SECURE DISTRIBUTED DATA STORAGE IN CLOUD COMPUTING USING ENCRYPTION & DECRYPTION

Richa Kunal Sharma
Research Scholar, Career Point University, Kota

ABSTRACT- **Achieving cloud computing empowers numerous paths for Web-based service offerings to meet differing needs. However, the data security and privacy has become a critical issue that restrain many cloud applications. One of the major concerns in security and privacy is caused by the fact that cloud operators have chances to reach the sensitive data. This concern dramatically increases users' anxiety and reduces the adaptability of cloud computing in many fields, such as the financial industry and governmental agencies. It is focuses on this issue and proposes an intelligent cryptography approach, by which the cloud service operators cannot directly reach partial data. The proposed approach distribute the file and separately stores the data in the distributed cloud servers and blob. The proposed scheme is entitled Distributed Data & Storage (D2S) model, which is mainly supported by our proposed algorithms, including Distributed & Store Algorithm (DS). Our experimental evaluations have assessed both security and efficiency performances and the experimental results depict that our approach can effectively defend main threats from clouds and requires with an acceptable computation time.**

Keywords: Encryption & Decryption Algorithm, Cloud Computing,DotNet,SQL

1. INTRODUCTION

According to U.S National Institute of Standards and Technology (NIST), ―Cloud Computing is a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or cloud provider interaction[1]. In simple words, Cloud Computing is the combination of a technology, platform that provides hosting and storage service on the Internet [2].In such an environment users need not own the infrastructure for various computing services. In fact, they can be accessed from any computer in any part of the world. This integrates features supporting high scalability and multitenancy, offering enhanced flexibility in comparison to the earlier existing computing methodologies. It can deploy, allocate or reallocate resources dynamically with an ability to continuously monitor their performance [1]. Moreover, cloud computing minimizes the capital expenditure. This approach is device and user-location independent. Main goal of the cloud computing is to provide scalable and inexpensive on-demand computing infrastructures with good quality of service levels [3.4].

"Cloud Computing refers to **manipulating, configuring,** and **accessing** the applications online. It offers online data storage, infrastructure and application. "

A. DISTRIBUTED DATA AND STORAGE

As one of the momentous technologies used in cloud computing, the distributed storage has empower the mass remote data storage via Storage-as-a-Service (STaaS) service model. This cloud service model has broadly become an acceptable approach in big data along with the development of Web services and networks [6,15]. Several cloud vendors have given attractive storage service offerings that provide huge and scalable cloud-based storage spaces for users, such as Amazon, Dropbox, Google Drive, and Microsoft's OneDrive [10,14, and 22]. However, the security issue caused by the operations on cloud side is still an obstruction of using SaaS for enterprises [2, 7,9,11 and 32]. Many cloud users concern about their sensitive data to which the cloud operators have the access [12, 29]. This matter embarrasses abreast implementations of SaaS, even though many prior researches have addressed this field [21, 26, 30, and 17].

Moreover, Mass Distributed Storage (MDS) has been explored to scale up the data storage size in recent years [18,27]. The high level performances of the scalable computation are considered benefits of implementing MDS. One aspect that needs improvements is to secure distributed data storage [4], in which the threats come from a variety of sides. The distributed storage manner can result in more chances of malicious attacks or abuse activities [5, 16], such as attack during data transmissions. Currently, the unexpected operations can also occur at the cloud server side, which are mainly constrained by laws and regulations. Meanwhile, it is difficult to balance functionality and security performances due to cost concerns [33]. Therefore, it is a challenging issue to efficiently secure distributed data in cloud systems, since the risks deriving from different network layers are hardly fully addressed [20,25] .

This paper focus on the problem of cloud operators abuse issues and attempts to avoid cloud users' data release from cloud servers. We propose an intelligent cryptography approach, named Distributed Data & Storage (D2S) model that is designed to obtain an efficient MDS service, as well as high level security protections. Our proposed mechanism aims to encrypt all data and distributed &store the data to the different cloud servers and blob without causing big overheads and latency & decrypt data and send data on user demand. Fig. 3 illustrates the architecture of D2S model

As shown in Fig.3 user's data are assessed. The solid arrow lines represent the data splits. The broken arrow lines represent the operational directions of the data and data storage. Normal data will be assigned to a single cloud server Cloud B. Meanwhile, the data with sensitive data are split into two parts that are assigned to Cloud A and blob. This process is mainly supported by our proposed algorithm Distributed and Storage (DS) Algorithm, which is designed to split data and store in secure manner.

The importance of the our proposed mechanism is that we provide an adaptable approach for those enterprises that intend to use SaaS but require a high level data storage security, such as the financial service industry. The main problem solved by our proposed scheme is preventing cloud providers from directly reaching users' original data. The main contributions of this paper are twofold:

□ We propose a novel cryptography approach for delivering mass distributed storage by which users' original data cannot be directly reached by cloud operators. The proposed method is an effectual cryptography means for defending malicious activities occurred on the cloud server.

□ We propose an efficient data split mechanism that does not produce big overheads, as well as ensures data output on user demand.

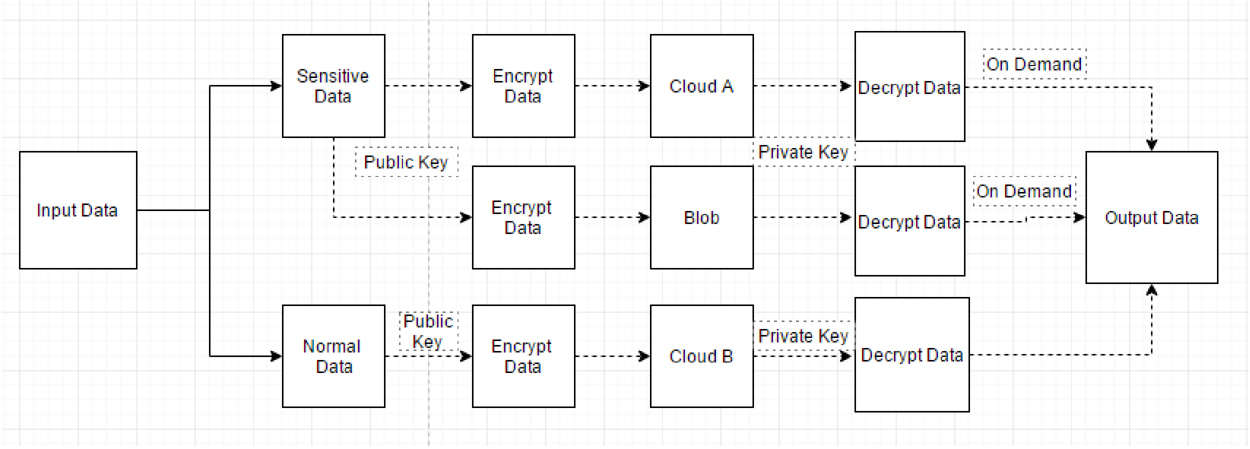

Fig. 1 Distributed Data and Storage (D2S)

II. RELATED WORKS

Various classical algorithms such as Alternative Data Distribution (AD2), Secure Efficient Data Distributions (SED2) and Efficient Data Conflation (ED Con) algorithms hemomorphic , encryption, Cryptographic File Systems. Verifiable computation, QCMC model and multiparty computation have been adopted for secure Data Storage in cloud computing. We present here a review of only some latest methods of Data storage. For the sake of completeness and clarity, certain older methods have been discussed based on which newer methods have been suggested. Also, methods for feature selection in unsupervised learning are studied and discussed.

YibinLia ,Keke Gai b , LongfeiQiu c , MeikangQiu b , Hui Zhao [31] proposed a Implementing cloud computing empowers numerous paths for Web-based service offerings to meet diverse needs. However, the data security and privacy has become a critical issue that restricts many cloud applications. One of the major concerns in security and privacy is caused by the fact that cloud operators have chances to reach the sensitive data. This concern dramatically increases users' anxiety and reduces the adoptability of cloud computing in many fields, such as the financial industry and governmental agencies. This paper focuses on this issue and proposes an intelligent cryptography approach, by which the cloud service operators cannot directly reach partial data.

AlbugmiMadini . Alas Safi Robert Walters &Gary Wills [19] proposed a data security that increased use of cloud computing for storing data is certainly increasing the trend of improving the ways of storing data in the cloud. Data available in the cloud can be at risk if not protected in a rightful manner. This paper discussed the risks and security threats to data in the cloud and given an overview of three types of security concerns.

On the other hand, Feng-Qing Zhang, Dian-Yuan Han have discussed a High availability, high fault tolerance and high efficiency accesses to Internet based cloud data centers where failures are normal rather than exceptional are significant issues, and are often considered more valuable than high performance. This paper presents a security module in cloud computing and introduces agent to the data protection. There are still some studies to be done in the future. For instance, further reducing the user waiting time, speeding up data access, and further increasing data availability. It is also planned to improve agents ability to satisfy the special demands of cloud computing. More verification should be done [23].

Sara Ibn El Ahrache , Hassan Badin , Parisa Ghodous , AbderrahmaneSbihi [24] suggest a The corresponding security of a distributed computing plan is a disputable matter that might be abating its reception

Abdelali El Boucht, Samir Bahsani and Tarik Nahhal [13] proposed a method of CaaS included the privet cloud open stack platform. CaaS secures sensitive data across private, hybrid and multi-tenant public clouds while extending customers' control of the encryption keys. In this paper, we have proposed a new hybrid architecture Included the private Healthcare cloud Open Stack platform. Which is designed to deploy IaaS infrastructure and provide tools for creating and managing VMs on top of existing resources and we implement our CaaS model based on encryption algorithms.

Jiawei Han, Yanheng Liu, Xin Sun, LijunSong[33] proposed a method which is QCMC model proposed in this paper is a model of effectively enhancing users' data and privacy security in mobile cloud computing environment through quantum cryptography technology.

M.B. Gawali and R.B Wag suggest a method that define a Cryptographic File Systems have been used to provide data storing with privacy. However, they do not appear in cloud estimations since it is part of user's VM installation. Although most privacy solutions use regular cryptography algorithms to provide confidentiality for persisting data, there are more elements to be considered when estimating the extra overhead of such solutions in a cloud environment. In doing so, this paper presented a mathematical model for extra CPU estimation when using Cryptographic File Systems. The model considers three main factors as essential in the overhead calculation: (a) the CPU load for encrypting and decrypting the data flow, (b) the memory size of the host machine, and (c) the throughput difference between raw in disk Operations and in-memory operations. The validation shows the behavior of CFSs considering the aspects explored in the model. Yet, it was possible to use the experimented values of CPU load, processing time, And workload size for fitting the model's variables. The fitted model was used to estimate the overhead of a CFS hosting files of an application execution (based on Big Data operations) and the model predictability accuracy was close to 90%. As future experiments specialized file systems will be considered in order to investigate the best mechanism for data privacy storage for cloud computing, taking into account not only the throughput but also the cache hierarchy, synchronization mechanisms and different cryptography algorithms [28].

Sushil Kr Saroj, Sanjeev Kr Chauhan, Aravendra Kr Sharma, Sundaram Vats [8] presented a new approach which provides security for data outsourced at CSP. Some approaches are given to secure outsourced data but they are suffering from having large number of keys and collusion attack. By employing the threshold cryptography at the user side, we protect outsourced data from collusion attack. Since, DO stores its data at CSP in encrypted form and, keys are known only to DO and respected users group, data confidentiality is ensured. To ensure fine-grained access control of outsourced data, the scheme has used capability list. Public key cryptography and MD5 ensure the entity authentication and data integrity respectively. Public key cryptography and D-H exchange protected the data from outsiders in our approach. No of keys (because in threshold cryptography, there is a single key corresponding to each group) have reduced in the proposed scheme.

III. METHODOLOGY

The research methodology adopted to conduct the proposed research is discussed here. Currently, some steps have already been completed. Rest will be followed as per the sequence discussed here. The entire project work and research can be divided into steps as follows:

Step 1: Literature Review

- Make a list ofrelated to cloud computing.
- Select article according to significance of work, refereed frequency and interest.
- Sort and manage articles according following tips

o Alternative Data Distribution
o Secure Efficient Data Distributions
o Efficient Data Conflation
o Cryptographic File Systems
o QCMQ Model.

- Filter the lists according to interest, availability, relevance in current technical scenario ease of understanding etc.
- Summarize each article as a findings and drawbacks.

Step 2: Identifying research gaps

According to Step 1, list all shortcomings which have not been addressed yet in the literature, or need more formal treatment and further research. List these research gaps. To identify the research gaps, a practical implementation of existing techniques is performed and the experiments on data are done to compare.

Step 3: Formulation of objectives

Identify few coherent objectives from these gaps so that a problem can be formulated.

State the objectives in quantifiable form. The objectives are:

- Design an algorithm, preferably through new initialization technique.
- Design a technique for divide the data and separately store in distributed cloud server.
- Send data on user demand.

Step 4: Design and Implementation of Algorithms

Design the algorithms as per set objectives. Construct theoretical proofs and claims (Hypotheses). Implement the designed algorithms through appropriate software .

Step 5: Data Preparation and Testing

Select real life data and construct own document corpus from blogs to test the Proposed algorithms. Test against the hypotheses set. Also, test other existing works and record The generated output.

Step 6: Analysis of Results and Comparison

The results are validated against the hypotheses. Also, Also, the results from existing

Algorithms are compared against proposed ones and comparison computation time was shorter than current active approaches. Future work would address securing data duplications in order to increase the level of data availability since any of data send on user demand.

IV. IMPLEMENTATION

The characteristics of this work are that The computation time was shorter than current active approaches, focused on the problem of the cloud data storage and aimed to provide an approach that could avoid the cloud operators reaching user' sensitive data. We proposed a novel approach entitled as *Distributed Data and Storage {D2S}* model. In this model, we used our proposed algorithms Distributed & Store Algorithm {DS} algorithm.

Majority of proposed work to be implement using RSA Algorithm and cloud base security using privet key and public key.in this approach we use cloud public key for encryption and privet key for decryption. Store data in different cloud storage based on data sensitization. We use cloud blob storage also to store sensitive data. It will help to maintain data and size of database and sufficient database management. This method maintain relationship between cloud data using unique key relationship. Process of Data Security Partitioned Storage is to when data will send on user demand. And data has been store in SQL injection secure .the computation time is shorter than current active approach .The main challenge is to split sensitive data and normal data and store for security purpose. Using blob is part of cloud server to store sensitive data.

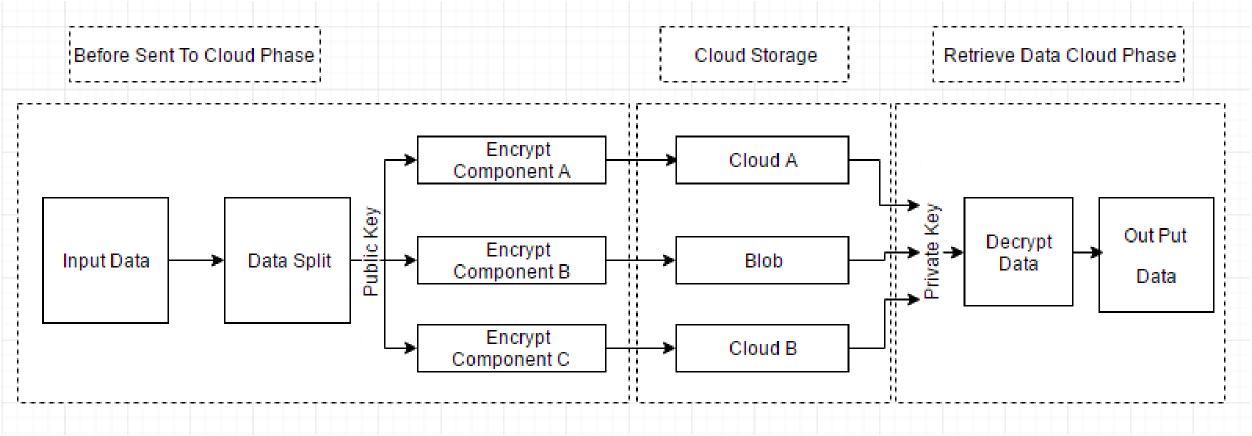

Fig. 2 Workflow structure of splitting data packets in the Distributed data & Storage Process

After identifying the research gaps in the field of Data Splitting, following objectives are formulated

- Design an algorithm based on RSA Algorithm. A proper formulation of objectives function that split data and store in distributed cloud server.
- Design a technique for secure data using encryption and decryption with public and privet key support.
- Data split into sensitive data & normal data. Sensitive data stored in cloud server and blob and normal data stored in cloud server.
- Propose a cryptography approach for delivering mass distributed storage by which users' original data cannot be directly reached by cloud operators.
- Design an efficient data split mechanism that does not produce big overheads, as well as ensures data output on user demand.

V.CONCLUSION

This integrates features supporting high scalability and multitenancy, offering enhanced flexibility in comparison to the earlier existing computing methodologies. It can deploy, allocate or reallocate resources dynamically with an ability to continuously monitor their performance . Moreover, cloud computing minimizes the capital expenditure. This approach is device and user-location independent. Main goal of the cloud computing is to provide scalable and inexpensive on-demand computing infrastructures with good quality of service levels.

REFRENCES

[1] Peter Mell, Timothy Grance, ―The NIST Definition of Cloud Computing‖, Jan, 2011. http://docs.ismgcorp.com/files/external/Draft-SP-800-145_cloud-definition.pdf

[2] Harjit Singh Lamba and Gurdev Singh, ―Cloud Computing-Future Framework for e-management of NGO's‖ IJoAT, ISSN 0976-4860, Vol 2, No 3, Department Of Computer Science, Eternal University, Baru Sahib, HP, India, July 2011.

[3] Dr. Gurdev Singh, ShanuSood, Amit Sharma, ―CM-Measurement Facets for Cloud Performance‖ IJCA, , Lecturer, Computer science & Engineering, Eternal University, Baru Sahib (India), Volume 23 No.3, June 2011

[4] Joachim Schaper, 2010, ―Cloud Services‖ 4th IEEE International Conference on DEST, Germany

[5] L.M. Vaquero, L. Rodero-Merino, J. Caceres, and M. Lindner, 2009, A break in the clouds: towards a cloud definition, SIGCOMM Comput. Commun. Rev., v. 39, n. 1, p. 50-55

[6] V. Chang , M. Ramachandran , Towards achieving data security with the cloud computing adoption framework, IEEE Trans. Serv. Comput. 9 (1) (2016) 138–151

[7] C. Chen , C. Zhang , Data-intensive applications, challenges, techniques and technologies: A survey on big data, Inf. Sci. 275 (2014) 314–347 .

[8] Sushil Kr Saroj; Sanjeev Kr Chauhan; Aravendra Kr Sharma; Sundaram Vats 2015 IEEE International Conference on Computational Intelligence & Communication Technology, Pages: 202 - 207

[9] K. Costa , L. Pereira , R. Nakamura , C. Pereira , J. Papa , A. Falcão , A nature-inspired approach to speed up optimum-path forest clustering and its applica- tion to intrusion detection in computer networks, Inf. Sci. 294 (2015) 95–108

[10] L. Darrell, Unlimited cloud storage at amazon.com, inc on black friday, Url = http://www.bidnessetc.com/58232-unlimited-cloud-storage-at-amazoncom- inc- on- black- friday/ .

[11] Y. Ding , Y. Hu , K. Hao , L. Cheng , MPSICA: An intelligent routing recovery scheme for heterogeneous wireless sensor networks, Inf. Sci. 308 (2015) 49–60 .

[12] “Introduction To Cloud Computing”,http://w.w.w.priv.gc.ac.

[13] Abdelali El Bouchti, Samir Bahsani , Tarik Nahhal , Encryption as a service for data health care cloud security, 2016 Fifth International Conference on Future Generation Communication Technologies (FGCT), pafes:48-54.

[14] K. Gai , L. Qiu , H. Zhao , M. Qiu , Cost-aware multimedia data allocation for heterogeneous memory using genetic algorithm in cloud computing, IEEE Trans. Cloud Comput. 1 (2016) 99

[15] K. Gai , M. Qiu , L. Chen , M. Liu , Electronic health record error prevention approach using ontology in big data, in: 17th IEEE International Conference on High Performance Computing and Communications, New York, USA, 2015, pp. 752–757 .

[16] K. Gai , M. Qiu , L. Tao , Y. Zhu , Intrusion detection techniques for mobile cloud computing in heterogeneous 5G, Secur. Commun. Netw. (2015) 1–10

[17] M. Qiu , L. Zhang , Z. Ming , Z. Chen , X. Qin , L. Yang , Security-aware optimization for ubiquitous computing systems with SEAT graph approach, J. Comput. Syst. Sci. 79 (5) (2013) 518–529

[18] K. Gai , M. Qiu , H. Zhao , Security-aware efficient mass distributed storage approach for cloud systems in big data, in: 2016 IEEE 2nd International Conference on Big Data Security on Cloud (Big Data Security), IEEE International Conference on High Performance and Smart Computing (HPSC), and IEEE International Conference on Intelligent Data and Security (IDS), IEEE, New York, USA, 2016, pp. 140–145 .

[19] Ahmed Albugmi Madini O. Alassafi Robert Walters, Gary Wills , Data Security in Cloud Computing , Southampton, United Kingdom, Pages: 55 – 59.

[20] Gai , M. Qiu , H. Zhao , L. Tao , Z. Zong , Dynamic energy-aware cloudlet-based mobile cloud computing model for green computing, J. Netw. Comput. Appl. 59 (2015) 46–54

[21] K. Gai , M. Qiu , H. Zhao , J. Xiong , Privacy-aware adaptive data encryption strategy of big data in cloud computing, in: The 3rd IEEE International Conference on Cyber Security and Cloud Computing, The 2nd IEEE International Conference of Scalable and Smart Cloud, IEEE, Beijing, China, 2016, pp. 273–278 .

[22] D.Howley, Is microsoft’ sonedrive the best cloud storage service?, Url = https://www.yahoo.com/tech/microsoft- kills-unlimited- onedrive- accounts- 1759 27221.html . Torry Harris/Cloud-Computing-Overview

[23] Feng-qing Zhang, Dian-Yuan Han, Applying Agents to the Data Security in Cloud Computing, Weifang 261061, China920120Pages: 1126 – 1128.

[24] Sara Ibn El Ahrache; Hassan Badir; Parisa Ghodous; Abderrahmane Sbihi

[25] M. Qiu , M. Zhong , J. Li , K. Gai , Z. Zong , Phase-change memory optimization for green cloud with genetic algorithm, IEEE Trans. Comput. 64 (12) (2015) 3528–3540.

[26] Y. Li , W. Dai , Z. Ming , M. Qiu , Privacy protection for preventing data over-collection in smart city, IEEE Trans. Comput. 65 (5) (2016) 1339–1350

[27] H. Wang , Z. Xu , H. Fujita , S. Liu , Towards felicitous decision making: An overview on challenges and trends of big data, Inf. Sci. 367 (2016) 747–765.

[28] Enhancement for data security in cloud computing environment M. B. Gawali; R. B. Wagh 2012 Nirma University International Conference on Engineering (NUiCONE) , Pages: 1 – 6.

[29] J. Yao , A. Vasilakos , W. Pedrycz , Granular computing: Perspectives and challenges, IEEE Trans. Cybern. 43 (6) (2013) 1977–1989.

[30] W. Pedrycz , M. Song , A granulation of linguistic information in AHP decision-making problems, Inf. Fusion 17 (2014) 93–101 .

[31] Yibin Li a ,Keke Gai b , ∗ , LongfeiQiu c , MeikangQiu b , 1 , Hui Zhao d, Intelligent cryptography approach for secure distributed big data storage in cloud computing, m3Gsc; September 9, 2016;8:5

[32] S. Yoon , K. Kim , J. Hong , S. Kim , S. Park , A community-based sampling method using DPL for online social networks, Inf. Sci. 306 (2015) 53–69.

[33] iawei Han, Yanheng Liu, Xin Sun,Lijun Song, Enhancing data and privacy security in mobile cloud computing through quantum cryptography,g2016 7th IEEE International Conference on Software Engineering and Service Science (ICSESS), Pages: 398 – 401