An Efficient Key-Accumulation Cryptosystem for Cloud

Tanvi Agrawal, Ambuj Kumar Agrawal, S.K. Singh

***Abstract*: Cloud computing has started to gain extensive appreciation inside the corporate world as well, because it has given permission to access the required resource as Internet. The process of accessing and sharing of the resources is performed in a very virtual and protected way so that a general user is not aware of the task that is performed. In this paper, we aim to derive a mechanism to make data safe and control the access of the sensitive information over the cloud servers.**

***Index Terms*: Authorization, Cloud computing, Cryptosystem, Threats, Vulnerability.**

I. INTRODUCTION

These days there is an increase in the importance of cloud computing and there is a rapid growth towards the attention towards the scientific and industrial community day by day. It enables ubiquitous, convenient, on-demand accessing of network for the sharing of pool of configurable computing resources which are able to be easily planned and released with minimum management efforts and interaction of service provider [1]. A growing subpart of computer system is safeguarding the security of network, and most commonly data fortification is cloud computing security. Wide collection of plans, technologies as well as controls which are deployed to shield the given resource, functions and the related infrastructure comes under this domain which works for the cloud computing [14]. Cloud computing data security should neither mystified with protection applications offered projects which are generally "cloud- based". The capacity of the cloud security stretches over all the main three cloud computing service delivery models and is deployed in any of the four cloud deployment models (private, public, hybrid and community cloud) and contains the five fundamental properties of the cloud. It is this reach of the extent of security in the cloud that forms it very important and at the same time much complex [3]. The large extent of the security now has multiple surfaces including but not only concerned to safety related to application, transmission of data, storage of data, authentication and authorization, virtualization of network and physical hardware. Several issues are raised with this side of work. This work gives a solution for the questions concerned with the application and security of data which mainly falls in the SaaS layer [9].

II. LITERATURE REVIEW

Safety of data stored in cloud is an encouraging matter of research, which is already explained in lots of research and academics publications.

Molnar and Schechter [1] have done the investigations about the pros and cons of the storage and process of data in regards of the data security which is provided by a general public cloud service provider. They have given the information regarding innovative forms of technical, organization, as well as jurisdictional ultimatum which results from the utilization of cloud, the have presented a selected view of countermeasures as well.

Akhawe et al [2] [12] conferred diverse threat as well as attack models which could be utilized for exploring formally the incursions under the cloud computing framework. Nevertheless, the attitude was confined for the HTTP for the communication process in this model the accountability of the application layer messages was not taken into consideration.

Youngmin Jung et al. [3] has given a proposal for an adaptive protection management sculpt for cloud computing environment. They recommended Role Based Access Control (RBAC) method, which is a malleable retrieval algorithm for choosing the control of accessing the resources. Their proposed approach finds out vigorously level of security and control of access for the given resources [15]. But this frame work is laid upon the proposal of the security depends on the decision of cloud service providers and concerned with the several types of resources arrived at the security level and the level of access control. The given framework is focused towards the commitment of the client and the services provided with the resources which are arrived at different security levels.

Extensible Markup Language (XML) Signature wrapping attacks were demonstrated by Gruschka and Lo Iacono[4]. These could be done to assail Amazon's EC2 facilities. The description of vulnerability for that assist an assistant to execute operation on the cloud control has been given. This is used during possession of when a genuine user passes a message from the signed control.

Manal and Yunis [5] delineated six security considerations for cloud computing namely data ownership, resource sharing compaction and data encryption favoring the speed, denial of services, loss of data because of technical breakdown and attackers moving after contributor or the application.

Revised Manuscript Received on December 22, 2018.

Tanvi Agrawal, Amity University, Lucknow, India.
Dr. Ambuj Kumar Agrawal, Teerthanker Mahaveer University Moradabad, India.
Prof (Dr.) S. K. Singh, AIIT, Amity University, Lucknow, India

They also proposed a theoretical model for overcoming these issues through policy management. For example, they proposed for the classification of the policies based upon the several types of data, for example Client financial data, scholarly property and so on. But the formation and the managing of these given policies are unmanageable and ineffective practically [6]. Though most of the reliability matter in the previous time was because of ineffectual strategies, allowing a competent proposal is next to impossible. Approaches can only be an additive step but as long as the security proposal is not proficient, although most tactically formed safety measures will be lacking.

Raj et al [7] promoted the process of resource isolation in order to guarantee shielding of data while processing, with the help of extrication processor caches inside the virtual machines, and the isolation of the virtual caches from the hypervisor cache is done here.

III. HOW CLOUD COMPUTING WORKS

A. *Figures and Tables*

When we talk about cloud computing it simply works as a metaphor of the internet [10]. In general terms it refers to the sharing of data, information and resources through the network over the internet. If we talk about cloud computing here data is stored on the virtual servers maintained by the service providers. Three main categories of cloud computing services can be given as a Rackspace with SaaS on the top PaaS in the middle and IaaS at the bottom [16]. SaaS is at the top because its primary work is to interact with the softwares hosted over the cloud. It doesn't have any work with the infrastructure on which it is actually working. PaaS is used for the creation and deployment of the applications. IaaS is used for providing infrastructure to the cloud.

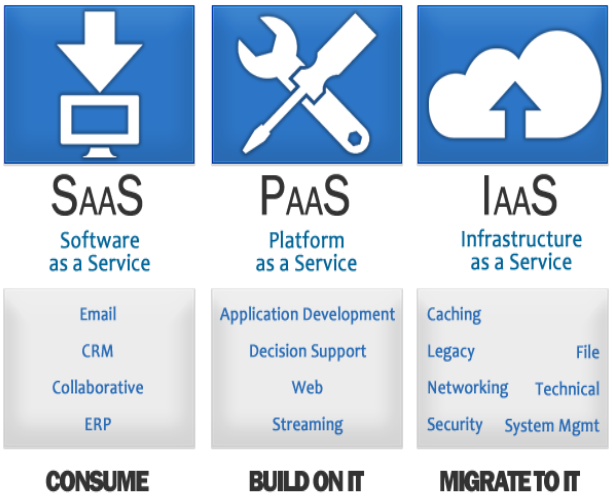

Fig 1: Figure depicting three layers of cloud

(i) Software as a Service (SAAS): It is the topmost layer of the cloud architecture. It is the layer which is vastly utilized by the cloud computing users. It provides the priced as well as free applications, programs and softwares for the users. This layer is largest and the most accessible layer for the cloud computing. This layer is used every time we use Google Pay, the App Store, Dropbox or any cloud-based software. Office 365 is the perfect example of SaaS.

(ii) Platform as a Service (PaaS): It acts as the middle layer of cloud computing which is used for development by web developers. This layer of cloud computing is used by the developers and programmers to create applications, programs, software etc. PaaS works by renting hardware from IaaS to build software, applications, programs etc. Generally, the PaaS space is being sold by the providers to the consumers for the resource allocation [17].

(iii) Infrastructure as a Service (IaaS): This layer is the bottommost layer used for the hardware, network equipment and web hosting servers. This layer is used by companies to rent out to consumers. This layer is comprised of all the hardware resources which is needed to make cloud computing possible. It is physical hardware layer.

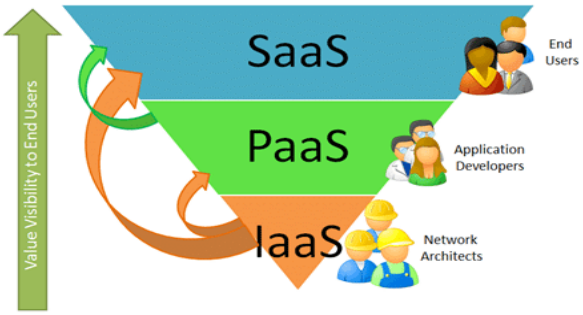

Fig 2: Rackspace architecture of three layers of cloud

IV. ACCUMULATION CRYPTOSYSTEM

The chief design goal of this system is assisting the owner of data for achieving superior control to access files saved on Cloud computing data Servers [8]. Basically, in the system the data owner is enabled to implement an exclusive accessing framework over every end user, who is responsible for designating the set of records which precisely whose access permission is granted to the user. The user here craves for averting Cloud computing data to bring them in a position for learning the data file contents as well as user access dispensation records. Along with this, the suggested plan must be planned in such a way to gain data reliability aims like user answerability and is able to perform basic executions such as user grant/revocation as a common one-to-many transmission process will be required.

Each design goals must be gained proficiently in such a manner that the given framework is extensible [9]. Accumulation cryptosystem is used to achieve secured access control of the given cloud outsourced data. An accumulation cryptosystem comprises of efficient Key Accumulation Cryptosystem algorithm. The owner of data is responsible for establishing the commonly available parameters with the Setup and forms a general public/private key and combine it with the help of the KeyGen.

The encryption of this confidential file is done with the help of DES algorithm. The data proprietor will utilize master-secret shown with accumulated clarification key for a group of records. The produced keys can be transferred to the representatives in a safer manner (with the help of secured e-mails or secured parameters). Now, each user with accumulated key would be able to do the decryption of the data file and can download it for its use. Figure 1 is used to show the structural working of the given framework. In the given framework, the outline of two general purpose individuals are taken as an example, in which first user have the requirement of uploading records on the clouds, while the second user needs downloading of the files from the cloud. During the uploading of data on the cloud is done by first user, firstly the encryption of data is done by using DES algorithm and then the uploading of records is being done on clouds. The particularly initiated private key for every document is shown as the acceptance of the uploaded file for the user-1. When user-2 want to easily have the permission of the access of the files of user-1 the requests is made by user-2 to the user-1 for sharing the accumulation key of the particular desired data files, with the help of which the download encrypted files are decoded with the help of fixed magnitude accumulation key. Now the user-2 is able to have the access all the files with the help of the accumulation key. With the help of an efficient Key-accumulation cryptosystem the constant size cipher text is produced in such a way that a systematic and productive legation of rights of decrypting a set of cipher text is achievable. While registering firstly the public key is created and then we login for the specific page. If we are valid user then we have the permission to upload as well as download the same file. If other person wants to retrieve the data then a valid public key is needed from a specified user to decrypt the downloaded file

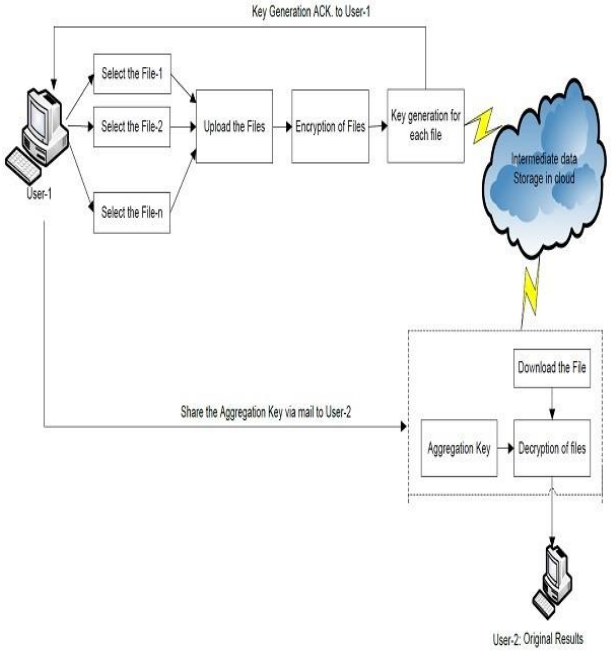

Fig 3: System Architecture

The data proprietor is responsible for the establishment of the general public system parameter with the help of Setup and gives the desired key and coalesce with the help of KeyGen. The encryption of confidential data is done using DES algorithm (data encryption standard). The proprietor of records will utilize the master-secret to get accumulation decoding key required for a set of records. The induced keys are transferred to the representatives in a safe manner (with the secured e-mails or with secured devices). Now, every user having that accumulation key is now be able to do the decryption and downloading of the records. The efficient key is contained in accumulation capability that contains the transferring, key accumulation generation and downloading methodology. In the upload part, the uploading permission of a number of files is granted to the sender with the help of private key. With the amalgamation of the public and private key the encryption of record information is done using the Data Encryption Standard (DES) algorithm and the data whose encryption is done is saved inside the cloud. The effective key accumulation method is employed for the combination of the private key and in the generation of the definite sized key known as, the accumulation key. The receiver is able to download the file in the download module, with the help of accumulation key which is send by the sender. In case a valid accumulation key is found, the user is allowed to download the data file. In the meantime, the downloading of file is done by the receiver, the verification of accumulation file is done and private keys are used for the extraction of the keys. DES algorithm is used for the decryption of the file[11]. The main aim the given proposal is to generate safer data depository and an enhanced form of information splitting inside cloud computing. In this new system the improvement of data sharing is done in cloud with the help of accumulation keys. The main thing to be considered in cloud is data. The sincerity for the data stored in cloud is also provided by the given system. In the process of key accumulation, a cryptosystem a new method is provided in the improvement of the sharing of data in cloud. The creativity is that one is able for accumulating a group of secured keys and combine them as a single accumulation key which is used to decrypt the message. All the set of files residing on the cloud are supposed to be found in according to the encryption standards. The Advanced Encryption Standard (AES) algorithm is mainly considered for the encryption and decryption of the files for saving the files inside the cloud. The data files which are securely stored inside the cloud storage and as long as it is required the user is able to use it from the cloud. As all the personalized files are saved, the safety needed to be given to the files for storage inside the cloud [12]. The main idea of key accumulation cryptosystem is to perk up the sharing of data by improving the safekeeping when different records are divided along the multiple number of cloud users. The novelty in this Key Accumulation Cryptosystem is that a user is able accrue a group of secret keys and form it as only found accumulation key. The owner of the given key is able for releasing this single key to any user which tries to have the access of the data saved inside the cloud.

User is allowed to have the ability for sending a single key to share a multiple number of files instead of sharing multiple keys to the user [13]. In the Setup section, the data proprietor accomplishes the setup stage for an un-trusted account on server. Only implicit safekeeping parameters are accepted by the setup algorithm. The pair of public keys or the master key (pk, msk) is produced by KeyGen segment when executed by data proprietor. The key for encrypting and decrypting the the files are needed to be generated. Anybody who desires to transfer the data which is encrypted, does the execution of the Encrypt segment. Encrypt (pk, m), which is an algorithm for encryption. Here input is given as pk and a message m is shown as public parameters. The encryption of message m is done by the algorithm and ciphertext C is produced in a way that a user only who is having a corresponding key will only be permissible for the decryption of ciphertext C.

Input= public key pk, message m

Output = ciphertext C.

The architecture of key Accumulation Cryptosystem is portrayed in the Figure 2.

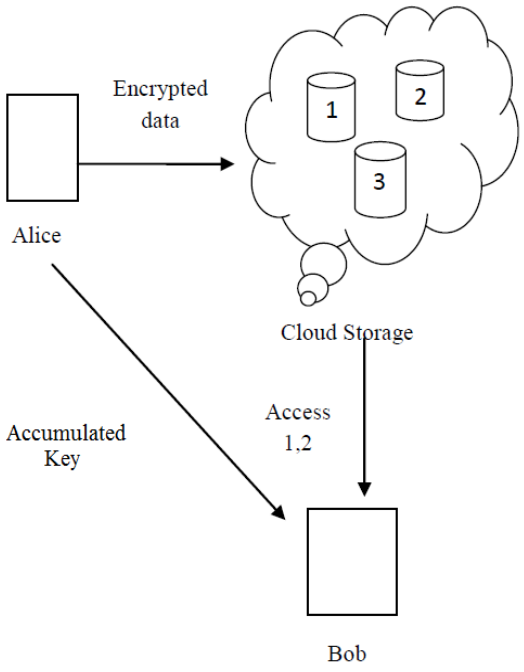

Fig 4: Architecture of Key Accumulation Cryptosystem

Data proprietor executes the Extract Phase for providing the decryption privileges for a consolidate group of classes of ciphertext to another cloud users.

1. Input = secret key k.
2. Outputs= accumulation key denoted by kS.

The candidates which have the authority of decryption, are responsible for the execution of the Decrypt Phase. Decrypt (kS, S, i, C), k is taken as input key by the decryption algorithm, and C is taken as a ciphertext. The ciphertext in the set S is denoted by i.

1. Input = kS and the set S
2. Outputs = m if i element of S

The group of notifications whose decryption is be taken and the related accumulation key is applied for the decryption of the files and the data decrypted files are constructed as output.

V. PROPOSED ALGORITHM

These applications of the algorithm have the steps as given below: Step1. On the cloud server the setup and creation of account is done to make the sharing of data possible over the cloud. The generation of this account is done by data owner by its own. Step2. The production of public key is done by KeyGen algorithm. The data proprietor is responsible for producing a public secrete key for the encryption of the data over the cloud. It furthermore forms an accumulation key to make the use of the block of ciphers of a limited size. Step3. Data provided by the data owner is encrypted using a secret key. Then this encrypted data is distributed among the cloud. Step4. Accumulation key is used for the extraction of a specific block of cipher from the cipher file keeping the encrypted data same and secure for the general use.

Step5. Finally, when the user wants to use the encrypted data is decrypted with the help of secret key which is used for encryption.

VI. CONCLUSION

This work gives a clear remedy for the questionnaire concerned with the application and security of data which is under the SAAS layer of cloud.

Our given proposal of framework can be able to work as an supreme solution for having control access of data in the growing environment of cloud computing. On the other hand, the currently prevailing access control algorithms in concerned areas are either have lack of adaptability and fine-grained, or does not gives appropriate evidence of data confidentiality.

ACKNOWLEDGEMENT

While writing this paper I would like to thank my guide Dr. S.K. Singh and my co-guide Dr. Ambuj Kumar Agrawal.

REFERENCES

1. Molnar, D. and Schechter, S. “Self-hosting vs. cloud hosting: Accounting for the security impact of hosting in the cloud”, In Proceedings of the Ninth Workshop on the Economics of Information Security (WEIS), 2010.
2. Akhawe, D., Barth, A., Lam, P. E., Mitchell, J.C. and Song, D. “Towards a formal foundation of web security”, CSF, pp. 290-304,2010.
3. Youngmin, J. and Mokdong, C. “Adaptive security management model in cloud computing environment”, In the 12th International Conference on Advanced Communication Technology (ICACT), pp 1664-1669, 2010.
4. Gruschka, N. and Iacono, L. “Vulnerable Cloud: SOAP Security Revisited”, In Proceedings of the IEEE International Conference on Web Services, IEEE Computer Society, pp. 625-631, 2009.
5. Manal, M.Y. “A ‘cloud-free’ security model for cloud computing”, In the International Journal of Services and Standards, Vol.5, No.4, pp. 354-375, 2009.
6. Tsai, W., Jin, Z. and Bai, X. “Internetware computing: issues and perspective”, In the Proceedings of the First Asia-Pacific Symposium on Internetware, ACM, Beijing, China, pp. 1-10, 2009.
7. Raj, H., Nathuji, R., Singh, A. and England, P. “Resource management for isolation enhanced cloud services”, In proceedings of the 2009 ACM workshop on Cloud computing security, Chicago, Illinois, USA, pp. 77-84, 2009.

8. Motawie, Rola, Mahmoud M. El-Khouly, and Samir Abou El-Seoud. "Security Problems in Cloud Computing." International Journal of Recent Contributions from Engineering, Science & IT (iJES) 4.4 pp 36-40, 2016.
9. Khan, Minhaj Ahmad. "A survey of. security issues for cloud computing." Journal of Network and Computer Applications 71 pp 11-29, 2016.
10. Agarwal, Ambuj. "Implementation of Cylomatrix complexity matrix." Journal of Nature Inspired Computing 1 (2013).
11. S. Shukla, A. Lakhmani and A. K. Agarwal, "Approaches of artificial intelligence in biomedical image processing: A leading tool between computer vision & biological vision," 2016 International Conference on Advances in Computing, Communication, & Automation (ICACCA) (Spring), Dehradun, 2016, pp. 1-6.doi: 10.1109/ICACCA.2016.7578900
12. Agrawal, Tanvi, Ambuj Kr Agarwal, and S. K. Singh. "Study of Cloud Computing and its Security Approaches."
13. Saleem, Ambreen, and Ambuj Kumar Agarwal. "Analysis and Design of Secure Web Services." Proceedings of Fifth International Conference on Soft Computing for Problem Solving. Springer Singapore, 2016.
14. D. Sehgal and A. K. Agarwal, "Sentiment analysis of big data applications using Twitter Data with the help of HADOOP framework," 2016 International Conference System Modeling & Advancement in Research Trends (SMART), Moradabad, 2016, pp. 251-255. doi: 10.1109/SYSMART.2016.7894530 URL: http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=7894530&isnumber=7894471
15. Sehgal D., Agarwal A.K. (2018) Real-time Sentiment Analysis of Big Data Applications Using Twitter Data with Hadoop Framework. In: Pant M., Ray K., Sharma T., Rawat S., Bandyopadhyay A. (eds) Soft Computing: Theories and Applications. Advances in Intelligent Systems and Computing, vol 584. Springer, Singapore.
16. S. Fatima, A. Agarwal and P. Gupta, "Different approaches to convert speech into sign language," 2016 3rd International Conference on Computing for Sustainable Global Development (INDIA Com), New Delhi, India, 2016, pp. 180-183.
17. Agarwal, T., Agarwal, A.K., Singh, S.K.: Cloud computing security: issues and challenges. In: Proceedings of SMART-2014, pp.10–14.