

# Improving Data Privacy through User Behavior Key Policy with Attribute-Based Cryptosystem

**Author: Mrs. Indira Shailendra Chadar<sup>1</sup>; Mr. Mohsin Sheikh<sup>2</sup>;**

Affiliation: PG Student, MIST Indore<sup>1</sup>; Assistant Professor, MIST Indore<sup>2</sup>;

E-mail:indira.chadar@yahoo.com<sup>1</sup>;er.mohsin.paper@gmail.com<sup>2</sup>;

## ABSTRACT

Cloud computing is a rapidly growing computational technology in recent days a number of application such as banking private organizational ERP and other applications are getting advantages of this technology. Additional cloud computing support different level of user access and support different computational needs of targeted users. Therefore a significant amount of private and sensitive data is hosted on these servers. Therefore in order to provide the security in these applications the cloud system usage the cryptographic technique. In this paper work the cryptographic security over cloud servers are investigated. Therefore various traditional and newly appeared cryptographic techniques are explored first then attribute based encryption technique are obtained. This cryptographic technique is adoptable for security and privacy management both. But the key generation policy is not much trustworthy. Therefore in this presented work the user behavioral attributes are identified for strong key generation for cryptosystem. Furthermore for key generation the user behavioral attributes into the cryptographic key the SHA1 algorithm is used and then that is used with the AES cryptographic standard.

**Keywords:** Data security, ABE, KP-ABE, Cryptographic algorithms, Cloud Storage.

## 1. INTRODUCTION

In computational domains and application data is valuable assets for clients. The client is always worried about their personal, commercial, social and health information, because of that these information are frequently accessed and shared among multiple parties. But due to the lack of computational ability or for preserving the expensive resource data storage is provided in cloud data centres. These data centres are transparently manage and store data. But sometimes due to malicious programs or users privacy of the data owner becomes major concerns for security and privacy in cloud data centres. To assure the client access to its own information's that is necessary the data is preserved in cloud in an unreadable format. In order to prepare such

kind of unreadable data from the recognizable data the most of security system utilizes the techniques of cryptography. Cryptography can be a mathematical model by which the data is altered or modified to generate unreadable format of data.

On the other hand now in these days the need of computational ability is increase continuously. In order to find the scalable computational resource the cloud computing is an appropriated resource provider. The key benefit of cloud computing infrastructure that is scalable, efficient, sharable and transparent. Additionally that offers the maintenance and installation free platforms for providing easy and convenience for end clients. Additionally through the distributed concept of information processing sharing of data resource are also obtained in efficient manner.

The security is a primary concern in different applications, now these days most of the applications are become online and consumes the essential and private data. These application servers are protected from different security algorithms and firewall mechanism. Additionally the data is also secured in the client machines but the transmission of data exchange between secured devices is performed in public entrusted networks. Thus security of data during transmission and storage is a major area of concern. In this present paper the security issues during data storage and transmission is investigated and a new solution for efficient storage and transmission. Thus a different method known as the attribute based encryption technique are developed for providing the security and privacy in cloud environment. This technique usage more than one cryptographic algorithm processes data for preserving the security and privacy in data. That method is called attribute based encryption technique. This technique utilizes the user behavioural data for key generation process and using the traditional cryptographic approach the data is modified for cipher text generation.

## 2. MOTIVATION

Motivation of the attribute-based encryption scheme is comes from two major scheme engineered in the field of encryption. These methods were ground on "Hierarchical Identity Based Encryption" (HIBE) which was first

introduced by *Yao et al.* in 2004. This HIBE was further extended as Fuzzy Identity Based Encryption in 2005 by *AmitShai and Brent Waters*. The scheme is also called Threshold Attribute-Based Encryption (thABE). The authors assume that a Fuzzy IBE can be implemented with the use of biometric inputs in form of Identities. Moreover, they demonstrated the application of their work in ABE a proved it as an error-tolerant and secure against collusion attacks scheme [1][2]. Subsequently, in 2005 on the basis

### 3. PROPOSED WORK

The proposed security system for secure data transfer and storage is presented using figure 1. In this diagram the blocks are represents the different data phases and the links between blocks are shows the relation between two processing blocks.

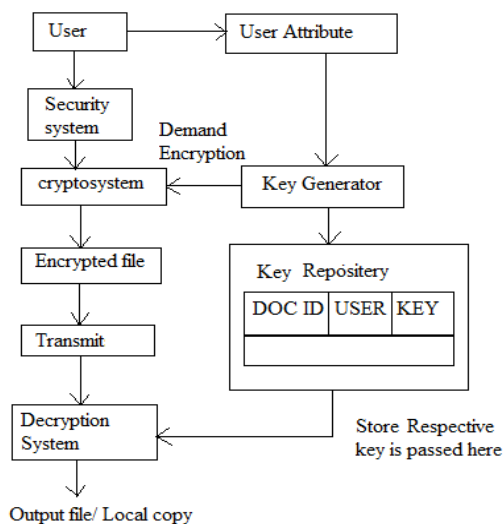


Figure 1. Proposed Cryptographic system

#### Working

The system initiated from the user request first of all user provides the document to upload or download to the secure data server. Additionally the user provides additional key as user attribute for securing the data using the input key. Using the user input attributes the key generator prepares a key for encryption algorithm in this phase the SHA1 hash generation algorithm is utilized for generating the strong key using user input parameters. The cryptosystem contains the cryptographic algorithms which utilizes the generated key as input and encrypts the file. For encryption of files the system utilizes the AES algorithm with the SHA1 generated hash code as key. The encrypted file is used for sharing at the receiving end the file is again processed in the reverses manner and the original file is recovered. In order to support the recovery of the original file the document information is preserved

separately in a key repository. This repository contains the document ID, user identity and the generated key which is used for encryption and decryption.

#### 3.1 User

That is the primary user of the system which provides the input for securing the targeted data.

#### 3.2 User Attribute

In order to secure the data the cryptographic algorithm used. Therefore user provides the input key.

#### 3.3 Key Generation

That is a secure key generation system which accepts the user input key and generate the SHA1 hash for further encryption purpose.

#### 3.4 Key Repository

Each time a new key is required for encryption and decryption of secured files thus the system utilizes a key storage unit. That keeps the file information and the secure key which used for cryptography.

#### 3.5 Cryptosystem

That is an implementation of AES cryptographic algorithm. In this step system accepts the user data and the SHA1 generated hash key encrypting the input data file.

#### 3.6 Encrypted File

The outcome of the previous phase of encryption the ciphertext is generated which is known as encrypted file for system.

#### 3.7 Transmit

After generation of ciphertext the system is ready to transmit the file in unsecure or entrusted network or storage.

#### 3.8 Decryption System

At the storage or receiver end the system accept the ciphertext and recover the data encapsulated in the ciphertext, using the key repository attributes.

### 4. Result analysis

After implementing the proposed security scheme the performance of implemented techniques are evaluated for finding the efficient methodology among both the systems.

#### 4.1 Encryption time

The total amount of time consumed during the encryption is termed here as the encryption time.

time. The key generation time of both the algorithms are given in terms of milliseconds.

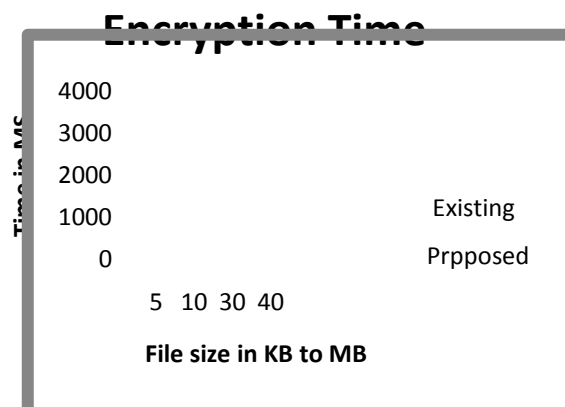


Figure 1.2 Encryption Time

According to the evaluated results the amount of time required encrypt by the traditional algorithm is much higher than the proposed algorithm. Additionally the time difference is increases as the file size for encryption is increases. Therefore the proposed cryptography data hosting techniques is much optimum as compared to the traditional method.

### 4.2 Key size

The key size of algorithms are computed dynamically therefore each time the new key values are generated. In order to generate the key values the traditional method consumes user name, password, date and time and trust values. In addition of that the proposed techniques only consumed only input attribute for the current session.

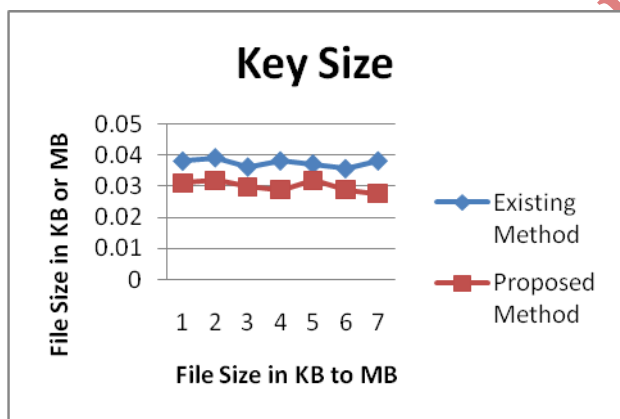


Figure 1.3 Key Sizes

According to the given figure the system simulates the two different key sizes in terms of KB to MB. These keys are recorded and preserved into a text file and after that the size of file is taken as key size. According to the evaluated result the proposed method generates the similar key size which is longer than the traditional approach. Long size key demonstrates the higher strength of cryptographic algorithm.

### 4.3 Key generation time

The amount of time of time consumed for generating the cryptographic key is termed as the key generation

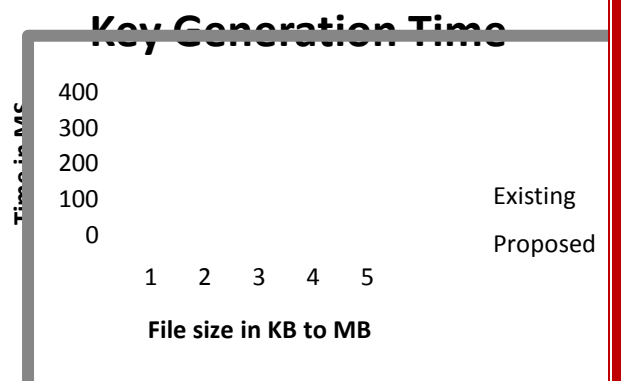


Figure 1.4 Key generation time

The key generation time of the traditional method is much higher than the proposed cryptographic technique. Therefore the proposed methodology generates the long key in less time which is adaptable for security.

## 5. CONCLUSION

The security is an essential factor in different aspect of computational and storage applications. Now in these days most of applications are working as web applications. These applications are able to serve efficiently at any time. In addition of that these applications are deployed as SAAS (software as service) for taking advantage of computational engines and huge data storage.

In order to secure these applications and their data these computational engines are frequently utilizes the techniques of cryptographic security. In during the literature analysis that is obtained the cryptographic security is completely depends on the cryptographic key policies. Strong key generation mechanism improves the security against the brute force attacks. Therefore, a user behavioural attribute based cryptographic key generation technique is proposed for further work. These user behavioural attributes can be the user application navigation habits or the other computational activities. Therefore that is required to utilize some technique by which these user behavioural attributes are convertible to the storage cryptographic technique development. The SHA1 algorithm is used for key generation and the AES algorithm is used for encryption of data. The implementation of the proposed user behaviour attribute based encryption techniques is performed using java development environment and their performance in terms of different performance parameters are evaluated. According to the obtained result the proposed cryptographic technique is efficient and adoptable as compared to the other available similar cryptographic techniques. Therefore the given work is adaptable due to less computational complexity and efficient working.

### ACKNOWLEDGMENT

I express my professional gratitude with a pleasure to

Mr. Mohsin Sheikh, Assistant Professor, Information Technology Department, whose constant encouragement enabled me to work enthusiastically; working under his guidance has been a fruitful and an unforgettable experience.

#### REFERENCES

- [1] Yao, Danfeng, et al. "ID- Based Encryption for Complex hierarchies with applications to forward security and broadcast encryption" proceedings of the 11<sup>th</sup> ACM conference on computer and communications security. ACM, 2004
- [2] Sahai, Amit, and Brent Waters. "Fuzzy Identity- Based Encryption." *Advances in cryptology-EUROCRYPT 2005*. Springer Berlin Heidelberg, 2005. 457-473.
- [3] Nali, Deholo, Carlisle M. Adams, and Ali Miri. "Using Threshold Attribute- Based Access Control." *IJ Network Security 1.3* (2005): 173-182.
- [4] Pırretti, Matthew, et al. "Secure Attribute-Based System." *Proceedings of the 13<sup>th</sup> ACM conference on computer and communications security*. ACM, 2006.
- [5] Goyal, Vipul, et al. "Attribute-Based Encryption for Fine-grained access control of encrypted Data" proceedings of the 13<sup>th</sup> ACM Conference on Computer and communication security. ACM, 2006  
(2002) The IEEE website. [Online]. Available: <http://www.ieee.org/>
- [6] Chase, Melissa. "Multi-Authority Attribute based Encryption". *Theory of Cryptography*. Springer Berlin Heidelberg, 2007. 515-534
- [7] Camenisch, Jan, and Anna Lysyanskaya. "An efficient System for non-transferable anonymous Credentials with optional anonymity revocation". *Advances in Cryptology-EUROCRYPT 2011*. Springer Berlin Heidelberg, 2011. 568-588.
- [8] Cheun, Ling, et al. "Collusion -Resistant group Key Management using Attribute -Based Encryption." *Group-Oriented Cryptographic protocols* (2007)
- [9] Goyal, Vipul, et al. "Bounded Ciphertext Policy Attribute-based Encryption ." *Automata language and Programming*. Springer Berlin Heidelberg, 2008, 579-591.
- [10] *Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specification*, IEEE Std. 802.11,

IJournals