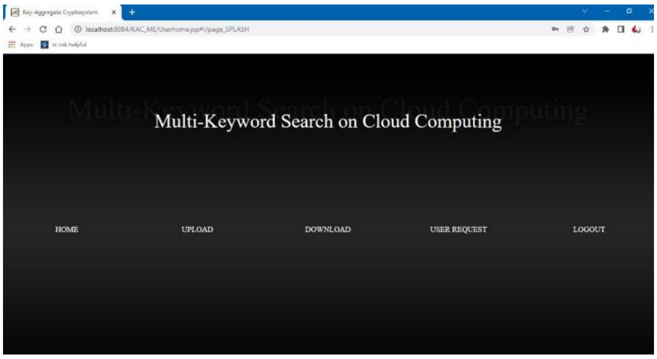
LOGIN PAGE

Username

Password

Select User Type: Data Owner

After user login this above page will open on this page there are 5 options
HOME, UPLOAD, DOWNLOAD, USER REQUEST, LOGOUT.

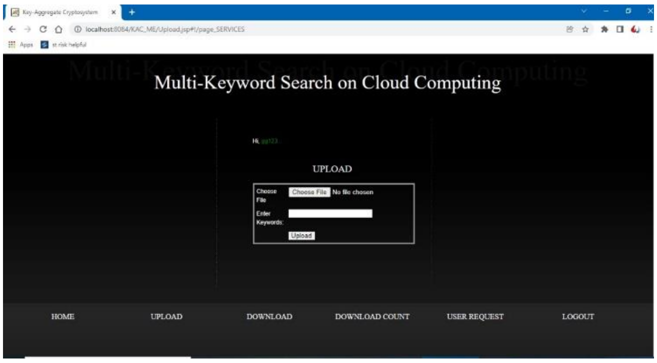


localhost:8084/KAC_ME/Userhome.jsp#!/page_SPLASH

Multi-Keyword Search on Cloud Computing

C. File Uploading

Next step is file uploading process, click on UPLOAD button then above page will open. To upload the file user, need to select the file from folders. As you can see there is one option that is Enter Keywords means you can enter any word that is related to your file .This Keyword option gives you benefit to search files by their short keyword.



localhost:8084/KAC_ME/Upload.jsp#!/page_SERVICES

Multi-Keyword Search on Cloud Computing

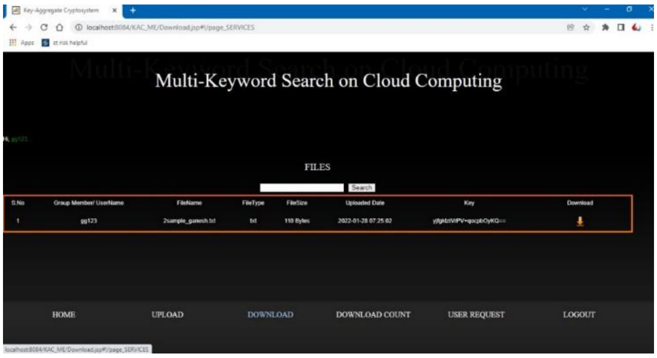
UPLOAD

Choose File: No file chosen

Enter Keywords:

D. File Downloading

In the file downloading process you need to click on the DOWNLOAD option. Then you will see all your file list. Only you have to search your file in the search box. after the search you can see this file with details like username, file name, file type, file size, uploaded date, key and download option just click on download option and use this secret key then download your file in readable format.



Multi-Keyword Search on Cloud Computing

FILES

S.No	Group Member/ UserName	FileName	FileType	FileSize	Uploaded Date	Key	Download
1	gg123	2sample_ganesh.txt	txt	110 Bytes	2022-01-28 07:25:02	yjfgkbIVrPV+qocpbOyKQ==	⬇

IX. ADVANTAGES OVER EXISTING SYSTEM

- **Cloud Storage Technique -** Storing huge amount of data in an organization. Cloud storage is a cloud computing model in which data is stored on the Internet by a cloud computing provider who manages and operates data storage as a service. It is delivered on demand with just-in-time capacity and costs, and it eliminates the need for you to purchase and manage your own data storage infrastructure.
- **Encryption technique -** Encryption is the process of converting a sender's original message into an unrecognisable form that no one on the network can read or understand. It transforms a normal message (plain text) into a meaningless or useless message (ciphertext). The unrecognisable form of the message is completely different from the original message. As a result, attackers and many external agents are unable to read the data because senders use an encryption algorithm. It occurs at the sender's end. Using the secret key or public key, the message can be easily encrypted.
- **Decryption technique -** Decryption is the process of converting encrypted code or data back to a form that a human or machine can understand and read. This is referred to as decoding encrypted data. It occurs at the receiving end. The message can be decrypted using either the secret or private key.
- **AES Algorithm -** AES is an iterative cypher, as opposed to a Feistel cypher. It is built on the 'substitution–permutation network.' It is made up of a series of linked operations, some of which involve replacing inputs with specific outputs (substitutions) and others which involve moving bits around. Surprisingly, AES bases all of its computations on bytes rather than bits. As a result, AES treats a plaintext block's 128 bits as 16 bytes. These 16 bytes are organised into four columns and four rows for matrix processing.
- **Blockchain technique -** Blockchain is a method of storing data that makes it difficult or impossible to change, hack, or cheat the system. A blockchain is essentially a digital ledger of transactions that is replicated and distributed across the blockchain's entire network of computer systems.

X. CONCLUSION

Every day, a large amount of digital data is exchanged between users. Some data is sensitive and must be protected from third-party access. The AES algorithm is critical in protecting original data from unauthorized access. When compared to other algorithms, the AES algorithm provides greater security.

This study examined how blockchain technology can secure cloud-based data. When examining data, the difficult tasks of security, storage, sharing, and authentication are what we looked into in terms of how blockchain overcomes.

When trust without the involvement of a centralised authority is sought, blockchain technology is used in many different industries.

The needs of shared storage, and particularly many terminal expansions on storage, were the focus of business diversification. Cloud storage seems to be a suitable option for companies with limited resources.

XI. REFERENCES

[1] Vinit Atul Shevade, D.A. Kulkarni: Redundancy Prevention and Secure Audit of Encrypted Big Data in HDFS Cloud using Cloud Guard+ System. https://www.sciencepubco.com/

[2] Cloud Computing-based Data Storage and Disaster Recovery Zhang Jian-hua and Zhang Nan School of Computer Science and Technology South-west University for Nationalities Chengdu, China.

[3] Enhanced Data Storage Security in Cloud Environment using Encryption, Compression and Splitting technique Kajal Rani1 , Raj Kumar Sagar2 Dept. of CSE Amity University Noida Uttar Pradesh.

[4] Enhanced RSA Algorithm with Varying Key Sizes for Data Security in cloud

[5] Avmalarethinam, I. George; Leena, H.M. (2017). [IEEE 2017 World Congress on Computing and Communication Technologies (WCCCT) - Tiruchirappalli, Tamil Nadu, India (2017.2.2-2017.2.4)] 2017 World Congress on Computing and Communication Technologies (WCCCT), 172–175. doi:10.1109/WCCCT.2016.50 .

[6] Securing Cloud Based Data Storage using Blockchain Aishwarya Patil Dept.of Computer Engineering, PCCOE Pune, India Swapnajit Patil Dept. of Computer Engineering, PCCOE Pune, India Sachin Rokade Dept. of Computer Engineering, PCCOE Pune, India

[7] Vijay Sharma Dept. of Computer Engineering, PCCOE Pune, India Prof. G. B. Sambare Dept. of Computer Engineering, PCCOE Pune, India.

[8] Blockchain-based Secure Big Data Storage on Cloud International Journal of Recen Technology and Engineering 9(4):37-45 DOI:10.35940/ijrte.D4744.119420

[9] Ruiguo Yu et al Text Encryption Protocol is used to prevent from malicious user while mining seed. RSA algorithm was also used prevent the data from the unauthorized users.

[10] Iqbal, Waseem; Khan, Suba's; Rauf, Bilal; Rashid, Imran (2018). [IEEE 2018 IEEE 27

[11] International Conference on Enabling Technologies: Infrastructure for Collaborative Enterprises (WETICE) - Paris, France (2018.6.27-2018.6.29)] 2018 IEEE 27th International Conference on Enabling Technologies: Infrastructure for Collaborative Enter prises (WETICE) - Decentralized Authentication for Secure Cloud Data Sharin,(), 95–99. doi:10.1109/WETICE.2018.00025

[12] Cloud Harmony, "Service Status," http://cloudharmony.com/ status-of-storage-group-by-regions, 2019

[13] Cloud Security Alliance, "Top Threats," http://cloudsecurityalliance.org/ group/top-threats/, 2016

[14] M. A. C. Dekar, "Critical Cloud Computing: A CIIP perspective on cloud computing service (v1.0)," European Network and Information security Agency (ENISA), Tech. Rep., 2012.

[15] Guiyi Wie, Jun Shao, Yang Xaing, Pingping Zhu, Rongxing Lu, "Obtain Confidential or/and authenticity in Big Data by ID-based Generalized Signcryption," Elsevier Journal on information Sciences, 2014.

[16] Zhiyuan Tan, Upasana T. Nagar, Xiangjian He, Priyadarsi Nanda, Ren Ping Liu, Song Wang, and Jiankun Hu, "Enhancing Big Data Security with Collaborative Intrusion Detection," IEEE Cloud Computing, 2014.

[17] Ali Dorri, Salil S. Kanhere, Raja jurdak and Praveen Gauravaram (2019), 'LSB: A Lightweight Scalable Blockchain for IoT security and anonymity,' Journal of Parallel and Distributed Computing, Vol. 134, pp. 180-197.

[18] Ana Reyna, Cristian Martin, Jaime Chen, Enrique Soler, and Manuel Diaz (2018), 'On blockchain and its integration with IoT challenges and opportunities,' Future Generations Computer Systems, 88, pp.173-190.

[19] Balachandra Reddy Kandukari, Ramkrishna Paturi V, DR. Atanu Rakshit, "Cloud security Issues", 2009 IEEE International Conference on Services Computing.

[20] "Cloud Computing Benefits, risks, recommendation for Information security cloud computing" November 2009, http://www.ensia.europa.eu

[21] Mandeep Kaur and Manish Mahajan, "Implementing Various Encryption Algorithms to Enhance the data Security of Cloud in Cloud Computing", 2012 VSRD International Journal of Computer Science & Information Technology .

[22] A. Juels and B. S. Kaliski, "PORs: Proofs of retrievability for large files," in ACM CCS, 2007.

[23] H. Shacham and B. Waters, "Cpmpact proofs of retrievalibity," in ASIACRIPT, 2008.