International Journal of Computer Networks and Applications (IJCNA)
DOI: 10.22247/ijcna/2016/v3/i4/48567 Volume 3, Issue 4, July – August (2016)

RESEARCH ARTICLE

A Novel Approach for Data Privacy Using Attribute Based Scheme Algorithm for Cloud Computing

A.Nithya
Research Scholar, S.T Hindu College, Nagercoil, Tamilnadu, India.
nithi91.nithya@gmail.com

B. Ramakrishnan
Department of Computer Science and Research Centre, S.T Hindu College, Nagercoil, Tamilnadu, India.
ramsthc@gmail.com

Resul Das
Department of Software Engineering, Firat University, 23119, Elazig, Turkey.
rdas@firat.edu.tr

Abstract – Cloud computing is the mass storage area that helps the user to access the data anywhere. There are so many platforms provided by the cloud service provider. They are SaaS (Software as a Service), PaaS (Platform as a Service) and IaaS (Infrastructure as a Service) etc. Though security is not fully provided by the cloud service provider to reshape the advances in information technology, cloud computing is expected as an updated technology. The data was securely stored in the cloud and if it is corrupted then the proxy is implemented to regenerate the corrupted data in the cloud. Thus security and integrity is successfully achieved. This is further extended by implementing efficient file fetching by the third party user. To maintain efficient file fetching system Multi authority cloud model is proposed. The model is continuing with the proposed entities such as Attribute authority (AA), Certificate Authority (CA) and Third party end user. The data is encrypted by the owner and stored in the cloud server. CA is used to delegate the Secret Key (SK) to AA and Public Kay (PK) to user. After Checking the authentication of the owner CA provides PK to the owner only then the owner is allowed to upload the data in cloud, the data is encrypted and outsource to the cloud server. Using SK the third party user is allowed to view the data from the cloud. If the user enter the wrong key or misuse the data, user will be revoked. If the User needs to download or update or delete the data in the cloud the user need to send a Data Access Privilege (DAP) request to the respective owner. Certificate authority is responsible to generate a key to the entities such as User, Data Owner and attributes.

Index Terms – Cloud Computing, Security, Third Party Auditor (TPA), Proxy, RSA Algorithm, Regeneration, Multiuser Authentication.

1. INTRODUCTION

W. Diffie and M. Hellman [1] described that cloud computing is the upcoming area where all the organizations prefer to store their data. The cloud computing model is introduced to maintain the server with user flexibility. The most important model is to maintain the multiple user storage schemes and also the cheap implementation. Q. Wang et al. [2] proposed that the cloud computing can offer various storage model for the user. The user can prefer either the private storage or public storage scheme. These models are maintained in the various schemes thus the user can select any scheme from the particular model. D. Boneh and X. Boeh [3] proposed that cloud computing can be classified into three. They are Public cloud, Private Cloud and the Hybrid cloud. The main reason for using public cloud is cost efficiency. The Cloud Service Provider (CSP) can provide this service to the data owner to store their data for free of cost with limited storage. Some of the examples are Gmail, drop box etc. The people can freely mail or store their personal data in cloud for free of cost. Another main disadvantage is the accessibility. User can access the data from anywhere in the world. Thus the processing capability is efficient. Boyang Wang and Baochun Li [4] described the next classification of cloud as the private cloud. The concept of buying an area in the cloud is called private cloud and then they can store their data in that particular area. In this case the people who do not belong to that area cannot store their data in the private cloud. The last classification model is the Hybrid cloud. In this model the data owner can store their data in any one of the cloud it may either private or public cloud. The main model is to support the simple and efficient process for maintaining the data. Thus the cloud provides lot number of advantages for the people to store their data.

Z. Liu et al. [5] described that the cloud computing should cover the complexities as well. Thus, the complexities are demerits that occur in the cloud due to security and the corruption. To maintain the data security many techniques are introduced in cloud. By using the systematic model it can be maintained under the simple concept. The model is based on the process of simple accessing parameters. C. Liu et al. [6] proposed that the security parameters always include the

RESEARCH ARTICLE

tedious and complexity parameter. The most common way of approach used in succeeding the security is Auditor. Auditing is the simple way to check the data stored in the server of cloud with the permission of CSP. Among the cloud types, security is lacking in the public cloud. Because all the data stored in the public cloud is workload. M. S. Premalatha and B. Ramakrishan [7] analyses the scheduling of various workloads of the cloud users. This research gives the details about the number of busy and idle servers based on their computational load and energy consumption. The server utilization and the load of servers give insight for the improvement of scheduling process.

Figure 1 Ratio of Workload

The Figure 1 shows the ratio of data taken from the Cisco Global Cloud index, 2015. The increasing of the data consumer of the cloud considerably increases the traffic rate. And the usage will be increased further in 2019. The workload is simple, but not efficient in the previous scheme. This need to be avoided in the proposed concept and scheme. Thus the auditor is built with the additional mechanism to overcome the hurdles of the security. Then the new concept of regeneration is implemented in this work to maintain the simple experiments of the regeneration code block mechanism. Though it can be maintained under the simple and efficient process of mechanism, through which it can be processed.

2. RELATED WORK

B. Wang et al. [8] described about the Personal Health Record (PHR) used in the first processing mechanism. The distributed algorithm is used to maintain by the Attribute Based Encryption (ABE) format. Through which it can be processed for the simple and efficient processing speed. This can be further modified by the simple mechanism that is used in the hospital. The hospital organization consists of doctors, patients, and staff members. These members are used to find the record but the security is still lacking to maintain the patient's detail. That is why a new mechanism is implemented in the project to build the security based mechanism for maintaining the patient's record. This record is used to find the simple concept through which it can be processed. And the main use of the Attribute based encryption is maintained in different ways of processing through which it can be processed in different format. The main use of the ABE is the simplest form of the program through which it can be used for different ways of processing. To verify data integrity on cloud servers, provable data possession technique was introduced by the researchers to validate the completeness of the data and to validate the integrity of the data, a number of provable data possession protocols have been used. The continuation of the data owner and the storage servers in the same domain are assumed by the traditional access control. This assumption, however, no longer remains the same when the data is carried to a remote control service provider, which takes the full control of the management outsourced data, and occupied outside the trust domain of the data owner. A good solution can be provided to enable the owner to enforce access control of the data stored in a remote untrusted server. By using this solution, the data is encrypted using certain keys, the decryption key is shared only with the trusted user. The untrusted users are unable to access the data. This general solution has been widely used in existing schemes.

Q. Wang et al. [9] described that the cloud computing moves the application software and the database to the centralized large data centers, it also manage the data and services but the management may not be fully trust worthy. This brings many new security challenges, but those are not well understood. The main problem pointed by this paper are the originality of data stored in the cloud are verified by the third party auditor instead of cloud client. The auditor eliminates the overburden of the client but also there is a chance of leaking of data by the auditor. Boyang Wang and Baochun Li Merkle [10] described hash Tree construction for block tag authentication. This paper improves the existing proof of storage model to achieve efficient data dynamics. The technique of more than one auditing task was performed by TPA simultaneously, it is done by the efficient handling of multiple auditing task. Extensive security and performance analysis have been achieved in the upcoming methods.

J. Yuan and S. Yu [11] described the main use of the simple concept of programming is used to maintain the IDDR scheme. The main use of the IDDR mechanism is to process for the cloud computing environment. The TPA mechanism is introduced in this model to develop the security in cloud computing. Thus the TPA secures the data while auditing the mechanism packet in the cloud. Through which it can protect the data in the cloud. The proposed model is used to maintain the simple mechanism of the system. The main approach is used to process the mechanism through which it can be used for maintaining the systematic model in the system.

RESEARCH ARTICLE

Y. Zhu et al. [12] described the promising approach of the TPA that establishes some drawback in the main area through which it can be processed in a simple concept. The main concept of the proposed model is to implement the systematic approach of proxy server in the model.

The proxy server is used to maintain a regenerating mechanism in the cloud. The regenerating process is used in the corrupted server, which is corrupted by the TPA because of the lacking security. Thus the new model is introduced in the proposed mechanism to implement a best process of developing a pure model of data process.

The main use of the systematic problem is to maintain the systematic development. The next mechanism is used to implement the unauthorized data in the cloud.

B. Wang et al. [13] described a main drawback that the owners of data faced today is data integrity and privacy. The data stored in the cloud are not safely available in it, because it is not only stored but also it is used by large number of peoples. So KNOX is proposed to maintain the correctness of data in the cloud. It is a privacy preserving auditing mechanism used for checking privacy of data available in the cloud and also to check the integrity of data. KNOX also reduce the storage area used to store the verification details by using homomorphic MAC.

3. PROBLEM IDENTIFICATION

The Existing work is based upon auditing and proxy regeneration process with the single user interface. The main use of the systematic development is based on the simple processing mechanism. The existing process is built with the auditing mechanism of single user model and it should be maintained for the simple accessing process. Proxy is used here to maintain the corrupted data in the server and regenerate it with the Exclusive OR (EOR) function. J. Suganthi and Ananthi. J [14] denotes proxy model that represent in the previous model is simple and efficient for processing the data in the cloud. The proxy is only used for regenerating the data in the server and the main use of the auditing is represented as the Third Party Auditor (TPA) which means it is simply denoted to maintain the mechanism of the verification process. This process will lead to the tedious work in the ancient introduction. Thus it is overcomes by the proxy. The data processing is maintained for the tedious complexities without any conclusion. It means the existing model focus only on storing and regenerating the code in the system. The process is fully maintained by the Proxy itself.

B. Wang et al [15] described data owner file security, accessibility of the third party user is not mentioned. Thus this process is still a drawback for the existing system. This overcomes by the simple and efficient work of the proposed model. Here the data that is corrupted by the third party user will be regenerated by using proxy.

3.1. ARCHITECTURE

The architecture of the existing working process is shown in Figure 2.

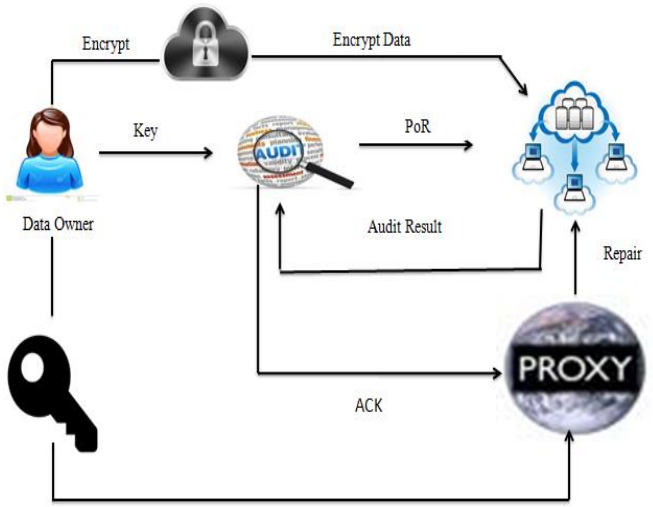


Figure 2 Architecture of Existing Model

The main use of the existing model is to secure the data owner file while storing the file in the cloud. The data that stored in the cloud can easily get corrupted through which it can be maintained.

As shown in the Figure 2, the main use of the proposed model is based on the data owner side. The entities that maintained in existing are Data Owner, Proxy and Auditor.

The first one is the setup phase. In this phase data owner uses the cryptographic model to build the data. Then the encrypted data is divided into packets and stored it in the cloud. The cloud service provider (CSP) stores the data in any of the server to which it belongs. Another entity is the TPA. The TPA's duty is to audit the result in the Cloud Server through which it can be maintained by the system.

The auditing process is maintained by the system through which the key is provided by the data owner. The TPA concept is used to overcome the overburden of the data owner. The processing ability of the auditing is simple and which is used for the security process. The main use of the data ability is to process the challenge case.

The challenge case is done by the auditor in the cloud. By receiving the challenge it produces access permission to the server. The main aim of the server is to reduce the complexity in owner side for verification.

D. Boneh and M. K. Franklin [16] described how the data is used for the simple and efficient access permission for the user through which it depends. The main aim of the challenge case

RESEARCH ARTICLE

is to verify all the files from the data user. Then the verified file is send to the Proxy.

Here Proxy who acts like a data owner and the main use of the model is that which it accessibly reduced the overburden of the owner and also the corrupted data is successfully regenerated by the Proxy.

The algorithm used is Block and Regeneration Block based mechanism. Thus it can be maintained for the Exclusive OR (EXOR) concept. The main attributes is used to form the little collaboration of the system through which it can be maintained.

3.2. FLOW CHART

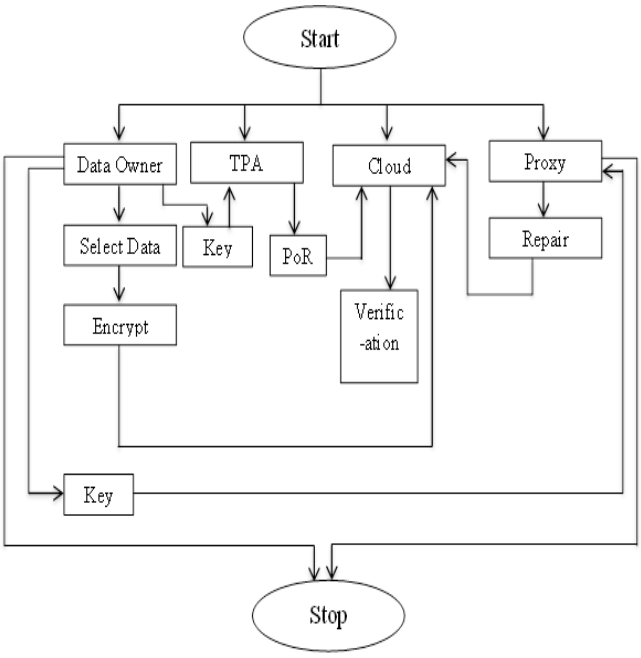


Figure 3 Flowchart of the Existing Model

The Figure 3 clearly described the working process model of the previous mechanism. The entities used are Data Owner, TPA, Cloud and Proxy. The data owner encrypt the data using an algorithm and stored it in different blocks of different servers i.e. the data is stripped and stored in different servers of cloud.

Now, the owner can send a key to the auditor, he can audit the data available in the blocks of server by using the key whenever the owner goes offline. If any data gets corrupted in the server it sends an ACK to the proxy.

The proxy checks the corrupted block and regenerate the corrupted data by using hash function. The main use of the mechanism is that it helps the data to be regenerated in an efficient way.

After introducing the accessibility the accessing scheme is still not provided for making the data flexible for all users and the end party user. These are considered as the future work and the concept is slightly recreated to achieve the full accessibility in the proposed scheme.

3.3. DEMERITS

The drawbacks of the existing schemes are third party user accessibility, security and regeneration coding. The data owner stores the data and retrieves the data thus security will not be achieved by giving permission to the third party user. This queries and model is not solved in the previous mechanism. Thus in this research work it is used to maintain the simple scheme through which it should be maintained.

4. PROPOSED MODELLING

The proposed work is based on the Attribute Based Scheme. This scheme is used to maintain the third party user to maintain their data with defined security parameters. The security parameters include the Certificate Authority and the key that is provided to the User.

The data storing process of the data owner is entirely same like the Existing System. The details that is used to fetch the information is processed in the simple and efficient attribute based scheme which is based upon the attributes through which it should be designed.

4.1. ARCHITECTURE FOR PROPOSED MODEL

The Figure 4 describes the design of this research work. Here the data owner is used to store the data in simple and efficient process through which it can be maintained. Before storing the data in the cloud, it needs a PK. The PK is given by the certificate authority. After receiving the PK the owner of the data is trusted as an authorized person. Only then the owner gets the rights to store the data in the cloud.

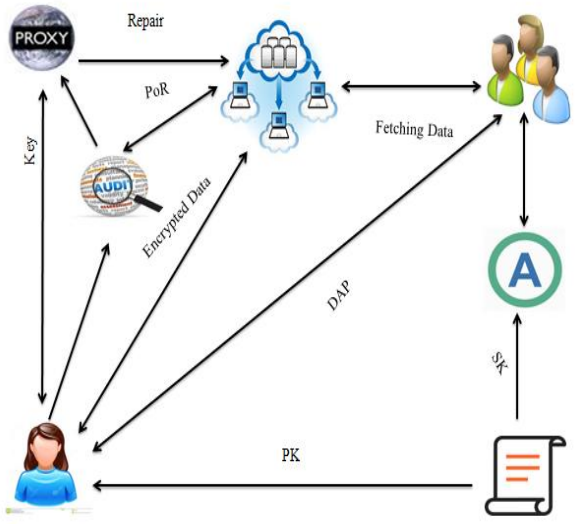


Figure 4 Architecture of the Proposed Model

RESEARCH ARTICLE

Certificate Authority is the one which can generate the keys to the owner and Attribute Authority after checking its authorization. The purpose of using keys is to increase the data security.

The certificate Authority generates a public and a secret key. The public key is distributed to the owner after checking that he is an authorized one or not. After receiving the PK the owner gets the rights to access the cloud. The secret key of the respective owner file is distributed to the attribute authority.

Now, the owner can store the file in the cloud after encrypting the data, here RSA algorithm is used for data encryption. The file is stripped and stored as different combinations in multiple servers on the cloud.

An auditor was implemented to audit the files stored in the cloud whenever the data owner goes offline. The auditor audits the data and sends an ACK to the proxy if any data gets corrupted in the cloud server. The proxy is a workstation implemented in an organization. After receiving the ACK from the auditor the proxy regenerate the corrupted data on the cloud server on behalf of the owner. The regeneration is done with the help of Hash function.

The next is the Attribute Authority; it has a collection of secret keys for the owner's files. If any user wants to access a file in the cloud, they must send a request to the attribute authority for the SK of the respective file. The AA checks the authorization of the user and provide the SK. After getting the SK, the user is able to access the cloud. By using the SK they can only view the data on the cloud. Here, the advantage is the user can directly view the data on the cloud without downloading and decrypting it. So, any user who requires the file just for a reference can use this technique, though downloading the file for viewing purpose is eliminated. They can directly view it from cloud by using the SK. So here the downloading cost is reduced.

If any user wants to download or modify or update the file on the cloud they can send a Data Access Privilege request to the respective owner of the file. The owner checks the user authorization and gives the permission to download or update or modify the file based on their privilege. Now the user can download the file and do any necessary operations on the file.

Thus the design is simply efficient for processing, which it can be maintained under the Attribute based scheme in which it can be processed. The main use of the model is to successfully reduce the authorized user to access the cloud without any complexity. Thus security is highly achieved and the main advantage of this work is cost reduction. This can be done by DAP technique.

Thus only valid user can access the cloud, if any un-authorized user tries to access the file on the cloud by entering the wrong key or misuse the data it will be revoked.

The Figure 5 describes the flowchart of this research work. It describes six entities like Certificate Authority, Attribute Authority, Owner, User, TPA and Proxy. The CA and AA are additional entities added to this research work.

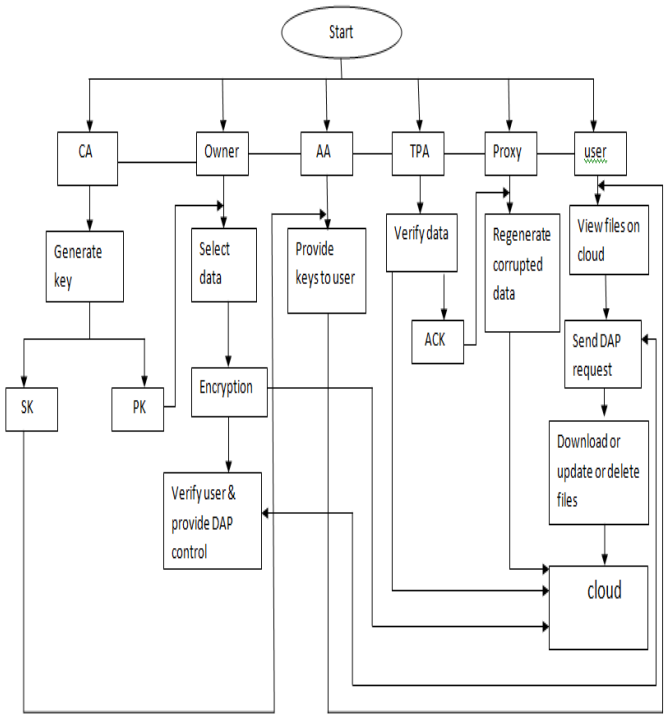


Figure 5 Flow Chart of the Proposed Model

4.2. Algorithm Used For Data Privacy

Attribute based scheme algorithm is used for data privacy. This algorithm includes three steps. They are key generation, encryption and decryption. The first step is key generation it is done with the help of CA. For that we have to find three large positive integers e, d and n.

The combination of (g, k) is the public key. It is distributed to the owner for data encryption. Private Key is (h, k) it is distributed to the user. Using the SK the user can view the files in the cloud.

The original message m is encrypted by performing the following operation

$$C=m^g \pmod k$$

Where c is the cipher text stored in the cloud.

Now, the original message m is decrypted by reversing the above operation, it is given below

$$C= (m^g)^h == m \pmod k$$

5.

RESEARCH ARTICLE

4.2.1. Distribution of PK after Checking Owner Authorization

Begin

1 CA checks owner authorization

2 if valid owner = True

3 then distribute PK

4 else

5 No distribution of PK

6 Continue step 1 to 5 to all the owners.

End

Key Generation

Begin

1 Choose two prime numbers i and j

2 compute k=i*j

3 compute totien t(k)= (i-1) (j-1)

4 Choose an integer g such that 1 < g < totient (k) and gcd (g, totient (k)) = 1;ie g ang totient (k) are co-prime.

5Compute value for h such that (h * g) % totient (k) = 1

End

From the above steps 1 to 5 we can find th PK and SK

Public Key is (g,k)

Private Key is (h,k)

Encryption

The original message m is encrypted by performing the following operation

$C=m^g \pmod k$

Decryption

Begin

1 AA checks the user authorization

2 if valid user = True

3 then distribute SK

4 else

5 No distribution of SK

6 The above step 1 to 5 is continue for all users

End

Now, the original message m is decrypted by reversing the above encryption operation, it is given below

$C= (m^g)^h \equiv m \pmod k$

Algorithm 1 Attribute based scheme algorithm

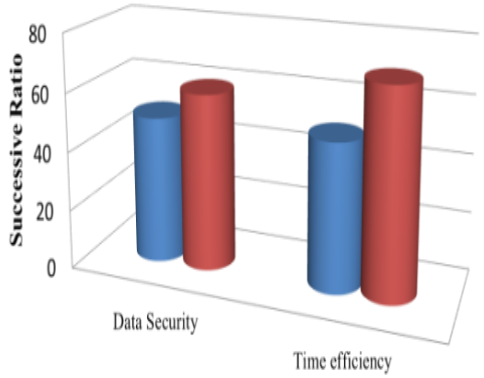
The algorithm used for data privacy is shown in above algorithm 1. By using this algorithm we can encrypt the data and stored it in cloud. Only authorized users can view the files in the cloud. So this algorithm is an efficient one when compared to others.

6. RESULTS AND DISCUSSION

The performance and evaluation of the two models are used to process under the different set of scenarios. This can be maintained and processed with the approximate ratio value of the existing and the proposed scheme through which it can be maintained.

The main scheme of the proposed and the existing work is based on the simple and efficient process of the scheme through which it can be maintained. Figure 6 shows the graphical representation the data security and time efficiency, it is proved that the data security and time efficiency is highly achieved in this research work.

By implementing the certificate and attribute authority the security of the data available in the cloud is highly achieved and by using a technique called Data Access Privilege, the data accessing time was reduced.



	Data Security	Time efficiency
Existing System	50	50
Proposed System	60	70

Figure 6 Comparison of Data Security and Time Efficiency with table

Figure 7 is used to display the security of data stored in the cloud server. The techniques used in existing system for data security is not efficient. Data leaking is still a main drawback in existing system, when compared to existing system, the proposed system is very efficient it use Attribute based scheme

RESEARCH ARTICLE

and also it implement the RSA algorithm. So here the security level of data is high.

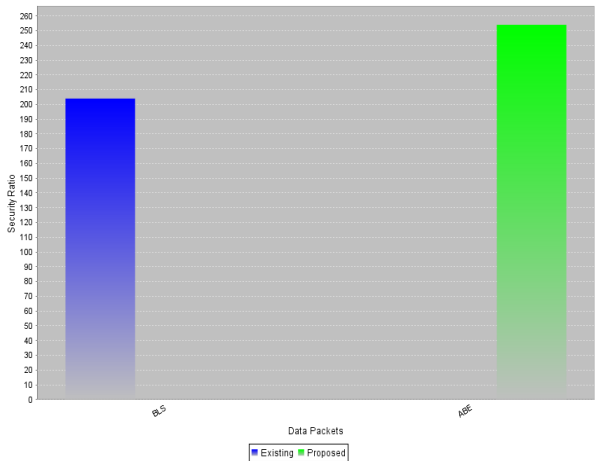


Figure 7 Comparison of Security of Data

Security is highly achieved by implementing CA and AA in the proposed modelling. The CA provides a PK to the owner after checking the owner authorization, only then the owner is allowed to access the cloud.

Like that CA provides SK of the respective owner to the AA. Any user who wants to access a particular owner file will request a SK to the AA. AA checks the user authorization and provides SK. By using the SK the user can only view the files of the respective owner. He is not allowed to download the file. If he want to download or modify the user needs to send a DAP request to the owner of the respective file.

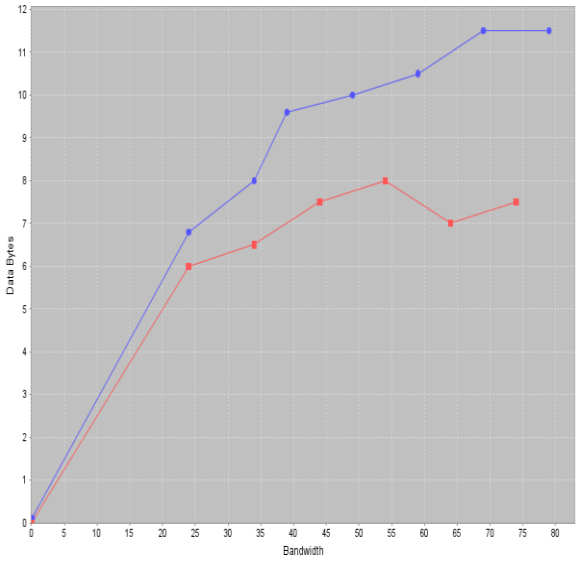


Figure 8 Comparison of Bandwidth

The comparison of bandwidth is shown in Figure 8. When compared to existing model, the bandwidth rate is efficient in this research work by implementing the Data Access Privilege Technique (DAP). After getting the SK from attribute authority the user can view the file from the cloud without downloading. So here the unnecessary downloading is avoided because for reference purpose they are not willing to download the file, they just like to have a glance of the file. If anyone wants to download or modify or update the file they have to send a DAP request to the respective owner.

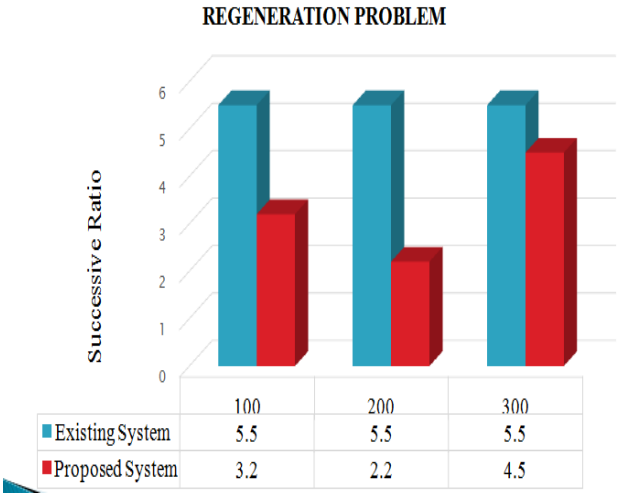


Figure 9 Regeneration Problem

The Figure 9 shows the regeneration problem of existing and this research work. The previous regeneration model is lacking to produce the accurate result. It depends on the owner of the file, if the owner goes offline then the work stops until the owner comes online. The owner has to regenerate the corrupted data. While the proposed work of the system produce the accurate result. This should be further maintained by the proxy regeneration code block system, the proxy can regenerate the corrupted data without the presence of the data owner. Thus the accurate rate of regeneration is achieved by the proxy in this research work.

7. CONCLUSION

The main problem faced by cloud users are data security and high cost. Attribute based scheme algorithm is used in this research work to provide high data security. It is achieved with the help of certificate and attribute authorities. By using the certificate authority the PK and SK is generated and distributed to owners and attribute authority. Only authorized users are allowed to access the files in the cloud. If any untrusted user tries to access the file by entering wrong keyword or misusing the data will be revoked. Another drawback overcome by this paper is cost overhead. By using a technique called DAP the unnecessary data downloading is eliminated, this will automatically reduce the cost. Thus, in this research work the main two problem are overcome by a simple and efficient way.

RESEARCH ARTICLE

REFERENCES

[1] W. Diffie and M. Hellman, "New direction in cryptography," *IEEE Information Theory*, vol. 22, no. 6, pp. 644-654, Sep. 1976.

[2] Q. Wang, C. Wang, J. Li, K. Ran, and W. Lou, ―Enabling Public Verifiability and Information Dynamic for Storage Security in Cloud Computing,‖ in the Proceedings of ESORICS 2009. Springer-Verlag, 2009, pp. 355–370.

[3] D. Boneh and X. Boeh, "Short signatures without random oracles, in *Proc. Annual International Conference on the Theory and Applications of Cryptographic Techniques*, 2004, pp. 56-73.

[4] Wang, Boyang, Baochun Li, and Hui Li. "Panda: public auditing for shared data with efficient user revocation in the cloud." *IEEE Transactions on services computing* 8.1 (2015): 92-106.

[5] Z. Liu, J. Li, X. Chen, J. Yang, and C. Jia, "TMDS: Thin-model data sharing scheme supporting keyword search in cloud storage," *Information Security and Privacy Lecture Notes in Computer Science*, vol. 8544, pp. 115-130, 2014.

[6] C. Liu, J. Chen, L. Yang, X. Zhang, C. Yang, R. Ranjan, and K. Ramamohanrao, "Authorized public auditing of dynamic big data storage on cloud with efficient verifiable fine-grained updates," *IEEE Transactions Parallel and Distributed Systems*, vol. 25, no. 9, pp. 2234-2244, Sep. 2014.

[7] M.S.Premalatha and Dr.B.Ramakrishnan "Green scheduling of Bag-of-tasks Applications in cloud data centre using green cloud simulator" Journal of Emerging technologies in web intelligence, vol.6, no.3, August 2014.

[8] B. Wang, B. Li, and H. Li,Oruta: "privacy-preserving public auditing for shared data in the cloud," in *Proc. IEEE International Conference on Cloud Computing*, 2012, pp. 293-302.

[9] Q. Wang, C. Wang, K. Ren, W. Lou, and J. Li, "Enabling public audit ability and data dynamics for storage security in cloud computing," *IEEE Transactions on Parallel and Distributed Systems*, vol. 22, no. 5, pp. 847-859, May 2011.

[10] Panda: Public Auditing for Shared Information with Efficient User Revocation in the Cloud Boyang Wang, Baochun Li, Member, IEEE, and Hui Li, Member, IEEE, transactions on service computing no:99 vol:pp year 2014.

[11] J. Yuan and S. Yu, "Efficient public integrity checking for cloud data sharing with multi-user modification," in *Proc. IEEE INFOCOM*, 2014, pp. 2121-2129

[12] Y. Zhu, G. Ahn, H. Hu, S. Yau, H.An, and S. Chen, "Dynamic audit services for outsourced storages in clouds," *IEEE Transactions on Services Competing*, vol. 6, no. 2, pp. 227-238, 2013.

[13] B. Wang, B. Li, and H. Li, "Knox: Privacy-preserving public auditing for shared data with large groups in the cloud," in *Proc. of ACNS*, 2012, pp. 507-525.

[14] Dr. J. Suganthi, Ananthi .J S. Archana," Privacy preservation and Public Auditing for cloud Data Using ASS", International Journal of Emerging Trends & Technology in Computer Science (IJETTCS), Volume 3, Issue 6, November-December 2014 PP: 242-247.

[15] B. Wang, B. Li, and L. Hui, "Panda: Public auditing for shared data with efficient user revocation in the cloud," in *Proc. IEEE INFOCOM*, pp. 2904-2912, 2013.

[16] D. Boneh and M. K. Franklin, "Identity-based encryptions from the wail pairing," in *CRYPTO'01. Springer-Verlag*, 2001, pp. 213- 229.

Authors

A.Nithya received her B.Sc Computer Science from Noorul Islam College of Arts and Science affiliated to Manonmanium Sundaranar University, Thirunelveli, India and MCA from St. Xavier's Catholic College of Engineering, affiliated to Anna University, Chennai. Presently she is a Research Scholar in Department of Computer Science and Research Centre, S.T.Hindu College, Nagercoil, India. Her Research interest includes Cloud Computing and Information Security.

B.Ramakrishnan is currently working as Associate Professor in the Department of Computer Science and Research Centre in S.T.Hindu College, Nagercoil. He received his M.Sc Degree from Madurai Kamaraj University, Madurai and received M.phil (Com. Sci) from Alagappa University, Karaikudi. He earned his Doctorate degree in the field of computer science from Manonmanium Sundaranar University, Thirunelveli. He has a researching experience of 29 years. He has twelve years of research experience, published more than 50 research articles in reputed international journal .His research interest lies in the field of Vehicular Network, Mobile Network and Communication, Cloud Computing, Ad-hoc Network and Network Security.

Resul Das received his BS and MSc. in Computer Science from Firat University in 1999, 2002 respectively. He received PhD degree from Electrical and Electronics Engineering Department in same university in 2008. He is an Assoc. Professor at the Department of Software Engineering of Firat University, Turkey. He has authored several paper in international conference proceedings and refereed journals, and has been actively serving as a reviewer for international journals and conferences. His current research interests include Knowledge Discovery, Web Mining, Complex Networks, Computer Networks, Information and Network Security.