# Attribute Based Encryption in Cloud Computing

**MANASA AKARAPU,**
**Assistant Professor,**
**Department of Computer Science and Engineering,**

**M VANISH SUCHARITHA SANTOSH,**
**Assistant Professor,**
**Department of Electronics and Communications Engineering,**

**Siddhartha Institute of Technology and Sciences,**
**Narapally, Hyderabad, Telangana – 500 088.**

**Abstract**

Cloud computing is a new paradigm that offers a variety of IT-related services. Security and privacy are two important impediments to the adoption of cloud computing. Security concerns explain why there are less real-time and business-related cloud apps than consumer-related cloud services. First, the advantages and disadvantages of various Attribute Based encryption algorithms are discussed. Second, a new encryption approach based on Attribute Based Encryption (ABE) that employs hash functions, digital signatures, and asymmetric encryption schemes is suggested. Our suggested technique is a simple yet efficient approach that may be used in cloud-critical applications.

## 1. Introduction

Cloud computing is a paradigm change from conventional computing in that it focuses on the sharing of computer resources rather than the use of personal devices1. Cloud computing enables end users to access data in a flexible and cost-effective manner across several platforms and at any time. Storage, software, and hardware are examples of shared resources. SaaS, PaaS, IaaS, MaaS, and SecaaS2 are some of the cloud services available.

Virtualization is the fundamental idea underpinning the cloud. The primary concerns of cloud computing are secrecy, accessibility, security, privacy, performance, and integrity. The cloud offers several cloud deployment methods such as public, private, hybrid, and community. Cloud computing is a new technology that has grown in popularity as the number of cloud service providers and cloud customers has grown in recent years. Cloud service companies' income has climbed year after year.

Cloud computing generated around 58 billion US dollars in sales in 2009. In 2010, 70 billion US dollars were spent. In comparison to last year, income increased by roughly 16-17%. The modern cloud application addressed consumer and small company demands rather than mission critical or big enterprise applications. Security breaches will have a much greater impact on large-scale businesses and mission-critical applications than on small-scale businesses.

The money earned by cloud computing is determined by the Quality of Service provided by the cloud service provider. The key aspect of Quality of Service is security, and the cloud service provider must provide full guarantee of security in terms of confidentiality, accessibility, privacy, and integrity. Among the considerations, privacy is a vital and uncompromising aspect of security. Encryption is a method of securing data on an untrusted cloud server. The majority of currently known encryption solutions had little effect on real-time cloud applications. Their use in crucial cloud applications is restricted. As a result, we classify encryption methods based on their usefulness and flexibility.

Attribute-Based Encryption (ABE). Unlike other encryption systems, ABE encrypts and decrypts data based on user characteristics. It offers promising and flexible access control by utilising restricted access structures connected with the private key, master key, and cypher text. When compared to other encryption kinds, such as role-based access, attribute-based encryption is the greatest approach to secure since it allows you to restrict access based on roles. As a result, it is only suitable for small-scale applications. In terms of data retrieval, the ABE is an overhead.

## 2. Literature survey

The data in cloud computing is stored at a location unknown to the end user. First and foremost, data in a database must be secure. Virtualization provides a solution for data security. The location of the data centre is kept hidden in order to achieve security and integrity. 6 \s. The question is whether to trust an untrustworthy cloud server. We argued that it is untrustworthy since it involves several harmful assaults during data processing.

To tackle the difficult access control mechanism over encrypted data, the ABE is presented. ABE is a one-to-many public key encryption that decrypts the cypher text only if the private key associated with the user matches the public key and master secret key. Data decryption is performed immediately by the server. As a result, good encryption approaches improve performance.

There are three algorithms in the KP-ABE. The user had complete access because to the access structure. This is a significant shortcoming of key policy attribute-based encryption. Giving a person full access causes a slew of issues. The KP-ABE fails to differentiate between the necessary access control for users and the access policy encoded in the decryption key. In 2011, Green et al presented the notion of outsourcing ABE decryption, implying that the user must encrypt the data.

The ABE with contracted decryption eliminates the water constraint and ensures protection against malevolent attackers. Only the public key that matches the user's private key is used to decrypt the encrypted text. The water algorithm is modified by the green et al algorithm, which includes a transformation key and a retrieving key. Against ensure data secrecy, the original

data is compared to partly encrypted data. The restriction includes the inability to verify data regardless of whether the appropriate cypher text is decoded.

It may generate the previous cypher text or any other cypher connected with a certain file or anything. Other downsides include the user having to do extra work to decrypt the data. The likelihood of attackers hacking the account is quite low. With verified data outsourcing, this solves the constraint of Green et al. The suggested algorithm compares cypher text to decoded cypher text.

## 3. Methodology

Based on cloud deployment methodologies, many types of cloud applications have previously been classed as private, public, and hybrid. We divide the cloud into three key groups based on the risk associated in cloud applications: high-critical, medium-critical, and low-critical. All cloud-based apps are crucial in nature since they store the user's data. Because it holds the users' information, search applications, forecasting applications, and other applications are deemed vital. Thus, t was classified based on aspects like as timeliness, correctness, reliability, secrecy, performance, privacy, security, scalability, robustness, and integrity, among others.

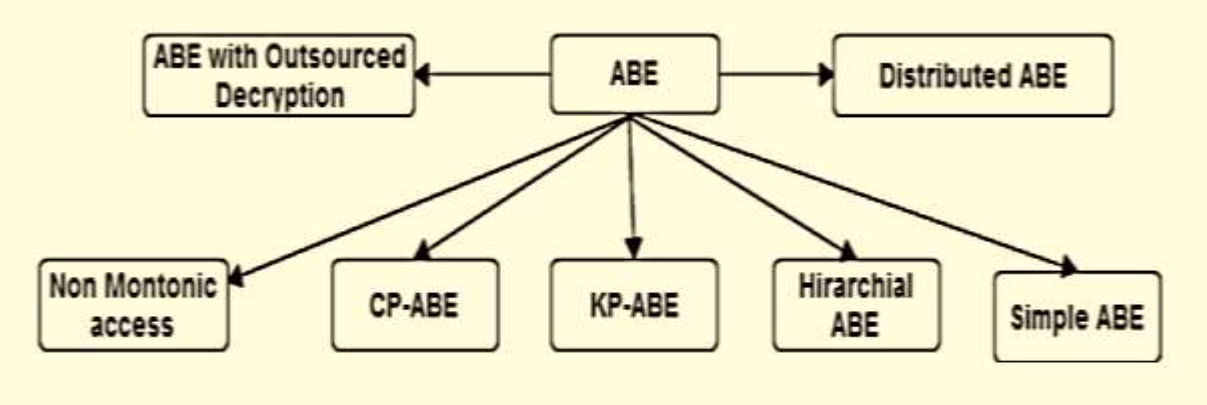


**Fig.1 Classification of Attribute Based Encryption**

All cloud applications do not have to use the same encryption mechanisms. We categorise the appropriate encryption methods based on the risk and cloud deployment models. Taking the train reservation system as an example, there will be a maximum server load and if it hits the maximum number of users, it will fail to function. However, cloud applications may tolerate server load better than traditional web servers if access control and data security are properly implemented. The ABE with fine-grained access control algorithm solves the aforementioned problem.

The cloud's scalability will be great since it is handled by a large number of servers. When compared to traditional servers, migrating to the cloud gives greater service to the user. Although this application is now unavailable in the cloud, it may be added in the future. It is low-cost and high-performance. To provide data secrecy in medium-critical applications such

as storage, ABE must be combined with verified outsourced decryption. The cost of decryption is decreased in comparison by outsourcing it.

The advantage of adopting attribute-based encryption with outsourced decryption is data secrecy. However, for project management, ABE with direct decryption / completely homomorphic encryption is preferable. Data verification is feasible, just as it is in the case of homomorphic encryption. Both solutions are roughly the same in terms of expense. ABE outperforms homomorphic encryption in terms of performance. Attribute-based encryption is better suited for low-critical applications. Because there is no data verification.

- **Access Structures**

The access structure specifies regulated access to genuine users. It also specifies alternative access topologies for users based on their role and characteristics. Let p1, p2,....pn be a collection of parties. Let A 2 power p1....pn) B and C. As a result, B is a subset of A, and C is a subset of A, making C A. And set A is a non-empty set. The set in A is known as an approved set; otherwise, it is an illegal set. In order to efficiently encrypt the data, the original message was partitioned to equal size.

- **Encryption**

It accepts both the public key and the secret key as input. H matches the access tree and encrypts the hash function using the produced Secret key (SK). As a consequence, a digital signature is created. The hash function is encrypted if and only if it fits the Access structure (A). Otherwise, it returns. The encryption method is used to determine the value of H. (x). As a result of encryption, the outcome is H. (x). As a result, data encryption is performed on a cloud server.

- **Decryption**

The public key, secret key, access structure, and private key are used as inputs to the decryption. The user who possesses the private key. As a result, the user can decode using a digital signature and a private key. The private key corresponds to the secret key and the access structure. If the private key matches, the hash function will be decrypted. Otherwise, it returns to the user. Decryption is performed immediately by the server in this case. And the data from the decrypted hash function H(y) = H(x) is validated. Decryption is performed immediately by the server in this case.

## 4. Result and discussion

The hash function, a digital signature, is used in the algorithm. It also adheres to asymmetric encryption. The algorithm is extremely tough for hackers to understand since it requires several phases. All of the steps are performed once per call server. If the authentication fails, the process does not proceed to the following stage. Furthermore, the dual authentication approach

employs both a digital signature and a public key. The secret key will be produced. As a result, decrypting the data is difficult. There will be some time overhead because it takes numerous processes in encryption and decryption.

However, in terms of security, it is insignificant. The adversary sends two messages, M0 and M1, and access structure A, with the limitation that S where D is empty set. And S is insufficient for A. The attacker then challenges through trial and error, picking the (0, 1) and attempting to decipher the message. Because CP-ABE is safe, our suggested approach must be 100% secure. As a result, the suggested ABE algorithm is a foundation for real-time systems. The suggested algorithm must be validated and verified using a simulator.

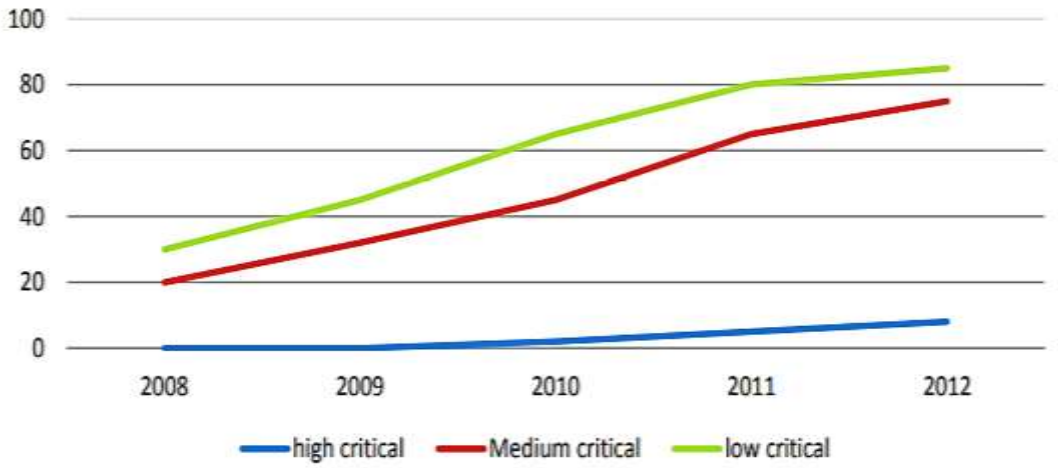


**Fig.2 Classification of Cloud Application Based on Risk**

The user properties of the user hierarchy are used to determine access constraints. The power hierarchy determines the user hierarchy, which represents the broader organisational structure. The fundamental advantage of attribute-based encryption is that each member in the access hierarchy has fine-grained and individual access. During the decryption phase, the potential of modifying the access structure based on the needs of the organisation is made feasible.

## 5. Conclusion

The present state of Attribute Based Encryption for cloud computing has been examined, along with its benefits and drawbacks. An in-depth examination of attribute-based encryption is carried out. And we classify the cloud application depending on the danger involved, and we classify the application with appropriate encryption techniques. Finally, we suggested a novel ABE-based encryption technique that includes hash functions, a digital signature, and an asymmetric encryption mechanism. The suggested technique is a simplified ABE, and it will be useful for applications that require high levels of security. The accessed time is lowered, and therefore the cost is reduced correspondingly.

**References**


1. Qiang Duan, Yuhong Yan, Vasilakos,AV.A Survey on Service-Oriented Network Virtualization Toward Convergence of Networking and Cloud Computing Network and Service Management, IEEE Transactions on, vol.9, no.4, pp.373,392.
2. Computing by Mohit Marwaha1, Rajeev Bedi. Applying Encryption Algorithm for Data Security and Privacy in Cloud in International Journal of Computer Science Issues, Vol. 10, Issue 1, No 1, January 2013.
3. Arshad, J, Townend, P, Jie Xu.Quantification of Security for Compute Intensive Workloads in Clouds Parallel and Distributed Systems (ICPADS), 2009 15th International Conference on , vol., no., pp.479,486, 8-11 Dec. 2009.
4. Sahai and B. Waters.Fuzzy identity-based encryption,‖ in Proc.EUROCRYPT, 2005, pp. 457–473.
5. Mihai Christodorescu, Reiner Sailer, Douglas Lee Schales, Daniele Sgandurra, and Diego Zamboni. 2009. Cloud security is not (just) virtualization security: a short paper. In Proceedings of the 2009 ACM workshop on Cloud computing security (CCSW '09). ACM, New York, NY, USA, 97-102.
6. Junzuo Lai,Deng, R.H, Chaowen Guan, Jian Weng,.Attribute-Based Encryption With Verifiable Outsourced Decryption Information Forensics and Security, IEEE Transactions on, vol.8, no.8, pp.1343,1354, Aug. 2013.
7. B. Waters. Ciphertext-policy attribute-based encryption: An expressive, efficient, and provably secure realization in Proc. Public Key Cryptography, 2011, pp. 53–70.
8. Vipul Goyal, Omkant Pandey, Amit Sahai, and Brent Waters. 2006. Attribute-based encryption for fine-grained access control of encrypted data. In Proceedings of the 13th ACM conference on Computer and communications security (CCS '06). ACM, New York, NY, USA, 89-98.
9. Matthew Green, Susan Hohenberger, and Brent Waters. 2011. Outsourcing the decryption of ABE ciphertexts. In Proceedings of the 20th USENIX conference on Security (SEC'11). USENIX Association, Berkeley, CA, USA, 34-34.
10. S. Chatterjee and A.Menezes. On cryptographic protocols employing asymmetric pairings—The role of revisited, ‖Discrete Appl.Math., vol. 159, no. 13, pp. 1311–1322, 2011.