ATTRIBUTE BASED SECURE SEARCHABLE AND REVOCABLE MULTI DATA ENCRYPTION SCHEME IN CLOUD

[1]Gunupati Venkateswarlu, [2]Prashant Singh
[1]Research scholar, Department of CSE, Shri Venkateswara University, gajraula, Uttar Pradesh, India.
[2]Research Guide, Department of CSE, Shri Venkateswara university, gajraula, Uttar Pradesh, India.

ABSTRACT: In recent times, cloud computing has emerged as a rapidly growing field. It serves as a platform for storing and managing data while ensuring the privacy of its users. Access control methods are employed to efficiently process and regulate data while ensuring a high level of security. Cloud environments constantly encounter various challenges, including security concerns and robustness, and so on. While conventional methods aim to provide robust security, the cloud environment still contends with challenges such as minimal efficiency and the absence of attribute revocation. Hence, this analysis specifically concentrates on utilizing the attribute-based mechanism to improve efficiency. The primary aim of this analysis is to define attributes for a specific set of users. Secondly, the data must undergo re-encryption based on the access policies specified for the particular file. Even when the owner is not available, the re-encryption process enables the cloud server to authenticate the user's identity by providing the necessary information. The primary benefit of this work arises from its ability to evaluate multiple attributes, thus facilitating data access for individuals possessing such attributes. The results indicate that the suggested data sharing scheme significantly contributes to enhancing efficiency, security, and timeliness.

Keywords: Cloud computing, Data encryptionkey, Authorization, Efficientrevocation, Security analysis

I. INTRODUCTION

Cloud storage is a key component of cloud computing. Cloud computing depends on the utilization of the internet and centralized remote servers for the maintenance of data and applications. Cloud computing provides users, both businesses and individuals, with the ability to access applications and services without the need for local installation. This allows for convenient access from any computer connected to the internet [8]. By centralizing storage, processing, bandwidth, and memory, this technology enables significantly improved computational efficiency. Yahoo Mail, Facebook, Gmail, and many other similar services are simple examples of cloud computing services. Cloud computing offers three primary services: PaaS (Platform as a Service), IaaS (Infrastructure as a Service), and SaaS (Software as a Service) [10].

Customers have the flexibility to choose one or more services based on their specific requirements. Data access control serves as an effective strategy for ensuring data security within cloud environments. Cloud storage services clearly distinguish between the roles and responsibilities of data owners and storage service providers. The data owner is not directly involved in providing data access services to the users. Implementing data access control in cloud storage systems faces a significant challenge due to the separation of data. Given the limited trust of data owners in cloud servers, traditional server-based access control approaches are no longer effective in ensuring security in cloud storage systems. Traditional methods commonly employ data encryption to safeguard sensitive data from untrusted servers. Through the utilization of data encryption, this approach ensures that only users possessing valid keys have the ability to access the encrypted data.

These methods necessitate complex key management schemes, imposing a demand on data owners to maintain a continuous online presence for the purpose of distributing keys to new users in the system. Furthermore, these methods result in significant storage overhead on the server as it is required to store multiple encrypted copies of the same data to accommodate users with different keys.

Ciphertext-Policy Attribute-Based Encryption (CP-ABE) is widely acknowledged as a highly appropriate technology for the implementation of data access control in cloud storage systems. CP-ABE empowers the data owner with increased authority over access policies, thereby removing the need for key distribution by the data owner [12].

In the CP-ABE scheme, a designated authority plays a crucial role in managing attributes and distributing keys.The authority can take diverse forms, including a registration office in a university or the human resource department in a company, etc. The data owner assumes the responsibility of defining access policies and encrypting the data based on those policies. Each individual user is assigned a unique secret key that is specifically associated with their set of attributes. Only users whose attributes fulfill the requirements set by the access policies can decrypt the cipher texts.

Despite the development of multi-authority CP-ABE schemes [15] for data encryption purposes, these schemes cannot be directly utilized for data access control in multi-authority cloud storage systems. This is due to the fact that these schemes either depend on a centralized attribute authority to handle attributes across various organizations or lack of efficiency in their operations. Efficiency in computation is a crucial factor to consider when designing access control schemes. Access control systems must be able to decrypt and revoke access quickly and easily.[9]

Efficiency is essential in data access control schemes, especially during the decryption process for each user. Additionally, When a user is degraded or leaves the system, it becomes necessary to revoke certain attributes associated with that user. For efficient attribute revocation, there are two requirements:

1) Backward security is ensured as revoked users, having their attributes revoked, are unable to decrypt new ciphertexts that require the revoked attributes for decryption.

2) Forward security ensures that newly joined users can decrypt previously published ciphertexts, regardless of whether those ciphertexts were encrypted with previous public keys, as long as they possess sufficient attributes for decryption.

When handling sensitive data, it is vital to ensure the privacy of information while maintaining a secure and safe environment. However, certain traditional methods store data without implementing any encryption measures directly. Therefore, implementing an encryption process is essential for effectively handling sensitive data. The encryption module should be implemented before the user uploads the data unit.

Users can access and utilize the services offered through the Application Programming Interface (API) in accordance with their individual requirements, subject to payment of the applicable fees. Cloud storage services (such as Google Drive and Microsoft OneDrive) offer this functionality. Maintaining privacy and security in cloud storage services poses several challenges. When handling sensitive data, ensuring the preservation of privacy in a secure and reliable manner is of utmost importance. In certain traditional methods, data is stored in an unencrypted format, without any encryption. Therefore, an encryption process is necessary to handle sensitive data. Before a user uploads a data unit, the encryption module is activated.

Traditional approaches frequently depend on symmetric-key algorithms for data encryption. When retrieving the data, the user must decrypt it using the symmetric key. Due to the frequent data sharing among users, this strategy may not provide complete security. These issues are addressed by using a private key to improve data security. When

data is shared, users can encrypt it using the public keys of the recipients involved, ensuring secure transmission and confidentiality.

Three main tasks are the cause of the problem. In the initial step, the data holder takes on the responsibility of obtaining the public key, which is utilized in the encryption process. Additionally, the data needs to be saved frequently. Lastly, this leads to the utilization of significant resources, including the requirement to re-encrypt the data. To address these challenges, the described research methodology primarily centers around the implementation of an attribute-based control strategy.

II. LITERATURE SURVEY

A. Sahai, B. Waters, et al. [16] presented an Attribute-Based Encryption (ABE) scheme that leverages the user's identity as an attribute for data encryption and decryption. By utilizing Attribute-Based Encryption (ABE), the user's identity is employed for authenticating the public key, thus reducing data duplication and ensuring secure access to the encrypted information. Attribute-based encryption offers several advantages, including reduced computation time for tasks such as downloading, decryption, and re-encryption of the entire data.

J. Li, J. Li, X. Chen, C. Jia, and W. Lou et al., [3] introduced a farm-out computation method for Identity-Based Encryption (IBE), which includes support for key-issuing, key generation, and key-update processes with various offloads. The Refereed Delegation of Computation (RDoC) approach is an additional security framework specifically designed to ensure secure data transfer.

K. Liang, W. Susilo, M. H. Au, J. K. Liu, G. Yang, Q. Xie and D. S. Wong et al., [5] provided a detailed explanation of the Proxy Re-Encryption (PRE) concept. For this research, the methodology involves encrypting the ciphertext by utilizing an index of flexible length. This approach enhances user flexibility and ensures a reliable decryption process. Efficient data sharing within large-scale internet services heavily relies on the utilization of configurable computing resources.

V. Goyal, A. Sahai, O. Pandey, A. Jain, et al. [14] also introduced an encryption framework associated with the bounded ciphertext policy. It facilitates progressive access structures and presents multiple theoretical propositions to provide security proof. Reducing network traffic offers a notable advantage in this context, as it leads to a significant improvement in performance. However, a limitation of this approach is its low communication capacity.

T. Naruse, Y. Shiraishi, M. Mohri, et al., [4] The issue in CP-ABE has been acknowledged, and a solution is proposed that utilizes the access structure of Linear Secret Sharing Schemes (LSSS), thereby eliminating the requirement for a key generation scheme. The secure module is maintained through the implementation of an encryption scheme and the delegation of the revocation process to a trusted authority, which ensures support and protection against attacks. Sometimes, security models are designed to hide policies within the access structure using AND gates. Regardless of that, the problem remains ongoing.

Zheng Q, Xu S, Ateniese G et al. [6] in 2014 introduced two schemes for Attribute-Based Keyword Search (ABKS). Through the establishment of a policy that enables users to access the search functionality, which improves the overall effectiveness of the search process. When a user's attributes align with the access control structure specified by the data owner, the cloud server will retrieve the relevant search results and transmit them to the user.

Qiu S, Shi Y, Liu J, et al. [1] Introduce a concealed strategy for developing a searchable encryption scheme for keywords in the hidden strategy. In the case where the attributes of the data user do not meet the requirements of the access policy, they will be unable to access the information or perform searches on the encrypted data. Its uniqueness derives from the creation of a keyword index with a hidden access structure. However, this article does not include any attribute-based encryption and solely addresses a scheme with a single data owner. In practical

scenarios, it is essential to accommodate multiple data owners within the system.

Tian Y, Peng X, Peng Y, et al. [7] proposed a project that focuses on attribute-based encryption with revocability. If a user is removed from this project, all other users in the system must be given new keys, except for the user that was removed. Then, a fresh encryption key is used to re-encrypt the ciphertext. Hence, an individual who access privileges have been revoked will no longer possess the ability to decrypt the corresponding ciphertext. In practice, the efficiency of the method may be compromised, as only a small fraction of users undergo revocation, whereas the majority of users remain unaffected by such events. As a result, such a procedure becomes unfeasible.

Zhang L, Xia Z, Liu D, et.al [2] A project was introduced focusing on attribute-based access control in cloud computing with an emphasis on effective revocation. The scheme effectively implements a revocation mechanism through the utilization of a version number associated with the private key. The method also offers support for backward security along with forward security. Extensive analysis has demonstrated that this scheme is both highly secure and efficient.

J. Benaloh, E. Horvitz, M. Chase, and K. Lauter et al.[13] Explored in this discussion are the traditional methods that are commonly used to prevent unauthorized access to sensitive data by untrusted servers. These approaches typically involve encrypting the data, allowing access and decryption only to users with authorized keys. Subsequently, the control over data access is dependent on the distribution of keys. Implementing these approaches requires the adoption of complex key management schemes, and data owners must remain continuously online to distribute keys to new users in the system. Furthermore, the server is burdened with significant storage requirements due to the necessity of storing multiple encrypted copies of the same data to accommodate users with different keys.

K. Ren, C. Wang, S. Yu, and W. Lou, et.al [11] They proposed the introduction of a trusted authority responsible for managing all attributes within the system and issuing secret keys to users. The capability of the centralized authority to decrypt all encrypted data introduces a potential security risk and poses a potential performance bottleneck in the system.

III. METHODOLOGY

The block diagram of an attribute-based secure multi-data encryption system in the cloud can be observed in Figure 1. A cloud storage server, assuming the role of the trusted authority, manages the shared settings and distributes private encryption keys to authorized users. Each user's private key is connected to their corresponding set of attributes. Data owners are responsible for message encryption and keyword index construction, while the cloud storage server offers storage capabilities. Subsequently, the Cloud Service Provider (CSP) gains authorization to access the data of all users. Such challenges can lead to significant limitations, and there is a potential for Cloud Service Providers (CSPs) to exploit the content for their own financial benefits. Therefore, this represents one of the most significant challenges in cloud computing. This issue can be addressed by introducing a fully trusted Key Authority (KA). Subsequently, ensuring the precision of the attribute set becomes a significant focus when addressing such challenges.

The control section is initially assigned by the Key Attributes Authority (KAA). It facilitates the generation of public keys to ensure the maintenance of encryption and decryption processes. Additionally, to maintain the security and confidentiality of each client's data, a unique private key is generated for the purpose of decrypting their files. The responsibility of managing these keys is assigned to a key server. By considering the user's role, the access key is constructed specifically for the encryption process.

Data owners can encrypt their messages, create indexes of keywords, and subsequently store the encrypted messages in a cloud environment. Search server stores the keyword index and is responsible for finding documents that match keywords. A verified user within the system has the ability to generate a keyword search token using their private key. The search server receives a search token from the user and subsequently performs a search using the relevant keyword index. When the user's attributes precisely match the access structure defined by the keyword index, the search server proceeds to transmit the search results to the cloud server. Next, the cloud storage server securely transfers encrypted data corresponding to the keyword index to the user.

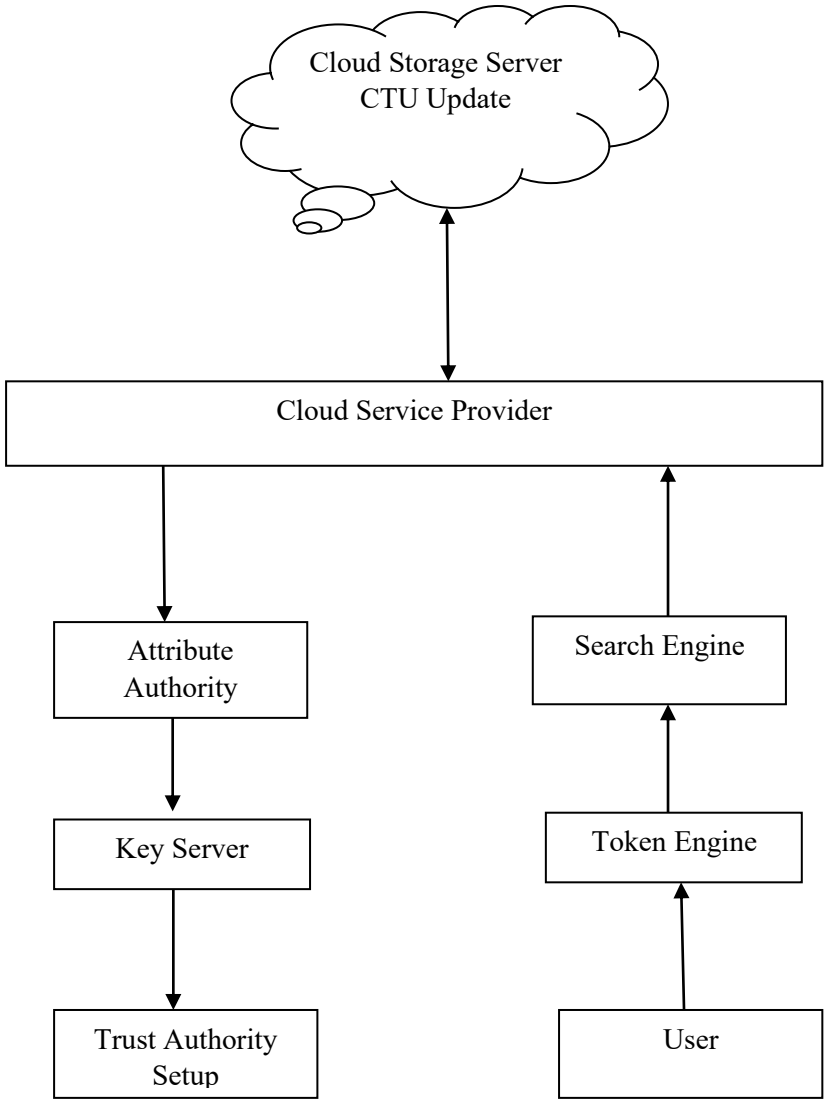

Fig.1: Attribute Based Secure Searchable and Revocable Multi Data Encryption Scheme In Cloud

IV. RESULT ANALYSIS

In this result analysis of Attribute Based Secure Searchable and Revocable Multi Data Encryption

Scheme In Cloud is discussed the performance analysis in terms of Security, efficiency, time.

Table.1: Performance Analysis

Parameters	Attribute-Based Multi-Keyword Search	Multi-Authority CP-ABE Access Control Scheme	Searchable Encryption Scheme	Multi Data Encryption Scheme in Cloud (Proposed)
Security	95.6	89.8	91.3	99
Efficiency	84.6	90.5	93.7	97.1
Key Generation Time (s)	13	15	26	18
Encryption Time (s)	11	33	28	12
Search Time (s)	39	42	41	42

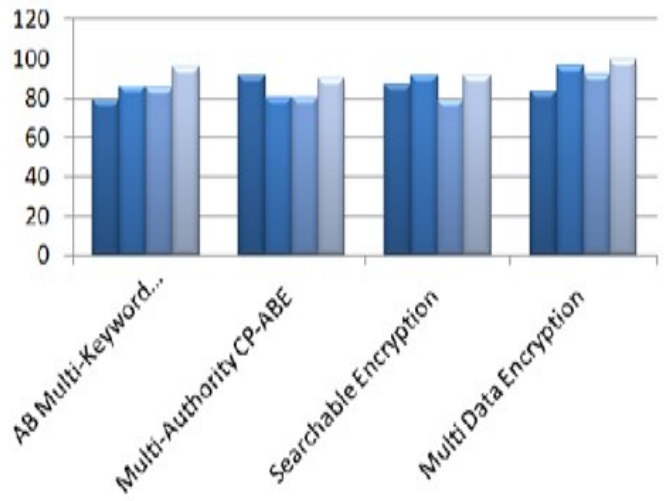

Fig.2: Security Comparison Graph

In fig.3, the graphical representation of security comparison is observed. The security comparison is performed between the methods of Attribute-Based Multi-Keyword Search, Multi-Authority CP-ABE Access Control Scheme, Searchable Encryption Scheme, Multi Data Encryption Scheme in Cloud (Proposed). The described scheme shows higher security.

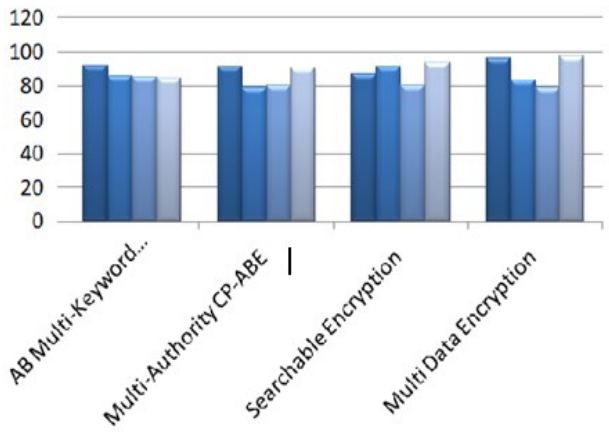

Fig.3: Efficiency Comparison Graph

In fig.3, the graphical representation of efficiency comparison is observed. The efficiency comparison is performed between the methods of Attribute-Based Multi-Keyword Search, Multi-Authority CP-ABE Access Control Scheme, Searchable Encryption Scheme, Multi Data Encryption Scheme in Cloud (Proposed). The Multi Data Encryption Scheme in Cloud (Proposed) scheme shows higher efficiency.

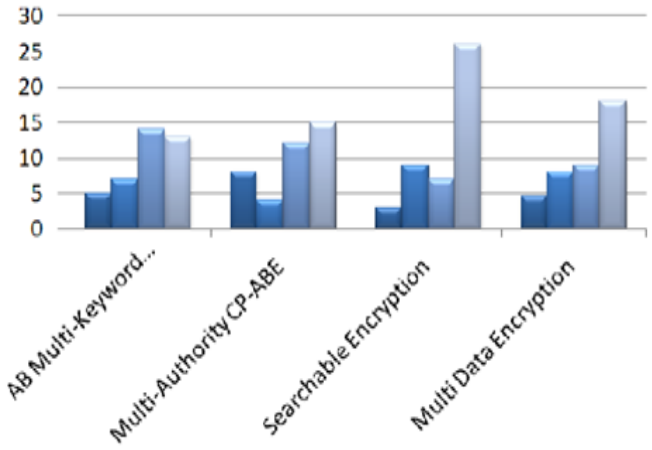

Fig.4: Key Generation Time Comparison Graph

In fig.4, the graphical representation of Key generation comparison is observed. The Key generation comparison is performed between the methods of Attribute-Based Multi-Keyword Search, Multi-Authority CP-ABE Access Control Scheme, Searchable Encryption Scheme, Multi Data Encryption Scheme in Cloud (Proposed). The Multi Data Encryption Scheme in Cloud

(Proposed) scheme shows low time for generating the key.

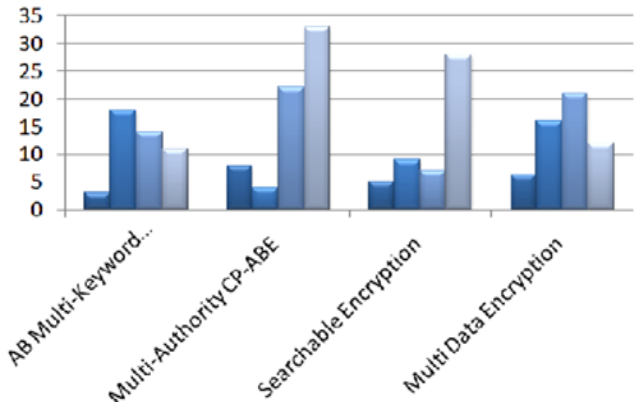

Fig.5: Encryption Time Comparison Graph

In fig.5, the graphical representation of encryption time comparison is observed. The Key generation comparison is performed between the methods of Attribute-Based Multi-Keyword Search, Multi-Authority CP-ABE Access Control Scheme, Searchable Encryption Scheme, Multi Data Encryption Scheme in Cloud (Proposed). The Multi Data Encryption Scheme in Cloud (Proposed) scheme shows low time for encryption.

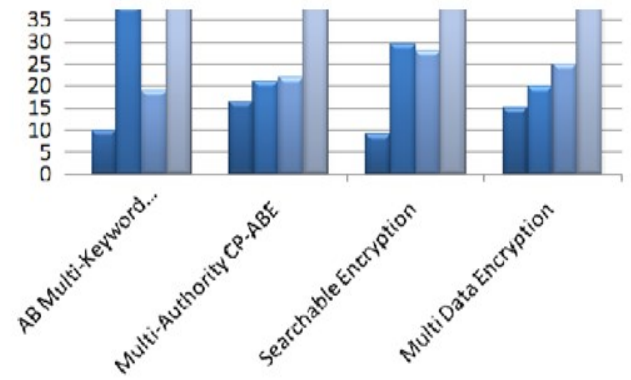

Fig.6: Search TimeComparison Graph

In fig.6, the graphical representation of search time comparison is observed. The Key generation comparison is performed between the methods of Attribute-Based Multi-Keyword Search, Multi-Authority CP-ABE Access Control Scheme, Searchable Encryption Scheme, Multi Data Encryption Scheme in Cloud (Proposed). The Multi Data Encryption Scheme in Cloud (Proposed) scheme shows low time for searching.

V. CONCLUSION

The newly developed attribute-based data sharing scheme offers a secure procedure that addresses many of the mentioned challenges. The presented access control models are designed to minimize the duration required for encryption, re-encryption, decryption, and key generation processes. The examined framework offers a fine-grained and trust-aware approach for implementing access control with precise granularity in an attribute-based access control context. By implementing the system, users can gain access to models that are specifically designed to address security concerns in cloud computing, according to their specific requirements. The system's efficient encryption unit effectively minimizes computation time, even in cases where attributes vary. Similarly, both the key updating operations and revocation processes make use of the complete access control module. In the future, there is potential for expanding this analysis to incorporate heterogeneity within the access control mechanism. Furthermore, there is the possibility of extending the model to enhance efficiency, security, and minimize time complexity.

VI. REFERENCES

[1] Qiu S, Liu J, Shi Y, Hidden policy ciphertext-policy attribute-based encryption with keyword search against keyword guessing attack. Science China Information Sciences, 2017, 60(5):052105.

[2] Xia Z, Zhang L, Liu D. Attribute-Based Access Control Scheme with Efficient Revocation in Cloud Computing . China Communication, 2016, 13(7):92–99.

[3] J. Li, J. Li, X. Chen, C. Jia and W. Lou, “Identity-based encryption with outsourced revocation in cloud computing.” IEEE Trans. Comput., Vol. 64, No. 2, 425 - 437, 2015.

[4] T. Naruse, M. Mohri, Y. Shiraishi, “Provably secure attribute-based encryption with attribute revocation and grant function using proxy reencryption and attribute key for updating.” Human-centric Comp. and Info. Sci., Vol. 5 No. 1, pp. 8, 2015.

[5] K. Liang, M. H. Au, J. K. Liu, W. Susilo, D. S. Wong, G. Yang, and Q. Xie, "A DFA-based functional proxy re-encryption scheme for secure public cloud data sharing." IEEE Trans. Inf. Forensics Secur., Vol. 9, No. 10, 1667 - 1680, 2014.

[6] Zheng Q, Xu S, Ateniese G. VABKS: Verifiable attribute based keyword search over outsourced encrypted data. In: Proceedings of IEEE Conference on Computer Communications, INFOCOM, Toronto, 2014. 522–530.

[7] Tian Y, Peng Y, Peng X, An Attribute-Based Encryption Scheme with Revocation for Fine-Grained Access Control in Wireless Body Area Networks. International Journal of Distributed Sensor Networks, 2014, 25(4):820–835.

[8] B. Waters, "Ciphertext-policy attribute-based encryption: An expressive, efficient, and provably secure realization," in PKC'11. Springer, 2011, pp. 53–70.

[9] A. B. Lewko and B. Waters, "Decentralizing attribute-based encryption," in EUROCRYPT'11. Springer, 2011, pp. 568–588.

[10] Ercan, T. (2010). "Effective Use of Cloud Computing in Educational Institutions," Procedia Social and Behavioral Sciences, 2,938–942;

[11] S. Yu, C. Wang, K. Ren, and W. Lou, "Attribute based data sharing with attribute revocation," in ASIACCS'10. ACM, 2010, pp. 261–270.

[12] Catteddu, D. & Hogben, G. (2009). "Cloud Computing: Benefits, Risks and Recommendations for Information Security," European Network and Information Security Agency.

[13] J. Benaloh, M. Chase, E. Horvitz, and K. Lauter, "Patient controlled encryption: ensuring privacy of electronic medical records," in CCSW'09. ACM, 2009, pp. 103–114.

[14] V. Goyal, A. Jain, O. Pandey, and A. Sahai, ''Bounded Cipher text Policy Attribute Based Encryption.'' in Proc. 35th Int' Colloquium on Automata, Languages, and Programming (ICALP'08), pp. 579 - 591, 2008.

[15] M. Chase, "Multi-authority attribute based encryption," in TCC'07. Springer, 2007, pp. 515–534.

[16] A. Sahai, and B. Waters, "Fuzzy identity-based encryption." In Annual International Conference on the Theory and Applications of Cryptographic Techniques, Springer Berlin Heidelberg, pp. 457 - 473, 2005.

[17] M. Kallahalla, E. Riedel, R. Swaminathan, Q. Wang, and K. Fu, "Plutus: Scalable secure file sharing on untrusted storage," in FAST'03. USENIX, 2003.

[18] E. Goh, H. Shacham, N. Modadugu and D. Boneh. "Sirius: securing remote untrusted storage," in Proceedings of NDSS. 2003. pp. 131-145.