Int. Conf. on Signal, Image Processing Communication & Automation, ICSIPCA

A Survey on Encryption Techniques used in Cloud Computing

Abhishek kumar singh[1], P Prathik R[2] and Dr Dayananda[3]
[1,2]Student, JSS Academy of Technical Education
abhi8jss@gmail.com, prathikramk@gmail.com
[3]Associate Professor, JSS Academy of Technical Education
dayanandap@gmail.com

***Abstract*—Information protection and security insurance are turning into the most critical perspectives for the future improvement and advancement of cloud computing innovation in the field of open and authoritative information. With its capacity to give shared assets over the Internet and maintain a strategic distance from expansive infrastructural speculations, distributed computing has as of late developed as a promising facilitating stage that gives a wise use of an accumulation of administrations, applications, data, and capacity assets. However alongside these points of interest, putting away a lot of mission critical information on the cloud rouses exceedingly gifted programmers in this manner making a requirement for the security to be considered as one of the top issues while considering Cloud Computing. This paper overviews the encryption methods utilized for the cloud information security as talked about in different research commitments and plays out an examination to recognize advancement highlights for cloud security.**

***Index Terms*— Cloud computing, Encryption, Security.**

I. INTRODUCTION

There are a ton of dangers to our data; however it's conceivable to create assurances for each like by secluding our home PC from outsiders and minors and utilizing a PIN on our telephone bolt screen, and so on. There is additionally a more flexible route – to make data coherent just by a true blue proprietor. Each one of those unbalanced minutes and incidents may be maintained a strategic distance from if private data is put away in an encoded frame.

Encryption is a technique by which information – computerized or something else – is changed over into an encoded frame that must be decoded and perused if the client has a proper encryption key.

The expanded interest for improved security and characteristic cut-off points of customary encryption plans for information on the cloud has driven the selection and execution of a few new encryption algorithms, for example, searchable; arrange protecting, and homomorphic methods. Searchable encryption enables us to encrypt information such that it can at present be sought. Clients can safely outsource information to an untrusted cloud supplier without requiring seek over it. A request saving encryption algorithm is an encryption method that produces cypher messages and keeps the numerical requesting of the plain texts. It is an imperative system for database related applications because of its capacity of supporting extent question handling straight forwardly on encoded information without expecting to decode them. Homomorphic

Grenze ID: 02.ICSIPCA.2017.1.29

encryption enables us to play out a numerical operation on the encoded information, and produces an indistinguishable answer from playing out a similar to operation on the decoded information.
This paper explores encryption conspires at present executed in many secure items in cloud situations. Every encryption scheme is assessed and examined in its proficiency, security. In section II different services provided in cloud computing is explained followed by a discussion on various encryption techniques in Section III. Section V consists of analysis done on the encryption techniques.

II. Services in Cloud Computing

A. Service Models

After foundation of the cloud, the cloud computing services contrast contingent upon prerequisites. The essential administration models in sending are regularly known as:
Software as a Service (SaaS) - Clients buy the capacity to get to and utilize an application or services that is facilitated in the cloud.
Platform as a Service (PaaS) - Clients buy access to the platforms, empowering them to convey their own product and applications in the cloud. The working frameworks and system get to are not overseen by the client, and there may be limitations as to which applications can be conveyed.
Infrastructure as a Service (IaaS) - Clients control and deal with the frameworks regarding the working frameworks, applications, storage, and system network, yet don't themselves control the cloud foundation
StaaS (Storage as a Service) - Cloud applications can scale past their constrained servers. StaaS enables clients to store their information at remote disks and get to them at whatever time from wherever. Cloud storage frameworks need to meet a few thorough necessities for keeping up clients' information, fusing high accessibility, unwavering quality, execution, replication and information consistency; but since of the clashing way of these prerequisites, there exists no framework that actualizes every one of them together.

B. Deployment Models

Cloud computing arrangement models can vary contingent upon necessities, and the accompanying sending models have been recognized, each with particular attributes that bolster the requirements of the administrations and clients of the cloud specifically ways.
Private Cloud - the cloud framework has been sent, and is kept up and worked by a specific association. The operation might be in-house or with an outsider prefacing.
Community Cloud - the cloud framework is shared among various associations with comparative interests and necessities. This constrains the capital use costs for its foundation as the expenses are shared among the associations. The operation might be in-house or with an outsider start.
Public Cloud - the cloud framework is accessible to general society on a business level by a cloud specialist co-op. This empowers a client to create and convey an administration in the cloud with insignificant money related expense contrasted with the capital use necessities regularly connected with other organization choices.
Hybrid Cloud - the cloud foundation comprises of various clouds of any sort, and the clouds have the capacity through their interfaces to permit information or potentially applications to be moved starting with one cloud then onto the next. This prompts a blend of private and open clouds that bolster the necessity of information maintenance in an association, and furthermore the need to offer administrations in the cloud.

III. Cryptographic Techniques

We can use different techniques for implementing Cryptographic storage service, in which some of the techniques are explicitly designed for the cloud supported platform. In the early stages of cloud computing Public Key Encryption (one of the most common encryption technique) were used for the implementation. As the traditional technique support only one to one encryption type communication so it was unable to deliver the expected result and scalability of Public Key Encryption is also not that high. So after this study, there was the need for moving towards some advanced cryptographic method. The different encryption methods to make cryptographic methods highly effective are explained below.

A. Searchable Encryption

A Searchable Encryption technique is consolidated at a conceptual level which encrypts the data content present in search indices to conceal it from others with exception of the approved party giving the tokens. For

generating the search index an accumulation of records consisting of full-text index or keyword is considered. Index encryption is performed on searchable encryption technique in such a fashion (i) Based on the token provided for the keyword pointers assigned to the encrypted files are retrieved. (ii) Contents are not accessible for index unless tokens are provided. Tokens get generated based on the secret key. The file content or the keyword is not revealed during the retrieval process except for the files containing the common keyword. As searchable encryption is considered for the security and it is little complicated the previous statement makes a major impact on the security challenges. Study of many researches has proved that the file sharing the same keyword has very high chances of leaking the information to the unauthorized identity. The server naturally surmises the keyword being searched based on the rehased seek of the customer search pattern. While searching, some data is spilled and this data is like the suitable document that is being come back to the client by server. This data that is spilled and in view of spilled data server recovered, the document is found out by the supplier or provider. We can likewise say the information spilled to the supplier depends on the administration is being utilized while it is not revealed by the cryptographic primitives. This spillage appears to be practically fundamental for both efficient and reliable administration in cloud storage, At most extreme scenario the information spilled from the general population cloud storage is having less data. Contingent upon various situations, there exist different sorts of searchable encryption techniques that can be connected. For instance, Symmetric Searchable Encryption (SSE) is executed for information preparing in little undertaking structures, though Asymmetric Searchable Encryption (ASE) is actualized for extensive venture engineering.

*Symmetric Searchable Encryption:*It is reasonable for the environment where the customer that pursuits the information and furthermore he is in charge of producing it, Single Writer/Single Reader (SWSR) is derived from cloud storage terminology. SSE terms were introduced in and improved developments and security terms were indicated in. SSE has two noteworthy favourable circumstances they are productivity and security. It additionally has weaknesses, for example, usefulness and trade-off productivity. SSE schemes are reasonable for the entity who play out the encryption and furthermore the substance who looks with a keyword from the cloud storage framework. Most SSE plans are productive in light of the fact that they utilize the idea of pseudo-random functions and furthermore block ciphers for encryption reason. Search procedure can be effective since SSE permits to pre-process the data and proficiently represents in data structure. SSE ensures security which is examined as (i) the information about the data is covered up until the tokens are uncovered. Since token is uncovered, the server adapts just the length data. (ii) When the token is accommodated a keyword the server look through the record contains the keyword without knowing the keyword. When contrasting asymmetric and searchable encryption, it is found that security certifications are substantially more grounded with no constraints. In view of the different issue which is talked about over, each development contains deterministic tokens. These deterministic tokens assist the service provider in identifying the rehashed queries without knowing the query. Curtmola[5] et al. Clarified the length of look time is optimal for the server yet the record are wasteful amid updates. Then again Goh[3] proposed that index can be refreshed effectively in the server yet the hunt time is not optimal. The previously mentioned scheme doesn't concentrate on the search based on conjunctions or disjunction of terms. SSE scheme alone handles the idea of conjunction by matching with the assistance of elliptic bends yet it is wasteful while applying Asymmetric Searchable Encryption schemes (ASE). Another requirement of some searchable encryption is that they are just secure in a few circumstances where the inquiries are delivered non-adaptively. In, a few inquiries which require the response for the past question can likewise be alluded and this is known as adaptive setting in a protected domain.

*Asymmetric Searchable Encryption (ASE):*This plan is appropriate for environment where the customer that inquiries the information is not quite the same as the person who produces it. This situation is known as Many Writer/Single Reader(MWSR). The fundamental idea of ASE plans were talked about in and the improved definitions were clarified. Various works have been performed to demonstrate accomplishing more troublesome questions in public key setting like conjunctive search and range queries. Various issues that emerge in different use of ASE has been reviewed. The entire protection of queries ensured in ASE.

The primary burden of ASE is weaker security and it is not effective while the real preffered standpoint is its usefulness. Contrasted with SSE conspire, The ASE is appropriate for gigantic measure of setting because of multiple writer and reader. ASE is wasteful in light of the fact that it make utilization of the idea of pairings on elliptic curves. This idea will make the operation ease back when contrasted with hash functions or block ciphers. ASE permits to pre-prepare the information and wastefully speaks to in data structures. ASE ensures security which are talked about as (i) the information about the data are covered up untill the tokiens are

uncovered. Since token is uncovered, the server adapts just the length data. (ii) When the token is accommodeted a keyword the server look through the record containg the keyword without knowing the keyword which is inefficient when constrated with SSE settings.

B. Homomorphic Encryption

This scheme is connected in the cloud condition to secure the information. This Homomorphic encryption scheme permits executing calculations on the encrypted information. It is just of the progressed cryptographic system. The significant downside of homomorphic encryption is clarified. It has a moderate handling time amid calculation.

C. Identity based Encryption

Identity Based Encryption cryptographic plan has been created by Shamir[13] in 1984. Real issue is the powerlessness to manufacture Identity Based Encryption framework which depends on RSA. Later in 2001 a proficient Identity Based Encryption has been produced by Boneh[15] and Franklin.

In Identity Based Encryption, a identity of the client assumes an imperative part. The sender who sends the message just has to know the recipient's character ascribe keeping in mind the end goal to send the encrypted messages. Email Encryption is one of the significant applications for Identity Based Encryption. In any case, key revocation is not accomplished in Identity Based Encryption.

D. Attribute based Encryption

Attribute based Encryption is one of the cryptographic systems utilized as a part of Cloud Computing Environment. Attribute based Encryption is first brought into utilization by Sahai[9] and Waters in the year 2005. The primary concentration of this Attribute-based Encryption plan is to give security to the information put away in the cloud. The four stages in Attribute Based Encryption are Setup, KeyGen, Encrypt, and Decrypt. The KenGen() algorithm is utilized to the make private key of the client for confidential sharing. The clients who are approved can decode the data utilizing their private key. In Attribute Based Encryption, information owner utilizes an set of features to encrypt the information and just the approved clients who has the anticipated or certain characteristics can decrypt the information. This encryption technique makes the cloud condition more secure. The different classes of Attribute-based Encryption are condensed.

*Key-Policy Attribute-based Encryption:*KP-ABE is presented by Vipul Goyal[18] and Omkant Pandey to accomplish fine-grained get to control in one-to-many communications. In Key-Policy Attribute-based Encryption, the encoded information is developed with the arrangement of characteristics. The individual is approved to decrypt the Cipher content if and just if the properties that are worked with the Cipher content fulfill the access structure of their private or secret keys. The four stages in Key-Policy Attribute Based Encryption are Setup, KeyGen, Encrypt, and Decrypt. The KeyGen and Decrypt algorithm get varied from the Attribute Based Encryption. In Key-Policy Attribute-based Encryption, private key of the client is cognated with access structure. However unapproved access may happen, the general population may decode the data. This can be overcome in the Cipher content Policy Attribute Based Encryption which develop the get to strategy in the encrypted information i.e., Cipher text utilizes an arrangement of ascribes to portray the private key of the client. Additionally in a few applications that uses this plan, proprietor of the information must have a firm conviction with the key guarantor.

Ciphertext Policy Attribute based Encryption: In 2007, Bethencourt[11] et al. proposed a cryptographic procedure named Cipher text approach attribute based strategy. The get to approach is worked with the information that has been encrypted. In CP-ABE the Cypher content is related to get to structure and the private keys with the characteristics. In Key-Policy Attribute Based Encryption, the main drawback is that the get to approaches were not made by the encryptor. This gave a course to the foundation of Cipher text Policy Attribute Based Encryption which enables the get to strategies to be worked with the encoded information. The proprietor who encodes the information, design the get to strategy. A proposal was made for the utilization of CP-AB strategy. The information proprietor is accountable for characterizing the get to arrangements. This anticipates unapproved get to and advances security. In CP-ABE, revocation is not accomplished proficiently. In this way it is not all that simple for the information proprietor to adjust the get to polices at whatever point required.

Multi Authority Attribute based Encryption: Multi-Authority Attribute Based Encryption is presented by Chase. The Multi-Authority Attribute Based Encryption (MA-ABE) is likewise a cryptographic system

which comprises of numerous authorities to deal with the properties and the circulation of the secret keys. The clients who wish to download the data will ask for the decryption keys from the quality specialist. The characteristic key generation is one of the algorithms in MA-ABE. This algorithm is controlled by the expert and thus the specialist will disseminate the keys to the clients. An approved client who has the suitable decryption keys can see the data. The algorithm required in this method incorporate Set up, Attribute Key Generation, Central Key Generation, Encryption, and Decryption. This crypto-graphic plan handles more number of clients. Information secrecy can be accomplished on utilizing this sort of system in cloud condition. As it is reasonable for different authorities' situation, this cryptographic procedure is most appropriate for the application which contains different areas. This cryptographic method enhances security and decreases key administration intricacy which is the real preferences.

*Hybrid Vigenere Caesar Cipher Encrypt on (HVCCE):*Nandita Sengupta and Jeffrey Holmes[10] have proposed another encryption method in light of the hybrid cryptography framework. Half breed Vigenere Caesar Cipher Encryption (HVCCE) is proposed which will keep the three cloud foundation like customer side, server side and system. This proposed cryptographic framework is composed that way the calculation time for decoding of the Cypher text is more contrast than with any single cryptographic framework for programmer. This encryption is connected on the encrypted data accomplished from the second stage. So also decoding of data is to be done in three stages. In the principal period of decoding, turn around Vigenere Cipher should be connected with the reverse keyword on the encoded cypher text. In the second stage of decoding, reverse Cypher text should be connected with the forward keyword connected on the decoded Cypher text accomplished from the primary stage of decoding. In the third period of decoding, reverse Cypher text should be connected on the Cyber text accomplished from the second stage of decoding and get the plain content to the client. The proposed method principle preferred standpoint is giving triple encryption to the information and a real disadvantage is less effective.

***Hierarchical Identity Based Encryption (Hibe)*:** Xin Dong[8] et al. have proposed encryption system "SECO" which is secure and productive collaboration scheme in light of Hierarchical Identity Based Encryption (HIBE). The proposed encryption system is to guarantee the information classification on the untrusted clouds.

Hierarchical Identity Based Encryption (HIBE) is an encryption system that is utilized to control clients who are unapproved or mostly approved clients and may offer private key to unapproved client which will lead to unapproved information get to. Hierarchical Identity Based Encryption involves five stages: setup, encode, key gen, decode and designate. In setup phase input is security parameters and the output is the master key, in encoding step it takes plain content, identity vector and open parameters as info and yield as Cypher text. In key gen step it takes the master key, identity vector and open parameters as info and yield as secret key for open vector, in decoding step takes Cypher text, secret key and open parameters as information and yield as plain content. In delegate step takes the secret key for identity vector, identity and open parameters as information and yield as secret key for identity, it link of identity and identity vector.

This strategy utilizes two levels of Hierarchical Identity Based Encryption to guarantee privacy of information documents in untrusted clouds. Encryption method initially investigates the safe information joint effort benefit that forestalls data spillage and empowers one-to-many encryptions. It likewise empowers the fine-grained get to control and information composing all the while. It gives the information of coordinated effort benefits backings the consistency and accessibility of the mutual information among the multi-clients. The two level HIBE method, which contains Private Key Generator is trusted outsider which doles out the secret keys to the Domain-Private Key Generator. Root Private Key Generator deals with the autonomous co-agent Domain Private Key Generators while Domain Private Key generator deals with the end clients. Root Private Key Generator produces the master key and private keys for the Domains. The Data proprietor needs to encode the information, it utilizes Public key of numerous beneficiaries so that lone pondered domains can decode that information. The client will decode the information, it ask for secret key to the domain Private key generator and Domain Private Key Generator giving the decryption key to decoding of information. The principle preferred standpoint of proposed procedure SECO is exceedingly productive and low overhead on calculation and correspondence.

IV. CLOUD DES ALGORITHM

This approach is pertinent for securing both the server and the customers. DES Cipher block is built for security design to wipe out the misrepresentation that is occurred in taking the information. The information

sent to the beneficiary who is hacked is supplanted with no risk. The framework with encryption is satisfactorily secure, yet the sort of encryption increments is specifically relative to registering power. Symmetric key are utilized to encode the model to bring about better secure correspondence system. The creator demand that the cloud information security by dissecting the encryption in light of different elements, for example, the information security necessities, information security prepare, the information security chance, security elements of information arrangement. The fundamental perspective of their paper is the encryption of information security arrangements, which is likewise vital and it can be connected as reference when planning the whole security arrangement.

This encryption method is considered for the security and protection issue in cloud storage. It likewise ensures the information display in secured cloud from unapproved get to. The information that is accessible in secure cloud can be assaulted in two ways

(i) insider assault

(ii) Outsider assault.

The insider assault is the administrator of an association who has the benefit to get to every one of client's information while the outcast assault has a place with the outsider attempting to get to the information of user's. A symmetric encryption calculation is actualized to monitor the information that is put away in distributed storage from the aggressors. The method is executed by changing over the plain content into figure message by utilizing ASCII code and key an incentive between 1 to 256. By consolidating substitution cypher and transposition cypher the established encryption method is improved. Symmetric encryption performs computational productivity and rapid to deal with vast measure of information in distributed storage.

V. Comparison Study

Their proposed method does not enable the heads or assailants to get to the information from the cloud storage since it the client information are encoded. The accompanying table portrays near examination of different cryptographic methods in light of Access control, Scalability, Flexibility, and Efficiency

VI. Conclusion

The cloud computing is one of the rising models, and data security in the cloud is the most critical issue which deters its development. This overview on the current information encryption strategies utilized as a part of cloud computing sets up the required level of security for data and secures data by marking a security level as demonstrated by the risk levels. Also, we survey the present encryption systems, that guarantee the security of information for the whole life cycle from the earliest starting point to the end in the cloud computing. The short review likewise gives an examination of existing encryption procedures utilized as a part of cloud computing. In this correlation contemplate where the upsides and downsides of various information encryption methods are thought about.

Schemes/Parameters	Access Control	Scalability	Flexibility	Efficiency
IDE	Low	Avg	Low	Low
HE	Low	Avg	Low	Low
ABE	Avg	High	Avg	Avg
KP-ABE	Avg	Avg	High	Avg
CP-ABE	High	Avg	High	Avg
MA-ABE	Better	High	High	High

Encryption Technique	Advantages	Limitations
Searchable Encryption	Efficiency and Security	Functionality and tradeoff efficiency
Homomorphic Encryption	Enhanced privacy Private Information Retrieval	Complexity – No Lattice Malware Poor Performance
Identity based Encryption	Eliminates the need for a public key distribution infrastructure	The private key generator generates private key for users. It may decrypt and/or sign any message without authorization.
Attribute Based Encryption	Improves security and reduces key management complexity	Access policies were not created by the encryption
HVCC Encryption	Providing triple encryption to the data	Less efficient
HIB Encryption	The main advantage of the proposed technique SECO is highly efficient and low overhead on computation and communication.	Collusion resistance and user accountability

REFERENCES

[1] Yong, P.E.N.G., Wei, Z.H.A.O., Feng, X.I.E., DAI, Z.H., Yang, G.A.O. and CHEN, D.Q., 2012. Secure cloud storage based on cryptographic techniques. *The Journal of China Universities of Posts and Telecommunications*, *19*, pp.182-189.2. Bessani A, Correia M, Quaresma B, et al. DEPSKY: dependable and secure storage in a cloud-of-clouds. 6th Conference on Computer Systems (EuroSys'11). 2011. p. 31–46

[2] Kamara, S. and Lauter, K., 2010, January. Cryptographic cloud storage. In *International Conference on Financial Cryptography and Data Security* (pp. 136-149). Springer Berlin Heidelberg.

[3] Song, D.X., Wagner, D. and Perrig, A., 2000. Practical techniques for searches on encrypted data. In *Security and Privacy, 2000. S&P 2000. Proceedings. 2000 IEEE Symposium on* (pp. 44-55). IEEE.

[4] Ballard, L., Kamara, S. and Monrose, F., 2005, December. Achieving efficient conjunctive keyword searches over encrypted data. In *International Conference on Information and Communications Security* (pp. 414-426). Springer Berlin Heidelberg.

[5] Curtmola, R., Garay, J., Kamara, S. and Ostrovsky, R., 2011. Searchable symmetric encryption: improved definitions and efficient constructions. *Journal of Computer Security*, *19*(5), pp.895-934.

[6] Dong, X., Yu, J., Luo, Y., Chen, Y., Xue, G. and Li, M., 2013, June. Achieving secure and efficient data collaboration in cloud computing. In *Quality of Service (IWQoS), 2013 IEEE/ACM 21st International Symposium on* (pp. 1-6). IEEE.

[7] Boneh, D., Di Crescenzo, G., Ostrovsky, R. and Persiano, G., 2004, May. Public key encryption with keyword search. In *International Conference on the Theory and Applications of Cryptographic Techniques* (pp. 506-522). Springer Berlin Heidelberg.

[8] Sengupta, N. and Holmes, J., 2013, November. Designing of cryptography based security system for cloud computing. In *Cloud & Ubiquitous Computing & Emerging Technologies (CUBE), 2013 International Conference on* (pp. 52-57). IEEE.

[9] Ostrovsky, R., Sahai, A. and Waters, B., 2007, October. Attribute-based encryption with non-monotonic access structures. In *Proceedings of the 14th ACM conference on Computer and communications security* (pp. 195-203). ACM.

[10] Boneh, D. and Waters, B., 2007, February. Conjunctive, subset, and range queries on encrypted data. In *Theory of Cryptography Conference* (pp. 535-554). Springer Berlin Heidelberg.

[11] Lewko, A. and Waters, B., 2011, May. Decentralizing attribute-based encryption. In *Annual International Conference on the Theory and Applications of Cryptographic Techniques* (pp. 568-588). Springer Berlin Heidelberg.

[12] Baek, J., Safavi-Naini, R. and Susilo, W., 2006, August. On the integration of public key data encryption and public key encryption with keyword search. In *International Conference on Information Security* (pp. 217-232). Springer Berlin Heidelberg.
[13] Shamir, A., 1984, August. Identity-based cryptosystems and signature schemes. In *Workshop on the Theory and Application of Cryptographic Techniques* (pp. 47-53). Springer Berlin Heidelberg.
[14] Fuhr, T. and Paillier, P., 2007. Decryptable searchable encryption. *Provable Security*, pp.228-236.
[15] Boneh, D., Kushilevitz, E., Ostrovsky, R. and Skeith III, W.E., 2007, August. Public key encryption that allows PIR queries. In *Annual International Cryptology Conference* (pp. 50-67). Springer Berlin Heidelberg.
[16] Goyal, V., Pandey, O., Sahai, A. and Waters, B., 2006, October. Attribute-based encryption for fine-grained access control of encrypted data. In *Proceedings of the 13th ACM conference on Computer and communications security* (pp. 89-98). Acm.