International Journal of Advanced and Innovative Research (2278-7844)/
Volume 9 Issue 10

A SURVEY: DATA SECURITY ENCRYPTION SCHEME OVER CLOUD STORAGE

PG Scholar Pooja Parihar, Mr. Sandeep Rai

CSE Department

Technocrat institute of technology (Excellence), RGPV University Bhopal

Pariharpooja715@gmail.com

ABSTRACT: Cloud computing is an interesting area of research, different components and architecture were proposed in the field of cloud communication with user. Cloud computing provides the data security and integrity check with the users data, also cloud provide on demand computing services and algorithms for cloud server usage. Cloud architecture contains TPA (third party auditor), cloud server (Data centre and server for computation), users input and data accessing system unit, where these components maintain a communication to process data. In order to maintain data privacy and provide data security to users uploaded data different encryption techniques were proposed by the different authors. In this paper contribution is to survey the different available encryption and data security technique to enhance data security to authentic data. Our work monitor the different algorithm of data security technique such as AES, KP-ABE, CP-ABE, Homo-orphic technique , ECC and other recent available algorithm. Our contribution further monitor pros and cons of the available technique in the same field of cloud computing. Upon consideration the available technique further work can be lead to maximize the cloud data security with highest efficiency and other computation parameters [1].

Keyword – Data sharing, cloud computing, query manipulation, data processing.

INTRODUCTION

Cloud computing technology of data storage and maintaining privacy to the data having its own advantage and thus it provide user a guarantee storage and access over from any part of the world. Cloud computing also offer on demand computation with user's data to support multiple device and compatibility. As compared to the traditional server computing there is limitation of storage and services for the user which user usage for its optimized requirement, such requirement lacking facilities overcome by the cloud computing dynamicity. Cloud provides a scalable and efficient solution for service usage. A dynamic storage, pay as per usage concept make cloud more usable as per requirement. As user utilizes a wide variety of available services, user required to pay only for those services.

Cloud computing provide a certain level of security via its secure structure which contain parts as : CSP (cloud service provider) a party in the scenario which uses as a owner of cloud services and maintain a data enter, data storage hardware and other related requirement service act as a provider. These are the vendor such as IBM, AMAZON, INTEL and other hardware efficient provider they do maintain the services and act as cloud service providers. TPA (third party authenticator) is an another important part of cloud computing scenario which deals or communicate in between the user end and CSP , it authenticate the computation, on demand data integrity checksum using different hashing scheme and other required computation done at this end. CU(cloud user) is a user or a client system user which actually utilize the service of the CSP and TPA , user can store and manipulate its textual and multimedia data in secure form by the permission of TPA and get authentication key from it , thus able to handle its data from the CSP or data enter. In order to get integrity verification for the already stored data, user can put a challenge to TPA and then TPA process the same with CSP and provides the originality response proof from the server data storage.

There are few Steps involve in cloud computing:

1. User gets a key from the TPA to connect with the cloud.
2. User get authentication and connect and further file storage and manipulation can be performed.
3. User can request a file data proof on assigning a file id and hashing value.
4. User gets the file originality proof based on the response provided by the cloud server.
5. finally TPA and CSP keep track of cloud data , all sort of monitoring of data and storage perform , thus scenario execute in this way.

LITERATURE REVIEW

In this paper[14] author proposed a hybrid encryption system where a hybrid algorithm for the data encryption is proposed in which consideration is done with three encryption approaches. In the paper author considered three different round for the encryption and data process , also the multiple level provide the high level of data security in cloud data. In first phase a mono alphabetic substitution is used which once take input as plaintext and apply the algorithm with the plaintext and provide an output of substituted data. The second round contains the scheme where the odd number letter is append with again the next letter after the odd position letter and then the data processing is performed pairing basis. Again the output of second encryption scheme is taken for third and then three co-efficient used for the fourth round of encryption. The output algorithm which is provided by the system is effective as it provides a combination of compressed data and output data size is reduced up to 50%.

In this paper [4] author present a new technique which use BLS technique for encryption which use a key pairing system and store the data with encrypted text, further upload to the cloud server data center. This paper also use hashing technique SHA-1 which is integrity verification technique for the data outperformed for the integrity and modification change. The security of this signature scheme depends on a new problem, namely k-CAA or k + 1EP. It is shown that k + 1EP is no harder than the CDHP. Based on this basic signature scheme, a ring signature scheme and a new method for delegation are proposed in this paper research, bilinear algorithm is a pairing based algorithm which is privacy preserving and able to perform the data security without interruption and

hiding the original data without interruption in the auditing process and the hashing was performed with the help of sha-1 which produce 128 bit key length in order to maintain the data in checksum process in verification, they have used JPBC java library[21] in order to perform the execution and perform the simulation for the present algorithm , the Boneh-Lynn-Shacham uses signature based scheme for the data verification, they uses elliptic curve scheme for the encryption based scheme. This scheme allow a shorter signature scheme than the FDH signature scheme. Also author uses BLS based scheme for the data security and storage purpose.

In this paper[13] they have worked on various attribute confidentiality, integrity, availability, accountability, and privacy-preservability and performed the various security concern issues in aspects, authors have systematically studied the security and privacy issues in cloud computing based on an attribute-driven methodology, We have identified the most representative security/privacy attributes (e.g., confidentiality, integrity, availability, accountability and privacy- preservability), as well as discussing the vulnerabilities, which may be exploited by adversaries in order to perform various attacks. Defence strategies and suggestions were discussed as well, thus this is the paper included the security and study aspects in cloud computing, the data integrity verification made dealing with encryption algorithm and the audit was performed with the help of hashing algorithm available in order to verify the value generated again while checking the data integrity available with the associated file, here they have worked on different aspects such as user account access approach, availability of data, data changing or integrity verification and the technique should be privacy preserving so that the data should not be leak during the cloud execution.

In their paper [11] proposes introducing a Trusted Third Party, tasked with assuring specific security characteristics within a cloud environment. The proposed solution calls upon cryptography, specifically Public Key Infrastructure operating in concert with SSO and LDAP, to ensure the authentication, integrity and confidentiality of involved data and communications. The solution, presents a horizontal level of service, available to all implicated entities, that realizes a security mesh, within which essential trust is maintained. in this research they have proposed identified generic design principles of a cloud environment which stem from the necessity to control relevant vulnerabilities and threats. A combination of PKI, LDAP and SSO can address most of the identified threats in cloud computing dealing with the integrity, confidentiality, authenticity and availability of data and communications. The solution, presents a horizontal level of service, available to all implicated entities, that realizes a security mesh through federations, within which essential trust is maintained, with the technique provided by them a deep entity analysis can be able to perform and combine technique was able address various threads and issues related problem with the data and its integrity related to the data storage.

In this paper [26] content based two round encryption scheme is used which utilizes symmetric key encryption technique for the data storage , this algorithm implement binary addition operation algorithm , circular bit shifting operation is also performed with symmetric key encryption technique is utilized by the author. For the Asymmetric key

encryption they have derived the concept of ECC, RSA and DES algorithm and for the symmetric key encryption technique 3DES, Blowfish and AES technique is utilized by the author for encryption purpose. Further a bitwise circular method which is content based and utilized for the image data security is used where key generation is done using MSB (most significant bit) of the input data file and further decryption is performed using its reverse process. In this paper author taken a simple plaintext Alice@202 as input string and performed two round encryption to provide data security. Finally according to author the encryption procedure is simple and use effective way of key generation and data encryption , also further enhancement can be done on taking multiple data formats for the encryption such as doc, text which can be combine with image steganography.

In this paper[10] The cloud must provide the proof that its providing or maintaining complete data storage and in that they have stated to provide the proof that is data is maintaining by the cloud, there they have stated the file information related to computer MAC address related to which data was generated and they have used MAC as a data integrity proof, their system allow for compact proofs with just one authenticator value this can lead to proofs with as little as 40 bytes of communication. They have provided two solutions for it two solutions with similar structure. The one is privately variable and builds elegantly on pseudorandom functions (PRFs); the second allows for publicly variable proofs and is built from the signature scheme of Boneh, Lynn, and Shacham in bilinear groups. Both solutions rely on homomorphism properties to aggregate a proof into one small authenticator value. They have worked with the parameters such as efficiency, public verifiable, public retrievable – where efficiency they have stated that the system should be as efficient as possible in terms of both computational complexity and communication complexity, that was given an emphasis to work on and A system is publicly verifiable if any (untrusted) entity can perform the verification audit. This is desirable in settings where many users might shareable storage or when a third party is employed to audit the storage servers.in the paper they have specified two schemes redundantly encode able with an erasure code and apply an audit that probabilistically ensures enough blocks are retrievable to reconstruct the file.

In this paper [4] author describe a new approach for the cloud data security which is the combination of two available algorithms, the first is DES which is data encryption system technique and other is CAST block cipher technique is used. According to author DES is proposed by IBM and it is based on the cipher which is fiestel based cipher scheme. It contains the bit shuffle, substitution and exclusive XOR operations were performed using the algorithm. The algorithm contains a key length of 64 bit which is strong in case of encryption. Author combines this algorithm with CASE block cipher encryption which based on the symmetric key encryption system. The algorithm architecture contains the S boxed substitution mechanism for the data encryption. The algorithm contains two sub steps such as confusion and diffusion. The implementation of the algorithm is performed using Python 3.4 and sample input taken as excel sheet data which is encrypted and stored over the cloud computing. According to author algorithm provide a high security and can be apply with 3G and 4G LTE environment. And further improvement can

be done to improve performance such that can be used for 5G environment.

In this paper[8] they study how to make a decryption key more powerful in the sense that it allows decryption of multiple cipher texts, without increasing its size. Specifically, The problem statement is "To design an efficient public-key encryption scheme which supports flexible delegation in the sense that any subset of the cipher texts (produced by the encryption scheme) is decrypt able by a constant-size decryption key (generated by the owner of the master-secret key)." They solve the problem of public key encryption which may share the public key concept to intruder, thus they given a new scheme which is key Aggregate scheme (KAC) for the data protection and stability. The key owner and data owner holds a master key technique which is treated as master data key for the data contribution and further data is encrypted and store using this secure technique.

In this paper [2] author describe the algorithm which uses trusted third party based encryption scheme. In the paper they combine both symmetric and Asymmetric based encryption scheme which utilize the advantage point of both the algorithm. The paper proposed three entities based scheme such as CSP module taken data and encrypt using the symmetric key encryption technique for the data transmission. Second TTP module which maintains a secret key and key exchange system using the cloud users rights for data exchange. Third the service provider store customer data and service key request secret key is generated. The algorithm uses AES symmetric key based algorithm for the encryption and finally three phase scheme architecture put data stability and security to user cloud data. According to author further work can be append on minimizing data transmission overhead and execution, response time with data exchange with the cloud should be reduce to match with real time requirement.

The aim of their proposed system [6] is to protect outsourced data in cloud storage against corruptions, adding fault tolerance to cloud storage, along with efficient data integrity checking and recovery procedures, becomes critical. Regenerating codes provide fault tolerance by striping data across multiple servers, while using less repair traffic than traditional erasure codes during failure recovery. They have design and implement a practical data integrity protection (DIP) scheme for a specific regenerating code, while preserving its intrinsic properties of fault tolerance and repair-traffic saves. DIP scheme is designed under a mobile Byzantine adversarial model, and enables a client to feasibly verify the integrity of random subsets of outsourced data against general or malicious corruptions. It works under the simple assumption of thin-cloud storage and allows different parameters to be fine-tuned for a performance-security trade-off. they further analyse the security strengths of our DIP scheme via mathematical models. They demonstrate that remote integrity checking can be feasibly integrated into regenerating codes in practical deployment.

Comparison analysis of different literature and technique is shown below.

S. No.	Author	Algorithm	Description	Advantage	Disadvantage
1.	**Henry C.H. Chen and Patrick P.C. Lee**	FMSR-DIP codes	functional minimum-storage regenerating (FMSR) codes is implemented in this paper which aims to provide , this algorithm give less fault tolerance and high accuracy in less time limit.	* Low bandwidth is used in this algorithm. * High fault tolerance value. * High security version is implemented.	* No encryption technique is investigated.
2.	**Seung-Hyun Seo, Mohamed Nabeel**	mCL-PKE plan	The algorithm aim to provide a low encryption cost on providing symmetric key encryption availability for different user data activity.	Low encryption time and computation cost. Encryption is done only by the data admin, so no access modification encryption rights to other shared users. Fast execution is performed.	Large data size is still need to investigate. Block number is high so it can further required to reduce , it may take long execution for large dataset.
3.	**Cheng-Kang Chu, Sherman S.M. Chow**	Key total cryptosystem(KAC)	In this approach an open key distribution is introduced.Key-aggregate cryptosystem produce constant size cipher texts such that efficient delegation of decryption rights for any set of cipher text are possible	Constant encryption and decryption key size. Key size is independent of the maximum number of cipher text classes.	Key leak may cause several data deletion or modification.

4.	**Nandita Sengupta∗ and Ramya Chinnasamy**	Hybrid DESCAST Algorithm	DES and Cast block cipher algorithm were combine and proposed as DESCAST algorithm.	Security provided using hybrid approach and multiple key is provided for the encryption.	The algorithm is relatively slow while dealing with large dataset.
5	**DimitriosZissis ,DimitriosLekkas**	SSO and LDAP technique.	SSO and LDAP, to guarantee the confirmation, uprightness and classification of included information and interchanges. The multiple functionality architecture is introduced.	A complex architecture provide high security model for data storage.	High execution time for large dataset, as it needs to process multiple steps.
6.	**Fangguo Zhang, ReihanehSafavi-Naini**	BLS, SHA-1 algorithm.	In this a cloud model is taken where the data is stored using the encryption technique bilinear mapping and data integrity verification is performed using SHA-1 hashing generation and verification technique.	Bilinear mapping provide a symmetric key approach which is fast execution technique. SHA-1 uses less computation due to moderate key size.	SHA-1 is having less key size, thus required more security to be added.

Conclusion:

Cloud computing technology for data storage and accessing system is required today , where the digital world require all sort of data in safe and structured format. Different schemes either independent or hybrid approach performed by different author. In this paper our discussion is about all the different techniques provided by the author contributed in cloud computing security. This paper also describe cloud structure, component, different research performed and advantage, disadvantage of the paper. Various security constraints were given in AES, KP-ABE, CP-ABE, Homo-orphic technique, ECC based cloud storage technique which claims for secure data maintenance. Our further work will be on finding a suitable algorithm which eliminate the drawback of existing scenario algorithms.

REFERENCE:

1. Vishwanath S Mahalle, Aniket K Shahade," Enhancing the Data Security in Cloud by Implementing Hybrid (Rsa&Aes) Encryption Algorithm", 2014 IEEE.
2. Syed rizvi, Katie cover, Christopher gates, "A trusted third party(TTP) based encryption scheme for ensuring data confidentiality in cloud environment", Procedia Computer Science 36 (2014) 381 – 386, Elsevier.
3. Feng Zhao ; State Grid Electr. Power Res. Inst., Guodiantong Corp., Beijing, China ; Chao Li ; Chun Feng Liu," A cloud computing security solution based on fully homomorphic encryption ",IEEE 16-19 Feb. 2014.
4. Nandita Sengupta∗ and Ramya Chinnasamy," Contriving Hybrid DESCAST Algorithm for Cloud Security", Procedia Computer Science 54 (2015) 47 – 56,Elsevier.
5. Fangguo Zhang, ReihanehSafavi-Naini and Willy Susilo "An Efficient Signature Scheme from Bilinear Pairings and Its Applications". IEEE 2013
6. Henry c.h. Chen and patrick p.c. Lee."Enabling data integrity protection in regenerating-coding-based cloud storage: theory and implementation".ieee transactions on parallel and distributed systems, vol. 25, no. 2, february 2014.
7. NuttapongAttrapadung, Benoıt Libert , and Elie de Panafieu," Expressive Key-Policy Attribute-Based Encryption with Constant-Size Ciphertexts".
8. Cheng-kangchu, shermans.m. Chow, wen-gueytzeng, jianyingzhou, and robert h. Deng, "key-aggregate cryptosystem for scalable data sharing in cloud storage" ieee transactions on parallel and distributed systems,vol. 25, no. 2, february 2014.
9. Qianwang, congwang, kuiren, wenjinglou, jin li," enabling public auditability and data dynamics for storage security in cloud computing"proc. Ieee transactions on parallel and distributed systems, vol. 22, no. 5, may 2011.
10. HovavShacham, Brent Waters stated "compact proof of retrievability" 2012.
11. DimitriosZissis ,DimitriosLekkas in Elsevier –" Addressing cloud computing security issues", IEEE 2012.
12. K. Ren, c. Wang, and q. Wang, "security challenges for the public cloud," ieee internet computing, vol. 16, no. 1, pp. 69–73,2012.
13. Zhifeng Xiao and Yang Xiao,– "Security and Privacy in Cloud Computing" IEEE June 2013 conference.
14. Rashmi Singha , Isha Panchbhaiyaa ,Abhishek Pandeya & R H Goudar ," Hybrid Encryption Scheme (HES): An Approach for Transmitting Secure Data over Internet", International Conference on Intelligent Computing, Communication & Convergence (ICCC-2014),Elsevier.

