Information security involving cryptography With Image and Text De-duplication in cloud

[1]Nayan Panpati, [2]Madhavi Birla, [3]Pragati Aher, [4]Suvarna Kandekar, [5]Prof. Priti Lahane

Department of IT (BE)
MET BKC, Nashik

***Abstract*: A convincing accumulating and the leading body of record systems is a ton of essential now a days to avoid the wastage of additional room given by the cloud providers. Data deduplication method has been used by and large which allows just to store a lone copy of a record and in this manner sidesteps duplication of archive in the appropriated stockpiling servers. It helps with diminishing how much additional room and save information transmission of cloud organization and as needs be in huge cost hold assets for the cloud organization allies. Today data that the proposed system need to store are in encoded game plan to ensure the security. So data encryption by data owners with their own keys makes the de-duplication inconceivable for the cloud organization endorser as the data encryption with a key followers data into an unidentifiable course of action called figure text thusly encoding, even comparative data, with different keys could achieve different code texts.**

***Keywords*: Cloud computing, Data security, encryption and decryption, data storage in cloud.**

Introduction

Distributed computing is network based figuring framework and it is the enormous extra room region where the approved client can get to the stage from anyplace and whenever with the great web or organization availability. Distributed computing is basically to shared assets, equipment, programming applications to give the gadget on request. It resembles a distant server on the web to store, make due, and process information as opposed to utilizing work area. Thus, the functioning time frame is quicker when contrasted with other nearby PCs. Distributed computing is the data innovation administrations and item. It support the virtualized assets, which depends on the reusability of IT foundation. Distributed computing is the grouping of all necessary equipment, programming, stage, applications, foundation and capacity just with online distinguishing proof. A legitimate security procedure can make it more secure and forestall information loses or taken by programmers or interlopers. Cryptography can ensure greater security in data innovation. An appropriate encryption and decoding technique can guarantee information security in distributed computing. Different calculation exists for cryptography, for example, DES, AES, RSA and so forth.

Writing Survey:

In writing study we learn guides or assists the analyst with characterizing/find out/distinguish an issue. It is something when you take a gander at a writing in a surface level, or an Ariel view. It incorporates the study of spot individuals and distributions is setting of exploration. [1] Medical associations observe it trying to embrace cloud-based electronic clinical records administrations, because of the gamble of information breaks and the subsequent split the difference of patient information. Existing approval models follow a patient driven approach for EHR the executives where the obligation of approving information access is taken care of at the patients' end. This anyway makes a critical upward for the patient who needs to approve each entrance of their wellbeing record. This isn't commonsense given the numerous work force engaged with giving consideration and that on occasion the patient may not be in that frame of mind to give this approval. Consequently there is a need of fostering a legitimate approval designation component for protected, secure and simple cloud-based EHR the board. We have fostered a novel, brought together, characteristic based approval component that utilizations Attribute Based Encryption (ABE) and considers designated secure access of patient records. This system moves the help the board upward from the patient to the clinical association and permits simple designation of cloud-based EHR's entrance power to the clinical suppliers. In this paper, we depict this clever ABE approach as well as the model framework that we have made to outline it. [2] The quickly developing interest for cloud administrations in the ongoing industry practice has inclined toward the outcome of the crossover mists and the appearance of cloud organization. The accessible writing of this point has zeroed in on middleware deliberation to interoperate heterogeneous cloud stages and arrange different administration and plans of action. Be that as it may, cloud alliance suggests genuine security and protection issues regarding information sway when information is re-appropriated across various legal and general sets of laws. This section portrays an answer that applies encryption to safeguard information sway in combined mists instead of confining the versatility and relocation of information across unified mists. [3] For building a solid distributed storage administration on top of a public cloud framework, property based encryption (ABE) has been a favored arrangement because of its adaptable access control. ABE, nonetheless, causes weighty calculation cost on clients during unscrambling. Accordingly, past examinations tackled this issue by empowering cloud servers to play out a piece of unscrambling procedure for the clients. To engage clients to confirm the accuracy of the appointed decoding by the cloud, they utilized a cryptographic responsibility or message verification code (MAC) to empower clients to really look at the rightness of fractional unscrambling of the cloud. In any case, the past plans neglect to guarantee the rightness of calculation within the sight of vindictive cloud servers. In this paper, we propose a novel and conventional responsibility plot for ABE, which is secure against altering assaults by malevolent cloud servers. As indicated by the exhibition investigation, the proposed plot is just 0.5 ms more slow on normal than the past responsibility based plans and a few times quicker than the MAC-based conspire. [4] Storage-asa-administration is a fundamental part of the distributed computing foundation. Information base reevaluating is a normal use situation of the distributed storage administrations, wherein information encryption is a decent methodology empowering the information proprietor to hold its command over the re-appropriated information. Accessible encryption is a cryptographic crude considering private catchphrase based search over the scrambled data set. The setting of big business re-appropriating data set to the cloud requires multi-client accessible encryption, though essentially all current plans consider the single-client setting. To overcome this issue, the framework propose a functional multi-client accessible encryption plot, which has various benefits over the known methodologies. [5] Cloud figuring is another innovation that move the registering system from PCs into cloud servers over the web. By the by, as the client data information is put away in the cloud supplier servers, the secrecy of the data become another worry. Various calculations in light of Encryption is introduced beforehand to give cloud clients classification. The primary thought of encryption calculations for cloud information is to allow cloud clients inquiries to be taken care of utilizing scrambled information without unscrambling. This paper presents another security instrument utilizing cross breed technique for encryption calculations and a dissemination framework to improve cloud data set privacy. An upward discontinuity procedure is taken on from alsirhani's model for disseminating information over mists. Be that as it may, to beat a shortcoming in alsirhani's model where compromises to a section can in any case make information significant. All things considered, the proposed model purposes a cross breed fracture strategy to make information on sections inane whenever split the difference. The proposed model conveys the cloud data set among the mists utilizing the supplier perspectives and level of classification that is conveyed by the utilized encryption calculations. To assess the proposed accessible encryption and cross breed discontinuity model, the review fostered a Java application for recreating the mixture cloud. The recreation joins public and private mists; as fundamental cycles is led inside the private cloud. The assessment of the work was led by contrasting the proposed model and existing arrangements in inquiry reaction and security attributes. Fundamental outcomes showed that the proposed accessible encryption and mixture discontinuity model gives a solid component that improves information secrecy concerning quicker reaction and extra security

System Architecture:

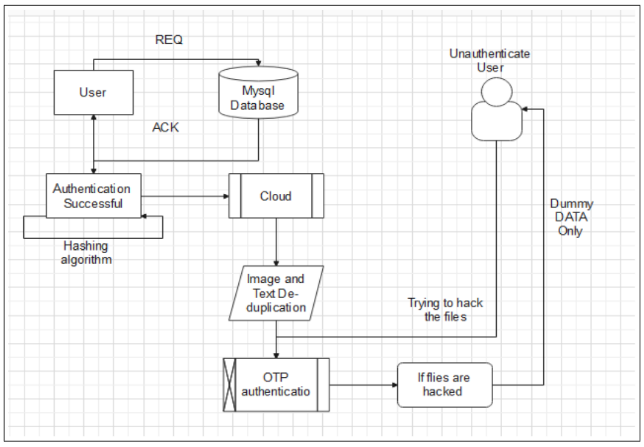


Fig.4. System Model of Secure Role Re-encryption System

A user sends a request to Management centre and encrypts the file, then it results as the cipher text to CSP. Users who belong to completely different role groups owning the corresponding role keys, with the role keys the user access cloud server, the user will upload or transfer the files from Cloud Service Provider. And user can download the file from the cloud server. A Cloud Service Provider is mainly for data storage, management and verification.

Cloud Service Provider stores and manages the uploaded files from authorized user Management centre is the trusted third party that is for the authorized user and for the role key management.

A. System Model: A user sends a request to Management centre and encrypts the file, then it results as the cipher text to CSP. Users who belong to completely different role groups owning the corresponding role keys, with the role keys the user access cloud server, the user will upload or transfer the files from Cloud Service Provider. And user can download the file from the cloud server. A Cloud Service Provider is mainly for data storage, management and verification. Cloud Service Provider stores and manages the uploaded files from authorized user Management centre is the trusted third party that is for the authorized user and for the role key management.

B. Adversary Model: A1 may has the communications between CSP and also the user to induce the transmitted info, and plays a job of the user to act with the CSP. A2 may listen the communications between CSP and also the user to urge the transmitted info, and cloud exchange S min bytes info with the user. A3 might discard the user’s knowledge that haven't been accessed or rarely accessed, and should tamper the user’s knowledge to take care of reputation. a role authorized tree to manage the user’s role and implement the role re-encryption key updating and revoking with efficiency, that satisfies the change of authorized user’s privilege. Once performing the secure knowledge deduplication, CSP will check the ownership of the licensed user. Security analysis shows that our proposed system is secure beneath the proposed security model, and performance analysis demonstrates the effectiveness and efficiency of our proposed system.

C. Design Goal: The main goal of the system is to protect the data from the cloud storage and the cloud server should be secure from the unauthorized user. So, then there will not any leakage in the cloud server.

D. Convergent Encryption: The same keys are always obtaining the same cipher text that can be by the two users with the new plaintext without the encryption keys.

E. Role Key Update: In role key updating, the generation of role keys is done in the management centre. The user can perform updating, downloading using the role re-encryption. And the management centre supports the role authorized tree.

Algorithm and methods:

I. Cryptography: is a method of storing and transmitting data in a particular form so that only those for whom it is intended can read and process A new key (KEY1) using a hash function with stored KEY and delivers to the user/client by a secured channel (email, mobile etc.). User will enter KEY1 into the system. System will match this KEY1 with its previously generated KEY. Successfully matched, system will generate again a KEY using anti-hash function from KEY1 and matched with its stored KEY. If matched again successfully, then system will treat this user as a valid user. This authentication system works in three steps. Firstly, supplying user ID and

2. Hash functions.3. Public-key cryptography

Our main goals are to secure stored data and authentication system in cloud environment. Many researchers tried to secure various credentials of users such as secure login, storing data/file with encryption, key management etc. By any means, if a hacker enters into the system, he may steal data/files from could end. If one intruder may successfully enter to cloud environment, then there is no way to detect him as a thief. By his credential he may access all data of the system. The system has offered such a system/environment that if any person enters into cloud end by any means, he will not succeed to get data/files from the cloud end. He will be caught. The procedures are described in next section.

A. Users Authentication:

When any clients/users will access his data/files or send new files, he has to login with his credential (user ID and password). If his credential is valid, then he will enter into next step of authentication. By this time, system will generate

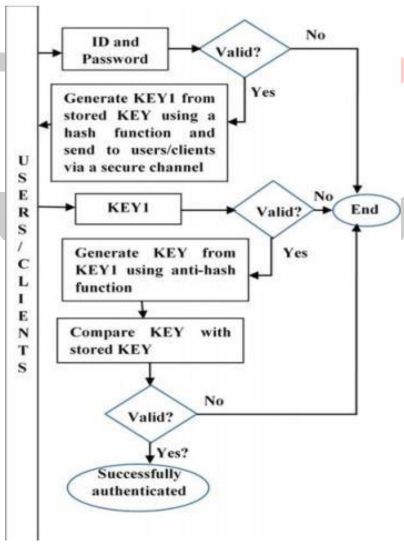


Fig. 01 User authentication process

using a hash function with stored KEY). This KEY1 will be sent by a secured channel to the user. Thirdly, verifying stored KEY with newly generated KEY using anti-hash function with KEY1 (user supplied KEY1). As the system has stated earlier that, hackers will be caught even he supplies valid user ID and password. He will also be caught even while accessing the file that stored KEYs. As system will generate KEY1 using a hash function with stored KEY and sends KEY1 to the user by a secure channel, the invalid users/ hackers will not be able to access this KEY1. So, he will not be able to supply new KEY1. So there is no way to access data/file by an invalid user. An extra protection is also available by verifying stored KEY with newly generated KEY using anti-hash function with supplied KEY1. This system is described in Fig. 1 and Algorithm 1. After successfully login, user will able to access his data/file or send new file to cloud. Encrypted files/data will be decrypted using valid KEY and will send to the users.

B. Cloud End Auto Encryption: Auto encryption procedure is described in Fig. 2 and Algorithm 2. In the Fig. 2, the system has proposed an automated encryption system. This encryption system may be used hybrid cryptography system including RSA and AES or any other suitable encryption method. After login (described in previous section) users may access or send new data/files to store in the cloud and later he may logout. After successful logout, the system will lock those files/data, the user has been accessed or stored. Then system will create a new key (KEY2) by using a hash function with previously used KEY. Using this new key (KEY2), those files/data will be encrypted and new key(KEY2) will be replaced with previous stored KEY.

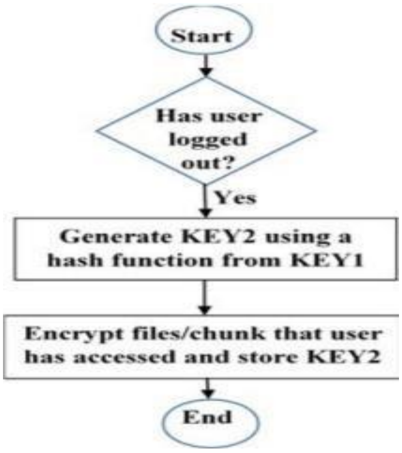


Fig. 02 Cloud end auto encryption

C. Algorithm 1:

1. User login will be verified by a suitable system. 2. If login credential is valid, generate KEY1 using a hash function with stored KEY and send to the user by a trusted/secured medium. 3. Provide new KEY1 (by the user) to get a chunk of encrypted data/files. 4. Compare provided KEY1 with system's KEY1, if matched, then go next step, otherwise exit. 5. Generate KEY using anti-hash function with user supplied KEY1; match this KEY with stored KEY; if does not match, then exit. 6. Decrypt data chunk by this KEY and send to the user. 7. If user wants to store file, then encrypt it by suitable encryption algorithm. D. Algorithm 2:

1. At first, User login will be verified Algorithm 1. 2. If user logout, then generate KEY2 using a hash function with KEY1. 3. Encrypt files/data that has been accessed/stored by this user using a suitable encryption algorithm. 4. replace KEY1 by KEY2 and exit.

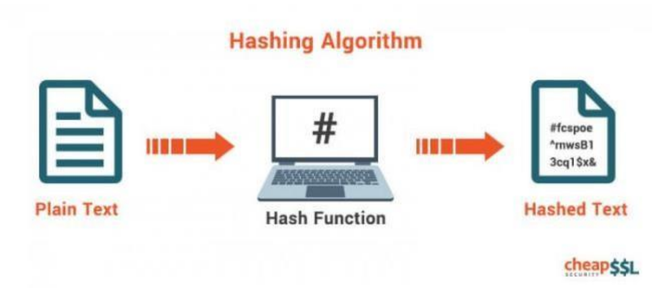
II] Image upload process:

For image uploading the user has to click the image upload button at the top of the Cloud system platform. Then from the user's image storage he/she has to select any image with any size and with any dimension. If some other user uploads the same image with same size, dimension then it will not upload into the cloud system (i.e. it gives notification as `the image is already present' to the user) And if the same user try to upload the same image with different size, dimension then it automatically uploaded into cloud system directly

III] Text upload process:

If the user wants to upload any text file then user has to click the text upload button at the top of the cloud system platform ,Then the text file which user has to be ready in their normal server storage in their platform, after this user has to click the choose file button then it goes to that saved area and it automatically inserted and user has to click the upload button, then it automatically uploaded. If some other authorized user uploads the same file then that particular file will not be uploaded and also it exists. For the text upload process. The proposed is using 3 main algorithms ,
1.Levenshtein string distance algorithm 2.Fuzzy string matching algorithm 3.Dice coefficient algorithm

A hashing algorithm is a mathematical algorithm that converts an input data array of a certain type and arbitrary length to an output bit string of a fixed length. Hashing algorithms take any input and convert it to a uniform message by using a hashing



2] Fuzzy string matching algorithm: Fuzzy Matching also called as Approximate String Matching is a technique that helps identify two elements of text, strings, or entries that are approximately similar but are not exactly the same. Fuzzy logic is a form of multi-valued logic that deals with reasoning that is approximate rather than fixed and exact. Fuzzy logic values range between 1 and 0. i.e. the value may range from completely true to completely false.

Architecture of Fuzzy Logic:

In the architecture of the **Fuzzy Logic** system, each component plays an important role. The architecture consists of the different four components which are given below.
1.Rule base 2.Fuzzification3.Inference engine 4.Defuzzification

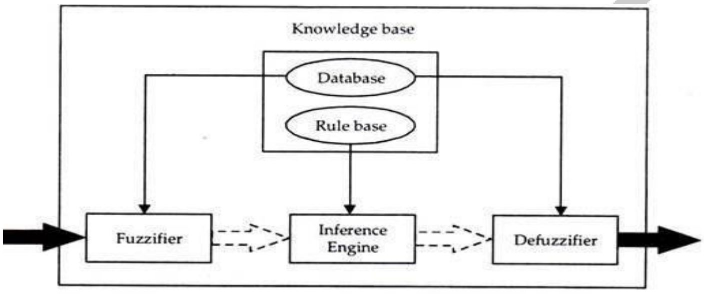


Fig. Architecture of Fuzzy logic.

Proposed Work :

The proposed framework is making a framework that permits client to give security to their records/information and shield them from programmers and keep away from the malevolent assaults. The proposed framework is involving hash work for encryption of the secret key but by some coincidence assuming the programmer breaks the hash code; he will get just the spurious information by the framework. OTP(one time secret word) will likewise show up for confirmation utilizing client's email or portable number. Network traffic in the Cloud encryption climate is described by huge scope, high dimensionality, and high overt repetitiveness, these attributes present genuine difficulties to the advancement of cloud. A compelling stacked contractive auto encoder (SCAE) strategy is introduced for unaided element extraction

Result :

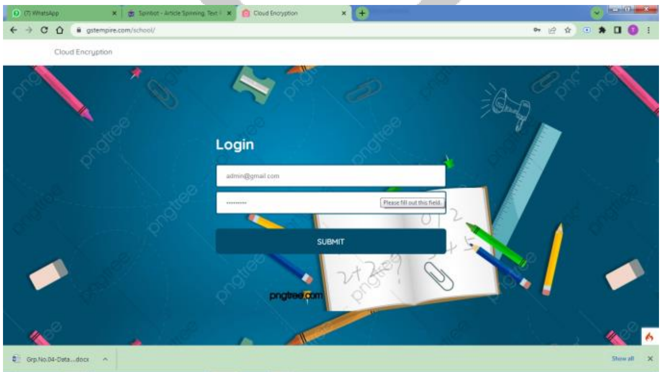


Fig : Login Page

This is our login page for user , where user will login to system for accessing the system.

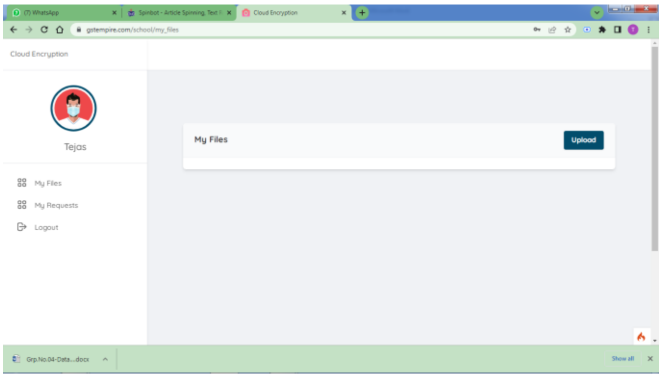


Fig: Homepage for user

This is a dashboard screen of user where he will upload the data in system and it will get display.

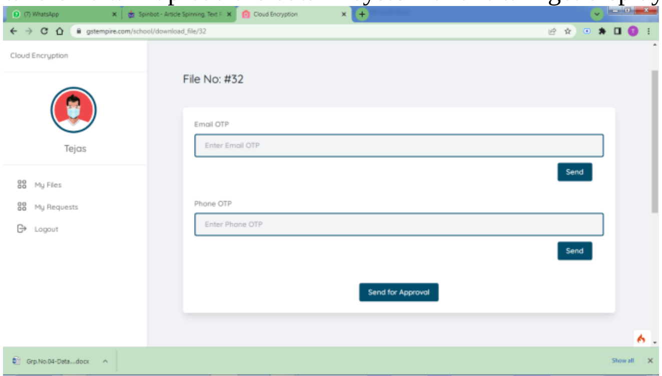


Fig : Authentication Page

When user will try to download the data , he will get the authentication stuff of Email otp and mobile otp.

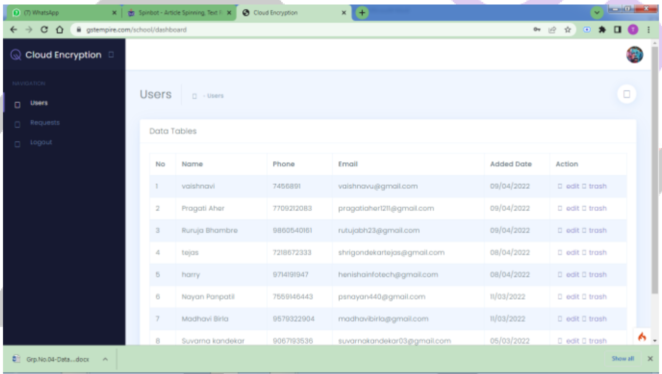


Fig: Admin Dashboard

Admin Dashboard is use to see the user list and , for creation of user.

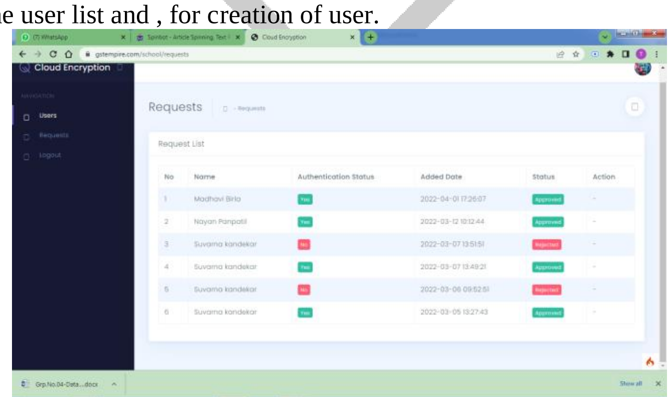


Fig: Request table for Admin

References:

[1] Maithili Arjunwadakr and R.V. Kulkarni, "The rule-based Intrusion Detection and Prevention Model for Biometric System", *Journal of Emerging Trends in Computing And Information Sciences*, OCT 2010.

[2] Todd Vollmer, Jim Alves-Foss and Milos Manic, "Autonomous rule creation for intrusion detection", *2011 IEEE Symposium on*

Computational Intelligence in Cyber Security.

[3] M. Sebring, E. Shellhouse, M. Hanna and R. Whitehurst, "Expert systems in intrusion detection: A case study", *Proceedings of the 11 th National Computer Security Conference*, pp. 74-81, 1988.

[4] T. Lunt, R. Jagannathan, R. Lee, S. Listgarten, D. Edwards, P. Neumann, et al., *IDES: The Enhanced Prototype. A Real-Time Intrusion Detection System*, 1988.

[5]D. Anderson, T. Lunt, H. Javitz, A. Tamaru and A. Valdes, *Detecting Unusual Program Behavior Using the Statistical Component of the NextGeneration Intrusion Detection Expert System (NIDES)*.

[6] H. Anggeriana, S. Kom and M. Kom, "Cloud Computing", Jurnal Teknik Informatika, vol. 1, 2011.

[7] T. Velte, A. Velte and R. Elsenpeter, Cloud computing a practical approach, McGraw-Hill, Inc, 2009.

[8] P. Mell and T. Grance, "The NIST definition of cloud computing", National Institute of Standards and Technology, vol. 53, pp. 50, 2009.

[9] A. Yousif, M. Farouk and M. B. Bashir, "A Cloud Based Framework for Platform as a Service", in Cloud Computing (ICCC) 2015
International Conference on, pp. 1-5, 2015.

[10] E. Hossny, S. Khattab, F. Omara and H. Hassan, "A Case Study for Deploying Applications on Heterogeneous PaaS Platforms", in Cloud Computing and Big Data (CloudCom-Asia) 2013 International Conference on, pp. 246-253, 2013.

[11] M. O. Imam, A. Yousif and M. B. Bashir, "A Proposed Software as a Service (SaaS) Toolkit for Cloud Multi-Tenancy", Computer Engineering and Applications Journal, vol. 5, 2016.

[12] M. M. Alani, Elements of cloud computing security: A survey of key practicalities, Springer, 2016.

[13] A. team, Open Source Metadata-Based Java ORM Framework for Cloud SaaS Applications, 2011, [online] Available:
http://www.athenasource.org/java/

[14] S. Paliwal, "Cloud application services (SaaS)-Multi-Tenant Data Architecture", Infosys technologies limited, Sep 2014, [online] Available:
http://www. cmg. org/wpcontent/uploads/2012/11/m_94_4. pdf.

[15] S. A. Elmubarak, A. Yousif and M. B. Bashir, Performance based Ranking Model for Cloud SaaS Services, 2017

[16] l. Xu, E.-C. Chang, and l. Zhou, ”Weak leakage-resilient client-side Deduplication of encrypted data in cloud storage,” in Proceedings of the Sd! ACMSIGSAC symposiwn on Information, computer and com-munications security. ACM. 20 J3, pp. 195-206.

[17] R. Oi Pietro and A. Sorniotti. ”Boosting efficiency and security in proof of ownership for deduplicatioll.” in Proceedings of the 7th ACM Symposium on Infonnation. Computer and Communications Security.ACM, 20 12, pp. 81-82.

[18] Halevi. D. Hornik. B. Pinkos. and A. Shulman-Peleg. ”Proofs of ownership in remote storage systems,”” in Proceedings of the 18th ACM SIGSAC Conference on Computer and Communications Security. ACM, 20 I I, pp. 491-500.

[19] l. N.i, K. Zhang, Y. Yu et aI., ”Providing task allocation and se-cure deduplication for mobile crowdsensing via fog computing,” IEEETrans. on Dependable and Secure Computing, vol. PP,no. 99,pp. 1-1,2018.

[20] Y. Zhang, X. Chen, l. Li. D. S. Wong, H. Li, and I. YOll, ”Ensuring attribute privacy protection and fast decryption for outsourced data security in mobile cloud computing,” Information Sciences, vol. 379.PI¿. 42-61,2017.