IJOSTHE

ISSN: 2349-0772 | Volume 5 Issue 3 June 2018 |www.ijosthe.com

A Survey: Attribute Based Encryption for Secure Cloud

Aayushi Priya
Department of CSE
SIRT Bhopal , India
aayu.rec@gmail.com

Rajeev Tiwari
Barkatullah Vishwavidyalaya
Bhopal , India
rajeevrnt@yahoo.co.in

Abstract: Cloud computing is an enormous area which shares huge amount of data over cloud services and it has been increasing with its on-demand technology. Since, with these versatile cloud services, when the delicate data stored within the cloud storage servers, there are some difficulties which has to be managed like its Security Issues, Data Privacy, Data Confidentiality, Data Sharing and its integrity over the cloud servers dynamically. Also, the authenticity and data access control should be maintained in this wide environment. Thus, Attribute based Encryption (ABE) is a significant version of cryptographic technique in the cloud computing environment. Public Key Encryption acts as the basic technique for ABE where it provides one to many encryptions, here, the private key of users & the cipher-text both rely on attributes such that, when the set of the attributes of users key matches set of attributes of cipher-text with its corresponding access policy, only then decryption is possible. Thus, an opponent could grant access to the sensitive information that holds multiple keys, if it has at least one individual key for accession. The techniques based on ABE consist of two types: KP-ABE (Key- Policy ABE) where the user's private key is linked to an access structure (or access policy) over attributes and cipher-text is connected to the set of attributes, and CP-ABE (cipher-text policy ABE) is vice versa. Hence, in this, Review we discuss about the various security techniques and relations based on Attributes Based Encryption, especially, the type KP-ABE over data attributes which explains secured methods & its schemes related to time specifications.

Key words: Cloud computing, Data sharing, Data confidentiality, Security, ABE, Access control.

1. Introduction

Now-a-days, in this big environment, data sharing over the cloud servers are highly accessible but has not remained secured, as the cloud service providers can't be trusted for long, but there are various developments which have been done by different authors in this cryptographic area. Cloud computing is defined as a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction [1]. Services catered by cloud computing are software as a service (SaaS), platform as a service (PaaS) and hardware as a service (HaaS). Amazon, Google, Microsoft, IBM are key companies in cloud computing. At present a lot of users outsource their data to the websites hosted by these companies. According to IDC the overall expenditure on software, storage structures, and licensed business by the public cloud service providers will escalate at a 21.9% Compound Annual Growth Rate (CAGR) to $12.2 billion in 2016 [2]. Lending data storage space is pivotal service of cloud computing. This service allows business organizations and individuals to shift their data from personal data centers to cloud based data servers. Moving data into the cloud servers lends much contentment to organizations and individuals since they need not to anguish about the management of complex hardware systems. However, once the ownership of data is dropped, it brings security and privacy issues with data. Without data security, success of cloud computing is abridged. Maintaining data integrity is one of the vital security concerns.

By outsourcing data, the data owner gave right to cloud service provider to perform any operation on data. Hence data owner suffers from loss of possession of data. Possession of data states the control of data which means that if data is on local systems then data owner has full control over any operation performed on data including block deletion, modification, and insertion. But if the data is on cloud storage server then cloud provider has all the power to control any operation performed on the data. Cloud provider can stop any operation on data, process any operation incorrectly and may produce incorrect results. The major problem with loss of data possession is that the cloud provider can hide such mistakes from data owner for some benefits. The cloud server may also face internal and external security issues including components failure, administration problems, and software bugs which can harm data owner's critical data.

There are several settings where a user would want to give access to documents based on certain credentials or the position/role of a person. This may be comparable with 'Views' in a database. We would want different kind of users of the database [14] to be able to see only those contents that are relevant to them. Similarly, in a distributed setting where all the data may be stored in a server, the server might allow access to files and documents based on some predefined access control policy, for instance, clients may have to provide proper certification to retrieve specific files. In such cases, if the data(storage) in the database or server is compromised, then although it may be in the encrypted form, anyone who has access to the database or server may be able to retrieve all information including those documents that may not be relevant to them . To be more specific, any normal user of the database who gets his/her hands on the compromised data may now be able to get those files which were restricted and whose access was determined by some application in the database or server.

ABE was first introduced by Sahai and Waters [1]. It provides a mechanism by which we can ensure that even if the storage is compromised, the loss of information will only be minimal. What attribute based encryption does is that, it effectively binds the access-control policy to the data and the users (clients) instead of having a server mediating access to files. To understand this better, we will take a closer look at what constitutes an attribute based system, with particular attention to ABE.

2. Literature Survey

Attribute-based encryption (ABE) presented by Sahai and Waters (2006) [1], is an assuring cryptographic method that reaches a fine-grained data access control. It highlights the way of determining the access control norms, based on various users attribute or over data objects. ABE scheme offers two of its different essence: Key policy attribute based encryption (KP-ABE) presented by Goyal (2006) and Cipher-text policy based encryption (CP-ABE) given by Waters (2011). In KP-ABE technique, the encryption & decryption process is featured when a set of attributes linked to a cipher-text and a user's private key is related with an access policy over data attributes, whereas, in CP-ABE when a set of attributes are connected to a user's private key and an access structure is linked a cipher-text over users attributes. Hence, decryption of a cipher-text is only possible when the attribute sets of that cipher fulfils the access policy (access structure) associated to the private key of that user.

Time management has always been important in communication. As Cryptographic techniques has been modified for the management of communication with Time specifically. Information can become unusable after any time duration. Timed-release encryption (TRE) provides an interesting service, during the process of encryption, an encryption key is allied to any predefined time duration of data discharging. Thus, at that point of time the end user can create only the matching decryption key. So, time period is taken as a critical condition for various computational processes over the processing system. Based on TRE, Paterson and Quaglia (2010)[5] introduced Time-Specific Encryption (TSE) as a overview of TRE (Time Release Encryption).That is in,[13] it provides decryption of data by any end user is possible after a specified predefined release time. And modifying its method in TSE there approach explains that specifically each user has a time instant key, and cipher-text could be decrypted by the users in only that time period allotted for the decryption and which is linked with that cipher-text.

Key Policy Attribute based Encryption (KP-ABE) is a novel security scheme which have been proposed by V. Goyal, O. Pandey, A. Sahai, and B. Waters(2006)[1]. It is a little transformed version of the traditional model of KP-ABE to overpower its limitations. Hence, Siqi Ma, Junzuo Lai, Robert H. Deng, Xuhua Ding (2016)[2] in "Adaptable KP-ABE with time interval" scheme, they have enhanced the KP-ABE scheme by adapting Time Specific Encryption with ABE technique and proxy re-encryption in efficient manner. Also, it merges with adaptable CP-ABE scheme which offers a fundamental approach for its security model. However, the adaptability of Time specific encryption with proxy re-encryption has revived the mutation of this system. In Adaptable Key policy ABE with Time Interval, a cipher-text is associated with an expressive attribute sets, and also related by the decryption time interval. As in the standard KP-ABE a user contains his private key allied to an access policy corresponding to its attributes, but in adaptable version it is connected to the time instant key as in TSE as well. Thus, adaptation server re-encrypts data to the cloud efficiently and maintains the data confidentiality contrary to the cloud server. Also, the data holder provides a new time interval to the time-modified server.

Jing Li, Xiong Li, Licheng Wang, Debiao He, Haseeb, Ahmad, Xinxin Ni[3] Proposed a “Fuzzy encryption in cloud computation: Efficient verifiable outsourced attribute-based encryption” in which they have proposed the modification of CP-ABE scheme by combining the outsourcing technique of ABE in an efficient manner. As users are burdened with a large computation costs, so they had taken a step for minimizing the overhead of encryption and decryption with huge calculations and maximum difficulties. They have tried to lighten the computational load of their scheme. Here, they have presented the efficient outsourcing CP-ABE scheme, by reducing exponential measures in the encryption to a constant involving blinding algorithm into it. Also they had provided the surety of accuracy and verifying mechanism of their proposed scheme which allows user to efficiently verify the data validity and compute the outsourced results.

Junzuo Lai, Robert H. Deng, Yanjiang Yang, and Jian Weng[4] had explained their mechanism in “Adaptable Cipher-text-Policy Attribute-Based Encryption”, where they discussed about extension of the traditional CP-ABE by allowing a semi- Yet, the primary plaintext is unknown trusted proxy to modify a cipher-text associated access policies. to the third party. Here, “adaptability” possesses the proxy which is a trapdoor. A cipher-text with an access policy into another cipher-text under any other access policies could be transformed by the third party, as the he is eligible for alteration part.

Priyanka Kumari et al. [5] stated that a number of data files authentication and integrity schemes have been conducted to recognize any modification in the exchange of data files between two entities within a cloud environment. Existing solutions are based on combining key-based hash function with traditional factors (steganography, smart-card, timestamp). However, none of the proposed schemes appear to be sufficiently designed as a secure scheme to prevent from attacks.

Arshi Jabbar et al. [6] work is to develop an auditing scheme that is secure, economical to use and possess the capabilities like privacy conserving, public auditing, maintaining the information integrity together with confidentiality. It comprises 3 entities: data owner, TPA and cloud server. The data owner performs numerous operations like splitting the file to blocks, encrypting them, generating a hash value for every, concatenating it and generating a signature on that. The TPA performs the main role of knowledge integrity check. It performs activities like generating hash value for encrypted blocks received from cloud server, concatenating them and generates signature on that. It later compares each the signatures to verify whether or not the information stored on cloud is tampered or not. It verifies the integrity of data on demand of the users. To make sure data protection or security of cloud data storage at cloud end, security architecture is designed that secures the data using encryption/decryption algorithm where the proposed algorithm is a hybrid encryption algorithm that uses the concept of EC-RSA, AES algorithm and Blowfish algorithm along with SHA-256 for auditing purpose. Presented experiment results show that the proposed concept is reasonable, it enhancing efficiency about 40% in terms of execution time i.e. encryption as well as decryption time and security and providing confidentiality of cloud data at could end.

3. Attribute based Encryption Techniques

Attribute based Encryption is a type of Public Key Encryption which is the most traditional Encryption technique has been applied for Public Health Records(PHR) concerning data security. But due to some limitations of Public-key Encryption Sahai and Waters (2005)proposed an attribute-based encryption (ABE) scheme for improving some techniques and limitations of Public-key Encryption, and this paper proposed the first concept of the attribute-based encryption scheme. As, ABE is a simplification of identity based encryption.

In Attribute Based Encryption, the secret key of a user and the cipher text reliant on attributes those allied to the data (e.g. the company he works, or the kind of registration he has). In such a system, the decryption of a cipher text is possible only when the set of attribute of the user key bonds the attribute of the cipher text. In ABE, for encrypting various copies of a file, different user’s key is required and the key management is also minimized. By applying access policy as stated in ABE, the data attributes of a user enables the user (patient) to share their data selectively by encrypting any of the records under its attributes set. In the classical model, it can be accomplished only when both end user and storage server remains in a trusted domain. Although, a single trusted authority not only creates a blockage of heavy load, but also have key escrow problem. However, the Trusted Authority could access all the encrypted files but, it unlocks the door for privacy exposure potentially. Hence, with this encryption method synchronization of other techniques were not possible. Thus, the prior aim for this scheme is to provide security, access control and the main aspects are to provide flexibility, scalability, and fine grained access control.

3.1 Key policy Attribute Based Encryption(KP-ABE)

KP-ABE is a first version of Attribute based Encryption. V. Goyal, O. Pandey, A. Sahai, and B. Waters (2006) [1] proposed a Key-Policy Attribute Based Encryption (KP-ABE) scheme. It is an enhanced version of the classical model of ABE. Thus, to overpower the limitation of old model, revised type of Attribute based encryption (ABE) scheme was presented that is key-policy attribute based encryption (KP-ABE). In this method an access structure is allocated to each of the end user which decides the type of key for the decryption of the cipher-text. Here, access structure can be reflected by a certain private key related to the data, so that the decryption could be possible by the end users. As explained earlier, the process of decryption of the cipher-text undergoes when attribute sets of the data satisfies the access policy linked to that cipher-text. The KP-ABE is suitable technique for providing the fine grained access control & confidentiality to data system where it can proficiently identify the area for accession of data system, for operation and execution of data over various parts of that system.

3.2 Expressive KP-ABE

Attrapadung, Libert, Elie de Panafieu[11] Proposed Expressive Key policy attribute Based Encryption scheme which is the another modified method of classical KP-ABE and it offers an expressive way of Attribute based encryption in its Key Policy flavour by allowing non- monotonic access structure with constant cipher-text size. As, primarily ABE permits dispatchers to encrypt messages under attributes set, where private key is related to an access structures that decides which key holder should decrypt the cipher-texts. Also, in previous ABE system, magnitude of cipher-text raises linearly along with the number of cipher-text attributes and only the known exceptions supports only those limited forms of the approached access policies. Towards attaining this objective, a certain class of identity-based broadcast encryption schemes have been described broadly that produces monotonic KP-ABE systems efficiently. Further, they had reduced the number of pairing evaluations to a constant, which appears to be a unique feature among expressive KP-ABE schemes which is more effective than KP-ABE.

3.3 Time Specific Encryption

Paterson and Quaglia (2010)[7],introduced Time-Specific Encryption(TSE)as a broad view of TRE(Time Release Encryption). In this technique, during an encryption process the sender of data can state any time period while the recipient should have corresponding time instant key for the message recovery. Simply, we can say that, the sensitive data is restricted to be released before a particular time; we could enable access to information for only a limited period of time. They had extended Plain TSE to the public-key and identity-based settings. Also they introduced security prototypes for the plain TSE, public-key and identity-based settings and combined those schemes & maintained the security from chosen cipher-text models.

3.4 Adaptable KP- ABE with Time Interval

In Adaptable KP-ABE with time interval scheme, Siqi Ma, Junzuo Lai, Robert H. Deng, Xuhua Ding(2016)[2], they have enriched the KP-ABE scheme by adapting Time Specific Encryption technique and proxy re-encryption in proficient manner and they also used the method of adaptable CP-ABE scheme. Adaptable KP-ABE with time interval scheme provides an actual amplification for supervising the task to restrict time interval for decryption. Specifically, in this technique generation of private key by both policy server and time server takes place, and it provides an access structure & time instant key where it acquires user private key. Here, as typical version of KP-ABE, a user contains a private key linked to an access structures and cipher-text is linked to a set of attributes. Whereas in TSE, users private key is allied to both access structure (access policy) over attributes as well as time instant key. Although, in adaptable KP-ABE with time interval cipher-text is connected to both vivid attribute sets in addition to decryption time interval, unless the access policy satisfies the set of attributes at a certain predefined decryption time period, the end user couldn't decrypt the cipher-text or he can otherwise. Firstly, a Key Generation Centre sends a private key that is associated to an access structure to the user. Then, a global system consideration and a time instant key (TIK) has been transmitted by (proxy) Time server at each time interval to all the users. Therefore, for adjustable decryption time interval, another semi-trusted space, called Adaptation Server, is introduced in Adaptable KP-ABE with time interval.

3.5 Adaptable Cipher-text Policy Attribute Based Encryption

Adaptable CP-ABE is proposed by Junzuo Lai, Robert H. Deng, Yanjiang Yang, and Jian Weng (2014) [4] where they have extended classic scheme of CP-ABE. They proposed an arrangement where a semi trusted proxy server is allowed to transform a plaintext to a cipher-text from diverse policies that means CT1 once modified under one access policy, then again it can be modified into CT2 under another access policies, as a result, original plaintext remains confidential in front of proxy. Thus, in traditional CP-ABE, a cipher-text is generated under an access policy (also called access structure), and the decryption keys of users are allied to the set of attributes. CP-ABE appears more organized, where the data owner directly specifies the access policy and recommends that which decryption key could decrypt which type of cipher-text. The 'adaptable' term explains the new version of CP-ABE where it adapts the Proxy re-encryption scheme. More specifically, adaptable CP-ABE offers an effective solution for heavy computation when the method of re-encryption of data is entrusted to the cloud as a proxy. The proxy is semi-trusted and it becomes a doorway for the data transformation. Consequently, the data owner has to instruct the cloud to re-encrypt the data under new access policies, and simultaneously recollecting the data confidentiality.

3.6 Efficient verifiable outsourced attribute-based encryption: Fuzzy Encryption

Jing Li, Xiong Li, Licheng W, Debiao He, Haseeb Ahmad, Xinxin Niu (2017) [3] Proposed the "Efficient verifiable ABE: fuzzy encryption", in this, Owing to the high complications and huge computation overhead of encryption and decryption in CP-ABE, users are loaded with bulky computational cost. So, they have tried to decrease the burden of their calculation. They have improved the outsourcing CP-ABE scheme by providing well-organized verification mechanism where they had used blinding algorithm for the decrement of number of exponential setups in the encryption to a constant. Thus, they have assured the check ability for reassurance of the accuracy of their scheme. This is based on a collision-resistance hash function, which allows the users to effectively verify the validity of messages and outsourced computation consequences. By merging the outsourcing technology in their method for the safety purpose, no useful information are exposed to the cloud servers from the outsourcing parameters, which creates the scheme more secured and provides confidentiality to the data.

4. Definition & Background

Access Policy

An access control policy [16, 17] would be a policy that defines the kind of users who would have permissions to read the documents. e.g In an academic situation, performance record of class students may be accessible only to a professor handling the course and some teaching assistants (TAs) of that course. We can express such a policy in terms of a predicate as shown in Figure 1:

((Professor AND CSE dept.) OR (M.tech scholar AND (CSE dept. OR IT dept.)))

We will call the various credentials (or variables) of the predicate as attributes and the predicate itself which represents the access policy as the access-structure. In the example here the access structure is quite simple. But in reality, access policies may be quite complex and may involve a large number of attributes.

Cloud service providers determine the access control mechanisms for data on the cloud. Access control is a procedure that restricts, denies, or allows access to system. In the cloud, data security is crucial to protect against inside attack, denial of service attack, and collision attack.

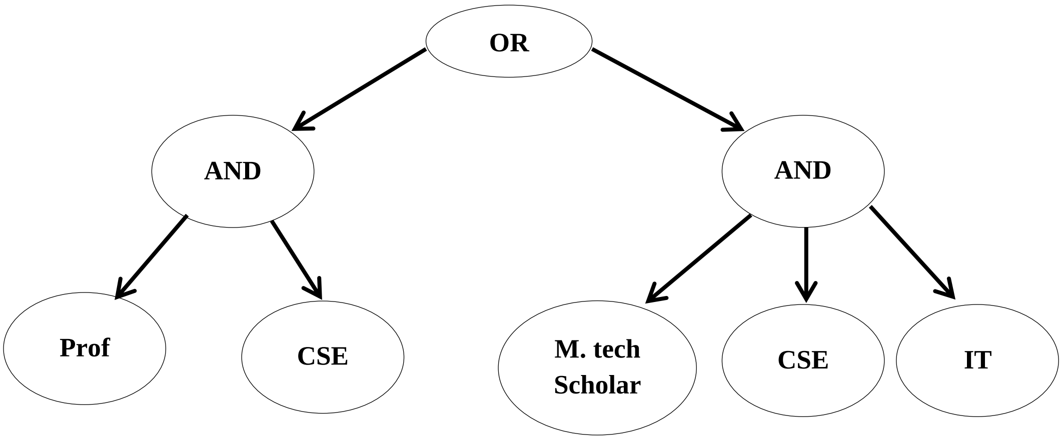

Figure 1: Access Policy representation as Tree

Traditionally, different expressive access control policies are used to protect data stored locally and data stored remotely. The approaches include Discretionary Access Control (DAC), Mandatory Access Control (MAC), Role-Based Access Control (RBAC), and Attribute-Based Access Control (ABAC) [15]

ABE scheme derives from IBE, so both algorithms look similar.

Definitions: The basic model originates from Fuzzy-IBE which contains setup, keygen, encrypt and decrypt algorithms. Most ABE schemes contain at least these four modules, but each of them has different formulas.

Setup: The setup algorithm first defines the bilinear mapping. It then takes security parameter _ that denotes the size of the attribute set as input, and generates a public key (PK) and master key (MK) as output.

KeyGen: The threshold access policy will generate a secret key consisting of abstractions of a user's attributes set S. For scheme features key policy, the KeyGen function will take MK and the access tree T as input and generate a secret key SK for the user.

Encrypt: For threshold policy, the encrypt algorithm takes a plaintext M as well as a set of expected attributes S' as input and outputs the ciphertext D. For ciphertext policy, the access tree T together with PK and message M will be used as input and the ciphertext CT will be the output.

Decrypt: The decryption function will take the user's SK as well as the ciphertext CT as input and generates the message M or NULL if access is denied.

An additional algorithm Global Setup is needed in decentralized authority schemes to coordinate all authorities for a global environment. Its setup algorithm is similar to the one in centralized authority schemes and will be used for Authority Setup.

At least one parameter or algorithms will be introduced to the system for each additional feature, and the system will become more complex, resulting in a trade-off of features for performance.

ABE has built-in access control, user authentication and revocation must be satisfied via a trusted authority. Additionally, all ABE systems must defend against collusion attacks to prevent users from accessing unauthorized information through collaboration.

5. Advantages & Limitations of ABE

There are few common advantages & limitations of Attribute based Encryption schemes & their types which could need the enhancement in it.

- **Advantages**

In ABE, it provides well security & privacy with fine grained access. Also, for huge storage of records it offers elasticity. Ultimately, advantage of ABE is that there is no one-to-one relationship in its encryption and decryption keys; means an encryption key can correspond to multiple keys for decryption. In the ABE technique, specific access policies and attribute sets could differ according to time, which is a versatile nature of the scheme. Whereas, KP-ABE has more advantage then ABE. It is further reconstructed with different techniques which provide better access control such as when it's combined with Re-encryption method. Also, it offers well security & privacy than ABE which is thus more efficiently available in version of expressive KP-ABE scheme where public parameters of constant size had been shown. Now-a-days, more feasible experiences had also been explained by adopting ABE on resource-controlled devices with IOT applications. Some advantages could be described in CP-ABE kind of encryption where it affords fine grained access alike KP-ABE. It has better efficiency in its security methods but consumes time. Similar to KP-ABE, also it can be merged to re-encryption techniques & hidden policy variants which provide adequate access control method & good security to the schemes.

Limitations –In ABE the public key of every authorized user is essential for the data owner but it prohibited in actual environment. As in ABE it suffers from high computational overhead whereas KP-ABE possesses less. And in KP-ABE, decryption of the encrypted text couldn't be decided by the person which encrypts it. It is more complex than ABE, as it is incompatible in some application because a data owner necessarily should trust the key issuer. Therefore, in CP-ABE, compared to ABE cons are limited, but in its variant of verification built on a collision-resistance hash function provides large computation overhead which is required to minimize.

6. Analysis and Discussion

Comparative analysis of some Encryption schemes are given in table 1.

Table 1: Comparative Analysis of Existing Techniques

Author Name	Mechanism Performed	Computational overhead	Access control	Security
Jing Li, Xiong Li, Licheng W, Debiao, Ahmad, Xinxin Niu (2017)	CP-ABE scheme Outsourcing+ Blinding technique(Verification)	Less as compared	Fine Grained access	RCCA security
Siqi Ma, Junzuo Lai, Robert H. Deng, Xuhua Ding(2016)	KP-ABE scheme with adaptation of Time specific Encryption	Less	Fine grained access	DBDH assumptions
Chao Li, Bo Lang and Jinmiao Wang(2014)	KP-ABE +Outsourcing technique	Average	Better access control	SE-CCA security
Junzuo Lai, Robert H. Deng, Yanjiang Yang, and Jian Weng (2014)	Adaptable CP-ABE +Re- Encryption technique	More	Good access control	CCA security
Paterson and Quaglia(2010)	Time Specific Encryption (public key & Identity based TSE)+Broadcast Encry.	Average	Fine access control as compared	CCA+IND-CPA security
Attrapadung, Libert, Elie de Panafieu(2008)	Expressive KP-ABE with constant cipher size	More	Good access control	DBDH assumptions
V. Goyal, O. Pandey, A. Sahai B. Waters (2006)	ABE +Secret sharing scheme+ Identity based Encryption	More	Good access control	DBDH assumptions

7. Conclusion

In this survey, the developed forms of Attribute based encryption techniques have been explained thoroughly. In all the types of KP-ABE & CP-ABE versions of Attribute based encryption the security terms is refined with good access control. Therefore, outsourced scheme defines reliable less computation cost with fewer loads, but barrier of complexity remains same. Hence, drawbacks of these encryption schemes could be prevailed. I have enriched the ABE scheme to reduce its complex calculations regarding time duration and lower the time management and upgraded its security under certain techniques and implemented mixture of basic encryption methods to reduce the computational overhead & algorithm complexities. Also, maintenance of data secrecy & data integrity is fulfilled in proposed methodology.

References

[1] Goyal V, Pandey O, Sahai A, Waters B (2006) "Attribute-based encryption for fine-grained access control of encrypted data". In: Proceedings of the 13th ACM conference on computer and communications security.

[2] Ma J, Lai J, Deng R H, Ding X (2016) "Adaptable key-policy attribute based encryption with time interval."

[3] Jing L, Xiong L, Licheng W ,Debiao H, Haseeb A, Xinxin N(2017) "Fuzzy encryption in cloud computation: efficient verifiable outsourced attribute-based encryption"

[4] Lai J, Deng RH, Yang Y, Weng J (2013) Adaptable ciphertext-policy attribute-based encryption. In: Pairing-based cryptography—pairing 2013. Springer.

[5] Priyanka Kumari, Raj Kumar Paul, "A Study for Authentication and Integrity of Data Files in Cloud Computing", IJOSCIENCE, Volume 2, Issue 9 December 2016, Available: http://ijoscience.com/ojsscience/index.php/ojsscience/article/view/109.

[6] A. Jabbar and P. U. Lilhore, "Design and Implementation of Hybrid EC-RSA Security Algorithm Based on TPA for Cloud Storage", INTERNATIONAL JOURNAL ONLINE OF SCIENCE, vol. 3, no. 11, p. 6, Nov. 2017. Available: http://ijoscience.com/ojsscience/index.php/ojsscience/article/view/148/175.

[7] Paterson KG, Quaglia EA (2010) Time-specific encryption. In: Garay JA, De Prisco R (eds) Security and cryptography for networks. Springer, Berlin.

[8] Green M, Hohenberger S, Waters B (2011) "Outsourcing the decryption of ABE cipher text".

[9] Huang X, Li J, Li J et al (2014) "Securely outsourcing attribute-based encryption with check ability".

[10] Xhafa F, Wang J, Chen X et al (2014) An efficient PHR service system supporting fuzzy keyword search and fine-grained access control.

[11] Nuttapong Attrapadung, Benoit Libert, and Elie de Panafieu(2008)" Expressive Key-Policy Attribute-Based Encryption with Constant-Size Cipher text"

[12] Chao Li, Bo Lang and Jinmiao Wang(2014) "Outsourced KP-ABE with chosen cipher-text security"

[13] J. Li, X. Chen, J. Li, C. Jia, J. Ma, and W. Lou, "Fine-grained access control system based on outsourced attribute-based encryption," in Computer Security–ESORICS 2013. Springer, 2013.

[14] J. Lai, R. H. Deng, C. Guan, and J. Weng, "Attribute-based encryption with verifiable outsourced decryption," Information Forensics and Security, IEEE Transactions (2013)

Rivest RL, Shamir A,Wagner D A (1996) "Time-lock puzzles and timed release- cryptography.

[15] Bethencourt, J., Sahai, A., Waters, B.: Ciphertext-policy attribute-based encryption. In: IEEE Symposium on Security and Privacy,(2007).

[16] Goyal, V., Jain, A., Pandey, O., Sahai, A. "Bounded Ciphertext Policy Attribute Based Encryption". In: Aceto, L., Damg˚ard, I. Goldberg, L.A., Ing´olfsd´ottir, A., Walukiewicz, I. (eds.) ICALP 2008.