International Journal of Management, IT & Engineering
Vol. 9 Issue 2,February 2019,
ISSN: 2249-0558 Impact Factor: 7.119
Journal Homepage: http://www.ijmra.us, Email: editorijmie@gmail.com
Double-Blind Peer Reviewed Refereed Open Access International Journal - Included in the International Serial Directories Indexed & Listed at: Ulrich's Periodicals Directory ©, U.S.A., Open J-Gate as well as in Cabell's Directories of Publishing Opportunities, U.S.A

# TO STUDY ABOUT THE MULTILEVEL SECURITY SYSTEM FOR BIG DATA CLOUD COMPUTING

Shakeb Khan, Research Scholar, Department of Computer Science, Himalayan Garhwal University
Dr. Harsh Kumar, Professor, Department of Computer Science, Himalayan Garhwal University, Uttarakhand

## ABSTRACT

Big data is a highly voluminous asset which requires cost-effective and innovative data processing in order to better understand, make decisions and optimize processes. Cloud computing provides the dispersed management systems with a reliable, defect-tolerant and scalable environment. Cloud computing is the method used to store, manage and process data by the network of remote servers hosted over the Internet. Cloud storage benefits can be readily accessed, scalable, resilient, and cost-effective and data reliable. As a result, every company transfers its data to the cloud and employs the cloud provider's storage services. However, threats to cloud security such as data infringements, data loss, account or traffic hijacking, unsafe APIs, denial of service, abuse of the cloud services, shared technologies and dangers and insufficient diligence harm data security. The protection of the data against illegal access, alteration or denial of services is therefore required.

**KEY WORDS: Big Data Cloud Computing, Algorithm, Cloud storage, information.**

## 1. INTRODUCTION

### 1.1 BIG DATA CLOUD COMPUTING

Large information and distributed computing are entwined. Clients can utilize large information to perform conveyed questions across different datasets and produce resultant sets without wasting any time utilizing products registering. A class of conveyed information preparing stages is given by distributed computing. Colossal information sources from the cloud and the Web are put away in an issue lenient appropriated data set and handled in a group utilizing a programming model for enormous datasets and an equal circulated calculation. Handling power is needed to do examination on gigantic datasets because of the intricacy and assortment of information types. Distributed computing framework can give a successful stage to putting away the information required for large information research. Distributed computing is connected to another example for giving registering foundation and a major information preparing approach for a wide range of cloud assets through information examination.

Since managing gigantic information for simultaneous preparing has developed progressively testing, some cloud-based frameworks should adjust to this new climate. Map Reduce is a genuine illustration of large information preparing in a cloud setting; it permits the group to deal with huge volumes of information in equal. In scattered framework settings, for example, PC force, stockpiling, and organization associations, bunch registering performs well. Additionally, group registering can build up a favorable climate for information development. Data set Management Systems (DBMSs) are essential for the present distributed computing design and assume a basic part in guaranteeing that applications move flawlessly from inheritance business foundations to new cloud framework structures. The strain on organizations to quickly take on and utilize new advances, for example, distributed computing, to meet the issue of enormous information stockpiling and handling requests accompanies startling risks and suggestions.

## 1.2 SECURITY IN BIG DATA CLOUD COMPUTING

On account of its captivating components, large information distributed computing has turned into an important and standard plan of action. Beside the quick advantages, the previous components additionally bring about evident cloud-explicit security hazards. The overall population is worried about cloud security, and customers are deferring moving their organizations to the cloud.

The progression and far and wide utilization of distributed computing has been hampered by security concerns. Understanding the security and insurance hazards in distributed computing, just as creating rich and strong arrangements, is basic to its prosperity. Regardless of the way that mists assist purchasers with staying away from startup costs, lessen working expenses, and speed up by quickly getting administrations and infrastructural assets when required, they do as such at an expense.

Most of enterprises in promoting and business utilize enormous information, yet fundamental security perspectives may not be carried out. In the event that a security break including large information happens, it will have impressively more genuine legitimate repercussions and reputational harm than it as of now does. Numerous organizations are embracing innovation to store and investigate petabytes of information about their firm, business, and buyers in this new time. Encryption, logging, and honeypot identification are altogether basic techniques for keeping immense information secure. The utilization of huge information for extortion identification is exceptionally engaging and valuable in many endeavors. The issue of perceiving and battling progressed dangers and noxious interruptions requires a major information approach.

Security challenges in distributed computing frameworks can be isolated into four classifications: organization, client validation, information, and nonexclusive issues.

**Network level:** Network level difficulties are those that arrangement with network conventions and organization security, like scattered hubs, appropriated information, and between hub correspondence.

**Authentication level:** Encryption or unscrambling strategies, confirmation techniques like managerial advantages for hubs, validation of uses and hubs, and logging are altogether issues that fall inside the client verification level.

**Data level:** Data trustworthiness and accessibility concerns, like information assurance and scattered information, are named information level difficulties.

**Generic sorts:** Traditional security instruments and the use of different advancements are instances of issues that may be delegated conventional.

## 1.3 DATA SERVICE OUTSOURCING SECURITY

In spite of the fact that distributed computing permits admittance to information, a test should be attempted to guarantee that main approved clients approach. At the point when clients work in a cloud climate, they depend on others to settle on choices about their information. Have fitting devices set up to keep cloud suppliers from taking advantage of customer information in manners that have not been settled upon. A specific method of keeping cloud suppliers from abusing buyer information in all occasions gives off an impression of being unreasonable. Therefore, accomplishing this will require a blend of mechanical and nontechnical methodologies. Customers require a significant degree of trust in their provider's specific ability and monetary sufficiency. Before reevaluating, information encryption was performed to give information security and moment battle admittance to the cloud and then some. Encoding, then again, additionally involves sending standard information usage administrations, for example, plaintext expression look over printed information or data set inquiries.

Due to the gigantic bandwidth cost, the inconsequential choice of downloading the entirety of the information and unscrambling it locally is silly. This issue of the best strategy for taking a gander at encoded information has as of late stood out enough to be noticed, provoking the improvement of open encryption arrangements. In a strange express, an open encryption plot utilizes a prebuilt mixed seek after record that permits clients with proper tokens to look for encoded information utilizing watchwords without first unscrambling it. In any case, given the huge number of on-request information buyers and the huge measure of re-appropriated information in the cloud, this issue stays hard to address since fulfilling execution, structure usability, and flexibility prerequisites is amazingly troublesome. One more significant thought while re-appropriating information administrations to the cloud is ensuring information uprightness and long haul stockpiling precision. In spite of the way that re-appropriating information to the cloud is financially savvy for long haul, enormous scope stockpiling, it doesn't guarantee information honesty and availability right away. This issue can possibly obstruct the arrangement of cloud engineering.

Since customers could never hold their information locally again, they will not be able to check its exactness utilizing common cryptographic natives. For uprightness confirmation, such natives every now and again require a neighborhood copy of the information, which is preposterous when capacity is reevaluated. Moreover, the tremendous measure of cloud information and clients' restricted computational abilities make information quality confirmation in a cloud setting exorbitant and possibly restrictive. Accordingly, for this rising cloud economy to take off, engaging coupled together stockpiling assessing engineering is required. Clients will request strategies for reviewing hazards and acquiring trust in the cloud. From the point of view of structure ease of use, such a methodology should result in incredibly low inspecting overhead as far as register and bandwidth, coordinate cloud information dynamic components, and ensure clients' security when a predefined outcast commentator is available.

## 2 RESEARCH METHODOLOGIES

### 2.1 CLOUD SERVICE USER SECURITY TOOL

This programme offers a range of security functionalities and functions beginning with secure user communication. Oracle database 12c encrypts data. Any cryptosystem can be utilized in this case. However, our approach uses the AES crypto scheme. JAVA, JSP and ECLIPSE is used to implement this utility.

### 2.2 MULTILEVEL SECURITY FRAMEWORK AND CLOUD SECURITY PROTOCOL

A cloud security architecture for Domain and Cloud Service Provider Security was proposed (Ning Liu,2013). There are a number of Cloud Service Users for the same trusted group in a domain. The suggested cloud security protocol should be used to evaluate and maintain confidence at the domain and at the CSP level. One of the main advantages of the approach in this work is that there is very little adaptation in the existing methodology for collaborative trust assessments to the suggested security framework. The domain level additionally uses a proxy server to guarantee all its CSUs have access to the CSP cloud resources via that proxy. The Proxy Server checks the trust level of the requesters CSU with the corresponds security agent in the domain. The claim is rejected if the trust value of the CSU is below the pre-set level. This ensures that a bad individual in a domain does not remain unaffected outside the domain's confidentiality. The application is sent to the CSP by a trustworthy CSU. The CSP then checks the confidentiality level of the related domain with its relevant security agent. You can access the cloud resource only if the domain has a confidence value greater than a predefined threshold level. During this access, the CSP actively monitors the resource status. The CSP shall consult the appropriate security agents to re-evaluate the level of confidence of the domain and the CSP, if the resources are compromised.

### 2.3 DATA STORAGE PROTOCOL

The DSP is designed to give additional security in data storage by remotely confirming data and server custody. DSP enables consumers of the storage service providers to get proof. Such evidence is utilized as verification that its data is saved there. One of the advantages of this protocol is that it may be demonstrated through access to even a tiny part of the total dataset by the storage service provider. In order to ensure a data set is stored as a collection of n blocks, the data owner conducts a protocol on a server machine. The data owner preprocesses the data set and generates a piece of metadata before uploading the data to the distant storage. The metadata is kept on the side of the data owner and the data set is sent to the storage server. The data set is saved by the cloud storage provider and sent to the user in the future to react to queries from the data owner. The data owner may do data operations such as data expands or generate additional information that is stored on the side of the cloud server. Before deleting the local copy, the data owner could execute the DSP to confirm that the uploaded copy was successfully stored on servers.

## 3. RESULTS AND DISCUSSION

### 3.1 Registration for big data cloud users and cloud providers

All data suppliers and users must first register their Identity Number (ID), username, password, role type, date of birth, mobile phone number, and email address in their systems. All of this data will be saved on a big data cloud server.

### 3.2 Authentication of big data cloud users and cloud providers

The first level of security is authentication. Cloud Service Provider authenticates data sources and data users (CSP). If the data provider wishes to upload a file, he or she must first log in to the system using their username and password. CSP checks and validates the data provider's username and password against the database before accepting or rejecting the request. This is referred to as CSP data provider authentication or un-authentication.

Similarly, if a data user wishes to download a file from the Big Data Cloud Server, he or she must first log in with their username and password. CSP verifies and validates the data user's login and password, which are stored in a database, before accepting or rejecting the request. This is referred to as data user authentication or un-authentication via CSP.

### 3.3 Authorization of big data cloud users and cloud providers

The secret key to encrypt the data file is requested by authenticated data providers. The data providers will be authorized by the Cloud Service Provider (CSP) by confirming their credentials in the database. All registered users are unable to upload data files. The data files can only be uploaded by authorized data suppliers.

Authenticated data users transmit a request for the One Time Password (OTP) to download the data file and the secret key to decrypt the data file in order to download the data file. Only authorized data users will receive the OTP and secret key when CSP verifies the data users' credentials. To download the data file, the OTP will be delivered to the data users' email address or mobile number, and the secret key will be sent to decrypt the data file. The second level of security is authorization.

### 3.4 Multi-level security system architecture diagram with SDBS algorithm

Various security services such as authentication, authorization, encryption and decryption enable four-tier data protection. Data protection The Big Data Cloud data file can only be accessed by authenticated users.

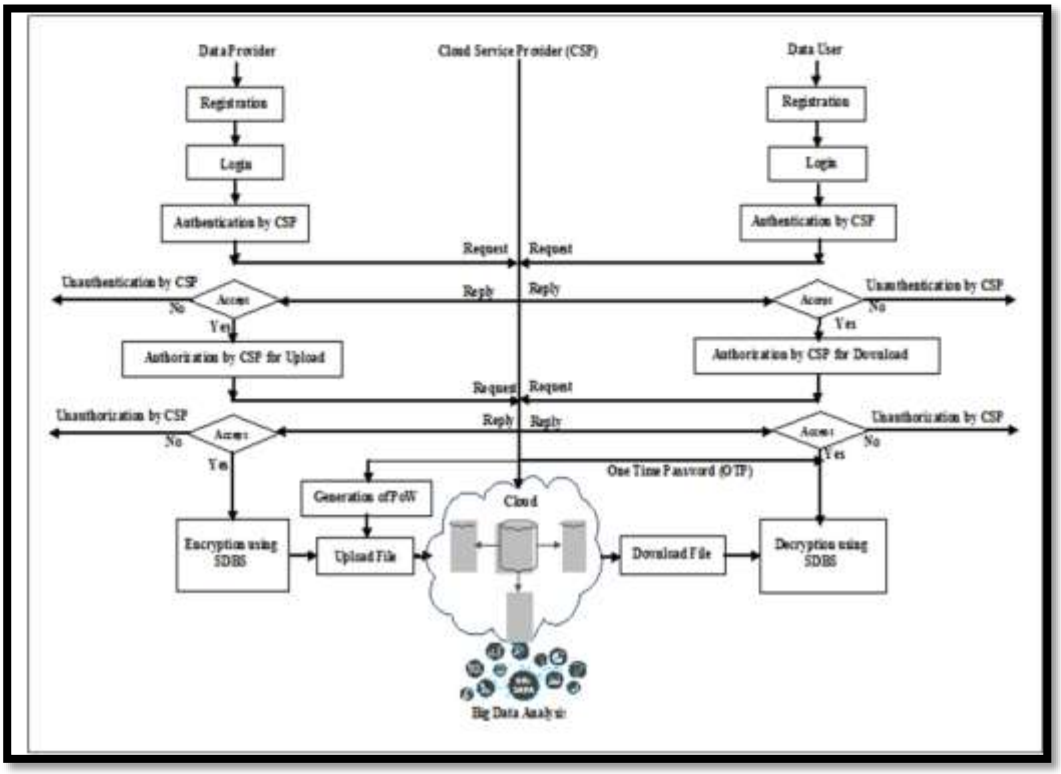

**FIGURE-1: BIG DATA CLOUD USE MULTI-LEVEL SECURITY SYSTEM SDBS**

### 3.5 BIG DATA CLOUD AND CLOUD PROVIDERS REGISTRATION

In the registration form, cloud users register their details. In the first phase the Identity Number (ID), user name, password, and kind of role, date of birth, mobile number, and e-mail ID must be registered for all data providers and data users. The Big Data Cloud server will store all this information.

### 3.6 Big data and cloud provider authentication

Cloud Service Provider (CSP) authenticates cloud users on the basis of the personal data of the cloud user. The first level of security is authentication. CSP is authorized for data suppliers and data users. The supplier must login with username and password to the system if the data provider wants to upload the database file. CSP verifies, validates and accepts the database account and password of the data supplier. This is called CSP authentication of data providers or CSP authentication of data providers.

In the same way, the users login to the system using the name and password if they wish to download the database file from the Big Data Cloud Server. The user name and password of the data user recorded in a database is verified and validated by CSP on the basis of acceptance or refusal. It is known as CSP authentication of the data user or CSP authentication otherwise.

### 3.7 Big data cloud user authorization and cloud provider authorization

By checking their credentials in the database, the Cloud Service Provider (CSP) will approve cloud users. Authenticated data providers send an application to receive the private data file encryption key. By confirming their credentials stored in the database, CSP will allow data providers.

Unable to upload the data files all registered users. Data files can only be uploaded by the authorized data suppliers.

Authenticated data users send an application to download the data file with one time password (OTP) and a secret key for decrypting the data file to download. CSP will check data users' credentials and send only authorized data users the OTP and Secret key. The OTP is provided to the data users' email ID and the secret key is forwarded to the data file to be decrypted. The second degree of safety is authorization.

### 3.8 Uploading data files encryption and downloading files decryption

The files are encrypted using the SDBS technique, and are uploaded from the permitted cloud providers to the cloud server

The data files are decrypted by means of SDBS algorithms and downloaded by the approved cloud users to the cloud server. Only legal data users can download and decode the file from the CSP through OTP.

### 3.9 RANDOM KEY GENERATOR FOR OTP (RKG)

Whenever Data User (DU) wants to download the data file, entering the data user name and password is the initial step. Using credentials the Cloud Service Provider (CSP), once the user has logged in, permits the data user. The data user will receive one time password via the Personal Email ID (OTP) or Mobile Numbers issued by CSP after receiving the permission.

The user requires two inputs to generate the transaction password. OTP is a combination of a random generator that generates the 16 or 24 or 32 alphabets, number(s) or special characters and is transmitted by its mailing id or mobile to the user of data. The encrypted data file is transferred to the data user together with the keys once OTP verification is completed.

### 3.10 OWNERSHIP EVIDENCE

Evidence of possession (PoW) is required to recognise the resource person who uploaded the file to the Big Data Cloud. The file ID, the role type, the name of the data provider, the date and the time when the file is uploaded are the details used to identify the resource creator who created and uploaded a file to the big data cloud. This displays the origin of the data file and the downloader could know who created the data file.

### 3.11 CRYPTOGRAPHIC ALGORITHM PROPOSED MERITS

The Secure Dynamic Bit Standard (SDBS) is for single to multiple encryption, where we get the same plaintexts and distinct ciphertexts, in different ways. In compared to other discussed encryption approaches, SDBS encryption is easy and secure. Even if SDBS is similar in structure to the Advanced Encryption Standard (AES), this approach is easy because the AES algorithm's complexity is removed. This makes the procedure simple and also less time-complex. SDBS is secure because any of the standards are randomly selected when the attacker is loaded and the size of the key and the processes confused. In this approach the master key is encrypted and only authorized users can get the keys. For additional protection two keys are utilized.

a) **Security:** Hybrid encryption is used for encryption. For data encryption, symmetrical key encryption is utilized and for key generation asymmetry key encryption is employed.

b) **Efficiency:** It's incredibly safe and gives an effective result because it uses both symmetric key and asymmetrical key cryptography.

c) **Data Integrity:** Since only authenticated user can uncode an encrypted data file, it is not possible to modify or delete the data file.

d) **Performance:** Data File Encryption is quick and performance is best to download and upload.

### 3.12 BIG DATA CLOUD SYSTEM FUNCTIONING

The process of downloading is as follows:

i. Registration phase: registration begins with a username, password, e-mail identification, mobile number, birth date, address, role type, etc. registration phase.

ii. Login phase: the data supplier uses username and password to login to the system.

iii. Authentication phase: CSP verifies and authenticates the data provider to get inside the system with his user name and password.

iv. Phase of authorization: The authenticated data provider sends a request for the file upload. With its credentials, CSP allows the data source to send the encryption key.

v. Phase encryption: data files are encrypted with CSP-compatible encryption via the data provider's SDBS method.

vi. Upload stage: Proof of Ownership (PoW) will be utilised to locate the resource person proof and the data provider and the encoded data file will upload to the big data cloud server.

The process of downloading is as follows:

i. **Enrollment phase:** the user begins to register by entering the username, password, e-mail identification, cell phone number, birth date, address, role type etc.

ii. **Login phase:** the data user uses his credentials such as user name and password to log into the system.

iii. **Authentication Phase:** CSP verifies the user's username and password to enter into the system.

iv. **Authorization phase:** By using his credentials, CSP authorized the data user and sent the decryption key. CSP also authorized the OTP to download the data file from the big data cloud by e-mail id or mobile number.

v. **Phase of download:** The encrypted data file is downloaded from the data user after verification of OTP.

vi. **Decryption stage:** The Data User decrypts the downloaded data file using SDBS decryption algorithms given by CSP and the decryred data file is saved to the system of data users.

Intel i7 and 8-GB Random Access Memory (RAM) workstation with Windows 7 – 64 bits Cloud Storage are implemented and tested (drop box cloud storage).

**TABLE-1: Multi-level security system role and operation for large data clouds**

| Role | Operation |
|---|---|
| Data Provider (DP) | Encrypt Data File |
| | Upload Data File |
| Data User (DU) | Download Data File |
| | Decrypt Data File |
| Cloud Service Provider (CSP) | Authenticate - Checking Username and Password |
| | Authorize – Checking credentials of the User |
| | Key Generation, OTP Generation, PoW Generation |
| | Block Unauthorized User |

The entire research was based on four schemes, firstly, the Attribute Based Encryption (ABE), then the Advanced Encryption Standard (AES) and, finally, the Secure Dynamic Bit Standard (SDBS) was implemented in a single environment, and the third hybridized the implementation of both the ABE and the AES. The functions of DP, Data User (DU) and CSP who all handle the various operations of the proposed system are explained in Table.

## 4. CONCLUSION

The data file will be encrypted or decrypted with the proposed SDBS technique while uploading or downloading. In this thesis, this innovative SDBS algorithm offers a high level of safety of the stored information. There are various advantages to the use of cloud computing worldwide. Cloud computing is a rapidly growing field of IT. Data and information are spread over the world through cloud computing. Many cloud security research is being carried out. Cloud data security in the last few days is a big necessity.

This work aims to provide more cloud security. Here, the data which will be placed in the cloud are given multiple layers of security. Here a new technique of key creation is applied. Following the key generation, several procedures include encryption, splitting; conversion and decryption of jar files have been followed. Instead of each file having independent key, the file sections are given different AES keys. Therefore, the data are more secure.

## 5. REFERENCES

- Paigude, T., Chavan, T.A.: A survey on privacy preserving public auditing for data storage security. Int. J. Comput. Trends Technol. 4(3), (2019)
- Baghel, S.V., Theng, D.P.: A survey for secure communication of cloud third party authenticator. Int. Conf. Electron. Commun. Syst. (ICECS-15) 1, 51–54 (2019)
- Wang, C., Chow, S.S.C., Wang, Q., Ren, K., Lou, W.: Privacy-preserving public auditing for secure cloud storage. IEEE Trans. Comput. I, 62(2), 362–375 (2019)
- Mohta, A., Awasti, L.K.: Cloud data security while using third party auditor. Int. J. Sci. Eng. Res. 3(6) (2019). ISSN 2229-8
- Wang, Q., Wang, C., Ren, K., Lou, W., Li, J.: Enabling public auditability and data dynamics for storage security in cloud computing. IEEE Trans. Parallel Distrib. Syst. 22(5), 847–859 (2019)
- Wang, C., Wang, Q., Ren, K., Lou, W.: Privacy-Preserving Public auditing for storage security in cloud computing. In Proceedings of the IEEE INFOCOM' 2019
- Erway, C., Küpçü, A., Papamanthou, C., Tamassia, R.: Dynamic provable data possession. In: Proceedings of the 16th ACM Conference on Computer and Communications Security, ser. CCS'09. New York, NY, USA: ACM, pp. 213–222 (2019)

- Wang, C., Wang, Q., Ren, K.: Ensuring data storage security in cloud computing. In: IEEE Conference Publication, 17th International Workshop on Quality of Service (IWQoS) (2019)
- Theng, D., Hande, K.N.: VM Management for cross-cloud computing environment. In: 2012 International Conference on Communication Systems and Network Technologies (CSNT), pp. 731, 735, 2019
- Theng, D.: Efficient heterogeneous computational strategy for cross-cloud computing environment. In: 2019 Second International Conference on Emerging Research in Computing, Information, Communication and Applications (ERCICA), pp. 8, 17, 2019
- Gourkhede, M.H., Theng, D.P.: Analysing security and privacy management for cloud computing environment. In: 2014 Fourth International Conference on Communication Systems and Network Technologies (CSNT), pp. 677, 680, 2019
- Gourkhede, M.H., Theng, D.P.: Preserving privacy and illegal content distribution for cloud environment. In: International Journal of Computing and Technology (IJCT), 2014, vol. 1, no. 1, 3, pp. 142, 148, 2019