International Journal of Recent Technology and Engineering (IJRTE)
ISSN: 2277-3878, Volume-8 Issue-3, September 2019

# A Systematic Framework for Securing Cloud Data

**P Namratha, C Shoba Bindu**

***Abstract*: Cloud usage has increased rapidly in many organizations and institutions. Data storage as a service is one among the cloud service, where data owner stores his information in cloud servers rather than in their own servers. Security and Privacy issues are one of the biggest challenges for cloud computing services. Cloud security intends data stored online to be safe by preventing it from being stolen and leaked. Cloud data security can be provided by adopting cryptographic techniques. Data Security includes different services like confidentiality, integrity and identity and access management. To ensure data security a systematic framework that offers key generation, confidentiality, authentication, and key exchange services. Data owner before storing his data on to cloud will implement Laplace transform based key generation service that generates an encryption key by accepting a random secret phrase (seed). Laplace transform encryption is executed by accepting generated secret key and data to provide data confidentiality. If any data user is willing to access the owner's data he has to be verified. User's identity as well as Owner's identity is verified by Knowledge based Authentication. After mutual authentication initial random secret phrase is securely shared between owner and user by initiating LU-key exchange method. Proposed framework is compared with different cloud security frameworks. Computational costs and drawbacks of frameworks are interpreted.***

***Keywords*: Authentication, Cloud computing, Confidentiality, Security, Secret Key.**

## I. INTRODUCTION

Cloud computing is a running technology in which users can calculate, arrange, manage and store information on remote servers. It is an advanced use of the internet. Cloud services can be expanded on demand. It requires less use of human power. Due to the multi-tenancy feature confidentiality is the most mandatory service for users by cloud service providers. Encryption and decryption algorithms are applied to provide confidentiality. A secret key is necessary for these algorithms and that key should be shared by two end-users. There are many widely used encryption algorithms like AES, Blowfish, and IDEA and so on. Diffie-Hellman key exchange [1] is the most popular key exchange algorithm. Shared key encryption can run on large plaintext messages which public key encryption cannot. A Pseudo-Random Number Generator is a computer algorithm that produces random secret key [10]. Cryptography is one of the applications of Laplace transform. The Laplace transform is an integral transform which transforms real variable 't' to a complex variable 's'. Laplace transform and its inverse works on continuous domain. Encryption can be executed by Laplace transform and decryption by inverse Laplace transform. Knowledge Based Authentication (KBA) is used to identify authorized users. It requires knowledge of private information of users to verify the identity of provided user with authorized one. Two types of KBA – Static KBA and Dynamic KBA. Static KBA contains questions and answers which are matched after user provides answers. But dynamic KBA is a high-level authentication that uses questions for which answers change for each session. A secret key is exchanged between two end-users securely. The most popular key exchange algorithm is Diffie-hellman key exchange algorithm.

Manuscript published on 30 September 2019
* Correspondence Author
**P Namratha***, Research Scholar, Department of Computer Science and Engineering, JNTUA, Anantapur, India. Email: namratha.reddy535@gmail.com
**C Shoba Bindu**, Department of Computer Science and Engineering, JNTUA, Anantapur, India. Email:shobabindhu@gmail.com



## II. SECURITY ISSUES

***Data Loss***

Loss of data is an error condition where information is destroyed by failures, transmission or neglected storage. The most common reasons for data loss are accidental deletion, overwritten mistakenly and due to any malicious attack. The solution to this data loss may be using backup, disaster recovery equipment, and processes that prevent data loss. These solutions are to be provided by cloud service providers.

***Data Privacy***

Data privacy is also called as Information privacy. It deals with the organizational or individual ability to determine what data can be shared with third parties. Data privacy is maintained by applying encryption algorithms like AES, Blowfish, etc.

***Data Theft***

Data theft is also known as a data breach. Data theft is confirmed when confidential information has been accessed by unauthorized persons. Data theft can be mitigated by implementing access control and authentication techniques.

***Data Integrity***

Data integrity assures that data remains the same as it is on server for long time. It means data is intact and unchanged. Hash functions are implemented to maintain data integrity. For example SHA variations and HMAC algorithms.

## III. RELATED WORKS

Youssef et.al.[14] proposed a security framework consisting of three components:

Security and privacy requirements, attacks and threats, and concerns and risks.

This framework presented a security model that helps in solving security challenges. But the security model is general enough for different types of cloud services.

Agent-based cloud computing was proposed in [13] by Venkateshwaran et.al. Security agent authenticates the customer and analyzes customers trust. This security model ensures that only trusted users can interact with the cloud service provider.

ArijitUkil et al., [ 15], proposed a security framework that provides confidentiality, integrity, and authentication of data. Security architecture and necessary security techniques for cloud computing infrastructure are given.

Malik et.al. [12]developed a methodology that protects the user's data. By providing countermeasures against various attacks that are major issues while adopting cloud services.

Basescu et.al.[11] presented a generic security management framework which allows cloud data management systems to define and enforce security policies. This framework can detect and avoid a large number of attacks defined through an expressive policy description language

Gentry [16] proposed a fully homomorphic encryption method. Any operation can be done on encrypted text without decrypting the text. But encryption system involves very complicated calculations and cost of computing and storage is high in this case.

N.Cao et al., [17]proposed a privacy-preserving multi-keyword ranked search approach over encrypted cloud data.This method can search the encrypted cloud data and rank the search results without leakage of the user's privacy.

## IV. PROPOSED FRAMEWORK

Proposed security framework provides key management, Confidentiality, and authentication services.
There are 7 phases in the proposed framework:

1. Registration Phase
2. Key generation phase
3. Encryption phase
4. Data Request Phase
5. Mutual Authentication Phase
6. Key Exchange phase
7. Decryption phase

Framework architecture is given below in fig:1.
Three entities are involved in this framework. They are Data Owner, Data User and Trusted Third Party (TTP ). TTP service is offered by the Cloud Service Provider (CSP). Fig 1 depicts the interaction of these three entities.

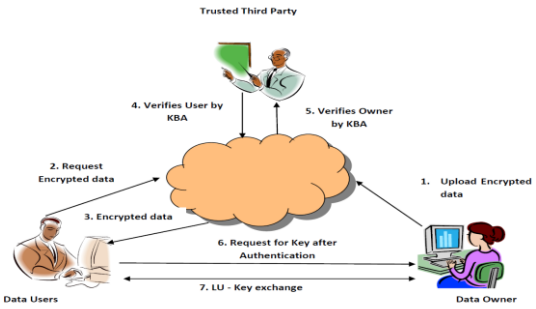


**Fig 1: Proposed Security Framework**

Cloud users should register with the cloud service provider to avail cloud services. Data owner has to generate a secret key and apply encryption technique to get encrypted data. Secret key should be maintained securely for future purpose. Cloud users are to be verified before getting access to the data. Finally to decrypt the data user needs a secret key which is to be exchanged .

Seven Phases are illustrated in the further sections.

### A. Registration Phase

Data Owner who wishes to store his data on cloud has to register with a cloud service provider (CSP).
Data Owner should provide the following details during registration phase:

1. Owner Name
2. Designation
3. Organization name
4. E-mail id
5. Mobile number
6. Service id (i.e. storage as a service)
7. Service specifications like storage capacity etc.
8. Static Knowledge based authentication information.

Data owner registration is approved after the successful remittance.

Data Owner profile details are given to a hash function and the hash values are stored in the server.

$$h_o = H(O_{id}||S_{id})$$
$$h_{qi} = H(R_i)$$
$$h_o, h_{qi}, I \rightarrow \text{Server}$$

Here every challenge is indexed (I)and its response is given to the hash function, so that its hash value is stored in the server with corresponding index(I).

Data user should register with a cloud service provider (CSP) to access data owner's data.
Data user should provide the following information to register:

1. Data User name
2. Designation
3. Organization name
4. E-mail id
5. Mobile number
6. Service id
7. Service specifications
8. Owner details whose data to access
9. Static Knowledge Based Authentication information.

Data User's registration is successful after approval of Data Owner and remittance to CSP.
After registration, a master key is shared among Trusted Third Party (TTP) and Cloud service users i.e. for both data owner and data user.
User profile details are given to a hash function and hash values are stored in the server.

$$h_u = H(U_{id}||S_{id})$$
$$h_{qi} = H(R_i)$$
$$h_u, h_{qi}, I \rightarrow \text{Server}$$

Where every challenge is indexed(I) and its response is given to the hash function,so that its hash value is stored in the server with corresponding index(I).
Hash Function applied here is SHA-512.

Table 1 gives the list of notations and descriptions that are used in proposed framework.

**Table1: Notations and their description**

| Sno | Notation | Description |
|---|---|---|
| 1 | H | Hash function SHA-512 |
| 2 | $h_0$ | A hash value of Owner details |
| 3 | $h_{qi}$ | A hash value of response for ith indexed query. |
| 4 | $h_u$ | A hash value of User details |
| 5 | I | Index of the query |
| 6 | L, U | Key factorization as L (lower triangular matrix)and U(Upper triangular matrix) |
| 7 | $N_i$ | Nonce |
| 8 | Mk | A master key shared by TTP and Cloud users |
| 9 | $T_i$ | Timestamp |
| 10 | E | Encryption algorithm |
| 11 | D | Decryption algorithm |
| 12 | R | Random secret key |
| 13 | $C_i$ | Challenge |
| 14 | $R_i$ | Response |
| 15 | $F_{id}$ | File Identifier |

### B. Key Generation Phase

Secret key applied for encryption is generated using Laplace transform based on a seed input to the algorithm. Here a random phrase is selected and key generation algorithm [2] applies congruence relation and multiplicative inverse to create actual expanded secret key whose size will be equal to block size.
Input parameters for this key generation algorithm are Random phrase 'R', Mc Claurin Series 'S', random prime number 'P' less than 256.R is the Initial key.
Steps for key generation:

1. The user selects a random phrase whose size is equal to block size.
2. Substitute corresponding numeric values of phrase in Mc Claurin series.
3. Laplace transform is applied on this series 'S'.
4. Modulus 256 is applied to the coefficients of series.
5. The coefficients are considered as an initial seed to generate expanded key.
6. A new key term is calculated using condition that product of initial seed key characters is congruent to prime 'P'.
7. Step 5 is repeated until the size of key is equal to block size.
8. Collectively all key terms are considered as Expanded Key (E-Key).

$$\text{Key-gen}(R, S, P) = \text{E-Key}$$

### C. Encryption Phase

McClaurin series- Laplace based encryption method in [2] is used in the proposed framework to provide confidentiality. Encryption algorithm accepts a plain text in the domain of 0 -25 and maps it to cipher text with the range of 0-Prime.This algorithm uses E [at] Sinhbt series.

$$\text{Cipher Text} = E(R, \text{Plain Text})$$

Sender constructs plain text and select series, parameters and secret key to be used. The encryption algorithm is executed to get ciphertext characters. Before sending the cipher text, the sender sends the secret key securely to the receiver. Selected series, parameters and sub-key are sent to the receiver by encrypting them with the secret key using the AES algorithm.

After successful encryption of data, the data owner uploads encrypted data file to cloud. The secret key is divided using Shamir secret key splitting algorithm, parts of the key are shared among registered users, Data Owner and Trusted third party (service offered by cloud).If any of them wishes to decrypt the file, then he has to get n shares among m parts where n<m( n=3). Data owner shares and trusted third party share is mandatory to recover whole key.

### D. Data Request Phase

Data user willing to access owner data sends request comprising of user details, data owner details, file name and access information to the Owner who in turn forwards request to the cloud service provider(CSP). If the request details are correct then CSP sends an encrypted file to the user. User needs secret key to decrypt the file. TTP of CSP initiates authentication process to verify both user and owner. On the completion of mutual authentication, a session key is exchanged between user and owner. Data user and owner will use the session key to securely share remaining parts of secret key to construct whole key, whereas trusted third party will send his share by encrypting it with the master key.

$$\text{Request: } (U_{id}||\ O_{id}||F_{id}||N_1) \rightarrow \text{Data Owner}$$

Knowledge based authentication and Key exchange algorithm are explained in further sections.

### E. Mutual Authentication Phase

Trusted Third Party performs a mutual authentication process of data owner and the data user. Correlation coefficient integrated knowledge based authentication protocol is designed.

Knowledge-based authentication (KBA) protocol using the correlation coefficient is implemented. Trusted Third-party (TTP) service is provided by the cloud and authentication is performed by TTP. The proposed KBA method utilizes both static KBA and dynamic KBA. Static KBA consists of queries on user data during registration. Dynamic KBA consists of queries based on the previous session of the user. Queries of static KBA and dynamic KBA are further classified in to hard and medium. Now there are four types of queries static hard, static medium, dynamic hard and dynamic medium.

Authentication is done by a challenge-response method. Challenges are given to users to respond. Each challenge can be either static or dynamic, having probability weight and response time limit. Initially threshold value is computed as a correlation coefficient on probability weight and bounded response time limit. For every response Karl's Correlation coefficient is calculated on probability weight and response time of user. User is authenticated if calculated correlation coefficient value is less than or equal to threshold value and greater than zero. After verifying the user, key exchange algorithm is initiated by the TTP.

TTP $\xrightarrow{\text{Challenge: C1}}$ User  TTP $\xrightarrow{\text{Challenge: C2}}$ Owner

User $\xrightarrow{\text{Response: R1}}$ TTP  Owner $\xrightarrow{\text{Response: R2}}$ TTP

. .

. .

. .

TTP ($\xrightarrow{\text{Correlation coefficient <= Threshold\&\&>0)}}$ Authorized User

TTP ($\xrightarrow{\text{Correlation coefficient >Threshold)}}$ Unauthorized User

### F. Key Exchange Phase

LU- Factorized key exchange algorithm is implemented to share session key among two end-users. After authenticating the users, trusted third party initiates key exchange.Authentication is explained in the previous section.TTP and individual users share master keys.TTP distributes the session key among the parties.

LU factorization factors a matrix as a product of Lower triangular matrix(L) and Upper triangular matrix(U). TTP generates a session key matrix randomly and decomposes that session matrix into L and U matrix.TTP arbitrarily sends L, U to both users A and B by encrypting them with the corresponding master keys ($M_{KS,}$ $M_{KR}$).Sender and receiver agree upon a matrix M whose inverse exists and size equal to the original session matrix.

For A $= \begin{pmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{pmatrix}$

Where L $= \begin{pmatrix} 1 & 0 & 0 \\ L_{21} & 1 & 0 \\ L_{31} & L_{32} & 1 \end{pmatrix}$ U$= \begin{pmatrix} U_{11} & U_{12} & U_{13} \\ 0 & U_{22} & U_{23} \\ 0 & 0 & U_{33} \end{pmatrix}$

Such that A = L*U

TTP sends L to owner and U to the user.

Then Owner sends L*M to User and the user sends U*M to Owner.

User computes Session matrix as follows:

$$A=(L*M)*M^{-1}*U$$

Owner computes Session matrix as follows:

$$A=L*(U*M)*M^{-1}$$

In this way Owner and user exchange session key securely.Further owner uses this session key to encrypt its own share of data encryption key to the user. AES Encryption algorithm is used.

Nonce values can be used to avoid replay attacks.

TTP $\xrightarrow{E\ (Mk,(L||T1||N1||N2)}$ Owner

TTP $\xrightarrow{E\ (Mk,(U||T2||N1||N2)}$ User

The owner $\xrightarrow{(L*M)+N2}$ User

User $\xrightarrow{(U*M)+N1}$ Owner

Owner computes Session key as follows:

⇨ (U*M)- N1

⇨ $L*U*M*M^{-1}$

Session Key = L*U

User computes Session key as follows:

⇨ (L*M)- N2

⇨ $L*M*M^{-1}*U$

Session Key = L*U

KBA followed by the key exchange is shown in the figure 2:

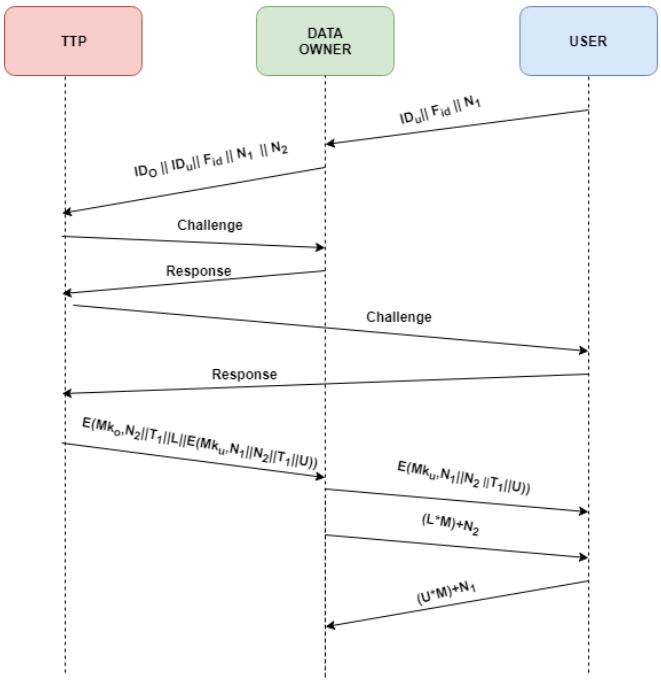


**Fig 2: KBA and LU-Key exchange**

### G. Decryption Phase

Decryption is the reverse process of encryption. Decryption is done after an initial secret phrase key is exchanged securely with the user. The receiver uses the initial key to generate an expanded key using the key generation algorithm.

After expanding the key, it is given as input to decryption algorithm [2] along with ciphertext to get back plain text.

Plain Text= D(R, Cipher Text)

## V. RESULTS AND DISCUSSION

The proposed framework is compared with existing frameworks proposed by different authors. Most of the frameworks offer confidentiality, Authentication, Key generation, and key exchange services. Security services provided by different frameworks are given in the following table 2.

**Table 2: List of security services provided by existing frameworks and the proposed framework.**

| Author | S1 | S2 | S3 | S4 |
|---|---|---|---|---|
| AshimaNarang et.al. [4] | ✓ | ✓ | ✓ | ✓ |
| Shalu Mall et.al.[5] | ✓ | ✓ | X | X |
| Sudha Devi et.al. [6] | ✓ | ✓ | ✓ | ✓ |
| Nishit Mishra et.al. [7] | ✓ | X | X | ✓ |
| Mohammed M. Dawoud et.al. [8] | ✓ | ✓ | X | X |
| OussamaArki et.al. [9] | ✓ | ✓ | X | X |
| Proposed Framework | ✓ | ✓ | ✓ | ✓ |

Where S1- Confidentiality, S2- Authentication, S3-Key generation and S4- Key Exchange.

Ashima Narang et.al. [4] Proposed a framework which implements confidentiality, authentication, key generation, and key exchange. The author proposed two-hybrid encryption algorithms, among them first algorithm combines Hierarchical Attribute Set Based Encryption (HBASE) and Blowfish algorithms and the other encryption algorithm combines RSA and ECC. Key generation is done using random number generator. The time complexity for encryption(RSA+ECC) is $O(\log(q)^4)$, where $F_q$ is a finite field of q elements, where q is some very large prime power q = p r for a prime p and a large positive integer r. The time complexity for another hybrid algorithm ( HBASE, Blowfish) is O ($\sqrt{N}$) where N is the number of users.

Shalu mall et.al. [5] proposed a framework that provides Confidentiality through genetic algorithm and authentication by Entity authentication i.e. comparing the entered user details at registration time. There is no need for key in genetic algorithm. Authentication is done by using an authorized group to identify the user. The time complexity of the genetic algorithm is O (g (nm + nm + n)) with g the number of generations, n the population size and m the size of the individuals. Therefore the complexity is O (gnm).

Sudha Devi et.al. [6] designed an adaptive multilevel security framework which offers confidentiality, authentication, key generation, and key exchange services. Encryption algorithms are chosen depending on the data sensitivity level i.e. simple encryption for normal data, AES for critical data and Blowfish for entire data. The time complexity for encryption algorithm here is O (M) where M is the size of data.

Nishith Mishra et.al.[7] proposed a secure framework for cloud data. This framework has designed confidentiality and key exchange or sharing. Confidentiality is provided by implementing AES algorithm. Key is shared through central key distribution center. The time complexity of the encryption algorithm is O(M) where M is the size of message.

Mohammed M. Dawoud et.al. [8] presented a security framework based on trust authority. The framework implements confidentiality and authentication services to the users. AES-128 is implemented to provide confidentiality. Authentication is verified using JWT token authentication. The time complexity for encryption is O(M) where M is the message size.

Oussama Arki et.al. [9] proposed a security framework for cloud data storage based on the agent. Framework offers confidentiality and authentication by implementing three layers:cloud provider layer, customer layer and trusted third party layer. Confidentiality is achieved by RSA algorithm. The proxy agent verifies the identity of the user. The time complexity of encryption algorithm is O ($(\log N)^2$) where N: p*q

(p ,q are large prime numbers).

Proposed Framework offers confidentiality, authentication, key generation, and key exchange. Confidentiality is provided by Laplace based encryption algorithm. Authentication is carried out by application of correlation coefficient. Lu- factorization based key exchange is implemented for key exchange. The time complexity for encryption algorithm is O (N) where N is the size of the plaintext.

The time complexity of encryption algorithm in the proposed framework is same as BlowFish algorithm. A new KBA authentication mechanism is designed that verifies user based on current data. LU-factorization method is used for key exchange.

Sudha Devi [6], Ashima Narang [4] and proposed frameworks provide four services confidentiality, authentication, key generation, and key exchange. Their computational costs are given below.

Sudha Devi [6]

Computational cost: 1C+ 1KG +1E + 1UA +1TK

(Where C: data sensitivity classification, KG: key generation E: Data Encryption, UA: user authentication, TK: Token passing associated with key sharing.

Ashima Narang [4]

Computational cost: 1HE+ 1AG + 1PEK

(Where HE: Hybrid encryption, AG: Authorized group user verification, PEK: proxy re-encryption for key management.)

Proposed Framework

Computational cost: 1RKGL + 1E + 1UA + 1K

(Where RKGL: random key generation by using Laplace transform, E: Encryption, KBA : knowledge based user authentication, K: LU- factorization based key exchange.)

Computational costs of all the three frameworks are different. The framework proposed in [6] makes use of token for user verification by cloud service provider which may be misused if captured by an unauthorized user. In the framework [4], they have not mentioned how user is identified as an authorized group member and Hybrid encryption algorithm is applied (whose computational cost is greater than normal encryption algorithm). In the proposed Systematic framework mutual authentication is carried by static and dynamic queries where there is no possibility of unauthorized access, Laplace transforms based Random key generation and encryption is implemented.

## VI. CONCLUSION

Cloud computing involves delivering services over the internet. Storage as a service is one of the services that cloud offers over internet. Data of cloud users are stored in remote data centres. Data security has received much attention over the last decade. Data security has been incumbent for the cloud service providers. A systematic security framework is proposed that implements security services in sequence. Foremost key generation algorithm generates a secret key which is fed to encryption algorithm along with data. Resultant cipher text is stored in the cloud. It is not safe to store key at Owner's site, so it is divided in to parts by Shamir key splitting algorithm. After splitting parts are distributed among owner, TTP and users. Cloud User who wishes to access the stored data would need the secret key to decrypt cipher text. Mutual authentication is done by Knowledge Based Authentication to verify both owner and user. After verification session key is exchanged by LU-key exchange. Users and owner share their individual parts of the key by encrypting them with session key where as TTP sends its share by encrypting with master key. As, TTP is having only a part of secret key, there is less chance of key compromise. Comparison of proposed framework with existing frameworks shows that confidentiality, authentication, and key management services are provided by most of the security frameworks to ensure that data stored in cloud is secured. Proposed Systematic framework presents steps in a sophisticated manner. The computational cost of proposed framework is reduced when compared to existing frameworks [4] and [6].

## REFERENCES


1. D. Boneh, "The decision Diffie-Hellman problem," in *Algorithmic NumberTheory*, vol. 1423, pp. 48– 63, Springer, 1998.
2. P. Namratha, C. Shoba Bindu, S. Sri Lakshmi "Key Generation and Encryption Using Laplace Transform For Data Security in Cloud" vol 11, issue-6 pp 170-180, Journal of Advanced Research in Dynamical and Control Systems(JARDCS),2019.
3. A. Kaur and M. Bhardwaj, "Hybrid encryption for cloud database security," Journal of Engineering Science Technology,vol. 2, pp. 737–741. 2012.
4. Narang, Ashima and Gupta, Deepali, "Comparative Analysis of Various Cloud Security Frameworks" (2018). International Journal of Advanced Studies of Scientific Research, Vol. 4, No. 1, 2019.
5. Mall, S., Saroj, S.K. "A new security framework for cloud data" Procedia Computer Science, Volume 143, 2018
6. Dorairaj, Sudha Devi & Kaliannan, Thilagavathy. "An Adaptive Multilevel Security Framework for the Data Stored in Cloud Environment". The Scientific World Journal. 601017. 10.1155/2015/601017.2015
7. Mishra, Nishit & Sharma, Dr. Tarun & Sharma, Varun & Vimal, Vrince. "Secure Framework for Data Security in Cloud Computing". 10.1007/978-981-10-5687-1_6. 2018
8. Dawoud, Mohamed & A. Ebrahim, Gamal & A. Youssef, Sameh.. "A Cloud Computin Security Framework Based on Cloud Security Trusted Authority". 133-138. 10.114/2908446.2908459. (2016)
9. Arki, Oussama & Zitouni, Abdelhafid. . "A Security Framework for Cloud Data Storage(CDS) Based on Agent. Advances in Intelligent Systems and Computing". 662. 62-73. 10.1007/978-3-319-67621-0_6.2018
10. Asif Mushtaque, Md & Dhiman, Harsh. "Implementation of new encryption algorithm With random key selection and minimum space complexity". 507-511. 10.1109/ICACEA.2015.7164797. (2015)
11. Basescu, C., Carpen-Amarie, A., Leordeanu, C., Leordeanu, C., Costan, A.,& Antoniu, G. . "Managing Data Access on Clouds: A Generic Framework for Enforcing Security Policies"..*Proceedings of the International Conference on Advanced Information Networking and Applications (AINA)*. doi:10.1109/AINA.2011.61. (2011)
12. Malik, A., &Nazir, M. M.. "Security Framework for Cloud Computing Environment: A Review". *Journal of Emerging Trends in Computing and Information Sciences*, *3*(3). (2012)
13. Venkateshwaran, K., Malviya, A., Dikshit, U., Venkatesan, S.: "Security frame-work for agent- based cloud computing". Int. J. Artif. Intell. Interactive Multimed.3(3),37- 40(2015)
14. Youssef, A. E. and Alageel, M. "A framework for secure cloud computing". *International Journal of ComputerScience Issues (IJCSI)* 9, 4 (Jul. 2012), 487-500. . 2012
15. Ukil, A., Jana, D., & De Sarkar, A.. "A security framework in cloud computing Infrastructure".[IJNSA].*International Journal of Network Security & Its Applications*, *5*(5), 11-24. doi:10.5121/ijnsa.2013.5502. (2013)
16. C. Gentry, "*A fully homomorphic encryption scheme" [Ph.D.thesis]*, Stanford University, 2009
17. N. Cao, C. Wang, M. Li, K. Ren, and W. Lou, "Privacy-preserving multi-keyword ranked search over encrypted cloud data," *IEEE Transactions on Parallel and Distributed Systems*, vol.25, no.1, pp. 222– 233, 2014.


## AUTHORS PROFILE

**P.Namratha** is a Research scholar in CSE at JNTUA. She received B.Tech Degree in Computer Science & Engineering from Sri Krishna Devaraya Engineering college Gooty affiliated to JNTU Anantapur India in 2007; M.Tech in Computer Science & Engineering from JNTU Anantapuramu in 2011. Her research interests are in the fields of Computer Networks, Network Security & Cloud computing.

**Dr. C. ShobaBindu** is presently working as Director Skill Development Centre & Incubation Centre, Professor in Department of CSE JNTU, and Anantapur. She received her B.Tech Degree in Electronics & Communication. Engineering from Jawaharlal Nehru Technological University, Anantapur, India, in 1997;

M.Tech in Computer Science & Engineering from Jawaharlal Nehru Technological University, Anantapur, India, in 2002. She was awarded Doctorate in the year 2010, from JNTU, Anantapur. Her research interests include Cloud computing, Network Security, Data analytics and Wireless Communication Systems.

.