American Scientific Research Journal for Engineering, Technology, and Sciences (ASRJETS)
ISSN (Print) 2313-4410, ISSN (Online) 2313-4402

http://asrjetsjournal.org/

Security of Information in Cloud Computing: A Systematic Review

Mehreen Ansar[a*], Ijaz Ali Shokat[b], Mubeen Fatima[c], Kashif Nazir[d]

[a,b,d]*Department of Computing, Riphah International University, Faisalabad, Pakistan*
[c]*Department of Computing, SEECS, National University of Science and Technology,Islamabad, Pakistan*
[a]*Email: mehreenansar02@gmail.com*
[b]*Email: ijaz342@yahoo.com*
[c]*Email: mubeenfatima40@gmail.com*
[d]*Email: kashifntuf@gmail.com*

Abstract

Data storage in cloud have become a great concern today. Many encryption and decryption methods have already been proposed to secure cloud data but everything comes with its pros and cons, this paper provides a critical overview of these cryptography techniques, issues and solutions regarding its security and availability.

Key words: Cloud Computing; Encryption; Decryption; Cryptography Protocols; Quantum Cryptography.

1. Introduction

Cloud computing is one of the special issue of the current big data needs. The world needs a secure and reliable mean to store and retrieve data. Internet has started driving all new techniques and terminologies. The Internet is strong but not fully safe. Cloud Computing has many data privacy concerns that are giving threats from the combined, virtualized and redistributed resources. Cloud security can be achieved by data integrity, data migration and by applying cryptography techniques. Cloud platform maintains the network connected to hardware for using services through a web application. For example: Amazon, Microsoft Azure, and Google Cloud. Due to big data issues in cloud storage, the need have also increased to every individual and even corporation. The data stored in remote cloud databases or servers can be harmed or attacked by third party and user claim for its security. The cloud storage should allow deletion of file, encryption of file and access to an encrypted file are basic requirement.

---

* Corresponding author.

Thus a technique named cryptography is used to secure data from the third party by converting text into the non-readable form. Security lies with the encryption and decryption techniques during data transfer and retrieval. For security the term cryptography is used to safely send data between two users. Cryptography is referred to encryption, which is the process of converting information from the plain text into cipher text. Two types of Cryptographic algorithms are basically used to share info between sender and receiver: Symmetric key algorithms include the same private keys: DES, AES, 3 DES and Blowfish algorithm. Asymmetric key algorithms include own private and public keys: RSA and Diffie- Hellman Key Exchange. Cryptography is basically encryption and decryption of data by using public and private keys or the hybrid of these in cryptography algorithms. The limitation lies in decrypting data before encryption process but only Homomorphic encryption allows such computations to encrypt safely without decrypting it. Data can be shared from untrusted mean by sharing secret decryption keys through secure channel. Homomorphic encryption allows such confidentiality of the ciphers by use of

- Partially homomorphic : allows only one algebraic operation
- Fully homomorphic : allows both addition and multiplication

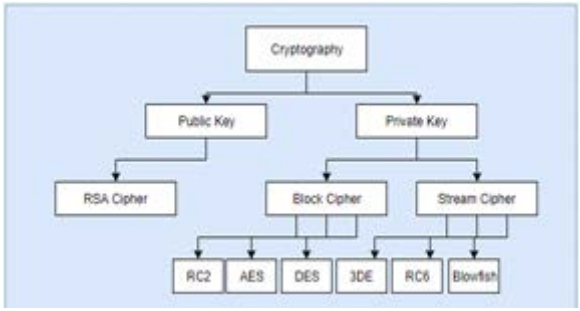

Figure 1: Cryptography Types in cloud

In the Attribute-based encryption (ABE) users have own private key to relate his attributes or access policy. Important ABE types are

- Key-policy: policy is bounded in the private keys,
- Cipher text-policy: policy is bounded in the cipher text

In cloud-based architecture, a client sends her private states to the cloud that performs the MPC computation and returns control inputs. In order to guarantee that the cloud can perform computation without obtaining anything about the client's private data, we employ a partially homomorphic crypto system on:

- A client-server architecture,
- A two-server architecture

In the first case, a control input for the system is privately computed by the cloud server, with the assistance of the customer. In the second case, the control input is privately computed by two independent, non-colluding servers with no additional requirements from the client. Remote data possession checking protocols (RDPC) provide high-quality data storage services. Because of big data cloud storage and servers are not trustworthy anymore; therefore, data owners need a proper medium to regulate the data files in a safe way. Cryptographic attack is basically an approach to crack or break a specific cipher by using any cryptanalysis methods or algorithms. In crypto-shredding, the keys can simply be deleted when there is no more use of the data. IaaS is the recommended for enterprise crypt analysis [1,4].

THE SERVICE MODEL

- PaaS
- SaaS (Less Secure)
- IaaS (More secure)

In Software as a service, users are able to use the application provided by the Cloud vendor. SaaS applications mainly include business applications such as ERP, CRM, SCM, etc. Organizations can also buy the applications from cloud-based vendors for their business purposes. The data is stored in the form of plaintext, which makes it more vulnerable to different types of attack and provides users the least control over the security. In Platform as a service, users can deploy their own application on the cloud infrastructure without installing on their own machine. PaaS don't provide secure connection to vendor. In Infrastructure as a Service users have better control over the security as there is no vulnerability in the Virtual machines provided by the service provider, thus providing the computation power, storage facility and the network facility, which can be vulnerable to the attack. VM's are usually copied with new passwords to provide flexibility to the user, but it can lead to unintentional data leakage.

2. The deployment model

In cloud[14] there are three basic deployment models: public, private, hybrid (public + private) and community cloudA cryptographic protocol or encryption protocol performs a security check and uses different cryptographic methods. A security protocol basically describes the algorithms about data structures and representations at specific point but for later multiple versions of a program can be implemented. Different cryptography protocols have discussed in the below table like Internet Key Exchange, IPsec, Kerberos, Off-the-Record Messaging, Point to Point Protocol, Signal Protocol. Cryptographic protocols are basically for secure and safe data migration at application level. A cryptographic protocol must have at least some of the following aspects:

•How to establish key

•How to authenticate the entity relation

•How to use the symmetric encryption method

•How to secure the application-level data

•How to act against the non-repudiation attacks

• How to share secret key

• How to manage the multi-party authentication while file sharing

Table 1: A table on cryptography algorithms in cloud

Sr. No.	Encryption Algorithms	Keys	Usage	Pros	Cons
1	Attribute-based encryption algorithms	Public key encryption Use private key to decrypt	Set of attributes are matched as private key. Used for open communication /Un protected channel or server.	Reduces the number of keys Fast encryption and decryption	Encrypt the message without obtaining the public key certificate. Dependent on location of user. Lack of Confidentiality.
2	Cipher text-policy ABE (CP-ABE)	public key and private key	Strategy depends on design of access structure and attributes.	Decrypt only if attributes are matched. Provides access control/ authorization facility.	The owner will select the recipient manually to access the file.
3	Key-policy ABE (KP-ABE)	private keys	Attribute sets are used for encryption and decryption	Collision Resistance. Prevent keys from hacks	Lack of monotonic structure Constant Pairing and ciphers schemes.
4	Homomorphic Encryption	Encryption on plain text using public key	Allow computation over encrypted data	Collision Resistant.	Less secure in terms of malleability. Lack of control in deciphers.
5	Partially homomorphic	Direct computations on encrypted data	Homomorphic with algebraic operation either addition or multiplication	Works on deciphering text	Not fully control. Confidentiality issues
6	Fully homomorphic encryption (FHE)	Direct computations on encrypted data	It allows for both sum and product computation	Works on noise in decipher Works in database information. Key recovery strategy.	Size of public key
7	Searchable encryption (SE)	Relay protocol Secret-key using private key Public key	SE for secret-key cryptography is accessible by sourced networks. SE for public-key	Private key help finding answers to particular query.	Lack of support for deletions and insertions

			cryptography are drawn from publicly available cloud analytic relay terminals	Reduce retrieval time	
8	Secret Sharing Scheme(SSS)	Private	Only authorized users will be able to access the secret key	Highly sensitive and secure for storing information.	Use random bits to share data Limited length must be shared or particular key
9	Chosen plain text	Public key cryptography	Attack model for ciphering plain text	Secure with certificates.	Lack of security. Data is loss
10	Known-Plaintext Attack	Use secret keys	Attack model for ciphering plain text	Secure with books and codes.	Short messages Key validity

Table 2: A table on cryptography issues in cloud

S No.	Year	Paper Title	Paper	Problem	Proposed Algorithms	Pros	Future Work
1	2018	Security Analysis of Homomorphic Encryption Scheme for Cloud Computing: Known-Plaintext Attack	[1]	Cloud servers cannot perform computations of encryptions without decrypting it. Homomorphic encryption provides the service but needs a suitable operations for homomorphic cipher	Homomorphic encryption with RNS property + theory of numbers	Used for key generation, data sharing and error correction	Directly related to data redundancy factorization is computationally complex. Proposed algo must have ability to resist plain text attacks.
2	2018	Privacy preserving k-nearest neighbor classification over encrypted database in outsourced cloud environments	[2]	Efficiently support computations but don't provide privacy for KNN classification over the encrypted data	DO's key also provide confidentiality and hiding data patterns to achieve query privacy	Efficient for synthetic and real databases	Need to protect privacy against collusion attacks.
3	2018	Secure attribute-based data sharing for resource-limited users in cloud computing	[3]	Attribute-based encryption (ABE) providing low computation in data sharing	Supports online/offline encryption. Chameleon hash function is used to generate a cipher text	secure and efficient	Need for direct data sharing
4	2018	Secure file storage on cloud using cryptography	[4]	No reliable way of transferring data in cloud	Use of AES, DES and RC2	Secure and have high performance	Not for group sharing One to many, many to one, many to many communication

							is not possible
5	2018	A fully homomorphic–elliptic curve cryptography based encryption algorithm for ensuring the privacy preservation of the cloud data	[5]	Increased complexity, time consumption, and reduced security	Fully homomorphic–elliptic curve cryptography (FH-ECC)	Efficiently reducing the complexity of encryption and decryption	
6	2018	A Novel Efficient Remote Data Possession Checking Protocol in Cloud Storage	[6]	Not fully trustworthy	RDPC protocols are based on homomorphic hash function technique	Reduces the storage costs and computation costs	Cannot insert, modify or delete operation on file blocks
7	2017	Cryptography in Cloud Computing: A Basic Approach to Ensure Security in Cloud	[7]	Data theft Integrity of data Privacy problems Infected Applications	Rijndael Encryption Algorithm along with EAP-CHAP.	Safe data	For linear searching on decrypted data Lattice based Cryptography and ID based Cryptography
8	2017	Security Enhancement for Data Migration in the Cloud	[8]	Exact location of data Vendor level Security User level Security	Advanced Encryption Standard-256 + Information Dispersal Algorithms + Secure Hash Algorithm-512.	Safe migration of data	Not for large files
9	2017	Efficient Protocol for Searchable Encryption and Secure Deletion on Cloud Storages	[9]	Security of cloud	Secure protocol PSS	The PSS supports a secure deletion, the EFS, and a searchable encryption	PSS in the real world
10	2017	Security in Cloud Computing using Honey Encryption	[10]	Security of cloud	Honey Encryption provides assurance against Brute force attack. + SRM	Secure and reliable	Honey encryption with AES for cloud security to lessen vulnerability. Plain text attack

3. Literature review

This section of Literature eventually reveals some facts of Cryptography on the analysis of the author's work.

The author has introduced cryptographic systems for encryption based on the homomorphic (RNS) and Secret Sharing Schemes which help against known-plaintext, where module RNS calculate the secret key to decrypt data [1]. In this paper, author aims to preserve privacy by KNN classification over the encrypted cloud thus saving time and cost [2].

The author aims at ABE, both online and offline cryptography and their computation. The proposed scheme supports both online and offline encryption by allowing anyone to check the validity of cipher texts before decrypting. ABE is less costly [3].

In this paper the main goal is to store and access data by exploiting the encryption technique of elliptic curve cryptography. The proposed approach ensures the privacy and security of client sensitive information by storing data across the cloud, using AES, DES and RC2 algorithm [4].

The author is enabling a security and privacy preservation for the cloud data is one of the demanding and crucial tasks in recent days. Thus, this paper aims to develop a new privacy preservation mechanism by implementing fully homomorphic–elliptic curve cryptography (FH-ECC) algorithm.

The data owner encrypts the original data by converting it into the cipher format with the use of ECC algorithm, and applies the FH operations on the encrypted data before storing it on the cloud. Then, the ECC decryption and FH operations are applied to generate the original text. Based on several analyses, the research work is evaluated with the help of different performance measures such as execution time, encryption time, and decryption time [5].

The author aims at user data storage and computation services. In this paper, author provides a RDPC protocol based hash function which help against forgery attack; replace attack, and replay attack based on a typical security model [6].

In this paper, the author focused on the cloud security issues by proposing cryptography algorithms to ensure and confirm the data security and safety in cloud [7].

The author proposes a model to enhance privacy and security of data by combining Advanced Encryption Standard-256, Information Dispersal Algorithms with Secure Hash Algorithm-512 for medium thresholds. [8]

In this paper the protocol designed is for secure storages inside cloud by Internet users. The performance evaluations support its efficiency [9].

In this paper, Honey encryption generates cipher text, which if provides believable plaintext if incorrect decryption key is used.

Honey Encryption basically helps against Brute force attack. In addition, after the data encryption, SRM (Secure Repository Manager) divides the data into chunks of small data and uploads it to cloud servers [10].

In this review paper a brief description is done on following mentioned proposed models and protocols.

- Homomorphic encryption schemes are dependent on the Residue Number System (RNS) and Secret Sharing Schemes which help against plain text attack.

- The proposed scheme efficiently protects by preserving k-nearest neighbor classification resulting in

DB security, confidentiality and privacy access to data sources.

- Attribute-based encryption (ABE) helps against adaptively chosen text attacks
- Storing data across single cloud, using AES, DES and RC2 algorithm.
- Remote data possession checking (RDPC) protocols with an operation record table (ORT) have been presented
- A model is proposed to enhance data privacy by hybrid combination Advanced Encryption Standard-256 and Information Dispersal Algorithms with Secure Hash Algorithm-512.
- The secure protocol PSS for a secure deletion and the EFS for searchable encryption.
- Honey encryption that generates cipher text, which if provided with an incorrect decryption key, produces a believable plaintext and provides assurance against Brute force attack.

Security in Cloud Computing is a challenging topic as more and more people and organizations are moving towards Cloud. Now, authentication and verification are considered as the most important goals to be fulfilled for physical world (the world we live in) or the virtual world (Internet).

To make the users convinced about the security of Cloud Computing, a lot of work still needs to be done. Cloud Cryptography is complex having limitations in the form of high storage and computation cost.

- User: store data in the cloud and rely on server for computation of data.
- Cloud Service Provider (CSP) manages distributed cloud servers.
- Third Party Auditor (TPA) provides access against risks of cloud data services instead of users.

Table 3: Table on cryptography protocols

Sr No.	Protocols	Usage	Pros	Cons
1.	Transport Layer Security (TLS)	Used to secure web (HTTP/HTTPS) connections using symmetric encryption key but does not have non-repudiation support. The identity of communicating parties is kept authenticated with public key cryptography.	Provide privacy and data integrity Reliable Use codes and certificates	Add latency Needs faster symmetric encryption foe session keys. Need certificates to work and maintain web servers

2.	Application Layer protocols	Basically used to identify threats using Diffie–Hellman key exchange protocol	Reliable Secure	Requires own proxy Is slow for new applications and protocols. Traditional packet filtering
3.	User Identity Management Protocol UIDM	Handling data in the cloud memory and data at rest by pattern matching. Sign in Feature	Authentication using certificates and passwords.	Identity can be hacked
4.	Secure Shell Protocol SSH1 and SSH2	Provides secure channels over untrusted networks in a virtual machine.	Need public key to authenticate Secure Login protocols	Need to download third party SSH client Insecure file transfer protocol/method
5.	Internet Protocol Security (IPSec) MYSEA	Provide the encryption and authentication services	Automatically secure applications at IP Layer Provide transparency	Less efficient to encrypt traffic load
6.	Kerberos	Working on 'tickets' by permitting the nodes to communicate over a secure network. Basically provide client authentication and authorization	Strict Time requirements using tickets Secure use semantics	Single point of failure at key distribution center. Need synchronized clocks. If Security is compromised, Reveal all user data.
7.	Wired Equivalent Privacy(WEP)	Symmetric algorithm provides a single secret key to facilitate communication between two devices. Use same master key	Removes eavesdropping in wireless data transmission Use WEP key as network passwords containing digital sequence	Same digital sequence is required to build a connection Easily crack able keys
8.	WiFi Protected Access(WPA)	It provides 104 bit or a 40 ranked bit encryption key and key does not change Use different master key	Support WEP encryption Use temporary keys to exchange data	Large bandwidth Increase in large data size results in longer transmission Incompatible with hardware

4. Proposed solution

Basic Cryptographic Process

The purpose of this paper is studying protocols for secure cloud computing and secure cloud storage.

The paper objectives can be summarized as:

- A description of the cloud architecture
- A description of hash tree authentication of data elements
- Considering an authentication protocol for cloud computing.

In cloud data is stored through Cloud Service providers (CSP) into a set of cloud servers. Data redundancy can be employed with the technique of erasure-correcting code to minimize faults and crash servers. Sometimes, the user also needs to perform block level operations on his data like the block update, delete, insert and append.

The basic cloud process is shown below in figure; the data is encrypted and decrypted in secure manner by encrypting the plain text and saving in cloud at safe place and on demand data is decrypted and send to user in secure channel. The owner of data store the data in encrypted form and the user who want the access to data needs a key to safely retrieve the data.

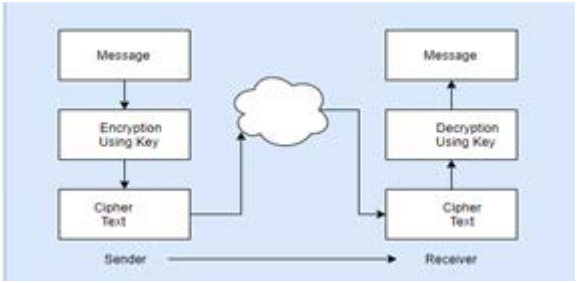

Figure 2: cryptographic process in cloud

But the problem lies when the key is hacked, or the channel is in secure to transfer the keys.

The author Gartner [1] discussed some security risks that are required to be considered before changing cloud computing model. Some problems are discussed as follows:

- Authorized user access provides risk of exposing data to some external platform due to the less control.
- Conformance to regulations: processing data against third-party.
- Storage space for customer and they even have no idea about the exact location of data.
- Data separation due to shared place in cloud reliable and well-tested encryption schemes are needed to sequentially store the data.
- Recovery are not specifically clear how to handle disasters and data failures
- Investigation due to the dispersion of the large amount of data is difficult to relocate data
- Long-term viability for organization to assure data loss because of huge amount for the long-run.

Quantum cryptographic Process:

However In this paper, a proposed architecture of quantum cryptography is discussed to access control in cloud computing. The proposed quantum protocol is used for key distribution, authentication and certification.

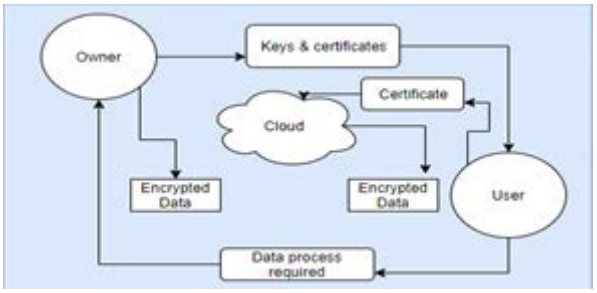

Figure 3: Quantum cryptographic in cloud

The quantum three-pass protocol is still vulnerable to the man-in-the-middle attack. The protocols is unconditional secure and implementable by the current technology. The data saved or retrieval is secure for owner and user as well. The secret key is assumed to the data owner and the user's identity. Quantum mechanics is related to fundamental blocks called bits and can be observed only in two states; 0 and 1 referred as qu bits.

5. Conclusion

In overall paper, I have briefly discussed the protocols, cryptography algorithms and security factors in dealing with the security issues of data retrieval in cloud. I have discussed the basic process and the proposed process for safe and secure communication.

However, the fact lies that the protocols used are still unable to provide confidentiality, integrity and availability of the data. The main concern lies with the dynamic scalability of data inside the cloud. The quantum cryptography is the next step for safe data transfer. For future work lattice based cryptography can be the area of research to ensure safe data storage, safe key sharing and for removing quantum limitations like qu bits and man in the middle attack. It is based on powerful and resistant geometric objects and to construct cryptographic primitives and boundaries by hiding the identity as well. For example it can be helpful during auctions or data mining, during voting's and negotiations.

Future Work:

Still there are challenges in Quantum computing which can become the source of future consideration including noise in electromagnetic couplings and Qubits suffer from bit-flips (a zero can become one and vice versa)

However, Lattices are geometric objects and a*re powerful, resistant to sub-exponential and quantum attacks

Our goal can be to use lattices to construct cryptographic primitives and boundaries which are truly efficient and functional.

It can be beneficial in cases when parties want to share the data abut don't want to reveal their identity for example, during auctions or data mining, during voting's and negotiations.

Secure multi-party computation (MPC) allows set of parties with a private input, to securely and jointly perform

such computations.

References

[1]. Babenko, M., Chervyakov, N., Tchernykh, A., Kucherov, N., Deryabin, M., Radchenko, G., & Svyatkin, V. (2018, January). Security analysis of homomorphic encryption scheme for cloud computing: Known-plaintext attack. In Young Researchers in Electrical and Electronic Engineering (EIConRus), 2018 IEEE Conference of Russian (pp. 270-274). IEEE.

[2]. Wu, W., Parampalli, U., Liu, J., & Xian, M. (2018). Privacy preserving k-nearest neighbor classification over encrypted database in outsourced cloud environments. World Wide Web, 1-23.

[3]. Li, J., Zhang, Y., Chen, X., & Xiang, Y. (2018). Secure attribute-based data sharing for resource-limited users in cloud computing. Computers & Security, 72, 1-12.

[4]. Selvanayagam, J., Singh, A., Michael, J., & Jeswani, J. (2018). Secure file storage on cloud using cryptography.

[5]. Kanna, G. P., & Vasudevan, V. (2018). A fully homomorphic–elliptic curve cryptography based encryption algorithm for ensuring the privacy preservation of the cloud data. Cluster Computing, 1-9.

[6]. Yan, H., Li, J., Han, J., & Zhang, Y. (2017). A novel efficient remote data possession checking protocol in cloud storage. IEEE Transactions on Information Forensics and Security, 12(1), 78-88

[7]. Chatterjee, R., Roy, S., & Scholar, U. G. (2017). Cryptography in Cloud Computing: A Basic Approach to Ensure Security in Cloud. International Journal of Engineering Science, 11818.

[8]. Ngnie Sighom, J. R., Zhang, P., & You, L. (2017). Security Enhancement for Data Migration in the Cloud. Future Internet, 9(3), 23.

[9]. Yu, J. W., & Choi, H. K. (2017, January). Efficient Protocol for Searchable encryption and secure deletion on cloud storages. In Consumer Electronics (ICCE), 2017 IEEE International Conference on (pp. 444-447). IEEE.

[10]. Min, Z., Yang, G., & Shi, J. (2017). A privacy-preserving parallel and homomorphic encryption scheme. Open Physics, 15(1), 135-142.

[11]. Mavroeidis, V., Vishi, K., Zych, M. D., & Jøsang, A. (2018). The Impact of Quantum Computing on Present Cryptography. arXiv preprint arXiv:1804.00200.

[12]. Lorünser, T., Krenn, S., Striecks, C., & Länger, T. (2017). Agile cryptographic solutions for the cloudWirkungsvolle Kryptographie-Lösungen für Cloud Computing. e & i Elektrotechnik und Informationstechnik, 134(7), 364-369.

[13]. Qiu, L., Sun, X., & Xu, J. (2017). Categorical quantum cryptography for access control in cloud computing. Soft Computing, 1-8.

[14]. Shankar, V., & Singh, K. (2018). Applications of Attribute-Based Encryption in Cloud Computing Environment. In Big Data Analytics (pp. 687-692). Springer, Singapore.

[15]. Hassan, N. A., & Hijazi, R. (2017). Cryptography and Secure Communication. In Digital Privacy and Security Using Windows (pp. 195-272). Apress, Berkeley, CA.

[16]. Hammami, H., Brahmi, H., Brahmi, I., & Yahia, S. B. (2017, September). Using Homomorphic Encryption to Compute Privacy Preserving Data Mining in a Cloud Computing Environment. In European, Mediterranean, and Middle Eastern Conference on Information Systems (pp. 397-413). Springer, Cham.

[17]. Alexandru, A. B., Morari, M., & Pappas, G. J. (2018). Cloud-based MPC with Encrypted Data. arXiv preprint arXiv:1803.09891.

[18]. Olanrewaju, R. F., Islam, T., Khalifa, O. O., Anwar, F., & Pampori, B. R. (2017). Cryptography as a Service (CaaS): Quantum Cryptography for Secure Cloud Computing. Indian Journal of Science and Technology, 10(7).

[19]. Ogiela, M. R., & Ogiela, L. (2017, November). Application of Cognitive Cryptography in Fog and Cloud Computing. In International Conference on Broadband and Wireless Computing, Communication and Applications (pp. 293-298). Springer, Cham.

[20]. Wang, X. A., Xhafa, F., Wu, G., & Wang, W. (2016, November). Toward Construction of Encryption with Decryption Awareness Ability for Cloud Storage. In International Conference on P2P, Parallel, Grid, Cloud and Internet Computing (pp. 281-291). Springer, Cham.

[21]. El-Sofany, H. F., & El-Seoud, S. A. (2016, September). Studying Security of Data in Cloud Computing Through Cryptographic Approach. In International Conference on Interactive Collaborative Learning (pp. 433-443). Springer, Cham.

[22]. Mohammad, O. K. J., El-Horbaty, E. S. M., & Salem, A. B. M. (2016). Ciphering of Cloud Computing Environment Based New Intelligent Quantum Service. In New Approaches in Intelligent Control (pp. 241-272). Springer, Cham.F

[23]. Ogiela, M. R., & Ogiela, L. (2016, November). Application of Personalized Cryptography in Cloud Environment. In International Conference on P2P, Parallel, Grid, Cloud and Internet Computing (pp. 253-257). Springer, Cham.

[24]. Parit, S. C., & Rachh, R. (2017). Ciphertext Policy Attribute Based Encryption.

[25]. Dai, W., Doröz, Y., Polyakov, Y., Rohloff, K., Sajjadpour, H., Savaş, E., & Sunar, B. (2018). Implementation and evaluation of a lattice-based key-policy ABE scheme. IEEE Transactions on Information Forensics and Security, 13(5), 1169-1184.

[26]. Odelu, V., Das, A. K., Rao, Y. S., Kumari, S., Khan, M. K., & Choo, K. K. R. (2017). Pairing-based CP-ABE with constant-size ciphertexts and secret keys for cloud environment. Computer Standards & Interfaces, 54, 3-9