J. Antony John Prabu, 2019, 7:5
ISSN (Online): 2348-4098
ISSN (Print): 2395-4752

International Journal of Science, Engineering and Technology
An Open Access Journal

A Novel CDL Framework for Trusted Data Transactions in Cloud Environment

J. Antony John Prabu[1], Dr. S. Britto Ramesh Kumar[2]

[1]Research Scholar and Assistant Professor, Department of Computer Science St. Joseph's College, Trichy, Tamilnadu, India- 620 002

[2]Assistant Professor, Department of Computer Science St. Joseph's College, Trichy, Tamilnadu, India- 620 002

Abstract- Cloud computing is an essential tool in the IT industry that offers a variety of services to both cloud suppliers and customers. The primary concern with cloud computing is security due to the fact that data is kept and managed inside a third-party environment. Cloud computing presents several challenges in managing transactional data inside cloud databases. It is necessary to uphold reliable assurances in order to carry out the transactional data. This study examines the architecture of a proposed cloud data locker in detail. It also depicts the requirements of significant security levels and guarantees the uniformity of data transfers. This article provides a comprehensive analysis of a suggested architecture aimed at enhancing the security and consistency of data transactions in cloud databases.

Keywords: Cloud DTM, 2-Phase Commit Protocol, Cloud Security, Consistency in cloud DBS, Cloud Controller, D1FTC and Cloud Data Locker.

I. INTRODUCTION

Cloud computing offers a comprehensive range of services and is available in many deployment options. It provides dependable service for analytical data but is not suitable for managing transactional data. The majority of cloud services are implemented inside a hybrid cloud architecture. The cloud vendors are establishing a service agreement with cloud providers in order to provide dependable services to their customers. Software and hardware providers are transitioning to a cloud environment instead of owning the software and gear. Cloud suppliers are relieved from the responsibility of managing software and hardware upkeep.

Cloud computing has technological challenges when processing data in a dispersed context [1-8]. The researchers in the field of cloud computing are creating and advancing novel methods for handling large-scale transactions in order to prevent workload inconsistencies. They are also working on concurrency controls to enhance the access of serialisation. Additionally, they are developing approaches to ensure consistency in transaction processing systems, with the aim of improving efficiency. Furthermore, they are designing a scalable data storage model to enhance data management, and explori Hence, ensuring security is a prevalent and significant issue in cloud computing.

Therefore, implementing layered security measures is essential to safeguard each service and prevent data loss. An important concern is the preservation of robust consistency state at the database level, particularly for services that handle transactional data [9-15]. Therefore, the majority of research efforts [15-24] are focused on developing robust methodologies and architectures to enhance the security of cloud services and reinforce the consistency of state in cloud distributed database systems. This study proposes a resilient security strategy for cloud transactions by using the CDL architecture. The primary contribution of this study is

- The development of an appropriate framework for managing transactional data.
- Data storage in the cloud occurs in a third-party environment and is accessible by distant clients. Cloud companies manage the database using their own infrastructure and provide it as a service.
- Cloud providers acquire and manage the infrastructure, platform, software, and database

of the cloud, offering various services to their customers.

- Consequently, ensuring security at the storage level in the cloud is a challenging task. The proposed CDL architecture has three sequential verifications in order to enhance data security.

The structure of the paper is as follows: Section 2 presents a comprehensive review of the existing literature. Section 3 provides a comprehensive explanation of the proposed work's overarching structure. Section 4 presents the outcomes and analysis of the suggested system in relation to several performance measures. The task is concluded in Section 5.

II. RELATED WORKS

"The use of remote storage systems, especially cloud-based storage services, has increased at an exponential rate due to recent technical developments. Data privacy, integrity, and confidentiality are just a few of the cloud-specific security concerns brought on by outsourcing. Consequently, data security is still the biggest problem with cloud storage and is preventing it from being widely used. The users entrust their data to third-party servers in the cloud, which are overseen and regulated by CSPs. However, it becomes exceedingly tough to offer confidential data in multi-tenant setups. One viable alternative to these methods of data secrecy is client-side encryption [7, 8].

The decryption keys are being kept by the user, away from the cloud provider. Nevertheless, this approach raises a number of important management issues, such as the need to store and ensure the availability of keys on the client side. When developing solutions to ensure the security and privacy of outsourced data, it is important to take factors such as usability, deployment simplicity, resilience, performance, and flexibility into account. Based on the first use of ID-Based Cryptography (IBC) to guarantee data secrecy, authors [9] suggested a cryptographic method for cloud storage. Under this scheme, each client computes an ID-based pair of keys that the data owner may use to control who has access to their encrypted data stored in the cloud.

The adaptable method of sharing that is made possible by using a key based on a data ID. In order to reduce computation complexity on the client side, a content hash keying method–based client side de-duplication strategy for cloud applications has been suggested [10]. To improve user-to-user dynamic sharing and data secrecy in cloud storage situations, CloudaSec [11] employs a public key based method. The data owner encrypts the data before uploading it to the cloud. They also encrypt the metadata, which helps keep the data private. To provide both forward and backward secrecy, CloudaSec uses a conference key distribution system based on simultaneous Diffie-Hellman exchanges.

Therefore, metadata and the keys to decrypt data can only be accessed by authorised users. The writers looked at several mobile cloud computing security frameworks. Because mobile devices have limited resources, most security frameworks use the cloud to offload tasks that are taxing on processors [12]. Service providers must resolve security concerns related to network security, data security, data confidentiality, data breach, and other related problems in order to achieve a mobile cloud computing environment that is safe. Lack of full isolation among instances of virtual machines operating on the same physical server also introduces additional security risks. A novel provenance system with granular access control was suggested by the authors, building on the Attribute-based signature (ABS) approach [13].

By combining ABS and group signature techniques, we can ensure that the user remains anonymous. The data owner experiences a decrease in compute and communication overhead when user access is transferred to the cloud server with broadcast encryption. In order to address security vulnerabilities such as mobile device compromise, traffic interception, and Identity Management Systems (IDM) server compromise, an architecture known as consolidated IDM (CIDM) was developed. This architecture separates the authorization credentials to prevent unauthorised access in the event of an IDM compromise or traffic interception.

To prevent mobile device compromise, it provides an extra layer of security by employing challenge-response methods that are based on humans. Based on the results of the trials, CIDM provides its customers with better security assurances while using less energy and communicating less than the present IDM systems.

The authors look at a method that uses digital signatures with qualities obtained from their construction and software activity to guarantee authenticity and provenance in cloud-based services. Keys are produced dynamically using the characteristics collected as the service execution progresses. We provide a method for generating keys in many dimensions by directly mapping from a space of multi-dimensional features to a key space. To determine the key space's entropy, an entropy algorithm is created [15].

Businesses may safeguard their customers' private information stored in the cloud with the help of the authors' suggested multi-factor biometric fingerprint authentication and protection gateway [16]. Cloud service providers and other dangerous users will not be able to access users' login credentials, ensuring data privacy and high security.

As an integral aspect of the protection gateway, the authors used data anonymization and sophisticated tokenization techniques to safeguard the confidentiality of the critical piece of information from malevolent individuals both within and outside the system. Cloud computing security necessitates a precise perspective, which may be fostered via confidence, reducing risk towards a reliable third party [17]. In this article, the authors provide a system that combines PKI, SSO, and LDAP to guarantee authentication, data availability, integrity, and secrecy in communications and data.

This method establishes a security mesh by ensuring that all involved entities have access to a horizontal level of service, which sustains crucial confidence. Incorporating client controlled encryption capabilities into the common cloud computing environment is crucial for guaranteeing data protection against the likely security holes in any given cloud system. Taking charge of the security of the data that clients might store on distant workstations is the key advantage of implementing a client controlled security approach. Data encryption technology allows for the most effective security of data, as we said before. Cloud systems have identified important channels for data to go to and from the central cloud area, necessitating the development of a dedicated encryption-decryption mechanism. In response, we built a cloud data locker algorithm that fixes this problem and all the security issues.

III. PROPOSED WORK

Cloud Data Locker (CDL) is a framework that includes components such as Communication Manager (CM), CDL Manager (CDLM), OTP Manager (OTPM), OTP Generator (OTPG), OTP Verifier (OTPV), DSN Manager (DSNM), DSN Generator (DSNG), DSN Verifier (DSNV), Security Manager (SM), Crypto Engine (CE), and Cloud DB (CDB). The features of this framework are illustrated in Figure 1. The connections between the Cloud Service Controller (CSC) and the D1FTBC server are initiated by the Communication Manager (CM). First, in order to send and receive one-time passwords (OTPs), Cloud Data Locker (CDL) verifies the user's information with OTP Manager (OTPM).

User information is validated by the OTP Generator and Verifier, which are maintained by the OTP Manager (OTPM). The second step is for the One-Time Password (OTP) to verify the service provider's data storage in order to transmit and receive the Data Security Number (DSN). Once the first two stages have been verified and executed successfully, the following step may be initiated.

The Security Manager (SM) is responsible for keeping the encrypted data stored in Cloud DB (CDB) via Crypto Engine (CE) up to date throughout this phase. After encryption, this engine stores the decrypted data in the cloud database and prepares it for execution. Cloud transaction data is accessible to the security manager (SEM) on the CDL server via the CDL crypto engine.

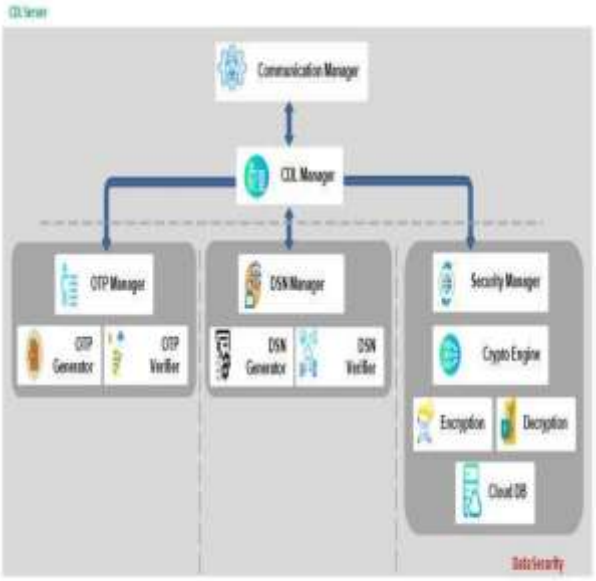

Figure. 1 Framework for CDL server

Data in the cloud is moved around in an open setting over a network. Customers want a cloud solution that can transmit data quickly and securely. The results of the comparison of several algorithms show that AES outperforms DES and RSA, among others. Because of this, the crypto engine uses AES for both encryption and decryption.

Table: 1 Comparative Analysis of RSA, DES and AES

Description	RSA	DES	AES
Developed	1977	1977	2000
Key Length	More than 1024 bits	56 bits	128,192,256 bits
Cipher Type	Asymmetric block cipher	Symmetric block cipher	Symmetric block cipher
Block size	Minimum 512 bits	64 bits	128 bits
Security	Least Secure	Not secure enough	Excellent Secured
Hardware and Software Implementation	Not Efficient	Better in hardware than software	Better in both
Encryption and Decryption	Slower	Moderate	Faster

Cloud data transaction services may see an improvement in response speed and an increase in data security. This implies that the supplier has no idea what information the clients and vendors keep. Authentication mechanisms like DSN and OTP prove this. Consequently, cloud data transactions are guaranteed to have top-level safety thanks to the three-level verification process.

Pseudocode for CDL

"Step 1 : Send OTP to user
Step1.2 : Get OTP from user
Step1.3 : Verify the user
Step2 : Send Data Security Number (DSN) to Cloud Data storage provider
Step2.1 : Data Security Manager match the DSN in Data storage provider
Step2.2 : Verify the Cloud Data storage provider
Step3: If (User & Data storage == Verified)
Step3.1 : Access the Crypto Engine and decrypt the data
Step3.2 : Send data to the transaction process
Step3.3 : Get the committed data
Step3.4 : Access the Crypto Engine and encrypt the data
Step3.5 : Update the data successfully."

Algorithm for Cloud Data Locker

When it comes to data-level security, the Cloud Data Locker has you covered. The three-stage verification approach was helpful in the efficient creation of this algorithm. It checks the user and data storage levels by calling UserVerification and DataStorageVerification, respectively. It may access the encrypted cloud data using an effective cryptographic mechanism when these two processes are successfully verified.

```
PROCEDURE CloudDataLocker
VARIABLES
ExitUserVerificationFlag IS BOOLEAN
ExitDataStorageVerificationFlag IS BOOLEAN
ExitTransactioncommitFlag IS BOOLEAN
BEGIN
    RESET ExitTransactioncommitFlag
    CALL PROCEDURE UserVerification
    CALL DataStorageVerification
IF ExitUserVerificationFlag and ExitDataStorageVerificationFlag is SET
  THEN encrypt the data in DBS and Data submitted for transaction
  SET ExitTransactioncommitFlag
```

```
    ELSE display 'Transaction not committed' message
ENDIF
IF ExitTransactioncommitFlag is SET
      THEN update encrypted data
            display 'Transaction Successfully committed' message
ELSE display 'Transaction not committed' message
ENDIF
END CloudDataLocker
PROCEDURE UserVerification
BEGIN
      RESET ExitUserVerificationFlag
      Send OTP to user device
      IF received OTP is correct
            THEN SET ExitUserVerificationFlag
      ELSE display 'out of service' message
      ENDIF
END UserVerification
PROCEDURE DataStorageVerification
BEGIN
      RESET ExitDataStorageVerificationFlag
      Send DSN to DataProvider
      IF DSN is correct
```

Figure 2 CDL algorithm

The suggested algorithms provide security at every level. The User Authentication Authorization and Accounting algorithm guarantees the authentication of users and devices, as well as the authorization and accounting for each new transaction. The Cloud Service Controller guarantees the security of service levels and monitors the state of virtual machines in the cloud. The D1FTBC protocol, along with the 3PSTBC protocol, guarantees security at the process level.

The Cloud Data Locker implements a three-stage data verification procedure in order to guarantee data-level security. The suggested D1FTBC is designed to easily attain a greater level of consistency in a cloud setting. In a cloud context, virtual computers are distributed across multiple locations, making it challenging to maintain optimal data transaction consistency. However, the proposed D1FTBC consists of many sub-components, including a Transaction Manager, Consistency Performance Metric, Transaction Tree, 3PSTBC Protocol, and Shortest Path Tree Manager (SPTM), all of which work together to achieve a better level of consistency for each transaction.

The proposed Cloud Data Locker guarantees data security by the deployment of a three-stage verification method to authenticate the user, service provider, and cloud data storage. Access to encrypted transactional data is only possible via a three-stage verification procedure. The two-phase commit mechanism is often used to guarantee the ACID characteristics. In a distributed cloud system, virtual nodes are widely dispersed and it is challenging to maintain ACID characteristics. The proposed 3PSTBC protocol guarantees ACID guarantees in a cloud context. The suggested D1FTBC uses an efficient tree-based replication technique. The third phase of the 3PSTBC protocol is designed to facilitate the replication of data across virtual machines in the cloud. The Shortest route Tree Manager (SPTM) generates an optimal shortest route tree to facilitate efficient replication and minimise execution time.

IV. PERFORMANCE ANALYSIS

This section presents the performance analysis of the proposed method. Figure 3 depicts the performance outcomes of CDL server authentication with a graph illustrating the relationship between average response times and the quantity of requests per minute.

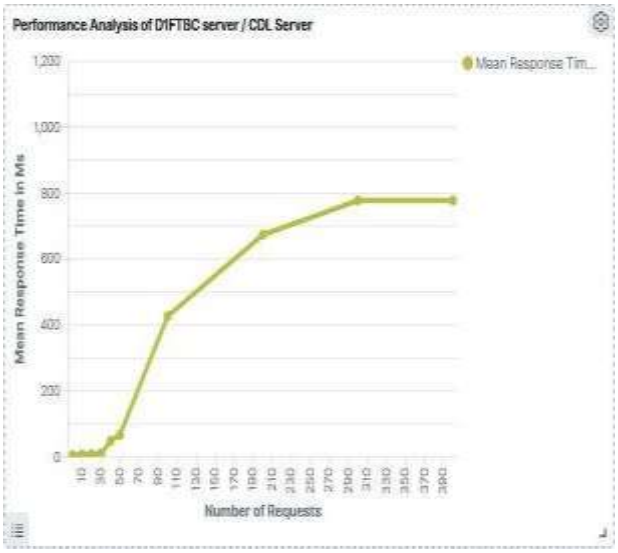

Figure. 3 Performance Analysis of D1FTBC server / CDL Server

Figure 3 displays the performance outcomes in relation to the average response time for authenticating the D1FTBC server and CDL server. Upon analysing the benchmark data from 50 to 300 service requests, it seems that the system demonstrates a linear increase in the average response time when compared to the benchmark data from 1 to 50 service requests. The rate of increase of the curve is beginning to decrease between 300 and 400 concurrent service requests. When the service requests to authenticate the D1FTBC server and CDL server are increased, there is a corresponding increase in the mean response time of these requests, reaching a balanced level.

Performance Analysis on Data level security

Figure 4 and Figure 5 provide the screenshot of the implemented OTP and DSN verification. The data illustrates the duration of execution for different components of the CDL server as the arrival rate increases.

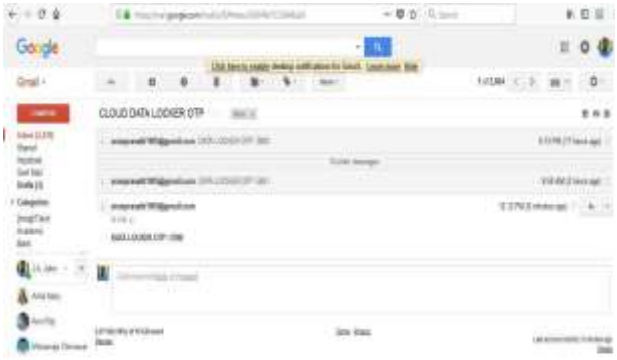

Figure. 4 Screen Shot of OTP verification

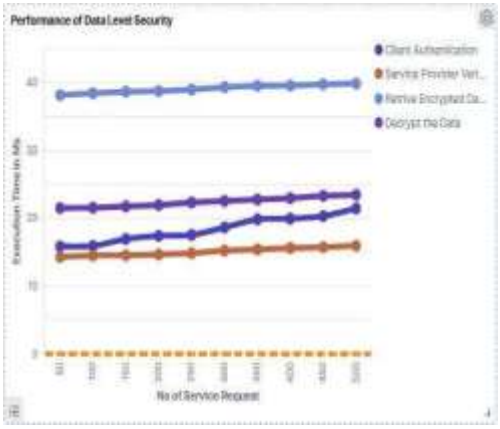

Figure. 5 Performance of Data Level Security

Figure 6 Screen Shot of DSN Verification

Figure 6 presents a performance study of the components of the proposed CDL server as the arrival rate increases. The graphic represents the relationship between the execution time and the number of service requests per minute. During the implementation of CDL, when there are a considerable number of service requests ranging from 50 to 500, the components of the proposed system seem to show a linear increase in execution time. The CDL component exhibits a superior level of responsiveness, necessitating the implementation of a three-stage verification process for data access and the adoption of a cryptographic method to manage transactional data.

The retrieval of encrypted data from the cloud database takes longer response time due to the implementation of three-stage verification procedures, which enhance security. Decrypting the cloud data using the cryptographic engine also requires a considerable amount of time, as shown in the benchmark. OTP verification is a client authentication technique that requires replies from every client before proceeding with a transaction. It exhibits superior reaction time compared to the processes of retrieving encrypted data and decrypting data. The service provider verification is an automated interaction between machines that

exhibits a shorter reaction time compared to other components in the CDL server. The figure illustrates the relationship between the execution time and the workload characteristics of each component. It demonstrates that as the system components increase, the performance of the CDL server improves in a linear manner.

Latency Analysis

The primary goal of this work is to determine the latency of various points (events) in the proposed design. Latency refers to the time delay between the start and end points of an event, which is quantified in terms of execution time.

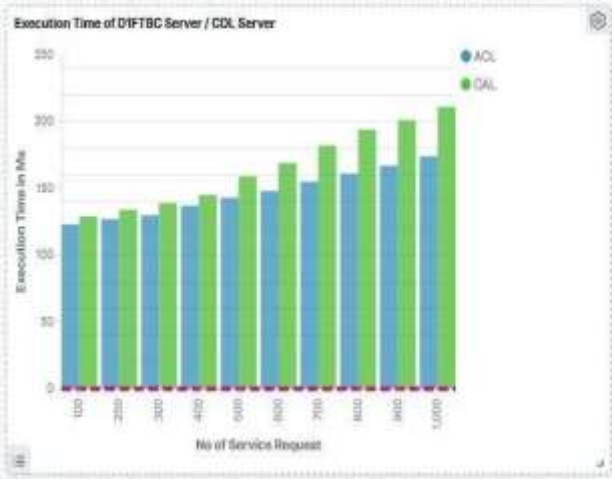

Figure.7 Latency for increasing service requests

Figure 7 displays the duration of the latency analysis, with the plot representing the relationship between execution time and the number of service requests. The graph precisely depicts the disparity in execution time for the given position.

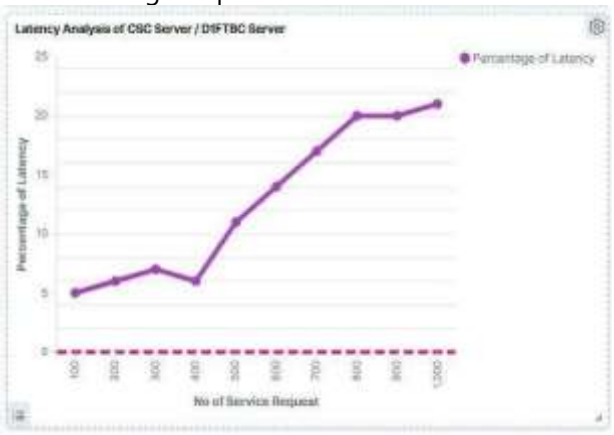

Figure 8 Latency Analysis of CSC Server / D1FTBC Server

Figure 8 depicts the graphical depiction of the percentage increase in delay. Based on the graph observations, it is apparent that the Latency Increment Percentage (LIP) grows as the service request increases. Nevertheless, the LIP (Limited Information Pool) approaches a saturation point of 21% when the number of service requesters surpasses 1000".

V. CONCLUSION

This article discusses many challenges in cloud computing, including security concerns, service availability, and authentication mechanisms. The focal point of the study is the implementation of the Cloud Data Locker Algorithm (CDL). This method is used to securely store sensitive data in the cloud. At this stage, we verify the legitimacy of a user who gains access to the cloud storage by using the key that is held on the Cloud Service Provider. The key is used to secure the given storage space for a user in any data centre. The user may retrieve or get their info at any moment by using the key. Efficient data retrieval may be achieved by implementing an index table inside the Cloud Service Provider. It allows for a situation where sensitive information may be securely stored and accessed from the cloud using effective security measures such as data encryption.

REFERENCES

1. G. Boss, P. Malladi, D. Quan, L. Legregni,H. Hall. Cloud Computing, 2007. www.ibm.com/ developerworks/ websphere/zones/hipods/
2. National Bureau Of Standards NIST. Data encryption standard (des). Technology,46-3(46):1-26, 1999.
3. N FIPS. 197: Announcing the advanced encryption standard (aes) Technology Laboratory, National Institute of Standards, 2009(12):8-12, 2001.
4. W. Diffie and M. Hellman. New directions in cryptography, 1976. [5] R. Rivest, A. Shamir, and L. Adleman. "A method for obtaining digital signatures and public-key cryptosystems. Commun," ACM, 21(2):120-126, 1978.

5. D. Hankerson, A. Menezes, and S. Vanstone. "Guide to Elliptic Curve Cryptography," Springer-Verlag New York, Inc., Secaucus, NJ, USA, 2003.
6. S. Kamara and K. Lauter. "Cryptographic cloud storage," In Proceedings of the 14th International Conference on Financial Cryptography and data security, FC'10, Berlin, Heidelberg, Springer-Verlag, 2010.
7. R. Chow, P. Golle, M. Jakobsson, E. Shi, J. Staddon, R. Masuoka, and J. Molina. "Controlling data in the cloud: outsourcing computation without outsourcing control," In Proceedings of the 2009 ACM workshop on Cloud computing security, pages 85-90. ACM, 2009
8. N. Kaaniche, A. Boudguiga, and M. Laurent. "ID based cryptography for cloud data storage," In IEEE Sixth International Conference on Cloud Computing, Santa Clara, CA, USA, June 28-July 3, 2013, pages 375-382, 2013.
9. N. Kaaniche and M. Laurent. "A secure client-side deduplication scheme in cloud storage environments," In 6th International Conference on New Technologies, Mobility and Security, NTMS 2014, Dubai, United Arab Emirates, March 30-April 2, 2014, pages 1-7, 2014.
10. N. Kaaniche, M. Laurent, and M. El Barbori. "Cloudasec: A Novel Public-key Based Framework to Handle Data Sharing Security in Clouds," In Proceedings of the 11th International Conference on Security and Cryptography - Volume 1: SECRYPT, (ICETE 2014) ISBN 978-989-758-045-1, pages 5-18, 2014.
11. Abdul Nasir Khan, M.L. Mat Kiah, Samee U. Khan, Sajjad A. Madani. "Towards secure mobile cloud computing: A survey," Future Generation Computer Systems, Volume 29 Issue 5, Pages 1278-1299. Elsevier Science Publishers B. V. Amsterdam, The Netherlands, The Netherlands, July 2013.
12. Jin Li , Xiaofeng Chen, Qiong Huang, Duncan S. Wong. "Digital provenance: Enabling secure data forensics in cloud computing," Future Generation Computer Systems, Volume 37, Pages 259-266, July 2014.
13. Issa Khalil, Abdallah Khreishah, Muhammad Azeem. "Consolidated Identity Management System for secure mobile cloud computing," Computer Networks, Volume 65, Pages 99-110, June 2014.
14. Bin Ye, Gareth Howells, Mustafa Haciosman and Frank Wang. "Multi-dimensional key generation of ICMetrics for cloud computing," Journal of Cloud Computing Advances, Systems and Applications, vol. 4, no. 19, 2015.
15. Nagaraju, S. & Parthiban,"Trusted framework for online banking in public cloud using multi-factor authentication and privacy protection gateway," L. J Cloud Comp, vol. 4, no. 22, 2015.
16. Dimitrios Zissis, Dimitrios Lekkas. Addressing cloud computing security", Future Generation Computer Systems Volume 28, Issue 3, Pages 583-592., March 2012.
17. J.Antony John Prabu, Dr.S Britto Ramesh Kumar, "Performance Analysis Of Proposed D1FTBC Approach For Improving Consistency In Cloud Data Transactions", International Journal of Scientific & Technology Research, ISSN: 2277-8616, Volume-8, Issue-08, pp: 1803-1807, August 2019.
18. J.Antony John Prabu, Dr.S Britto Ramesh Kumar, "Performance of Proposed Architecture for Data Transactions in Cloud using D1FTBC", International Journal of Recent Technology and Engineering (IJRTE), ISSN: 2277-3878, Volume-8, Issue-2, pp: 5390 - 5395, July 2019.
19. J.Antony John Prabu, Dr.S Britto Ramesh Kumar, "Proposed Architecture for Improving Security and Consistency of Data Transactions in Cloud Database using Tree-Based Consistency Approach" International Journal of Computer Science and Information Security (IJCSIS), ISSN: 1947-5500, Volume-15, Issue-12, pp 118-126, December 2017.
20. J.Antony John Prabu, Dr.S Britto Ramesh Kumar, "An Efficient Depth 1 Fixed Tree Consistency (D1FTC) Method for Distributed Data Transactions in Cloud Environment", International Journal of Advanced Research in Computer Science, ISSN: 0976-5697, Volume-8, Issue-7, pp: 936 – 942, July – August 2017.
21. J.Antony John Prabu, Dr.S Britto Ramesh Kumar, "Proposed Architecture for Secure Distributed Data Transaction Management in Cloud Environment", International Journal of Applied

Engineering Research - (IJAER), ISSN: 0973-4562, Volume-10, Issue -82, pp: 489 – 497, 2015.

22. J.Antony John Prabu, Dr.S Britto Ramesh Kumar, "Issues and Challenges of Data Transaction Management in Cloud Environment", International Research Journal of Engineering and Technology (IRJET), e-ISSN: 2395 -0056, p-ISSN: 2395-0072, Volume-02 Issue – 04, PP.: 123-128, July-2015.