Data Security and Access Control Policies In Cloud Computing: A Review

Jobandeep Kaur[1], Dr.Vishal Bharti[2]
[1]M. Tech (Scholar), [2]Head of Department
Department of Computer Science and Engineering, Chandigarh University, Gharuan, Punjab (INDIA)

Abstract – The main goal of access control is to freeze the actions of users as per their authorizations. The basic idea initiated from the concept of multiuser framework n 1970s. Several access requirements are essential for access control. Access control is essential for data storage on cloud. Cloud computing architecture consists of hardware, application, and platform and infrastructure layer. Various types of clouds are available. We studied the validation and advanced mark conspires that are created so far require an outsider server which is aimlessly trusted by the greater part of the imparting substances. In the verification frameworks, the trusted outsider is acknowledged as a validation server by means of which the confirmation messages go through. Be that as it may, in the computerized signature frameworks, the trusted outsider is an expert which confirms the character of a few elements of the system. Verification is the procedure in which a substance demonstrates his/her personality to the associate element. In the event that the correspondence is bona fide, at that point the beneficiary can fulfil himself that the sender is really who he claims to be. Be that as it may, the beneficiary can't demonstrate this reality to a third individual. This question can be settled by computerized marks. An advanced mark is a snippet of data that is sent alongside the message and can be produced just by the sender. We surveyed several previous literatures to get better view of third party authentication, digital signature system, key related issues and certification mechanisms and several cryptography algorithm such as DES, Blowfish and AES, etc.

Keywords *– Cloud Computing, Encryption, Data Storage, TPA (Third Party Authentication).*

I. INTRODUCTION

The access control is an essential part of data sharing framework. It depends upon the security features of computer. The idea of access control starts with multi-application and multi-user online framework in 1970s. New applications and systems are incorporated with new permissions granted, and permissions can be revoked from roles as per requirements. [1] Many organizations preferred to centrally control and maintain access rights, not so much at the system administrator's personal discretion but more in accordance with the organization's protection guidelines. The restriction of access control is actions of user as well as execution of programs on behalf of users are allowed to do. This way access control seeks to prevent activity that could lead to security breach. The access control is not an entire solution to system security, it must be coupled with auditing. [2]

Access Requirements

Several requirements of generic access control model for collaborative environments must support:

Multiple, dynamic user roles: The model should allow users' access rights to be inferred from their roles. Moreover, it must allow users to take multiple roles simultaneously and change these roles dynamically during different phases of collaboration.

Collaboration rights: Besides traditional operations such as read and write, all other operations whose results can affect multiple users should be protected by collaboration rights.

Flexibility: The system should support fine-grained subjects, objects, and access rights, that is, it should allow independent specification of each access right of each user on each object.

Easy specification: Users should be able to specify access definitions easily.

Efficient storage and evaluation: The storage of access definitions and evaluation of the access checking rule should be efficient.

Automation: The model should make it easy to implement access control in multi-user applications. These requirements are motivated in more detail in the following sections along with our approach for meeting them. [3]

The idea of encryption is simple enough. The sender applies an encryption functions to the original plain text message, the resulting cipher text message is sent over the network, and the receiver applies a reverse function known as the decryption to recover the original plain text. The encryption/decryption process generally depends on a secret key shared between the sender and the receiver. When a suitable combination of a key and an encryption algorithm is used, it is sufficiently difficult for an eavesdropper to break the cipher text, and the sender and the receiver can rest assured that their communication is secure. The familiar use of cryptography is designed to ensure privacy-preventing the unauthorized release of information and privacy. It also is used to support other equally important services, including authentication (verifying the identity of the remote

participant) and integrity (making sure that the message has not been altered).

II. CLOUD COMPUTING TYPES AND ARCHITECTURE

Cloud computing is a vague technique terminologies. Cloud computing is used in several scenarios, and cloud computing are hyped by many companies for business promotion. CC is a computing technique where IT services are provided by massive low-cost computing units connected by IP networks. Cloud computing is rooted in search engine platform design. Various features of cloud computing: (1) Large scale computing resources (2) High scalability & elastic (3) Shared resource pool (4) Dynamic resource scheduling and (5) General purpose. [4]

Cloud Computing Architecture

The architectural, business and various operation models of cloud computing. The architecture of a cloud computing environment is divided in 4 layers:

- Hardware Layer
- Infrastructure Layer
- Platform Layer
- Application Layer

Contrasted with conventional administration facilitating conditions, for example, devoted server cultivates, the design of distributed computing is more measured. Each layer is inexactly combined with the layers above and beneath, enabling each layer to advance independently. This is like the plan of the OSI show for organize conventions. The engineering seclusion permits distributed computing to help an extensive variety of utilization prerequisites while lessening administration and support overhead. [5]

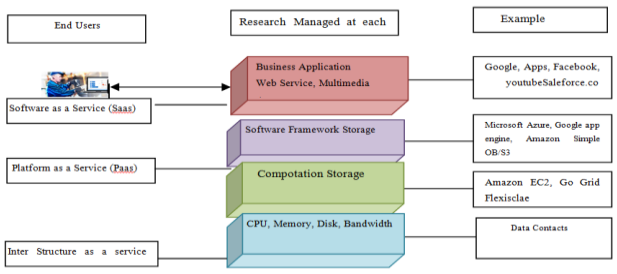

Fig 1. Architecture of Cloud Computing

Types of clouds

There are many issues to consider when moving an enterprise application to the cloud environment. Different types of clouds, has their own benefits and drawbacks:

Public clouds: service providers offer their resources as services to public in these clouds. Public clouds offer several key benefits to service providers, including no initial capital investment on infrastructure and shifting of risks to infrastructure providers. Such clouds deprived of fine-grained control over data, network and security settings, which hampers their effectiveness in many business scenarios.

Private clouds: These are designed for exclusive use by an organization. It offers the highest degree of control over performance, reliability and security. These clouds are usually denounced for being identical to traditional proprietary server farms and do not provide benefits such as no up-front capital costs.

Hybrid clouds: It's an integration of public and private cloud models and tries to address the restrictions of each approach. In a mixture cloud, some portion of the administration framework keeps running in private mists while the rest of the part keeps running in broad daylight mists. Half breed mists offer more adaptability than both open and private mists. In particular, they give more tightly control and security over application information contrasted with open mists, while as yet encouraging on-request benefit development and withdrawal.

Virtual Private Cloud: An alternative solution to addressing the limitations of both public and private clouds is called Virtual Private Cloud (VPC). A VPC is essentially a platform running on top of public clouds. [5]

III. LITERATURE REVIEW

D Koo et al., 2013 [6] Proposed a magnificent data retrieval approach using attribute-based encryption. The proposed scheme was best suited for cloud storage systems with massive amount of data. It provides rich expressiveness as regards access control and also fast searches with simple comparisons of searching entities. The proposed scheme guarantees data security and user privacy during the data retrieval process.

Hoang T. Dinh, et al., 2013 [7] surveyed the Mobile cloud computing to provide overview of concept, architecture and its implementation along with challenges and existing solutions. Additionally, with a numerous growth of mobile applications and appearance of cloud computing concept, mobile cloud computing (MCC) has been introduced to be a potential technology for mobile services. MCC integrates the cloud computing into the mobile environment and overcomes obstacles related to the performance and security discussed in mobile computing.

Hyun Kim et al., 2004 [8] presented a technique to encrypt a digital hologram of a three-dimensional (3D) object into a stationary white noise by use of virtual optics and to decrypt it digitally. In this approach the digital hologram is encrypted by our attaching a computer-generated random phase key to it and then forcing those to Fresnel propagate to an arbitrary plane with an illuminating plane wave of a given wavelength. The proposed system is robust to blind decryptions without knowing the correct propagation distance, wavelength, and phase key used in the encryption. Signal-to-noise ratio (SNR) and mean-square-error (MSE) of the reconstructed 3-D object are calculated for various

decryption distances and wavelengths, and partial use of the correct phase key.

Jianghong Wei et al., 2016 [9] presented a secure and economical attribute based access control for cloud storage framework. Cloud storage facilitates both individuals and enterprises to cost effectively share their data over the Internet. However, this also brings difficult challenges to the access control of shared data since few cloud servers can be fully trusted. They developed Cipher text-policy attribute-based encryption (CP-ABE) approach that enables the data owners to place fine-grained and cryptographically-enforced access control over outsourced data.

Jawahar Thakur et al., 2011 [10] compared three common symmetric key cryptography algorithm i.e. DES, Blowfish and AES. Security is the most challenging aspects in the internet and network applications. Internet and networks applications are growing very fast, so the importance and the value of the exchanged data over the internet or other media types are increasing. Thus search for optimal solution to offer necessary protection against data intruders' attacks along with providing these services in time is one of the most interesting subjects in security. The comparison made on the basis of parameters: block size, speed, and key size.

Kan Yang et al., 2016 [11] It presents an efficient and a fine grained big data access control scheme with privacy preserving policy. **It generally** Control the access of huge amount of big data becomes a very challenging issue, basically when big data are stored in the cloud. The Cipher text-policy attribute-based encryption (CP-ABE) is a promising encryption technique that basically enables end users to encrypt their data under the access policies that are defined over some attributes of data consumers and only allows data consumers whose attributes satisfy that access policies.

K Liang et al., 2015 [12] proposed a new Cipher-text policy attribute based Proxy Re-Encryption (PRE) to handle the issue of combining the dual system encryption technology with selective proof method, which is useful cryptographic primitive and allows data owner to delegate the access rights of encrypted data stored on cloud storage system to others without leaking the information of the data to the honest-but-curious cloud server. This supplies the potency for data sharing as the data owner even using limited resource devices (e.g. mobile devices) can offload most of the computational operations to the cloud.

L Kocarev et al., 2003 [13] proposed a public-key encryption algorithm based on Che-byshev maps that is secure, practical and can be used for both encryption and digital signature. Software implementation and properties of the algorithm are also discussed in detail. Over the past decade, there has been tremendous interest in studying the behaviour of chaotic systems.

NK Nishchal et al., 2003 [14] implemented a fully phase encryption system, using fractional Fourier transform to encrypt and decrypt a 2-D phase image obtained from an amplitude image. The encrypted image is holo-graphically recorded in a barium titanate crystal and then decrypted by generating through phase conjugation, a conjugate of the encrypted image. The decrypted phase image is converted into an amplitude image via phase contrast method using electrical spatial light modulator.

Hsiao-Ying Lin, et al., 2012 [15] analysed and suggested suitable parameters for number of copies of message send to storage servers and number of storage servers queried by key server. A cloud storage system, comprising of a gathering of capacity servers, gives long haul stockpiling administrations over the Internet. Putting away information in an outsider's cloud framework causes genuine worry over information secrecy. General encryption plans ensure information privacy, yet additionally confine the usefulness of the capacity framework on the grounds that a couple of operations are upheld over encoded information. They also proposed an edge intermediary re-encryption conspire and coordinate it with a decentralized deletion code to such an extent that a safe conveyed stockpiling framework is figured. The proposed technique completely incorporates scrambling, encoding, and sending. These parameters permit more adaptable modification between the quantity of capacity servers and power.

IV. THIRD PARTY AUTHENTICATION AND AUTHENTICATION/ DIGITAL SIGNATURE SYSTEM

The validation and advanced mark conspires that are created so far require an outsider server which is aimlessly trusted by the greater part of the imparting substances. In the verification frameworks, the trusted outsider is acknowledged as a validation server by means of which the confirmation messages go through. Be that as it may, in the computerized signature frameworks, the trusted outsider is an expert which confirms the character of a few elements of the system. The affirmations issued by this expert can be utilized different circumstances. By and by in either case, the clients must put stock in the best possible conduct of the verification servers and affirmation experts. In any case, the trade-off of them may cause some deadly issues and those issues influence the majority of the system clients. This issue is known as the confided in outsider issue.

The trusted outsider issue can be illuminated by joining an open key based computerized signature convention with the idea of mystery sharing. There are a few mystery sharing plans, yet sadly they are not straightforwardly pertinent in a validation and computerized signature plot, since they require legitimate mystery merchant, fair mystery recuperation unit, called combiner, and all the more significantly, require private and bona fide correspondence channel between the merchant and investors, and between the investors and the combiner. Be that as it may, one can't expect such necessities in a verification and advanced mark plot with no single put stock in outsider [16].

Authentication and Digital Signature Systems

Verification is the procedure in which a substance demonstrates his/her personality to the associate element. In the event that the correspondence is bona fide, at that point the beneficiary can fulfil himself that the sender is really who he claims to be. Be that as it may, the beneficiary can't demonstrate this reality to a third individual. This question can be settled by computerized marks. An advanced mark is a snippet of data that is sent alongside the message and can be produced just by the sender. Everybody (counting the collector) can confirm this advanced mark and ensure about the root of the message. By along these lines, the sender can't later disavow sending the message. In this way, non-renouncement is accomplished by computerized marks. There are two sorts of confirmation and advanced mark frameworks: private key based frameworks and open key based frameworks. The private key based frameworks, for example, Kerberos can be utilized just for mystery and confirmation bolster. They can't bolster non-disavowal and advanced marks on account of the idea of the cryptographic plans utilized. In broad daylight key cryptography, the keys can be utilized for both encryption and computerized signature purposes. In this manner, open key based frameworks bolster mystery, verification and advanced marks. Diffie and Hellman are the primary who portrayed such a framework. Open key based validation and computerized signature conventions are institutionalized by International Telecommunications Union (ITU) standard suggestion X.509, The Directory - Authentication Framework [17].

V. CERTIFICATION MECHANISM AND WRONG PUBLIC KEY PROBLEM

A standout amongst the most essential issue of the general population key based verification and advanced mark conventions is to get the right open key of a client. People in general keys can be acquired by everybody. However to do this, there ought to be a few spots to get those open keys, in light of the fact that generally everybody should know each other's open key, which isn't an achievable approach. Subsequently, some open key storehouses are required. In addition, these archives ought not to work just in read way, on the grounds that the clients should reach there to distribute their open keys moreover. In this manner, a threatening interloper can without much of a stretch supplant general society key of a client with his/her open key. This circumstance causes pantomime. Another result of utilizing an off base open key is a refusal of administration assault in signature check. Keeping in mind the end goal to evade those issues, confirmation instrument can be utilized. In this component, an open key is marked with some other individual's private key. This mark is known as the affirmation and the proprietor of the private key is known as the certifier or the Certificate Authority (CA). By along these lines, if the verifier knows the general population key of the certifier, at that point it can confirm the rightness of the marked open key.

In this approach, the certifier ought to be commonly put stock in both by the general population key proprietor and the verifier. Particularly in substantial systems like the Internet, there ought to be a method for grouping the clients and the certifiers. The ITU standard suggestion X.509, The Directory - Authentication Framework, proposes such a bunching. This is really a tree chain of importance of clients and CAs. In this progression, affirmation ought to be issued by approved servers, specifically CAs. Every hub issues confirmation to its youngsters and every hub believe its parent hubs until the root [17].

Authentication Server/Certificate Authority Reliability

Security issues happen if the private key of a validation server or a CA is traded off. In a private key based framework, if the key of the verification server is traded off, at that point the gate crasher can get validated access to any server which believes the bargained confirmation server. At the point when this trade-off is detected, the framework can be re-established by changing the key of the validation server. In an open key based framework, an interloper can make legitimate yet caricaturing authentications by getting the private key of a CA, and can imitate any client which believes the traded off CA by utilizing these testaments. When this bargain is detected, the majority of the endorsements that are issued by this CA must be renounced recursively towards to the leaves of the pecking order. This is really an extremely costly process. In the event that the private key of the best level expert is traded off, at that point the majority of the authentications of the framework ought to be disavowed. The denied authentications make a security bottleneck in the framework. In this way, the general population key based frameworks are less secure than the private key based frameworks. Besides, the various levelled structure of an open key based framework may cause another put stock in issue, that is some contending organizations or foe nations might not have any desire to confide in a typical expert. By the by, everybody should believe the best level specialist in an open key based framework.

VI. KEY DISTRIBUTION PROTOCOLS AND STORAGE SCHEMES IN ENCRYPTION

Key Distribution Protocols are utilized to encourage sharing mystery session keys between clients on correspondence systems. By utilizing these mutual session keys, secure correspondence is conceivable on uncertain open systems. Notwithstanding, different security issues exist in ineffectively composed key appropriation conventions; for instance, a pernicious aggressor may get the session key from the key circulation process. A honest to goodness member can't guarantee that the got session key is right or crisp and a honest to goodness member can't affirm the character of other member. Planning secure key appropriation conventions in correspondence security is a best need. In some key conveyance conventions, two clients

get a mutual session key by means of a Trusted Center (TC). Since three gatherings (two clients and one TC) are associated with session key arrangements, these conventions are called outsider key dispersion conventions, as interestingly with two-party conventions where just the sender and collector are engaged with session key transactions.

- ***Classical Cryptography*** In classical cryptography, three-party key dispersion conventions use challenge reaction instruments or timestamps to forestall replay assaults. In any case, challenge reaction components require no less than two correspondence adjusts between the TC and members, and the timestamp approach needs the suspicion of clock synchronization which isn't useful in dispersed frameworks (because of capricious nature of system postponements and potential unfriendly assaults). Moreover, traditional cryptography can't recognize the presence of aloof assaults, for example, listening stealthily. In actuality, a quantum channel disposes of listening stealthily, and consequently, replay assaults. This reality would then be able to be utilized to diminish the quantity of rounds of different conventions in light of test reaction component to a confided in focus.

Table 1. Data encryption Scheme

Number of Attributes	Traditional ABE	Scheme (8HF)	Scheme
0	0.05	0.06	0.09
5	0.1	0.3	0.6
10	0.18	0.19	0.2
15	0.26	0.28	0.3
20	.33	0.37	0.39

- ***Quantum Cryptography*** In quantum cryptography, Quantum Key Distribution Protocols (QKDPs) utilize quantum systems to appropriate session keys and open dialogs to check for meddlers and confirm the restorative ness of a session key. Be that as it may, open discourses require extra correspondence adjusts between a sender and recipient and cost valuable qubits. By differentiate, established cryptography gives advantageous systems that empower productive key check and client validation [18].

Table 2. Data Decryption

Number of Attributes	Traditional ABE	Scheme 8HF	Scheme 16HF
0	0.02	0.04	0.11
5	0.09	0.2	0.0
10	0.12	0.14	0.10
15	0.26	0.22	0.27
20	0.29	0.25	0.28

Encryption methods could be implemented to information on the drive or sun of element at the host. We study the key hardware based schemes and products available for storage of the data security.

- ***Advanced Encryption Algorithm:*** The AES Algorithm is a symmetric-key cipher, in which both the sender and the receiver use a single key for encryption and decryption. The data block length is fixed to be 128 bits, while the length can be 128, 192, or 256 bits. In addition, the AES algorithm is an iterative algorithm. Iteration of AES process can be called a round, and the total number of rounds is 10 for 128, 12 for 192, and 14 for 256 bit key length. The 128 bit data block is divided into 16 bytes. These bytes are represented to a 4 x 4 array. This array is called the State. All the internal operations of the AES algorithm are performed on the State.
- ***RSA algorithm:*** RSA algorithm is one of the best Asymmetric cryptosystems for encryption of blocks of data or digital signatures or key exchange. This algorithm uses a variable size key and encryption block. It is based on number theory and uses two prime numbers to generate the public and private keys. These keys are used for encrypt and decrypt the data. RSA operations can be divided into three main steps:
  (i) key generation,
  (ii) data encryption;
  (iii) Decryption

  But this algorithm has many flaws in its design that's why it is not preferred for commercial use. When designing the key if small values are selected for RSA then it makes encryption process very weak and if takes too large values then it consumes time and also affected the performance.

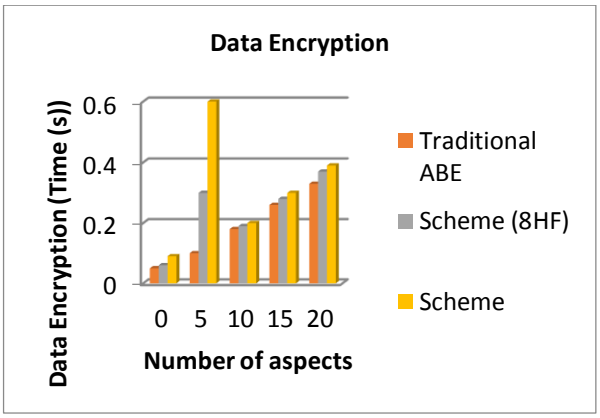

Fig 2. Data Encryption Time

The figure 2 described that the encryption time across the number of attributes entangled in the access policy.

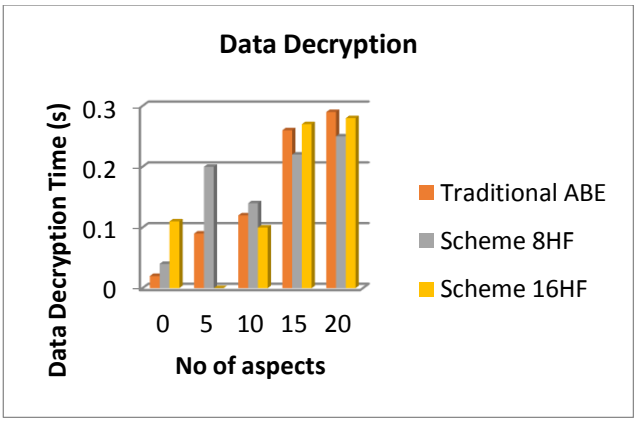

Fig 3.The Data Decryption Time (s)

The above figure defined that the decryption time in this method basically consists of every ABF query interval of time and the data. The attribute number here describes total how many attributes are tested by running the ABF query algorithm. Therefore, our scheme can conserve the privacy of the access policy without expand much computation above for both data encryption on end-users and data decryption on data users.

VII. CONCLUSION

In this paper basically, we have surveyed different fine-grained and efficient data access control methods for the big data storage in the cloud, where the access policy will not spill any private information. The fundamental objective of access control is to solidify the activities of clients according to their approvals. The fundamental thought started from the idea of multiuser system n 1970s. A few access necessities are basic for get to control. Access control is fundamental for information stockpiling on cloud. Distributed computing engineering comprises of equipment, platform, and application and foundation layer. Different kinds of clouds are accessible. Henceforth, based on our analysis scheme are terms to be the best a few cryptography calculations, for example, DES, Blowfish and AES, and so forth. Encryption time across the number of aspects involved in the access policy. The time of decryption in our method contained of every ABF query interval of time and the data. The attribute number here also measure how many attributes are being tested by running the ABF query algorithm. Therefore, our scheme can keep the privacy of the access policy without enlarge more computation overhead for the both data encryption on end-users and data decryption on data users. We execute the ABF function by using Murmur Hash function and the access control method to manifest that the method could maintain the privacy form any LSS access rules without appoint the much overhead.

VIII. REFERENCES

[1]. Sandhu, Ravi S., Edward J. Coyne, Hal L. Feinstein, and Charles E. Youman. "Role-based access control models." Computer 29, no. 2 (1996): 38-47.

[2]. Sandhu, Ravi S., and Pierangela Samarati. "Access control: principle and practice." IEEE communications magazine 32, no. 9 (1994): 40-48.

[3]. Shen, HongHai, and Prasun Dewan. "Access control for collaborative environments." In Proceedings of the 1992 ACM conference on Computer-supported cooperative work, pp. 51-58. ACM, 1992.

[4]. Qian, Ling, Zhiguo Luo, Yujian Du, and Leitao Guo. "Cloud computing: An overview." Cloud computing (2009): 626-631.

[5]. Zhang, Qi, Lu Cheng, and Raouf Boutaba. "Cloud computing: state-of-the-art and research challenges." Journal of internet services and applications 1, no. 1 (2010): 7-18.

[6]. Koo, Dongyoung, Junbeom Hur, and Hyunsoo Yoon. "Secure and efficient data retrieval over encrypted data using attribute-based encryption in cloud storage." Computers & Electrical Engineering 39, no. 1 (2013): 34-46

[7]. Dinh, Hoang T., Chonho Lee, Dusit Niyato, and Ping Wang. "A survey of mobile cloud computing: architecture, applications, and approaches." *Wireless communications and mobile computing* 13, no. 18 (2013): 1587-1611.

[8]. Kim, Hyun, Do-Hyung Kim, and Yeon H. Lee. "Encryption of digital hologram of 3-D object by virtual optics." Optics express 12, no. 20 (2004): 4912-4921

[9]. Wei, Jianghong, Wenfen Liu, and Xuexian Hu. "Secure and Efficient Attribute-Based Access Control for Multiauthority Cloud Storage." IEEE Systems Journal (2016).

[10]. Thakur, Jawahar, and Nagesh Kumar. "DES, AES and Blowfish: Symmetric key cryptography algorithms simulation based performance analysis." International journal of emerging technology and advanced engineering 1, no. 2 (2011): 6-12.

[11]. Yang, Kan, Qi Han, Hui Li, Kan Zheng, Zhou Su, and Xuemin Shen. "An efficient and fine-grained big data access control scheme with privacy-preserving policy." IEEE Internet of Things Journal 4, no. 2 (2017): 563-571.

[12]. Liang, Kaitai, Man Ho Au, Joseph K. Liu, Willy Susilo, Duncan S. Wong, Guomin Yang, Yong Yu, and Anjia Yang. "A secure and efficient ciphertext-policy attribute-based proxy re-encryption for cloud data sharing." Future Generation Computer Systems 52 (2015): 95-108.

[13]. Kocarev, Ljupco, and Zarko Tasev. "Public-key encryption based on Chebyshev maps." In Circuits and Systems, 2003. ISCAS'03. Proceedings of the 2003 International Symposium on, vol. 3, pp. III-III. IEEE, 2003.

[14]. Nishchal, Naveen Kumar, Joby Joseph, and Kehar Singh. "Fully phase encryption using fractional Fourier transform." Optical Engineering 42, no. 6 (2003): 1583-1588.

[15]. Lin, Hsiao-Ying, and Wen-Guey Tzeng. "A secure erasure code-based cloud storage system with secure data forwarding." *IEEE transactions on parallel and distributed systems* 23, no. 6 (2012): 995-1003.

[16]. Longjun, Zhang, and Zou Tao. "A trusted third party based secure authentication scheme of E-commerce." In *Embedded and Ubiquitous Computing, 2008. EUC'08. IEEE/IFIP International Conference on*, vol. 2, pp. 590-594. IEEE, 2008.

[17]. Levi, Albert, and M. Ufuk Caglayan. "The problem of trusted third party in authentication and digital signature protocols." In the Proceedings of the Twelfth International Symposium on Computer and Information Sciences, ISCIS, vol. 12, pp. 317-324. 1997.

[18]. Ranganathan, Suganya, Nagarajan Ramasamy, Senthil Karthick Kumar Arumugam, Balaji Dhanasekaran, Prabhu Ramalingam, Venkateswaran Radhakrishnan, and Ramesh Karpuppiah. "A three party authentication for key distributed protocol using classical and quantum cryptography." International Journal of Computer Science Issues (IJCSI) 7 (2010).