# Enhanced Approach for Secure Stored Data in Cloud

[1]Abhishek Gaur, [2]Mallikarjuna Shastry .P.M

[1]PG Student, [2]Professor, [1,2]School of C and IT REVA, University, Bangalore, Karnataka, India
[1]abhishekgaur964@gmail.com, [2]mallikarjunashastry@reva.edu.in

***Article Info***
***Volume 83***
***Page Number: 5044-5050***
***Publication Issue:***
***May - June 2020***

***Article History***
***Article Received:****19 November 2019*
***Revised:*** *27 January 2020*
***Accepted:*** *24 February 2020*
***Publication:*** *16 May 2020*

**Abstract**

Disseminated registering is nowadays a making field thinking about its showcase, high accessibility, ease. In the cloud, different associations are given to the customer by the cloud. The information store is a significant future that cloud association accommodates the relationship to store colossal extents of the cutoff. Anyway, different affiliations are not set up to execute passed on figuring advancement because of nonattendance of fitting security control game-plan and shortcoming in attestation which prompts numerous tests in scattered preparing. The endeavour will bases on, to predict data access from unapproved gets to, it proposes an appropriated course of action to give security of the information in the cloud. This could be developed by utilizing a homomorphism token with a dispersed check of obliteration coded information. The proposed game plan is required to superbly stores the information and sees the change at the cloud server. Also, in the like way plays out a touch of the undertaking like information stimulating, erasing, affixing. Also, it is required to leave behind a philosophy to keep from plot assaults of server change by unapproved clients.

***Keywords:*** *Distributed Computing, Encryption, Decryption, Homomorphic Token*

## 1. Introduction

Distributed computing is the conspicuous subject in present time. Distributed computing gives various administrations to the clients over web. Distributed storage information is kept up by capacity specialist organization. Cloud can be considered as a huge pool of virtualized and effectively open assets. Organizations like Amazon, Google run stock piling mist son the open web. Distributed storage may differ as far as space, size and usefulness. Clients can remotely store their information, and can impart assets to one another. Distributed computing permit putting away and sharing huge sum information in cloud. Distributed storage gives rapid information move benefits over web. Distributed computing give stockpiling to a wide range of information. Cloud information Storage permits clients to gather information or offer information from any place by means of web. Distributed computing information stockpiling became progressively well known system[10]. Distributed computing is the most requesting and developing innovation all through the world. Distributed computing is an Internet based PC innovation. A portion of the significant firms like Amazon, Microsoft and google have executed the ”CLOUD” and have been utilizing it to accelerate their business. Distributed computing has given another measurement to the total re-appropriating field (SaaS, PaaS and IaaS) and they furnish ever less expensive ground-breaking processor with these registering engineering.

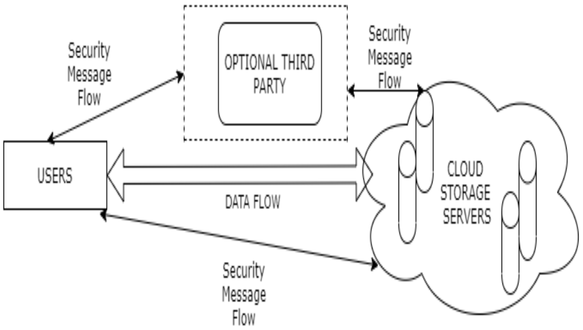


Figure 1: Cloud data storage architecture [13]

The significant thing that a PC does is to store in the accessible space and recover data at whatever point mentioned by the validated client [10].

The pioneer of Cloud Computing vendor, (example) Amazon S3 is capacity for the Internet. Amazon S3 gives a straight- forward web administrations interface that can be utilized to store and recover any measure of information, whenever, from anyplace on the web. It likewise permits engineer to get to the profoundly versatile, dependable, secure, quick, modest foundation that Amazon uses to run its own worldwide system of sites. From the perspective of information security, which has consistently been a significant part of nature of administration, cloud computing unavoidably presents new testing security dangers for number of reasons as shown in the Fig.1[10].

Distributed computing gives fast administration sat exception- ally minimal effort. Distributed computing makes new issues and testing security dangers. For security reason there are diverse numerous current strategy and strategies that are utilized in distributed computing condition. Cloud information stock piling alludes as disseminated framework. In cloud information stockpiling client normally refreshes put away information, documents. He may play out a few tasks including inclusion, erasure, change, reordering on put away information. Cloud information stockpiling has a few highlights like versatility, minimal effort administrations, unwavering quality, support, area freedom [10].

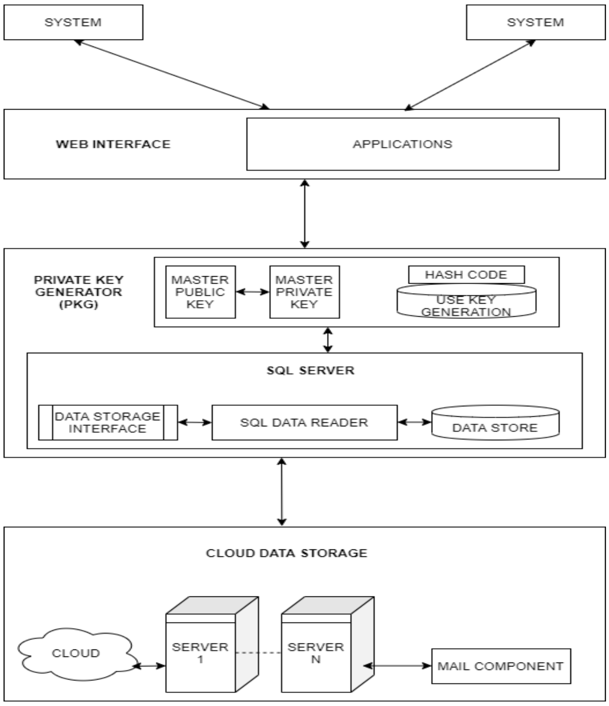


Figure 2: Architecture of cloud server for data storage

The main focus of this paper is required to splendidly stores the information and recognizes the alter at the cloud server and likewise plays out a portion of the undertakings like information refreshing, erasing, attaching. Also, it is required to give a procedure to keep away from plot assaults of server adjustment by unapproved clients as shown in Fig.2.

There mainder of the paper is composed as follows. Segment 2 gives a short review of the related work. Area 3 gives a concise diagram of cloud information stock piling security issues and difficulties. Area 4 gives an outline of the proposed targets and usage. Area 5 talks about the outcomes. Segment 6 gives a concise diagram of the end.

## 2. Related work

### A. Cloud Computing and it's Data Security

Numerous players in the business have bounced into distributed computing and actualized it. Amazon has assumed a key job and propelled the Amazon Web Service (AWS) in 2006. Likewise Google and IBM have begun look into ventures in distributed computing. Eucalyptus turned into the main open source stage for sending private mists. Cloud administrations are commonly grouped into Software as a Service (SaaS), Platform as a Service (PaaS), furthermore, Infrastructure as a Service (IaaS), for example, crude figuring force or distributed storage, assisting with relieving the accompanying security concerns: loss of data, malware infections, economics of scale and division of labor. Directly off the bat, regular cryptographic locals with the ultimate objective of data security protection cannot be honestly grasped in view of the customers' adversity control of data under Cloud Computing. Thus , check of right data accumulating in the cloud must be driven without express data when all is said in done data [13][1].

### B. Unapproved access to outsider stockpiling information

The upgraded information security model for distributed computing has researched by Eman M. Mohamed et.al [3] that diverse cryptographic methods are utilized to make sure about information in the cloud and looked at the outcomes relying on the P-worth and dismissal rate. Usage of the RSA calculation in google cloud utilizing cloud SQL has been created by Saravanan.N et.al. [4] in which they have a procedure for guaranteeing security by applying cryptography calculations using cloud SQL for the information that was put away in the outsider area. Made sure about customer server correspondence in the cloud condition has been researched by C.Nithyaet.al.[5] for the customary cryptography systems which were embraced by the customer to the client power over whole information. A productive and light weight secure structure for utilization of cloud condition utilizing the character encryption technique has been created by E.Sathiyamoorthy et.al. [6] in which theyhave permitted a few spaces to execute autonomously and portray plainly the multifaceted nature associated with endorsement based foundation while empowering the utilization of novel character-based framework. Secure offering to cryptographyin distributed computing has been created by Kajal Chachapara et.al. [14] for a blend of two cryptographic calculations to share various documents restrictively and consequently can make sure about sharing.

### C. Unsecured data transaction

A tale strategy to make sure about distributed computing through multi-cast key administration has been created by K.Sriprasadh et.al. [8] in which the framework gave better information progress security through keying and re-keying scrambled information by one of the cryptographic calculations. Secure key trade for cloud condition utilizing cell automata with triple-DES and blunder location has been researched by Govinda.K et.al.[9] for a joined solid encryption calculation with cell automata to produce secure exchange key in private or open cloud advanced by mistake recognition technique to guarantee the information honesty. Improving the security of equal calculation utilizing a key encryption system has been created by G.Sujitha et.al. [10] for three degrees of security with client MapReduce procedure and HDFS level to improve cloud framework security. Boolean polynomial math-based viable and proficient Hilter kilter key cryptography calculation: BAC Algorithm has been created by Niraj Kumar et.al. [11] for another 32-piece encryption and unscrambling calculation as little and enormous documents to make sure about information moved in the cloud.

### D. Combination of unauthorized access to third party storage data and unsecured data transaction

A joined way to deal with guarantee information security in distributed computing has been created by SandeepK.Sood et.al. [12] in which they had built up a structure that could productively tie down the information from start to the end i.e., from the supplier to the cloud and afterward to the client dependent on different systems and explicit methods. Utilization of computerized signature with Diffie-Hellman key trade and AES encryption calculation to upgrade information security in distributed computing has been created by Rewagadet.al. [13] for a mix of validation system and key trade calculation, mixed with an encryption calculation was utilized to guarantee confirmation, information security, and check.

## 3. Cloud Data Storage Security Issues and Challenges

In cloud-based condition there are various security issues, for instance, check, reliability, insurance, virtualization, protection, enormous total data getting ready, flexibility, get the chance to control, etc. Standard security approaches are never again sensible for data and applications in the cloud. Circulated processing has versatile and zone opportunity incorporates so application and data set aside in the cloud have no fixed limitations. Uncertainty bursts it is exceptionally difficult to decide a particular center point in which perils occurred.

Due to the straightforwardness of cloud condition data may be gotten to by unapproved customers. In the cloud, the issue of checking the rightness of cloud data accumulating ends up being also trying. Circulated registering speaks to a couple of security risks due to various reasons. Data Breaches is moreover critical security stress in circulated capacity. The customer set aside huge educational assortments in the cloud so the conceivably malignant customer might be entered in the dispersed stockpiling system.

There is a high possibility of ambush and threat. In circulated capacity data, dependability must be kept effectively to avoid data hardship. In appropriated capacity data is taken care of over the remote server so it is essential to secure mystery. Security game plans should be followed cautiously. Data gets to gives the customer access to the data limit. The data should be shared extraordinarily between endorsed customers so it is required to give supported customers get to. Trust worthiness is also a huge issue in disseminated capacity since data is taken care of in virtual machines.

Multi-residency is a huge attribute of a disseminated process- ing procedure. Multi-inhabitance permits various customers to access and store data on cloud servers. so there is a threat of data interference. By mixing client code data can infringe.

## 4. Proposed Enhanced Homomorphic Token Pre-Computation

Proposed system has following objectives to:

- Comprehend the security issues identified with distributed storage.
- Give excellent administrations to validated clients.
- Give high information security in the cloud-based condition utilizing improved homomorphic token pre-calculation.

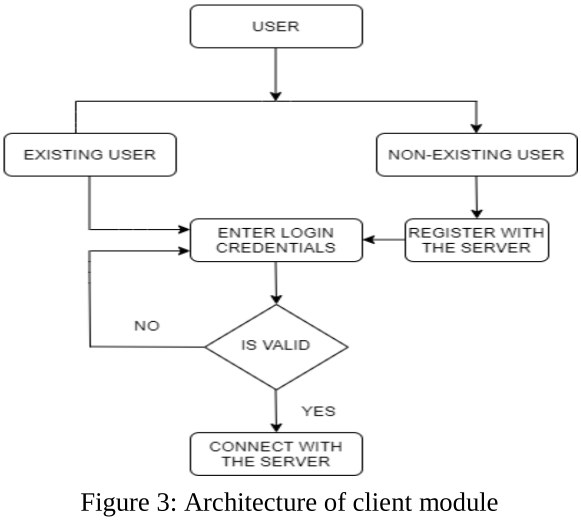


Figure 3: Architecture of client module

- Limiting information transferring and downloading time on distributed storage.

Proposed system has following modules which is been used.

They are discussed briefly below:

- **Client Module:** In this module, client connects with the server and can perform various functions given to an authorizedclient.AsshowninFig.3.
- **System Module:** This module basically work on the request comes from client then sent the request to cloud service provider after giving the access to client they can perform the task in cloud. Also, optional third party auditor comes in action when any untrustworthy client comes in and block's there resources.
- **Cloud Data Storage Module:** Using this module we can store the data in cloud and access the data storage functionality given by server-side.
- **Cloud Authentication Server Module:** The Authentication Server (AS) gives the authenticity to the cloud server after which the client can use the server to use the functionality.
- **Unauthorized Data Modification and Corruption Module:** According to this module unapproved data modification is restricted to any third-party client comes into the sever. This module will block the IP-address of the untrustworthy client and stops all the functionality given to that client.
- **Adversary Module:** This module comes in action when the data stored in the cloud server want to accessed by two untrustworthy sources that is weak adversary and strong adversary.

### A. Token Correctness

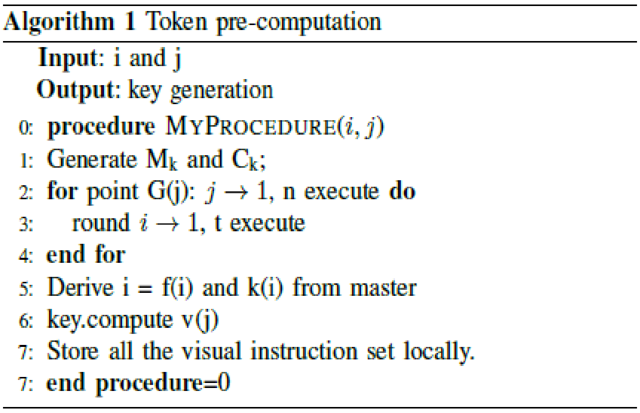
It accomplishes confirmation for information stockpiling accuracy and information blunder limitation, utilizing pre- processed token. Before sharing record dispersion utilizing pre-processes a specific number of most brief confirmation token is created that will guarantee security for a square of information in a document in distributed storage. At the point when the client needs to ensure the capacity accuracy for the information in the cloud, he challenges the cloud servers with a lot of arbitrarily produced square lists.

In the cloud information stockpiling framework, clients store their information in the cloud and no longer have the information locally. In this way, the accuracy and accessibility of the information documents being put away on the disseminated cloud servers must been sured. One of the key issues is to viably recognize any unapproved information change and defilement, conceivably because of server bargain and additionally arbitrary Byzantine disappointments. Furthermore, in the appropriated situation when such irregularities are effectively-identified, to discover which server the information mistake lies in is additionally of extraordinary centrality, since it very well may be the initial step to quickly recoup the capacity blunders.

After getting affirmation of the client it again requests validation by which the client is affirmed to be the confirmed client. After accepting affirmation, each cloud server registers a short ”signature” over the predetermined squares and returns them to the client. The estimations of these marks should coordinate the relating tokens pre-registered by the client. All servers work over a similar subset of the files, the mentioned reaction esteems for trustworthiness check should likewise be a substantial codeword controlled by amystery grid.

Expect the customer needs to challenge the cloud server's *t* times to guarantee the precision of data accumulating. Bythen, he ought to pre-process *t* affirmation tokens for every limit, a test key and an expert key are used. To create the *i*-th token for server *j*, the customer goes about as follows the nuances of token ages have shown up in Algorithm1:

- Determine a discretionary worth i and a change key dependent on thecae stage key.
- As certain the arrangement of the arbitrarily picked files.
- Ascertain the token utilizing an encoded record and the subjective worth inferred.
- Block of data is represented as ***l***.
- Number of blocks is denoted as ***n***



**Algorithm 1** Token pre-computation

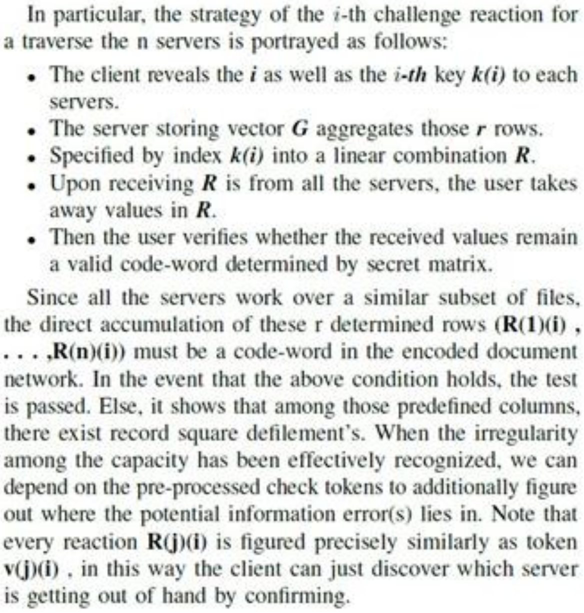
```
Input: i and j
Output: key generation
procedure MyProcedure($i, j$)
Generate $M_k$ and $C_k$;
for point G(j): $j \rightarrow 1$, n execute do
    round $i \rightarrow 1$, t execute
end for
Derive i = f(i) and k(i) from master
key.compute v(j)
Store all the visual instruction set locally.
end procedure=0
```

Figure 4: Algorithm-1: Token pre-computation

### B. Correctness Verification and Error Localization

Error localization is a key prerequisite for destroy blunders away frameworks. Nonetheless, numerous past plans don't unequivocally consider the issue of information mistake restriction.

The difficulties reaction convention in our work future gives the confinement of information blunder which just gives paired outcomes about the capacity state over the circulated administration in antecedents. The reaction esteems from servers for each challenge not just decide the rightness of the dispersed stockpiling, yet in addition contain data to find potential information error(s).



In particular, the strategy of the *i*-th challenge reaction for a traverse the n servers is portrayed as follows:

- The client reveals the ***i*** as well as the ***i-th*** key ***k(i)*** to each servers.
- The server storing vector ***G*** aggregates those ***r*** rows.
- Specified by index ***k(i)*** into a linear combination ***R***.
- Upon receiving ***R*** is from all the servers, the user takes away values in ***R***.
- Then the user verifies whether the received values remain a valid code-word determined by secret matrix.

Since all the servers work over a similar subset of files, the direct accumulation of these r determined rows **(R(1)(i) , . . . ,R(n)(i))** must be a code-word in the encoded document network. In the event that the above condition holds, the test is passed. Else, it shows that among those predefined columns, there exist record square defilement's. When the irregularity among the capacity has been effectively recognized, we can depend on the pre-processed check tokens to additionally figure out where the potential information error(s) lies in. Note that every reaction **R(j)(i)** is figured precisely similarly as token **v(j)(i)** , in this way the client can just discover which server is getting out of hand by confirming.

Figure 5: Algorithm-2: Correctness verification and error localization

## 5. Results and Discussion

Proposed system is developed as an work area application. For actualized the proposed system built up a page to enroll the client and login on the cloud also proposed system provides a technique where client can share documents to different clients.

In the proposed system client can essentially enter the id of individual whom to move the documents and record gets transferred to cloud server and name of the records gets pared to MSAccesstable. The beneficiary will get a notice that someone has imparted a document to you. System also executes improved homomorphic token pre-calculation for security upgrade and diminish the byzantine issue. By executing this calculation proposed system can process encryption and decryption.

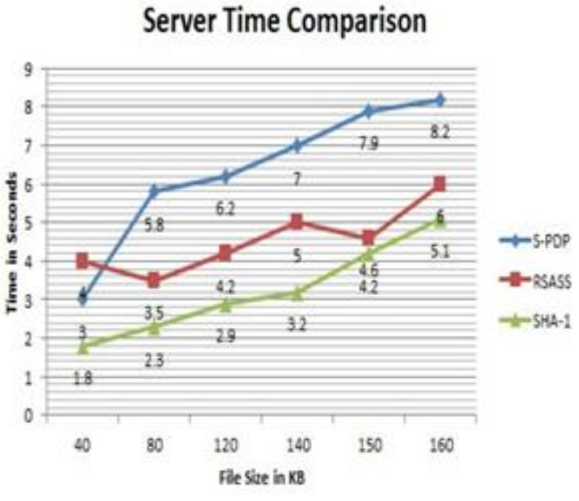


Figure 6: Server time comparison between S-PDP (Proposed Enhancement), RSA and SHA-1algorithm

As per discussion the proposed system S-PDP (Enhanced Homomorphic Token Pre-Computation) in comparison of RSA and SHA-1 algorithm gives 10% of increased server time response as shown in Fig.4.

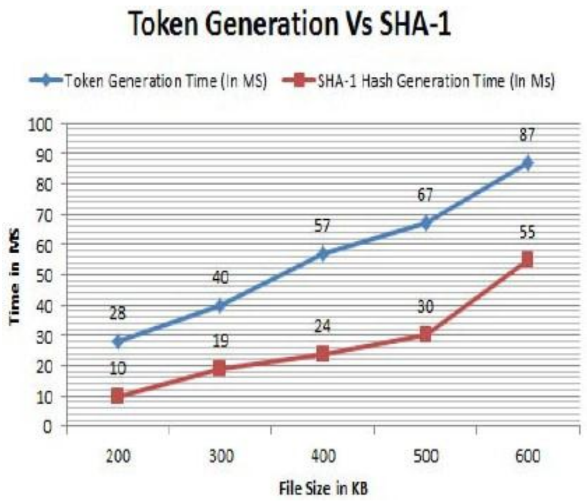


Figure 7: File size comparison between enhanced token generation method and SHA-1 token generation

Further, proposed system is been compared for the file sizes of token generated between enhanced token generation method and SHA-1 which also gives the 10% improvement in the file sizes generated for the desired token as shown in Fig.5.

## 6. Conclusion

Proposed framework revolve's around the issue of data security in cloud data accumulating, which is essentially a scattered amassing structure. To ensure the rightness of the customer's data in cloud data storing, the proposed framework is required to bean amazing and versatile flowed plot with express novel data support, including square update, delete, and annex. By utilizing the homomorphic token with an appropriated check of annihilation coded data, this arrangement is depended upon to achieves the mix of limit rightness security and data botch repression, i.e., at whatever point data pollution has been recognized during the limit exactness affirmation over the scattered servers, it can almost guarantee the synchronous conspicuous verification of the turning crazy server(s). At long last, the proposed framework upgrades the framework by 10% when contrasted with before advancements.

## 7. Acknowledgment

I thank my colleagues from REVA University who provided insight and expertise that greatly assisted the research. I would also like to show my gratitude to Dr. Mallikarjuna Shastry, Professor, REVA University for sharing their pearls of wisdom with us during the course of this research, and I thank "anonymous" reviewers for their so-called insights.

## References

[1] Abhishek Gaur, Sohini Bhar, Gopal Krishna Shyam "Security In Cloud Computing: A Survey", International Journal of Computer Sciences and Engineering Survey Paper — Journal Paper, Vol.07, Special Issue.14 , pp.76-82,May-2019.

[2] Basu, Srijita "Cloud computing security challenges solutions-A survey", 2018 IEEE 8th Annual Computing and Communication Workshop and Conference (CCWC). IEEE, 2018.

[3] KajalRani, RajKumarSagar, "Enhanced Data Storage Security in Cloud Environment using Encryption, Compression and Splitting technique", 2017 IEEE 2nd International Conference on Telecommunication and Networks (TEL-NET2017),pp.1-5.IEEE,2017.

[4] Abd, Sura Khalil, et al. "A review of cloud security based on crypto- graphic mechanisms. "2014InternationalSymposiumonBio-metricsand Security Technologies (ISBAST). IEEE,2014.

[5] Giuseppe Aceto, Alessio Botta, Walter de Donato and Antonio Pescapè," Cloud monitoring: A Survey", Elsevier Computer and Tele-Communications Networking, Vol. 57, 19 June 2013, pp.2093-2115, doi:10.1016/j.comnet.2013.04.001.

[6] C.Nithya, A.Parvathy, Pethuru Raj, K.Thenmozhi, J.B.B. Rayappan and Rengarajan Amirtharajan, "Secured Client Server Communication in Cloud Environment", International Journal of Engineering and Technology (IJET), Vol. 5, Jun-Jul 2013, pp.3123-3129, ISSN : 0975- 4024.

[7] E.Sathiyamoorthy and S.S.Manivannan, "An Efficient and Light Weight Secure Framework for Applications of Cloud Environment Using Identity Encryption Method", International Journal of Engineering and Technology (IJET), Vol. 5, Jun-Jul 2013, pp.2093-2100,ISSN:0975-4024.

[8] Kajal Chachapara and Sunny Bhadlawala, "Secure Sharing with Cryp- tography in Cloud Computing", Proc. IEEE Conf. Nirma University International conf. on Engineering (NUiCONE), IEEE Press, 28-30 Nov. 2013, pp. 1-3,doi:10.1109/NUiCONE.2013.6780085.

[9] K.Sriprasadh, Saicharansrinivasan, O. Pandithurai and A.Saravanan, "A Novel Method to Secure Cloud Computing Through Multi-cast Key Management", Proc. IEEE Conf. Information Communication and Embedded System (ICICES), 21-22 Feb. 2013, pp. 305-311, doi:10.1109/ICICES.2013.6508325.

[10] Govinda.K, Sathiyamoorthy.E and Surbhit Agarwal, "Secure Key Ex- change for Cloud Environment Using Cellular Automata with Triple- DES and Error-Detection", International Journal of Engineering and Technology (IJET), Vol. 5, Apr-May 2013, pp.1004-1009, ISSN: 0975- 4024.

[11] G.Sujitha, M. Varadharajan, Y. Vignesh Roa, R. Sridev and Sarvesh Gauthaum, "Improving Security of Parallel Algorithm Using Key Encryption Technique", Information Technology Journal, Vol. 12, 2013, pp. 2398-2404, doi:10.3923/itj.2013.2398.2404.

[12] Niraj Kumar, Pankaj Gupta, Monika Sahu and M.A Rizvi, "Boolean Algebra Based Effective and Efficient Asymmetric Key Cryptography Algorithm: BAC Algorithm", Proc. IEEE Conf. Automation, Computing, Communication, Control and Compressed Sensing(iMac4s), IEEE Press, 22-23 March 2013, pp.250-254, doi:10.1109/iMac4s.2013.6526417.

[13] Prashant Rewagad and Yogita Pawar, "Use of Digital Signature with Diffie Hellman Key Exchange and AES Encryption Algorithm to Enhance Data Security in Cloud Computing", Proc.17 IEEE Conf. Communication Systems and Network Technologies (CSNT), IEEE Press, 6-8 April 2013, pp.437-439, doi:10.1109/CSNT.2013.97.

[14] Mark D. Ryan," Cloud computing security: The scientific chal- lenge and a survey of solutions", Elsevier Inc, Published in Journal of Systems and Software, Vol. 86, Sep 2013, pp. 2263–2268, doi:10.1016/j.jss.2012.12.025.

[15] Chunming Rong, Son T.Nguyen and Martin Gilje Jaatun, "Beyond lightning: A survey on security challenges in cloud computing", Elsevier Inc, Vol. 39, January 2013, pp. 47–54, doi:10.1016/j.compeleceng.2012.04.015.

[16] Chou TS. "Security threats on cloud computing vulnerabilities". Interna- tional Journal of Computer Science Information Technology. 2013 Jun 1;5(3):79.

[17] ZhifengXiao and YangXiao, "Security and Privacy in Cloud Computing", IEEE Communication Surveys Tutorials, Vol. 15, 2013, pp. 843-859, DOI available site: doi:10.1109/SURV.2012.060912.00182.

[18] Sandeep K. Sood, "A combined approach to ensure data security in cloud computing", Elsevier Network and Computer Applications, Vol.35, Nov. 2012, pp.1831–1838, doi:10.1016/j.jnca.2012.07.007.

[19] Chen D and Zhao H, "Data Security and Privacy Protection Issues in Cloud Computing", 2012. International Conference on Computer Science and Electronics Engineering, Hangzhou, 2012, pp.647-651.

[20] N. Saravanan, A. Mahendiran, N. Venkata Subramanian and N. Sairam, "An

Implementation of RSA Algorithm in Google Cloud Using Cloud SQL", Maxwell Engineering and Technology, Vol. 4, 1st Oct. 2012, pp. 3574-3579, ISSN: 2040-7467.

[21] Eman M.Mohamed and Hatem S. Abdelkader, "Enhanced Data Security Model for Cloud Computing", Proc. IEEE Conf. On Informatics and Systems (INFOS),14-16May2012,pp.cc-12-cc-17.