International Journal of Recent Technology and Engineering (IJRTE)
ISSN: 2277-3878 (Online), Volume-7, Issue-6, March 2019

# An Efficient Multi Level Client Integrity Verification and Encryption Model on Cloud Data Security

**Lakshmi Naga Divya Tamma, Shaik Shakeel Ahamad**

***Abstract*: With the immense growth of distributed technology, cloud computing has gain vast popularity among service providers and their customers. Service providers initiate their services by using cloud platform; the clients are required to access their services through a secured channel. As the client sensitive data are stored in cloud server either in public or private access, there exists a malicious or an unauthorized access to cloud storage data against third party attacks. For this, number of cloud security models have been proposed in the literature to secure the sensitive storage against unauthorized access. But the existing security models are having issues due to memory and time constraints. Hence, the data security issues and data privacy preservation issues have become the prime concern for both service providers and cloud service users. In this proposed work, An Efficient Client Integrity Verification based Q-CPABE (Q-CPABE) model was implemented as an extended data security and privacy preserving model on the storage of cloud data. The main motto of this model is to secure the user's sensitive data with a strong access control mechanism using the chaotic integrity verification based Q-CPABE technique. Our results showed that the Chaotic Integrity Verification of Q-CPABE model is having efficient accuracy and time constraints compared to the traditional CPABE models.***

***Index Terms:* Quantum cryptography, CPABE, Client integrity validation, Cloud security.***

## I.. INTRODUCTION

Now-a-days, as the size of the data increases with technology, cloud computing has become popular data storage system and computing services for a large number of applications. As it overcomes all the disadvantages of traditional computing mechanisms of centralized system, it has become widely accepted and distributed computing in various domain fields. Cloud computing serves both service providers or organizations and clients or users. Various organizations provide their services via cloud platform and allow their users to access it. As a part of these services, users can store or upload their sensitive information to the cloud server. This sensitive data always suffer from data security and data privacy threats[1]. Therefore, the need of an efficient cryptographic scheme arises. Cloud security is the process of securing sensitive information those are transmitted through the network by encoding them. The process of encoding original sensitive message is known as encryption in which plain text is converted to cipher text with the help of an encryption key. Later, many cryptographic approaches are integrated with each other to form hybrid and more secure approaches. Since years vast amount of research works have been carried out in order to develop an efficient and advanced cryptographic scheme. Data security issues and privacy preservation issues are identified as complex and challenging issues for many service providers. Clients want to make their sensitive information secure, before uploading them into the cloud server. Therefore, these sensitive details are needed to be encrypted before uploading. In this research paper, we thoroughly studied and analysed several previously developed attribute-based encryption as well as decryption approaches. The benefits and limitations of each and every attribute-based model are also studied and a comparative analysis is performed[2]. There are some most commonly implemented and widely accepted attribute-based encryption techniques which are described below:-

***Attribute-Based Encryption Model:***

Initially in 2005, Attribute-based encryption and decryption model was proposed by *Sahai* and *Waters*. They tried to enhance the security and privacy of all existing traditional cryptographic models and hence developed attribute-based encryption model (ABE). The above proposed model is capable of resolving all limitations of traditional cryptographic schemes. Here, users' attributes are used in constructing secret key and cipher text. [3].

***Key Policy Attribute-Based Encryption Model:***

Previous attribute-based encryption model is slightly changed and it was extended with Key policy attribute-based encryption model. This model overcomes all the issues of traditional attribute based encryption technique. Here in this model, access tree structures are implemented to represent it. The nodes of the access trees are denoted by threshold gates. There also exist a major disadvantage of the presented model, that is:- it is incapable of controlling the decryption rights. It has four algorithms[4]:-Setup: Setup generates public key PK, master secret key MK with the help of input plain text M. These two keys will be used in the encryption. Master secret key has the responsibility of generating user secret key. Encryption: Encryption is responsible for encrypting plain text M with the help of public key PK and set of attributes. Cipher text is the outcome of this algorithm.

**Revised Manuscript Received on 30 March 2019.**
***** Correspondence Author
**Lakshmi Naga Divya Tamma**, CSE, KLU, Vijayawada,,India.
**Dr.Shaik Shakeel Ahamad**, CCIS, Majmah University, Al Majmaah,Riyadh, Kingdom of Saudi Arabia and CSE,KLU,Vijayawada,India.

Key Generation: Access structure tree T and master key MK are inserted in key generation algorithm. One more secret key SK is produced which is required in the process of decryption. The process of decryption is possible, when it matches with access tree. Decryption: Secret key SK is responsible for the production of access structure T and cipher text E. When the attribute set is equivalent with T, the process of decryption is possible.

***Cipher Text Policy Attribute-Based Encryption Model:***

CPABE model was developed by *Sahai.* This model is based on the basic idea of cipher text associated with access control mechanism. Here, secret keys are also integrated with attributes. The process of decryption is permitted, when corresponding attributes satisfies its intended access policy. The whole working process of CP-ABE model is completely reverse of previously developed KP-ABE. [5].

The problem of CP-ABE model was detected and many research ideas are proposed subsequently in order to overcome it. Finally, *Bobba* and *Waters* became successful in finding the appropriate solution for this problem. They developed a new and advanced technique which is an extended version of traditional CP-ABE technique. They termed their presented approach as CP-ASBE. According to this model, the attributes are associated along with a recursive set structure. Another vital characteristic of the above approach is dynamic constraints. Some essential key attributes are generally chosen out of the vast attribute sets by users. Though the above technique is very much efficient to overcome the only disadvantage of traditional CP-ABE, but it also fails in case of integrating attributes of multiple keys.

***Hierarchical Attribute-Based Encryption Scheme:***

At first, *Wang* introduced the above Hierarchical attribute-based encryption model. The above approach hierarchy structure as the basic component. The root master which is denoted by root node has the responsibility of managing the process of key generation. Throughout this process, it also interacts along with some other domain masters.

These domain masters have the responsibility of interacting with each and every enterprise users individually. The hierarchical model can be easily and efficiently implemented in cloud enterprise domain and in proxy re-encryption applications. This approach has no practical implementations till date. In other words it can be stated that, this approach is not applied to any real world applications and executed successfully. The above proposed technique will become very costly and cost infeasible, if will be implemented in practical applications. Domain authority is capable of handling the conjunctive clause attributes and numbers of different domain authority work together in order to handle the similar attributes effectively.

## I. RELATED WORK

*N. Kaaniche et.al.* emphasized on several issues of security in cloud storage [1]. With these security issues and privacy preservation challenges a new model was developed for secure cloud storage. A thorough survey and comparative analysis is performed on various previously developed traditional cryptographic algorithms. These techniques somehow enhance overall security of cloud storage, but they are inefficient to provide complete security.

*C. Guo, et.al.* developed a Key-Aggregate authentication cryptosystem to manage data sharing in dynamic cloud storage [2]. The prime concern of above approach is to propose a new method by which users will be able to upload files more frequently to the cloud. Apart from this, the presented authentication technique resolves the issue of key leakage during the process of data sharing. The above presented approach supports both the needs at the same time. As the number of cipher text grows rapidly in dynamic cloud, this system can be proved as an efficient one. The size of public system parameter is related linearly with cipher text classes.

*A. Alabdulatif, et.al.* introduced a privacy preservation anomaly detection technique in cloud [3]. In this research, a new cloud-based framework is introduced which is light weight. It has the responsibility to carry out the process of anomaly detection with extended security and privacy preservation. The privacy server is integrated with a group of other public servers in order to execute the necessary tasks in homomorphic technique. Further, the traditional homomorphic encryption approach can be modified and extended significantly in order to increase the performance of the system.

*Q. Huang, et.al,* implemented hierarchical attribute-based encryption technique to develop an advanced and efficient data collaboration system in case of cloud computing environment [4]. Additionally, there also exist other problems such as:- problem in key management process and evaluation of complex overheads. The presented approach provides data security in public cloud with the help of HABE integrated delegation method. In case of huge numbers of users, the proposed technique withdraws the key management load of authority. The process of partial delegation along with the signing method is responsible for delegation of decryption as well as signing evaluation overheads.

*X. Liu, et.al,* implemented data access policies in cloud based Personal Health Record systems [5]. As the use of cloud based systems are growing exponentially, large number of users are using cloud based personal health record system in the recent time. Because the PHR systems want to keep their patient sensitive details private, thus there is an essential need of enforcing data privacy constraints much prior to the process of outsourcing. This enhances the overall performance of the system significantly. By using the features of HCBE technique, they also introduced an advanced Dynamic Policy Updating approach. The above DPU approach is influenced by proxy re-encryption method. By using synthetic dataset the overall efficiency of the system can be evaluated. Further works can be done to prevent CP attacks, KS-CDAs, and SS-CDAs.

*V. Odelu, et.al,* developed a new approach of parsing-based CP-ABE which is an extended version of the traditional CP-ABE technique [6]. Further, the above suggested technique can be implemented in many real-world applications efficiently.

Further works can involve applying a prototype for this approach along with a real-world setting. Further fine tuning is an essential need of this method. Additionally, the presented approach can be extended in order to implement other access structures like OR-gate and threshold.

*M. Sookhak,* developed an attribute-based access control in case of mobile computing [7]. They have studied and identified all previously existing access control schemes along with their limitations. In this research paper, attribute-based access control policies are implemented in distributed cloud. Initially, the concept of IBE is implemented and PRE as well as RBAC are described by three basic cryptographic approaches. The traditional ABE approach is modified and extended to a new variety of IBE approach. They also perform classification analysis of traditional frameworks. The similarities and differences of several attribute based schemes are studied and thoroughly analysed. Benefits and limitations of all previously existing approaches are compared with each other. Pre-existing problems are identified and further research solutions are analysed.

*S. Souza et.al,* proposed a client-side encryption technique for privacy preservation on cloud [8]. In the field of data security and privacy preservation, client side encryption is considered as an efficient way. There is no such approach developed till date which can provide a complete solution for data security and privacy preservation on cloud.

*X. A. Wang et.al,* presented a new and advanced privacy preserving predicate encryption approach [9]. The above proposed encryption scheme is associated with fine-grained searchable capability for cloud storage. The process of predicate encryption is more secure and can handle more complex data in cloud than that of all other conventional public key encryption approaches. In this above research, the traditional predicate encryption approach is slightly modified and extended when integrated with dual system encryption approach.

*G. Kalpana, et.al,* introduced a new technique in order to provide better data security and privacy preservation in mobile cloud [10]. They termed their proposed approach as Shifted Adaption Homomorphic Encryption. The limitations of computing capacity and storage space in mobile device increases the need of developing efficient mobile cloud computing discipline.

## II. PROPOSED MODEL

In our new model we are introducing a Novel Client Integrity Verification of Quantum Key distribution with Cipher text Policy based Attribute Based model was done on storage of cloud data. This model was shown in three phases as shown in Figure 1. In the Phase 1, Unique Identification Key (UIK) is generated to authorized cloud user for integrity verification. In the Phase 2, control access mechanism and the encryption operations will be performed on the authorized user's cloud data. In the Phase 3, user control access verification, decryption operations will be done on encrypted cloud data. Here, a Quantum key distribution based CPABE encryption and decryption model was used for data encryption and decryption process. Quantum cryptography is a technique used to secure information exchange between legitimate users along communication lines. Chaotic Quantum Cryptography can be defined as an integration of two separate topics known as quantum cryptography and chaos functions. According to the chaos function and random processes in quantum cryptography, a chaos function and its initial condition is responsible for defining random numbers. Also, a novel chaotic hash algorithm is used for integrity verification.

Trusted Authority Agent (TAA) is a server program used to verification and validation of cloud user's integrity as access control mechanism. TAA takes cloud parameters, attribute list and policies as input to generate unique identification key (UIK) as client integrity value.

**Phase 1:** In the first phase, each user's attribute(s) and their policies are added to the user's property list at the server side. Each user is verified by the trusted authority agent (TAA) for unauthorized access or malicious access. Here, TAA generates a chaotic hash value to each user's property list for unique identification key(UIK). Table 1 describes the unique identification key generation using the user's attributes and cloud credentials.

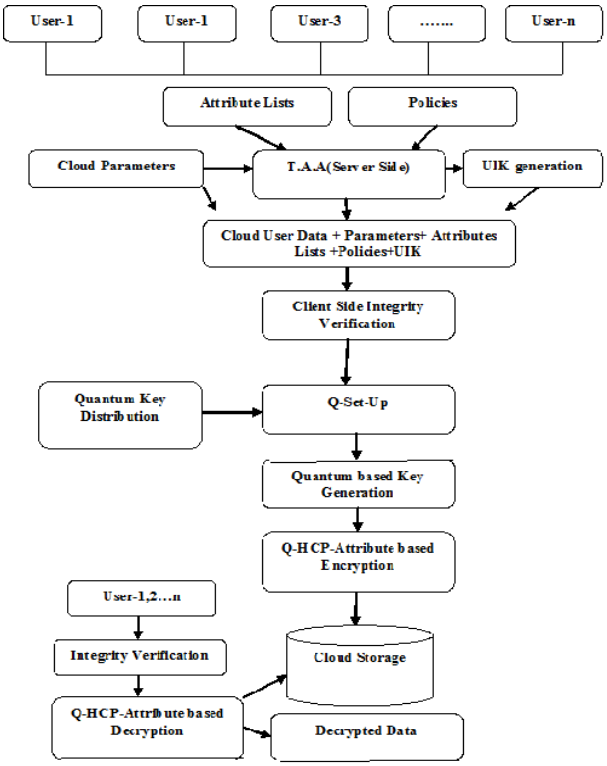


**Figure1: Proposed Model**

**Table 1: User to Unique identification Key Generation**

| User(U(i)) | Attribute(s) | Unique Identification Key(UIK) |
|---|---|---|
| U(1) | $A_1 = A_{10}.A_{12}.A_{13}....A_{1n}$ | UIK(U(1)) |
| U(2) | $A_2 = A_{20}.A_{22}.A_{23}....A_{2n}$ | UIK(U(2)) |
| U(3) | $A_3 = A_{30}.A_{32}.A_{33}....A_{3n}$ | UIK(U(3)) |
| ..... | ..... | ..... .... |
| U(n) | $A_m = A_{m0}.A_{m2}.A_{m3}....A_{mn}$ | UIK(U(n)) |

**Table 2: Multiple Users to Unique identification Key Generation**

| User(U(i)) | Attribute(s) | Unique Identification Key(UIK) |
|---|---|---|
| U(1), U(2), U(3),.... U(k) | $A_1 = A_{k0}.A_{k2}.A_{k3}....A_{kn}$ | UIK(U(1), U(2), U(3),.... U(k),) |

Table 2, describes the unique identification key generation using the multiple users using the users attributes and cloud credentials.

**Proposed Extended Chaotic Integrity Generator:**

Chaotic property is an aperiodic long term random behaviour in a dynamically computing system that possesses great randomness to initial conditions. Also, the chaotic code generated from chaotic maps is featured by very low similarity, low auto correlation, high randomness and boundedness in the given range. In this work, we have computed an extended generalized chaotic map(GCM)[1] using the following formula.

$P(n+1) = (c1+c2)\ \{P(n)+Q(n)\} \bmod (2\pi)$

$Q(n+1) = \{c1.P(n)+c2.\cos(P(n))\} \bmod (2\pi)$

Where $\pi$=3.14159 and c1, c2 are random cyclic group elements which are normalized to 0-1.

$P(n+1)$ and $Q(n+1) \in [0, 2\pi]$

Proposed chaotic hash system can be computed using the piecewise linear chaotic map(PWLCM)[1] and the extended GCM equation as given below:

$$\text{Extended GCM}(EGCM) = EGCM(n+1) = r1.\frac{m(n+1)}{256} + r2.|\cos(m(n+1))|^2 + r3.|\sin(P(n+1))|.|\cos(m(n+1))|^2$$

$$+ r4.|\sin(Q(n+1))|.|\cos(m(n+1))|^3 + r5.|\sin(m(n+1))| + r6.(1-X(n)) + r7.(1-EGCM(n)^3)$$

Here r1…r7 are the boolean 0 or 1 of the m(t+1)th ASCII binary value.

m(n+1) is the (n+1)th ASCII value of the message.

**Phase 2:** In this phase, TAA verifies user access control and grant access to cloud data encryption. In this phase, user to UIK verification and users to UIK verification takes place at the server side for client integrity verification. Only authorized users are allowed to perform Q-CPABE encryption on the cloud storage data.

**Phase 3:** In this phase, TAA verifies user access control and grant access to cloud data decryption. In this phase, user to UIK verification and users to UIK verification takes place at the server side for client integrity verification. Only authorized users are allowed to perform Q-CPABE decryption on the cloud storage data.

## III. EXPERIMENTAL RESULTS

Experimental results are performed on the realtime cloud computing environment such as Amazon EC2 servers. Proposed client integrity verification based Quantum –CPABE model is executed on Amazon EC2 cloud services. Here, Amazon S3 is used for client data storage and access control mechanism.

**Statistical Integrity Randomness:**

Shannon proposed two measures namely confusion and diffusion as essential features for strong integrity verification process. For an efficient diffusion property, there should be 50 percent bit change in the hash value. Let the initial message and its bit values are taken as original data. The changed bits of the computed hash value are

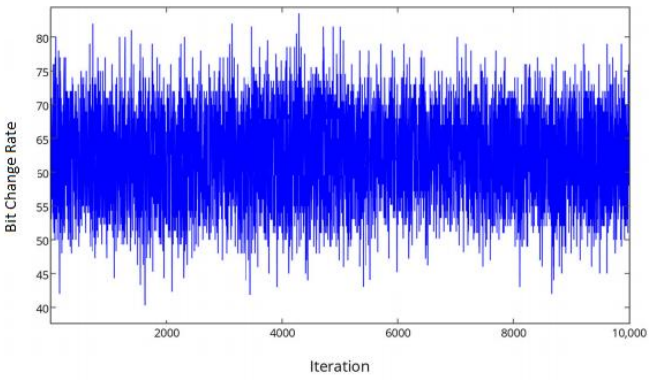


**Figure 2: Sensitivity of the proposed model tin terms of bit change variation in input data**

marked as B(i). The computational measures used to compute the confusion and diffusion are given below.

Changed Minimum bit rate:

B(min)=min({B(1),B(2),….B(k)});

Changed Maximum bit rate:

B(max)= min({B(1),B(2),….B(k)});

$$\text{Mean changed in bit rate } \bar{B} = \sum_{i=1}^{n} B(i) / N$$

$$\text{Standard variance in bit rate} = \{\sum_{i=1}^{n} (B(i) - \overline{B(i)})^2 / N\}^{1/2}$$

**Table 3: Comparison of Client Integration based Quantum Cipher text policy attribute based Encryption and Decryption models**

| Algorithms | Integrity Time(ms) | Data size |
|---|---|---|
| MD5+CPABE | 5864 | 2048 |
| SHA512+KPABE | 4793 | 2048 |

| | | |
|---|---|---|
| MD5+FHEncryption | 4653 | 2048 |
| Whirlpool+KPABE | 4396 | 2048 |
| QCP-ABE+ProposedEGCM | 4194 | 2048 |

Table 3 explains our new model has low integrity verification time when it is compared with previous existing models

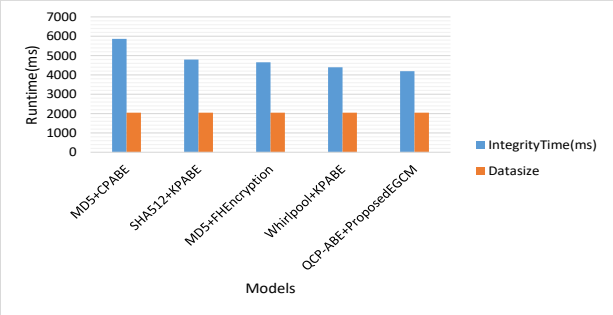


**Figure 3: Comparison of New the model with previous models in terms of integrity verification time.**

**Table 4: Comparative results of new model with previous models**

| Algorithms | Encryption Time(ms) | Data size |
|---|---|---|
| MD5+CPABE | 6294 | 2048 |
| SHA512+KPABE | 6194 | 2048 |
| MD5+FHEncryption | 5983 | 2048 |
| Whirlpool+KPABE | 5784 | 2048 |
| QCP-ABE+ProposedEGCM | 4074 | 2048 |

Table 4 explains our new model has low encryption time of data during the data security when it is compared with previous existing models .

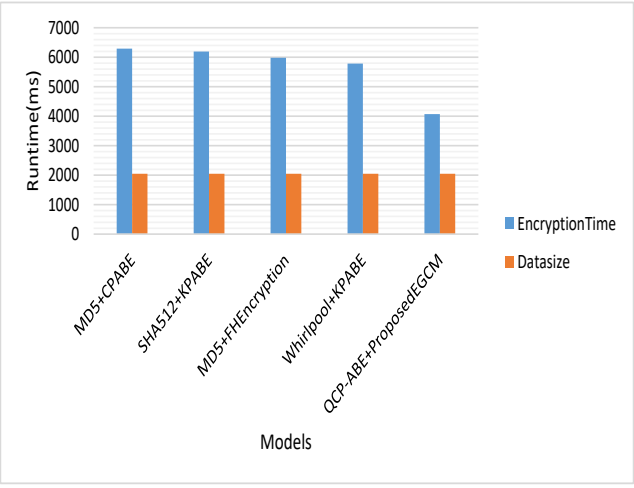


**Figure 4: Comparison of the New model with previous models in terms of Encryption time**

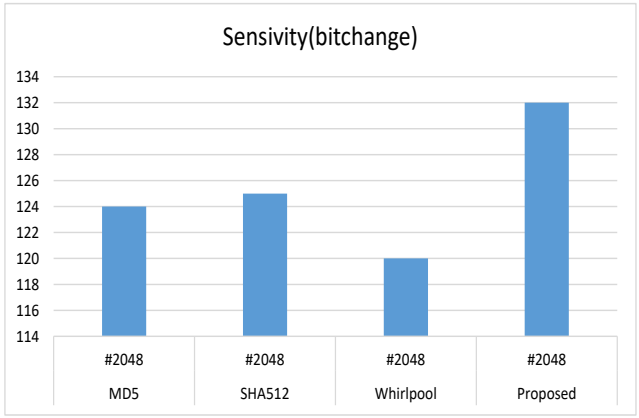


**Figure 5: Comparison of the New model with previous models in terms of integrity sensitivity of the large data size.**

## IV. CONCLUSION

In the recent era, cloud computing has become very popular both among service providers and customers. Service providers have accepted cloud platform for the growth of their business. In the traditional models, cloud users are required to upload their sensitive details to gain access to several cloud services which may lead to some data security and privacy issues. Also, most of the existing security models are having issues due to high memory and time constraints. Hence, the data security issues and data privacy preservation issues have become the prime concern for both service providers and cloud service users. In this proposed work, an efficient client integrity verification based Quantum CPABE (Q-CPABE) model was implemented as an extended data security and privacy preserving model on the storage of cloud data. Experimental results proved that the present model is better applicable to large set of textual data and media data files with high computational accuracy.

## REFERENCES

1. N. Kaaniche and M Laurent, “Data Security and Privacy preservation in Cloud Storage Environments based on Cryptographic Mechanisms”, “Preprint submitted to Computer Communications”, pp. 1-70, 2017.
2. C. Guo, N. Luo, Md. Z. Bhuiyan, Y. Jie, Y. Chen, B. Feng and M. Alam, “Key-Aggregate Authentication Cryptosystem for Data Sharing in Dynamic Cloud Storage “, “Future Generation Computer Systems”, pp. 1-29 2017.
3. Alabdulatif, H. Kumarage, I. Khalil and X. Yi, “Privacy-Preserving Anomaly Detection in Cloud with a lightweight Homomorphic Approach”, “Preprint submitted to Journal of Computer and System Sciences”, pp. 1-41, 2017.
4. Q. Huang, Y. Yang and M. Shenc, “Secure and efficient data collaboration with hierarchical attributebased encryption in cloud computing “, “Future Generation Computer Systems”, pp.1-28, 2016.
5. X. Liu, Q. Liu, T. Peng and J. Wu, “Dynamic Access Policy in Cloud-Based Personal Health Record (PHR) Systems”, “Preprint submitted to Information Sciences”, pp. 1-39, 2016.
6. Odelu, A. K. Das, Y. S. Rao, S. Kumari, M. K. Khan, K. R. Choo, “Pairing-based CP-ABE with constant-size ciphertexts and secret keys for cloud environment “, “Preprint submitted to Elsevier”, pp.1-10, 2016.
7. M. Sookhak, F. R. Yu, M. K. Khan, Y. Xiang and R. Buyya, “Attribute-based data access control in mobile cloud computing: Taxonomy and open issues”, “Future Generation Computer Systems”, pp. 1-14, 2016.

8. S. Souza and R. S. Puttini, “Client-side encryption for privacy-sensitive applications on the cloud “, “Procedia Computer Science 97 ( 2016 ) 126 – 130”, pp. 126-130, 2016.
9. X. A. Wang, F. Xhaf, W. Cai, J. Ma and F. Wei, “Efficient privacy preserving predicate encryption with fine-grained searchable capability for Cloud storage”, “Computers and Electrical Engineering 0 0 0 (2016) 1–13”, pp. 1-13, 2016.
10. G. Kalpana, P. V. Kumar, S. Aljawarneh and R. V. Krishnaiah, “Shifted Adaption Homomorphism Encryption for Mobile and Cloud Learning”, “Computers and Electrical Engineering 0 0 0 (2017) 1–18”, pp.1-18, 201

## AUTHORS PROFILE

**Lakshmi Naga Divya**, Tamma received her B. Tech in Computer Science and Engineering from JNTUKakinada, Andhra Pradesh and received M. Tech in Computer Science and Engineering from JNTUKakinada, Andhra Pradesh India. Currently she is working as an Assistant Professor in Saraswati College of Engineering, Kharghar, NaviMumbai, India. Her research includes Network Security.

**Dr. Shaik Shakeel,** Ahamad is currently working as an Assistant Professor in CCIS, Majmaah University, Kingdom of Saudi Arabia. He was a Professor in the Department of CSE, KL University, Guntur, India (now on lien). He holds a PhD in Computer Science from the University of Hyderabad, India in the realm of secure mobile payments protocols and formal verification. His research interests include cloud-based mobile commerce, secure mobile healthcare frameworks and protocols, wireless public key infrastructure and digital forensics.