Journal of Contemporary Issues in Business and Government Vol. 27, No. 3,2021
https://cibg.org.au/

P-ISSN: 2204-1990; E-ISSN: 1323-6903
DOI: 10.47750/cibg.2021.27.03.238

A COMPREHENSIVE STUDY OF CRYPTOGRAPHY AND KEY MANAGEMENT BASED SECURITY IN CLOUD COMPUTING

[1]S.Vinothkumar, [2] J.Amutharaj, [3]S.Jeyabalan
[1]Department of CSE, ACS College of Engineering, Bengaluru, Karnataka, India.
[2]Department of ISE,Rajarajeswari College of Engineering ,Bengaluru, Karnataka, India.
[3]Department of CSE, Rajarajeswari College of Engineering, Bengaluru, Karnataka, India.
[1]svinothkumar1984@gmail.com, [2]amutharajj@yahoo.com,
[3]kavijeyabalan1968@gmail.com

ABSTRACT: Cloud computing is a cost effective flexible and proven delivery platform for providing consumer IT services or business services over internet. It has an ability to provide many services over internet. It not only provides computing services but additional computing resources. To interact with various services in the cloud and to store retrieve data from cloud several security mechanism is required. Cryptography and key management mechanism are one of the import services in the cloud to secure data. In this context, this paper investigates the basic problem of cloud computing with cryptography and key management system for enabling support of interoperability between cloud cryptography client and key management services.

Keywords— Cloud Computing, Cryptography, Key Management.

1. Introduction

Cloud computing is a computing model, in which all resource on Internet form a cloud resource pool and can be allocated to different applications and services dynamically. Compared with traditional distribute system, a considerable amount of investment saved and it brings exceptional elasticity, scalability and efficiency for task execution. By utilizing Cloud Computing services, the numerous enterprise investments in building and maintaining a supercomputing or grid computing environment for smart applications can be effectively reduced. Despite these advantages, security requirements dramatically rise when storing personal identifiable on cloud environment. With the view of privacy protection and data security, users usually choose to encrypt the data before uploading. How to search for encrypted data on a cloud without divulging the content of the data has always been a requirement for user privacy protection.

Cryptography can help dawning integration of Cloud Computing by increased number of privacy related companies. The primary level of privacy where cryptography can help Cloud computing is safe and secure storage. Cryptography is the science of storing messages securely by converting the raw data into forms which is not readable [28]. In today's world, cryptography is considered as a collection of

P-ISSN: 2204-1990; E-ISSN: 1323-6903
DOI: 10.47750/cibg.2021.27.03.238

three algorithms. These algorithms are Symmetric-key algorithms, Asymmetric-key algorithms and Hashing. In Cloud computing, the main problems are related to problem in data security, backup data, network traffic, file storage system, and security of host, and cryptography alone can solve these issues to extents. For a safe and secure communication between the guest domain and the host domain, or from hosts to management systems, encryption technologies, such as Secure HTTP, encrypted VPNs, TLS, Secure Shell and so on should be used. Encryption will help to prevent such exploits like man-in-the-middle, spoofed attacks, and session hijacking.

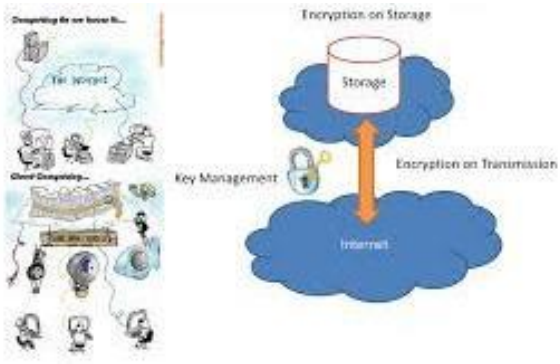

Fig: 1.Data Encryption and key management [31]

Key is important aspect for maintaining security. e.g maintaining security of home, maintaining security of data. Cryptography key can be used to keep the data confidential from the others. e.g. Symmetric key or asymmetric key. So if there are multiple users in the system, key management system (KMS) has to create the key for each user, distribute it to the users. If the key is crashed, KMS has to recover the key. If key is not being used, KMS has to delete the key. Key is associated with the metadata. Metadata contains information about Key label, Key identifier, Key life cycle states, cryptographic algorithm, parameters for the key, length of key, key usage count. Key life cycle contains various states such as creation, initialization, full distribution, active, inactive and termination [35].

2. Related work

Si Han et al.[1] proposed a novel group key management protocol for the data sharing in the cloud storage. In secret sharing group key management protocol (SSGK), uses RSA and verified secret sharing to make the data owner achieve fine-grained control over the outsourced data without relying on any third party. Moreover the author demonstrate that protocol exhibits less storage and computing complexity. Security mechanism in scheme guarantees the privacy of grids data in cloud storage. Encryption secures the transmission on the public channel; verified security scheme make the grids data only accessed by authorized parties. The better performance in terms of storage and computation make the scheme more practical.

Jinan Shen et al[2], approached on the characteristics and data security requirements of the cloud environment, present a scheme for a multi-security-level cloud storage system that is combined with AES symmetric encryption and an improved identity-based proxy re-encryption (PRE) algorithm. The optimization includes support for fine-grained control and performance optimization. Through a combination of attribute-based encryption methods, add a fine-grained control factor to algorithm in which

P-ISSN: 2204-1990; E-ISSN: 1323-6903
DOI: 10.47750/cibg.2021.27.03.238

each authorization operation is only valid for a single factor. Based on the characteristics and data security requirements of the cloud environment, present a scheme for a multi-security-level cloud storage system that is combined with AES symmetric encryption and an improved identity-based proxy re-encryption (PRE) algorithm. The optimization includes support for fine-grained control and performance optimization. Through a combination of attribute-based encryption methods, add a fine-grained control factor to our algorithm in which each authorization operation is only valid for a single factor.

Shengmin Xu et al. [3] summarized a down to earth trait based access control framework for IoT cloud by presenting a productive revocable quality based encryption conspire that allows the information proprietor to effectively deal with the qualifications of information clients. The proposed framework could effectively manage both mystery key disavowal for defiled clients and incidental decoding key introduction for legitimate clients.

Kwangsu Lee [4], in this researcheed on revocable attribute-based encryption (RABE) systems, which provided user revocation function and ciphertext update function by extending attribute-based encryption (ABE) systems that provide access control to ciphertexts, are actively being studied. A new RABE scheme that combines ABE and identity-based encryption (IBE) schemes to efficiently handle ciphertext update and user revocation functionality. In this paper, showed that there is a serious security problem in RABE scheme such that a cloud server can obtain the plaintext information of stored ciphertexts by gathering invalidated credentials of revoked users. Additionally, also showed that the RABE scheme of can be secure in a weaker security model where the cloud server cannot obtain any invalidated credentials of revoked users. In addition, if a self-updatable encryption scheme is used, a data owner does not need to use a secure channel when he sends a ciphertext to cloud storage.

Rashad elhabob et al [5] explained goal of this paper is an approved cloud server has the consent to execute the correspondence test on scrambled information and recover the outcome without knowing any important data about the ciphertext. The technique utilizing is a Certificateless Public Key Cryptography with Equality Test (CL-PKC-ET) conspire is shown under the Bilinear Diffie-Hellman suspicion in the irregular prophet model.

Shakkeera L et al [6] proposed the work is to build up a safe community oriented key administration framework for versatile cloud information stockpiling by executing record encryption, key age, key conveyance (key encryption and key decoding) and document decoding strategies. For the information stockpiling DriverHQ open cloud foundation is utilized. It tends to be effortlessly gotten to, oversaw, share or distribute the documents from anyplace whenever. RSA calculation is utilized for documents encryption and unscrambling. The mystery keys are created by utilizing PRNG calculation that produces successions of irregular numbers. For the key encryption and unscrambling forms, key example coordinating calculation is executed. In key unscrambling, transitional keys of customer, cloud server and decoding server are coordinated by design coordinating procedure. The calculation accomplishes the security for the document information and key by dispensing with key escrow and key introduction issues. Information trustworthiness and information secrecy in portable cloud storage is accomplished and the framework additionally limits calculation and capacity overheads in customer cell phones, and limits the vitality utilization of cell phones.

Jing Wang et al [7] explained the ability to accomplish private and secure correspondence between end clients and edge servers is vital in edge registering based keen lattice foundation. In this paper

P-ISSN: 2204-1990; E-ISSN: 1323-6903
DOI: 10.47750/cibg.2021.27.03.238

introduced a novel unknown confirmation and key understanding convention with productive key administration, the proposed convention not just gives fundamental security properties (i.e., shared verification, secure key understanding and replay assaults) however it additionally accomplishes other significant security properties. The feature of this convention is that it offers proficient key update and renouncement with diminished correspondence costs, and contingent personality secrecy with decreased calculation costs discoveries of the exhibition assessment additionally shows that the proposed convention is much increasingly effective.

Junsong Fu et al [8] used two methods of Key-Policy Attribute-Based Hierarchical document collection Encryption (KP-ABHE) plan and Cipher content Policy Attribute-Based Hierarchical report assortment Encryption(CP-ABHE) plan to limit the size of ciphertext and security enters essentially decline as far as encryption/unscrambling proficiency and extra room. In any case, each record is encrypted individually what's more, an information client can unscramble a record by using attribute keys set matches the access structure of the document.

Jinbo Xiong et al [9], proposed a novel secure role re-encryption system (SRRS), which is based on convergent encryption and the role re-encryption algorithm to prevent the privacy data leakage in cloud and it also achieves the authorized deduplication and satisfies the dynamic privilege updating and revoking. Meanwhile, system supports ownership checking and achieves the proof of ownership for the authorized users efficiently. Specifically, introduce a management center to handle with the authorized request and establish a role authorized tree (RAT) mapping the relationship of the roles and keys. With the convergent encryption algorithm and the role re-encryption technique, it can be guaranteed that only the authorized user who has the corresponding role re-encryption key can access the specific file without any data leakage.

Yanqing Yao[10], proposed a key-aggregate encryption scheme and a key-aggregate searchable encryption scheme which are both based on a lattice problem (i.e., the Learning with Errors problem).In this a basis delegation algorithm is designed to generate the aggregate key without increasing the lattice dimension. The encryption algorithms of the two schemes are trickily devised to make the encrypted files decryptable or searchable. The presented the schemes' correctness proof, formal security analysis as well as performance analysis, which confirm that, are provably secure and practically efficient. To the best of knowledge, the former is the first lattice-based key-aggregate encryption scheme and the latter is the first lattice-based key-aggregate searchable encryption scheme. Also demonstrated application to cloud storage for searchable group data sharing by combining the two schemes.

Shangping Wang [11], proposed a verifiable and multi-keyword searchable attribute-based encryption (VMKS-ABE) scheme for cloud storage, in this new scheme multi-keyword can be searched and the search privacy is protected. That is, the cloud sever can search the multi-keyword with keyword search trapdoor but it does not know any information of the keywords searched. In the proposed scheme, many computing tasks are outsourced to the cloud proxy server, which greatly reduces the computing burden at user client. Besides, the scheme also supports the verification of the correctness of outsourced private key. The proposed scheme is proved secure that the keyword index is indistinguishable under the adaptive keyword attacks in the general group model, and the ciphertext is selective secure under selective plaintext attacks in the random oracle model.

Manreet Sohal et al. [13] expressed a novel symmetric key cryptographic procedure which is

P-ISSN: 2204-1990; E-ISSN: 1323-6903
DOI: 10.47750/cibg.2021.27.03.238

propelled by DNA cryptography. The proposed conspire utilizes dynamic encoding tables that are irregular in nature which prompts higher security. The security examination demonstrates that the proposed conspire is CPA-secure. The trial results show that proposed approach outperforms other symmetric key encryption algorithms (DNA, AES, DES, Blowfish) in terms of ciphertext size, encryption time and throughput. It is explained dynamic encoding tables that are random in nature which leads to higher security. In this paper security analysis proves that the proposed scheme in CPA-secure. They reduce the size of ciphertext, encryption time and throughput.

Ahmed bentajer et al. [14] introduced the CS-IBE design based upon ID-based encryption, that aims to strengthen the sensitive data confidentiality in public cloud storage. The CS-IBE design associates files with at least one file access policies, namely the user identity (ID) that will be used as the encryption key. Files are encrypted with the user identity key before outsourcing them to cloud storage side which will add a security layer to the outsourced data. Furthermore, CS-IBE works as an overlay system atop cloud storage solutions. In order to evaluate its security and efficiency, a CS-IBE's prototype design is implemented and analyzed.

Kumar, V,et al[15],with the fast progress of network communication, its technologies and the developing popularity of telecare medical information system (TMIS), doctors provide treatment to patients via Internet without visiting hospitals. By using mobile device, wireless body area network and cloud based architecture, the patients can gather their physiological information and upload to cloud via their mobile devices. The authenticated doctor provides online treatment to patient at anytime and anywhere. Moreover, TMIS maintains security and privacy of the patients in information communication and authenticated to all the participants before assessing this system. The paper is the approach of an enhanced secure and efficient elliptic curve cryptography based mutual authentication protocol for cloud-assisted TMIS. The proposed protocol secure against man-in-the-middle attack, patient anonymity, replay attack, known-key security property, data confidentiality, data non-repudiation, message authentication, impersonation attack, session key security and patient unlinkability. This ensures of all desirable security prerequisites and managed the efficiency in terms of computation and communication costs for cloud-assisted TMIS.

Maadala Chandra Sekhar[16], proposed a notion called revocable-storage identity-based encryption (RS-IBE), which can provide the forward/backward security of cipher text by introducing the functionalities of user revocation and cipher text update simultaneously. Furthermore, the author presents a concrete construction of RS-IBE, and proves its security in the defined security model. The performance comparisons indicate that the proposed RS-IBE scheme has advantages in terms of functionality and efficiency, and thus is feasible for a practical and cost-effective data-sharing system. It is provided implementation results of the proposed scheme to demonstrate its practicability.

Luca Ferretti et al. [17] proposed a novel plan that permits cloud occupants to distinguish unapproved changes to information re-appropriated to untrusted cloud suppliers. Open cloud databases are engaging administrations that permit organizations to redistribute information the board frameworks, however their selection is frustrated by worries about secrecy and trustworthiness of data oversaw by a third subject. The creator show that the arrangement, in light of scrambled Bloom channels, is appealing particularly on account of metered organize traffic and capacity, that is regular in cloud database administration offers. The proposed arrangement permits the inhabitant to tune the exchange off between

P-ISSN: 2204-1990; E-ISSN: 1323-6903
DOI: 10.47750/cibg.2021.27.03.238

the likelihood of identifying unapproved information changes and capacity and system overhead. It show that the convention is relevant to designs that depend on a halfway confided in intermediary and to disseminated autonomous customers. The systematic procedures that permit to figure the best size of the Bloom channels to limit stockpiling and system overhead and the cloud administration costs.

Niharika Singh[18], presented a state-of-the-art review of the methodologies and approaches that are currently being used to cope with the significant issue of privacy. In this categorized the privacy-preserving approaches into four categories, i.e., privacy by cryptography, privacy by probability, privacy by anonymization and privacy by ranking. Moreover, developed taxonomy of the techniques that have been used to preserve the privacy of the governing data. And also presented a comprehensive comparison of the privacy-preserving approaches from the angle of the privacy-preserving requirements' satisfaction. Therefore, it is highly desirable that the mechanisms should be developed to deploy efficient auditing and accountability mechanisms that anonymously monitor the utilization of data records and track the provenance to ensure the confidentiality of the data.

Guofeng Lin et al[19], propose a novel collaborative key management protocol to enhance both security and efficiency of key management in ciphertext policy attribute-based encryption for cloud data sharing system. Distributed key generation, issue and storage of private keys are realized without adding any extra physical infrastructure. Authors introduce attribute groups to build a private key update algorithm for fine-grained and immediate attribute revocation. The proposed collaborative mechanism perfectly addresses not only key escrow problem but also a worse problem called key exposure that previous research hardly noticed. Meanwhile it helps to optimize clients' user experience since only a small amount of responsibility is taken by them for decryption. Thus, the proposed scheme performs better in cloud data sharing system serving massive performance-restrained front-end devices with respect to either security or efficiency.

Baojiang Cui et al[21], addressed the implied need for secure communication, storage, and complexity, these clearly renders the approach of practical problem, which is largely neglected in the literature, by proposing the novel concept of key-aggregate searchable encryption and instantiating the concept through a concrete Key-Aggregate Searchable Encryption(KASE) scheme, in which a data owner only needs to distribute a single key to a user for sharing a large number of documents, and the user only needs to submit a single trapdoor to the cloud for querying the shared documents. The security analysis and performance evaluation both confirm that proposed schemes are provably secure and practically efficient.

Kefeng Fan[22],In this paper, a new usage control protocol model—multi-UCON (MUCON) based on usage control (UCON), combined with encryption technology and the digital watermarking technology, is proposed with the characteristics of flexible accrediting, feature binding, and off-line controlling. The analysis and simulation experiments indicate that the proposed protocol model is secure, reliable, and easy to be implemented, which can be deployed in cloud computing environments for data protection.

Lewis Nkenyereye [23], presented a secure billing protocol over attribute-based encryption in vehicular cloud computing. In this way achieved the identity privacy of the vehicles and their requested services through pseudonym techniques. Certificateless signature scheme is used to assure the authentication of legitimate vehicles which can enjoy the provided services. Used attribute-based

P-ISSN: 2204-1990; E-ISSN: 1323-6903
DOI: 10.47750/cibg.2021.27.03.238

encryption to guarantee access control based on the purchased services. Author make use of hash chain technique to provide authorization through electronic voucher (credits) which a vehicle has to possess in order to purchase a service. Unlike existing protocols in VANETS, the proposed protocol is not built on expensive bilinear pairing operations. This is provided the efficiency of the proposed protocol through performance analysis and simulation.

Jongkil Kim et al [24], Introduced a cloud storage system that offers cryptographically enforced security. In contrast to other cryptographically protected cloud storage systems, this supports a fine-grained access control mechanism and allows flexible revocations of invalid users without moving the data and relying on the cloud service providers. This system employs an attribute-based encryption technique to support a complex access structure that allows a user to define human readable access policies to the data in the cloud storage. In addition, system supports a flexible revocation scheme that can revoke invalid users directly by updating the revoked users' list or indirectly by updating an epoch counter. The system administrator can choose one of these options flexibly depending on the needs. This system also allows authorized users to update the encrypted data, and any users accessing such updated data in future can verify whether the data are modified by authorized users.

Jiguo Li, Xiaonan Lin et al[25], explained as the amount of encrypted files stored in cloud is becoming very huge, which will hinder efficient query processing. To deal with above problem, presented a new cryptographic primitive called attribute-based encryption scheme with outsourcing key-issuing and outsourcing decryption, which can implement keyword search function (KSF-OABE). The proposed KSF-OABE scheme is proved secure against chosen-plaintext attack (CPA). CSP performs partial decryption task delegated by data user without knowing anything about the plaintext. Moreover, the CSP can perform encrypted keyword search without knowing anything about the keywords embedded in trapdoor.

Rishi Kumar Sharma et al [26], discussed the key management mechanisms in order to protect the confidentiality of the data. The authors realize that the key management mechanism is more important than the key generation. Various stages, many challenges, few techniques are discussed in this paper to understand the Re-key management mechanisms in a better way. The scheme is suitable for personal cloud storage and especially available to enterprise users to management their key of different kinds of resources. The Re-key management mechanism along with its components discussed here solves better solution and gives a new approach for the confidentiality of the data.

Lan Zhou et al [27], introduce a cryptographic administrative model AdC-RBAC for managing and enforcing access policies for cryptographic RBAC schemes. The AdC-RBAC model uses cryptographic techniques to ensure that the administrative tasks are performed only by authorised administrative roles. Then proposed a role-based encryption (RBE) scheme and show how the AdC-RBAC model decentralises the administrative tasks in the RBE scheme thereby making it practical for security policy management in large-scale cloud systems.

P-ISSN: 2204-1990; E-ISSN: 1323-6903
DOI: 10.47750/cibg.2021.27.03.238

Table 1.Comparesion of different cloud security techniques

Authors	Proposed Scheme	Privacy	Integrity	Availability	Confidentiality
[1]Si Han, Ke Han, And Shouyi hang,2019	Sharing group key management protocol (SSGK), uses RSA to data owner achieve fine-grained control.	97%	96.29%	92%	97.61%
[2]Jinan Shen,Xuejian Deng, Zhenwu Xu,2019	Multi-security-level cloud storage system that is combined with AES symmetric encryption.	92.84%	86.82%	97.54%	95.39%
[3].Shengmin Xu, Guomin Yang, Yi Muc, Ximeng Liu,2019.	Access control framework for IoT cloud by presenting a productive revocable quality based encryption	80%	86.56%	88%	91.72%
[4]. Kwangsu Lee,2019.	Revocable attribute-based encryption (RABE) systems	91.77%	89%	93.29%	92.29%
[5].RashadElhabob, YananZhao,Iva Sella,AndHu Xiong,2019.	Certificateless Public Key Cryptography with Equality Test (CL-PKC-ET)	94%	84%	82.92%	90.11%
[6].Shakkeera L , Saranya A,Sharmasth ValiY,2019.	Data storage DriverHQ public cloud infrastructure is used.	90%	92%	95.34%	89.82%
[7].Jing Wang, Libing Wu, Kim-Kwang Raymond Choo, Debiao He,2019.	Novel anonymous authentication and key agreement protocol with efficient key management.	90.44%	91.98%	85.11%	86.39%
[8].Junsong Fu, Na Wang,2019.	Key-Policy Attribute-Based Hierarchical document collection Encryption(KP-ABHE).	91%	97.23%	90.54%	87.55%

P-ISSN: 2204-1990; E-ISSN: 1323-6903
DOI: 10.47750/cibg.2021.27.03.238

[9]. Jinbo Xiong, Yuanyuan Zhang, Shaohua Tang, Ximeng Liu, and Zhiqiang Yao 2019.	A novel secure role re-encryption system (SRRS).	84%	87%	91.65%	85.21%
[10] YANQING YAO, Zhengde Zhai, Jianwei Liu, Zhoujun Li,2019.	A key-aggregate encryption scheme and a key-aggregate searchable encryption scheme.	92%	94.78%	95%	92.36%
[11]. Shangping Wang, Shasha Jia, And Yaling Zhang,2019.	Multi-keyword searchable attribute-based encryption (VMKS-ABE) scheme.	92%	91.71%	90.22%	94.11%
[13].Manreet Sohal, Sandeep Sharma,2018	Novel symmetric key cryptographic technique using DNA cryptography.	88%	85.32%	90%	93.00%
[14].Ahmed Bentajera, Mustapha Hedaboub, Karim Abouelmehdic, Said ELFEZAZI,2018	ID-based encryption, that aims to strengthen the sensitive data confidentiality in public cloud storage.	91.05%	82.11%	90.23%	93.11%
[15] Kumar, V., Ahmad, M., Kumari, A.,2018	An enhanced secure and efficient elliptic curve cryptography based mutual authentication protocol.	94%	93%	90%	90.49%
[16] Maadala Chandra Sekhar, Keerthi Kethineni,2018	Revocable-storage identity-based encryption (RS-IBE), for provide the forward/backward security.	90%	82.83%	84.94%	91.21%

P-ISSN: 2204-1990; E-ISSN: 1323-6903
DOI: 10.47750/cibg.2021.27.03.238

[17].Luca Ferretti, Mirco Marchetti, Mauro Andreolini, Michele Colajanni,2017.	A novel plan Encrypted Bloom filters, that permits cloud occupants to distinguish unapproved changes to information re-appropriated to untrusted cloud suppliers.	92%	91%	88.03%	84.33%
[18].Niharika Singh, Ashutosh Kumar Singh,2017	A state-of-the-art review of the methodologies and approaches used to with the significant issue of privacy.	93%	84.328%	86%	82.93%
[19].Guofeng Lin, Hanshu Hong, and Zhixin Sun,2017	A novel collaborative key management protocol to enhance both security and efficiency of key management.	92%	90.34%	91%	94.32%
[21]. Baojiang Cui, Zheli Liu, and LingyuWang,2016	Key-Aggregate Searchable Encryption (KASE) scheme, a data owner only needs to distribute a single key to user.	93.22%	91%	93%	94.24%
[22]. Kefeng Fan, Xiangzhen Yao, Xiaohe Fan, Yong Wang and Mingjie Chen,2016	Multi-UCON (MUCON) based on usage control (UCON), combined with encryption technology and the digital watermarking technology.	91.22%	92.99%	91.77%	90.64%
[23] Lewis Nkenyereye, Youngho Park and Kyung Hyune Rhee,2016.	A secure billing protocol over attribute-based encryption in vehicular cloud	91.56%	89.55%	90.22%	93.67%

P-ISSN: 2204-1990; E-ISSN: 1323-6903
DOI: 10.47750/cibg.2021.27.03.238

	computing.				
[24]. Jongkil Kim, Surya Nepal,2016.	An attribute-based encryption technique to support a complex access structure	89.44%	92.83%	94.55%	95.22%
[25] Jiguo Li, Xiaonan Lin, Yichen Zhang and Jinguang Han, 2016.	Implement keyword search function (KSF) is secure against chosen-plaintext attack.	93.79%	95.22%	94.21%	91.86%
[26] Rishi Kumar Sharma, Dr. R.K.Kapoor, Pavan Kumar Sharma,2016.	Re-key management mechanism	92.97%	88.63%	90.32%	90.69%
[27] Lan Zhou, Vijay Varadharajan, Michael Hitchens,2014.	A role-based encryption (RBE) scheme.	82.57%	89.78%	92.34%	90.32%

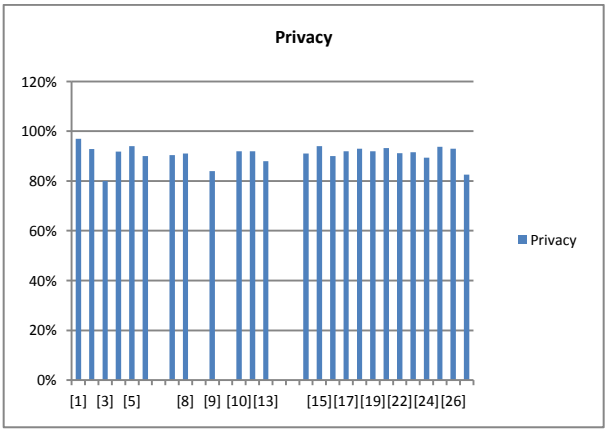

Fig.2.Comparison of Privacy

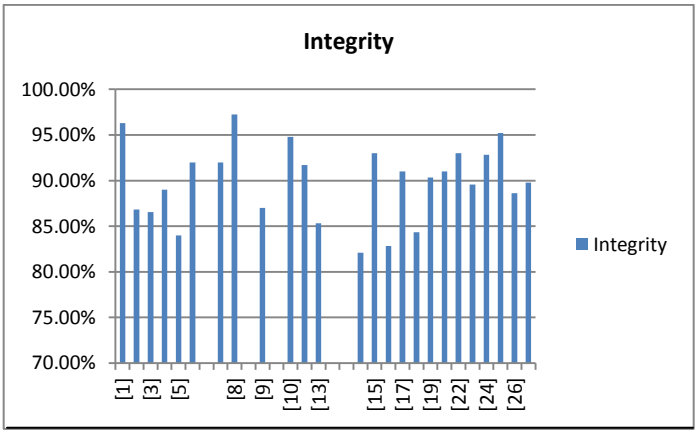

Fig.3 Comparison of Integrity

P-ISSN: 2204-1990; E-ISSN: 1323-6903
DOI: 10.47750/cibg.2021.27.03.238

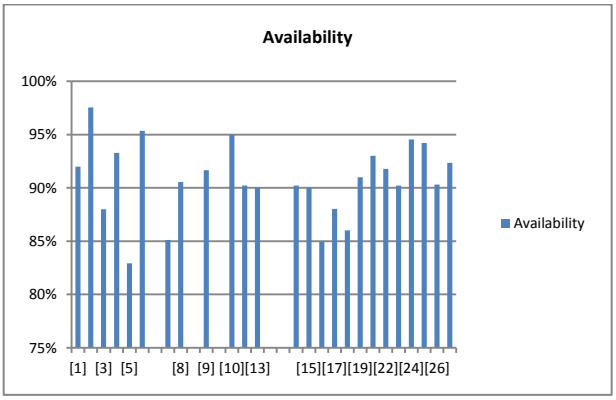

Fig.4.Comprison of Availability

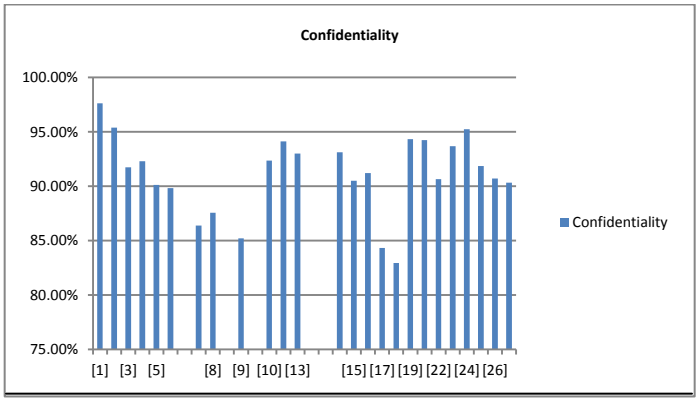

Fig.5.Comparison of Confidentiality

Based on analysis in table and graphs some of the suggestions to secure data with privacy, integrity, availability and confidentiality on cloud are as follows.

a) Suggestion to achieve privacy

Using to secure data Sharing group key management protocol (SSGK), with RSA to data owner achieve highest privacy. Secret sharing group key management protocol (SSGK) to protect the communication process and different from the prior works, a group key is used to encrypt the shared data and a secret sharing scheme is used to distribute the group key in SSGK for privacy. Whereas a productive revocable quality based encryption technique using access control framework for IoT cloud give less privacy.

b) Suggestion to achieve Integrity

Using Key-Policy Attribute- Based Hierarchical document collection Encryption (KP-ABHE) technique getting high integrity. The security of cloud is theoretically proved based on the decisional Bilenear Diffie-Hellman in KP-ABHE and the results illustrate that KP-ABHE and (ciphertext-policy attribute based encryption) CP-ABHE performs very well in terms of security, efficiency and the storage size of the ciphertext. But using ID-based encryption technique provides the integrity is less.

c) Suggestion to achieve availability

Multi-security-level cloud storage system is combined with AES symmetric encryption is concern for achieve to high availability. In multi-security-level cloud storage system implements services such as the direct storage of data, transparent AES encryption, PRE protection that supports fine-grained and ciphertext heterogeneous transformation, and other functions authentication and data management. While using Certificate less Public Key Cryptography with Equality Test (CL-PKC-ET) is give less availability.

d) Suggestion to achieve confidentiality

In sharing group key management protocol (SSGK), uses RSA help to achieve high confidentiality. In SSGK, an efficient solution is proposed to solve the secure problems of data sharing on the cloud storage without relying on any trust third party. Beyond using symmetric encryption algorithm to encrypt the shared data, asymmetric algorithm and secret sharing scheme , is used to prevent the key used to decrypt the shared data from getting by unauthorized users. While using state-of-the-art review of the methodologies and approaches getting less confidentiality.

P-ISSN: 2204-1990; E-ISSN: 1323-6903
DOI: 10.47750/cibg.2021.27.03.238

4. Conclusion

With the continuous promotion of cloud computing, security has become one of the core issues. Cloud computing platform need to provide some reliable security technology to prevent security attacks through cryptography with key management, as well as the destruction of infrastructure and services. In this paper analyzed cryptography and key management security considerations and challenges which are currently faced in the Cloud computing are highlighted. Many enhancements in existing solutions as well as more mature and newer solutions are needed to ensure that cloud computing benefits are fully realized as its adoption accelerates. It is still in infancy, and how the security and privacy landscape changes will impact its successful, widespread adoption. These issues mentioned above will be the research hotspot of cloud computing.

References:

[1].Si Han, Ke Han, and Shouyi hang, A Data Sharing Protocol to Minimize Security and Privacy Risks of Cloud Storage in Big Data Era, *IEEE Access*, volume 7, 2019.

[2]. Jinan Shen,Xuejian Deng, Zhenwu Xu, Multi-security-level cloud storage system based on Improved Proxy re-encryption,https://doi.org/10.1186/s13638-019-1614-y, *springer*, 2019.

[3].Shengmin Xu, Guomin Yang, Yi Muc, Ximeng Liu, A secure IoT cloud storage system with fine-grained access control and decryption key exposure resistance, *Future Generation Computer Systems 97, Elsevier*, (2019) 284–294.

[4]. Kwangsu Lee, Ciphertext Outdate Attacks on the Revocable Attribute-Based Encryption Scheme with Time Encodings, DOI 10.1109/2953300, *IEEE Access*, 2019.

[5].Rashad Elhabob,Yanan Zhao,Iva Sella, and Hu Xiong, Efficient Certificateless Public Key Cryptography with Equality Test for Internet of Vehicles, *IEEE Access*,Volume 7, 2019.

[6].Shakkeera L , Saranya A,Sharmasth ValiY,SecureCollaborative Key Management System for Mobile Cloud Data Storage, *International Journal of Engineering and Advanced Technology (IJEAT)*, Volume-8 Issue-5S3, July, 2019.

[7].Jing Wang, Libing Wu, Kim-Kwang Raymond Choo, Debiao He, Blockchain Based Anonymous Authentication with Key Management for Smart Grid Edge Computing Infrastructure, *IEEE Transactions on Industrial Informatics*, 2019.

[8].Junsong Fu, Na Wang, A Practical Attribute-Based Document Collection Hierarchical Encryption Scheme in Cloud Computing, *IEEE Access*, 2019.

[9]. Jinbo Xiong, Yuanyuan Zhang,Shaohua Tang, Ximeng Liu,And Zhiqiang Yao Secure Encrypted Data With Authorized Deduplication In Cloud,*Digital Object Identifier 10.1109/Access.2019.2920998, IEEE Access*, 2019.

[10] Yanqing Yao, Zhengde Zhai, Jianwei Liu, Zhoujun Li, Lattice-based Key-Aggregate (Searchable) Encryption in Cloud Storage, DOI 10.1109/ACCESS.2019.2952163, *IEEE Access*, 2019.

[11]. Shangping Wang, Shasha Jia, And Yaling Zhang, Verifiable and Multi-keyword Searchable Attribute-based Encryption Scheme for Cloud Storage, DOI

P-ISSN: 2204-1990; E-ISSN: 1323-6903
DOI: 10.47750/cibg.2021.27.03.238

10.1109/ACCESS.2019.2910828, *IEEE Access*, 2019.

[12]Samana Paudel, Data Breach a Cybersecurity Issue in Cloud, https://www.researchgate.net/publication/33 5243297, *IEEE Access*,August,2019.

[13].Manreet Sohal, Sandeep Sharma, BDNA-A DNA Inspired Symmetric Key Cryptographic Technique to Secure Cloud Computing, *Journal of King Saud University - Computer and Information Sciences*, *Springer*, 2018.

[14].Ahmed Bentajera, Mustapha Hedaboub, Karim Abouelmehdic, Said ELFEZAZI, CS-IBE: A Data Confidentiality System in Public Cloud Storage System, *Elsevier*, pp.559–564, (2018).

[15] Kumar, V., Ahmad, M., Kumari, A., A Secure Elliptic Curve Cryptography Based Mutual Authentication Protocol for Cloud-assisted TMIS, doi: https://doi.org/10.1016/ j.tele.2018.09.001. *Elseveir*, 2018.

[16] Maadala Chandra Sekhar, Keerthi Kethineni, Secure Data Sharing in Cloud Computing Using Revocable- Storage Identity-Based Encryption,*IJCSE*, Vol.-6, Issue-7, July 2018.

[17].Luca Ferretti, Mirco Marchetti, Mauro Andreolini, Michele Colajanni,A symmetric cryptographic scheme for data integrity verification in cloud databases, *Journal of Information Sciences*, 2017.

[18].Niharika Singh, Ashutosh Kumar Singh, Data Privacy Protection Mechanisms in Cloud, *Springer*, 2017.

[19].Guofeng Lin, Hanshu Hong, and Zhixin Sun, A Collaborative Key Management Protocol in Ciphertext Policy Attribute- Based Encryption for Cloud Data Sharing, *IEEE Access*, 2017.

[20]Rishav Chatterjee, Sharmistha Roy, Cryptography in Cloud Computing: A Basic Approach to Ensure Security in Cloud, *IJESC*, 2017.

[21]. Baojiang Cui, Zheli Liu, and LingyuWang, Key-Aggregate Searchable Encryption (KASE) for Group Data Sharing via Cloud Storage, *IEEE Transactions On Computers*, Vol. 65, No. 8, August 2016.

[22]. Kefeng Fan, Xiangzhen Yao, Xiaohe Fan, Yong Wang and Mingjie Chen, A new usage control protocol for data protection of cloud environment, DOI 10.1186/s13635-016-0031-6,*springer*,2016.

[23] Lewis Nkenyereye, Youngho Park and Kyung Hyune Rhee, A secure billing protocol over attribute-based encryption in vehicular cloud computing, DOI 10.1186/s13638-016-0687-0, *springer*,2016.

[24]. Jongkil Kim, Surya Nepal, A Cryptographically Enforced Access Control with a Flexible User Revocation on Untrusted Cloud Storage, DOI 10.1007/s41019-016-0014-0, *Springer*, September 2016.

[25] Jiguo Li, Xiaonan Lin, Yichen Zhang and Jinguang Han, KSF-OABE: Outsourced Attribute-Based Encryption with Keyword Search Function for Cloud Storage, DOI 10.1109/TSC.2016.2542813, *IEEE access*, 2016.

[26] Rishi Kumar Sharma, Dr. R.K.Kapoor, Pavan Kumar Sharma, Re-Otp Key Management Mechanism for the Cloud Data Security,*Vol. 5, Issue. 11, November 2016, IJCSMC, pg.44 – 51.*

[27] Lan Zhou, Vijay Varadharajan, Michael Hitchens, Secure administration of cryptographic role-based access

P-ISSN: 2204-1990; E-ISSN: 1323-6903
DOI: 10.47750/cibg.2021.27.03.238

control for large-scale cloud storage systems, http://dx.doi.org/10.1016/j.jcss.2014.04.019,*Elsiver*,2014.

[28]Rajani Devi.T, Importance of Cryptography in Network Security, International Conference on Communication Systems and Network Technologies, *IEEE*, 2013.

[30].Khaled Salah, Jose M. Alcaraz Calero, Sherali Zeadally, Sameera Al-Mulla and Mohammed Alzaabi, Using Cloud Computing to Implement a Security Overlay Network, *IEEE Computer and Reliability Societies*, 2013.