Revocable Identity - Based Encryption For Secure Data Storage In Cloud

N.Sunanda , N.Sriyuktha , P.Sai Sankar

Abstract: ***Cloud Computing gives an adaptable and advantageous route for sharing of the data , which in-turn have advantages for the public and the people. There might be a case, there exists a natural resistance for clients to straightforwardly redistribute the mutual information to the cloud server since the information regularly contain significant data. In this way, it is important to put cryptographical access control on the data we share through cloud. Identity based encryption builds a practical data sharing system. Here the access control not being static, it is the point at which some client's authorization is lapsed, there ought to be an mechanism that can revoke him/her from the system. So that the revoked client cannot access the shared data. To this extent , in our research we propose a model called revocable-storage identity based encryption (RS-IBE), which can give the forward/backward security of cipher text by presenting the functionalities of client revocation and cipher text update. The performance of the RS-IBE model has its own advantages in terms of efficiency and thus is a cost-effective data sharing system.***

Keywords : cryptographical , RS-IBE , revocation, Cipher text, Cloud.

I. INTRODUCTION

Cloud computing is a standard that gives high computation limits and massive memory space at low cost. It enables clients to get desired services independent of time and area over various platforms (e.g., cell phones, PCs). Among various services provided by cloud computing and cloud storage service, for example, Apple's iCloud , Microsoft's Azure and Amazon's S3, can offer an increasingly adaptable and simple approach to share information through the Internet, which will give different advantages to our general public . Be that as it may, it additionally experiences a few security issues, which are the concerns of cloud clients . The main idea of this research is to construct a basic identity based cryptographical tool to achieve security goals such as authenticity and availability[1] of shared data. Identity-based encryption is a cryptosystem that eliminates the public key infrastructure which leads to the revocation problem. Several revocation techniques have been proposed for out-sourcing data like key-update security provider(KU-CSP)[3], cloud revocation authority(CRA)[4]. The first IBE scheme was proposed in 2001 by Boneh and Franklin[5] ,which periodically generates new private key for the users set to a week or month. The sender uses receivers ID and current time to encrypt the data while the receiver uses current private key to decrypt the data. If a user is to be revoked, Private Key Generator (PKG)[2] stops providing private keys. But a secure channel must always provide secret keys for the users, so it is necessary to update private keys which results in load to private key generator.

So Boneh and Franklin introduced another revocation scheme called immediate revocation. This introduces a trusted mediator to share the private keys of users which will reduce load to PKG. When a user is revoked the third mediator stops sending private keys. In this the third party should help the users to decrypt the data which rises another problem.

An identity-based public key system have users and a third party (i.e private key generator). The trusted third party generates secret key using users id. Hence when the user wants to download the data he can use that private key under his/her id. Since a public key system should have user revocation system, this research focus on issue how to revoke the compromised/authority expired users and how to un-revoke if the user is valid. Here we have a data sharing system through cloud, a key authority and data provider who uploads the data to cloud. The data sharing between the users is done as shown in the Fig.1. The proposed system can ensure the forward and backward secrecy by revoking the unauthorized users[6].

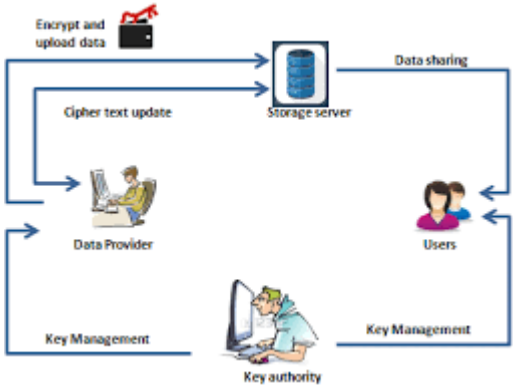


Fig.1. Data Sharing System Using RIBE

II. LITERATURE SURVEY

In 2008 Boldyreva introduced an efficient key updation process with binary tree data structure. Later Seo and Emura extended theconcept proposed by Boldyreva and used Hierarchical identity based encryption (HIBE)[8]. But these schemes also have their disadvantages regarding the efficiency. So we extended the concept of RS-IBE introduced by Shamir.

In 2012, Tseng and Tsai introduced a ID-based public key system and

Revised Manuscript Received on May 10, 2019

N.SRIYUKTHA, Department Of Computer Science, KLEF, Guntur, India.
P.SAI SANKAR, Department Of Computer Science, KLEF, Guntur, India.
N.SUNANDA, Department Of Computer Science and Engineering, KLEF, Guntur, India.

revocation method with a public channel. In this mechanism the private key has two components, the initially generated secret key is fixed and the time update key is updated frequently for non-revoked users. Thus the non-revoked users can directly decrypts the data stored in cloud while PKG stops issuing private keys for revoked users. This eliminates the concept of secure channel. By doing this there is no need for any encryption/decryption between PKG and revoked users. Later Tseng and Tsai extended their work by introducing a secure public channel by revocable identity- based encryption. The Tseng and Tsai framework have two roles: PKG and users. The PKG selects a private key and some parameters. When the time period begins , a time updating key is generated by PKG using secret key for each non-revoked user and send them using a secure channel. By doing this a revoked user, will unable to receive the associated time updating key for the current time period[2].

By improving the above mechanism in 2015, a cloud service provider called *Li et al*, introduced data outsourcing technique for IBE scheme with key-update service provider (KU-CSP). In this mechanism the key updation is done by KU-CSP in order to reduce the load to PKG. The PKG sends the users identities through a secure public channel and generates a random value and sends it to KU-CSP . Now KU-CSP generates update time value for user with their identities. So when the unauthorized user tries to access data the PKG sends message to KU-CSP, so that KU-CSP stops updation of secret key to unauthorized user. This system model is shown in the below Fig.2.

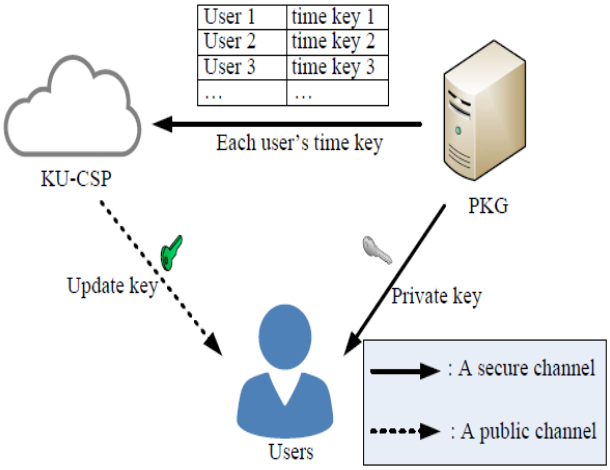


Fig.2. *Li et al* model for key updation.

However this scheme has two drawbacks, the communication costs are higher and is un-scalable as the KU-CSP[12] must generate time key for each and every user. Our work includes reducing the communication costs and also to make an efficient key updation system using RS-IBE with key authority.

The whole idea of revocable identity based encryption (RIBE) might be a promising method that security requirements we recently found for sharing of data. SO, the RIBE makes the sender to add the time stamp to cipher text so that user who is not under revocation can decrypt the cipher text.

Step1- At first the data provider encrypts the data under users who shares the data and uploads the cipher text of data which is being shared.

Step2- When either of the users want to acces shared data in cloud , he/she can access by downloading the data under their identity.

Step3- When if one of the users authorization gets expired, the data provider downloads the cipher text, decrypts and again encrypts and uploads the data to cloud thus preventing the expired user from accessing shared data.

Thus the above system can provide forward secrecy, backward secrecy and confidentiality. Obviously, such a system uses a secret key for the encryption and decryption of data, thus leading the system to new attacks.

DATA CONFIDENTIALITY:

Data Confidentiality means, preventing the shared data from unauthorised access which is stored in the cloud storage.

FORWARD SECRECY:

If the users authorization gets expired he/she should be not be able to access the data shared that was previously been accessed from the cloud storage.

BACKWARD SECRECY:

If the users authorization gets expired he/she should bot be able to give further access of data shared from cloud storage.

Apart from these security goals we have another problem i.e un-scalability which was the main issue in Li et al model for key updation.

UN-SCALABILITY:

The KU-CSP model have a new time key for each and every user to reduce the load for PKG which results in un-scalability[7]. By using RS-IBE scheme we try to overcome this problem.

REVOCABLE STORAGE:

By this the removed user cannot get any access to data shared that is stored in cloud storage which is known as revocable storage identity based encryption. The user is revoked by his/her time period functionalities[8] by the cloud storage.

III.PROPOSED MODEL

In our system we have a data provider, key authority(KA)[9] , cloud and users.

DATA PROVIDER:

The data provider first decides who will share the data and he will upload the data with their identities. The data provider uploads the data by encrypting it. Data provider can check for number of uploads and number of downloads of the data.

KEY AUTHORITY:

The key authority generates secret key when a user requests for data accessing.

CLOUD STORAGE:

The data uploaded by data provider is stored in cloud. The cloud enables the users to download by entering the secret key. The cloud storage will also have a revocation list, if an unauthorized/authority expired user tries to access data he/she is revoked. The revoked user is not allowed to login again.

USER:

The function of the user is to request for secret key and accessing the data stored in cloud. The user decrypts the data by downloading it from cloud.

If a unauthorized user attempts to login it will show a message you are under revocation. If the user is authorized and yet revoked due to his/her expiration he/she can be unrevoked by checking the validity to access the data. To implement this we propose an identity based encryption model using a binary tree structure for storing identities and time period functionalities of the users.

Now we take a binary tree B, revocation list RL, current time ct, revocation time rt and nodes as v_i. Take two null sets X,Y corresponding to non-revoked and revoked users. If an unauthorized/authority expired client wants to access the shared data he/she must use secret key. At the time of accessing cipher text, if the users current time is more than the revocation time he/she is marked as revoked and thus prevented from further access of shared data. The non-revoked users secret key is updated and they can access the data using updated secret key which is provided by the key authority. This overcomes the un-scalability problem mentioned in previous schemes. The pictorial representation of revoked and non-revoked users are shown in Fig.3.

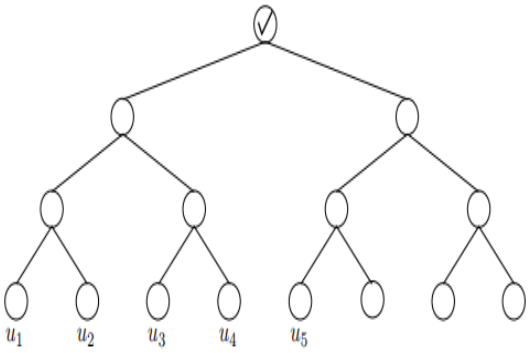
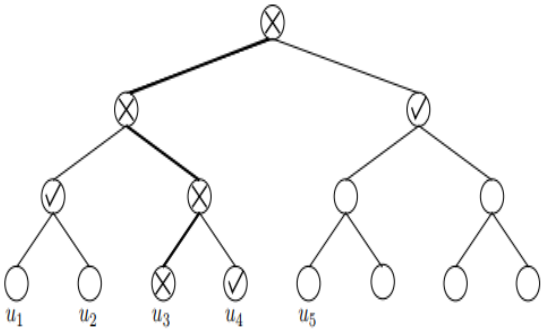


Fig.3. (a). No user is under revocation.

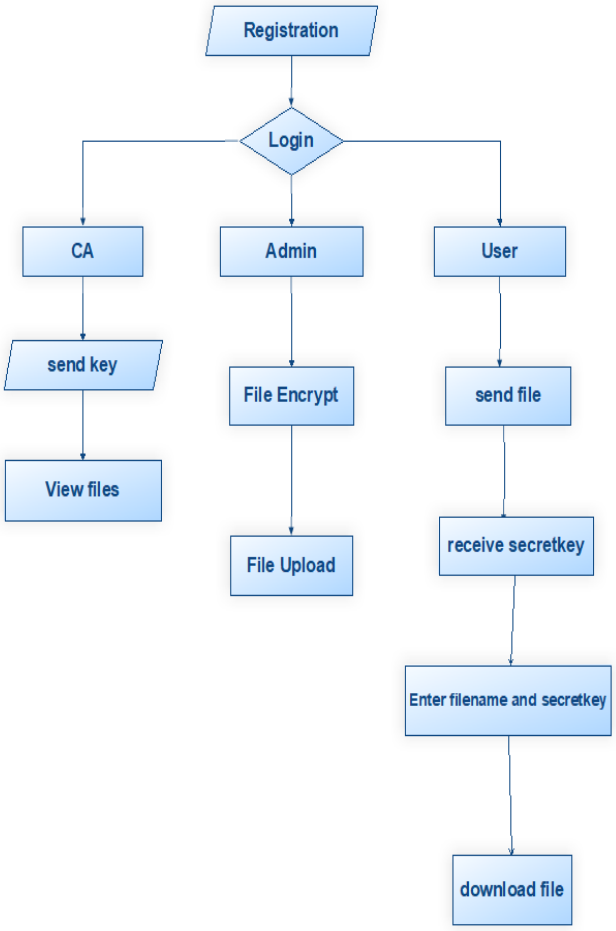


(b).User u_3 is under revocation.

IV.IMPLEMENTATION

In this paper we introduce cost-effective RS-IDE that fulfills our three security goals data confidentiality, forward secrecy and backward secrecy. We constructed an algorithm KUNodes[10] to update the key when user tries to access and revokes unauthorized user.

The flow diagram for the above mentioned model is shown below in Fig.3.



The KUNodes algorithm works as follows:

a. First when a user have to access data from cloud storage, the cloud server asks for secret key.

b. If the user enters the secret key correctly he/she will be allowed to access the data.

c. If the user fails to enter correct secret key or the authorization is expired, the cloud server restricts the user by revoking his identity by checking the time period of user in revocation list.

d. Now the cloud server checks the revocation list to find if there are any valid users that belongs to the organization.

e. If cloud finds a valid user it again un-revokes the user and allow to access data stored in cloud.

A.MODIFIED KUNODES ALGORITHM

The modified KUNodes algorithm[9] takes two null sets X,Y to store corresponding non-revoked

and revoked users. If an user whose authority got expired tries to access the shared data he/she is marked under revocation and is given as output to set Y. The non-revoked users are given as output to set X and their secret keys are updated.

ALGORITHM:

KUNodes(B,RL,tp)

X,Y←Ø

∀ (u_i, ct_i) ε RL

If $ct_i \leq tp$ then add path(u_i) to X.

Return X

∀ $ct_i \geq tp$ then add path(u_i) to Y.

Return Y.

If Y → Valid(B) then

Unrevoke.

The KUNodes algorithm helps in validating the authorized users by checking the revocation list. This RS-IBE scheme reduces the computational costs and un-scalability than the previous KU-CSP scheme.

B.ENCRYPTION AND DECRYPTION:

The data shared is encrypted to the cloud server based on identity of the data provider, so that when he/she wants the decrypt the data they can access the cipher text by providing name of the data provider and file name. A trusted third party provides the secret key to the users while accessing stored data in cloud. The simultaneous key updation when a user is revoked results in achieving our three security problems data confidentiality, forward secrecy and backward secrecy.

C.REVOCATION:

The user is revoked when his/her authority is expired or security key is compromised and thus preventing the data from unauthorized access.

D.UN-REVOKE:

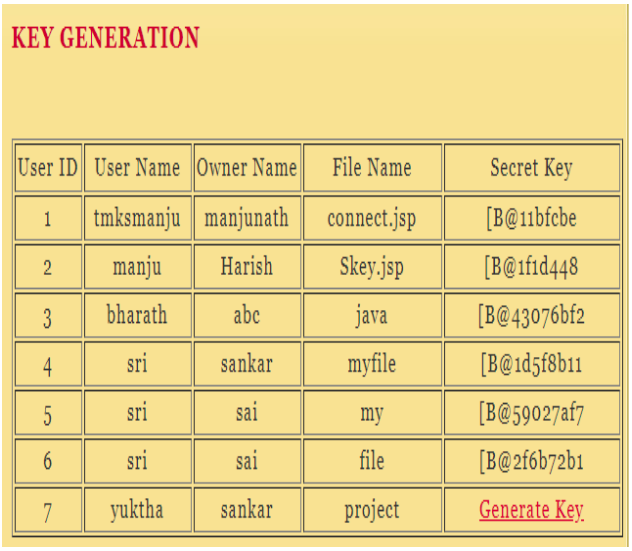
The cloud checks for the validity of users in the revocation list and un-revokes if he/she is valid and grant access for previously or subsequently shared data.

V .RESULTS AND FUTURE SCOPE

By following the RS-BIE scheme reached our one of the security problem i.e un-scalability. The scheme proposed by Li et al lacks in reducing the computational costs and un-scalability. So we proposed a model by introducing key authority to overcome these security problems. The major challenge in cloud is security of data. So we concentrated mainly on data confidentiality, forward and backward secrecy but this results in reducing computation costs and increasing complexity. So we look forward to reduce the complexity in our future work by re-encryption of cipher text without any key updation process. The data provider encrypts the data as shown below in Fig.4.

Fig.4. Encrypted Data.

The key authority generates key as shown in Fig.5.



User ID	User Name	Owner Name	File Name	Secret Key
1	tmksmanju	manjunath	connect.jsp	[B@11bfcbe
2	manju	Harish	Skey.jsp	[B@1f1d448
3	bharath	abc	java	[B@43076bf2
4	sri	sankar	myfile	[B@1d5f8b11
5	sri	sai	my	[B@59027af7
6	sri	sai	file	[B@2f6b72b1
7	yuktha	sankar	project	Generate Key

Fig.5. Key Generation.

The uploaded, updated and retrieved data in cloud storage are shown in Fig.6 in the form of graph.

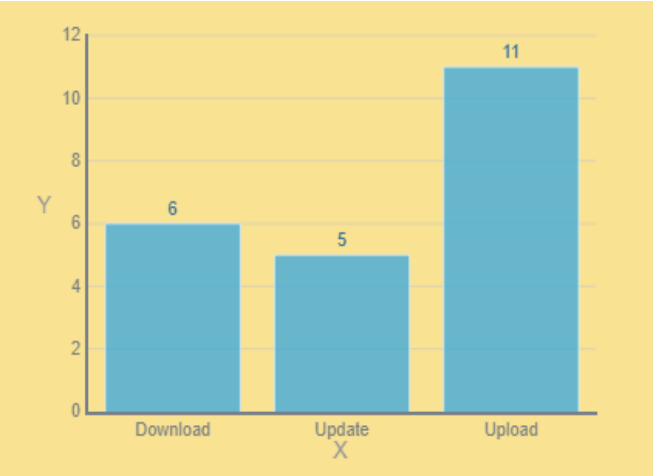
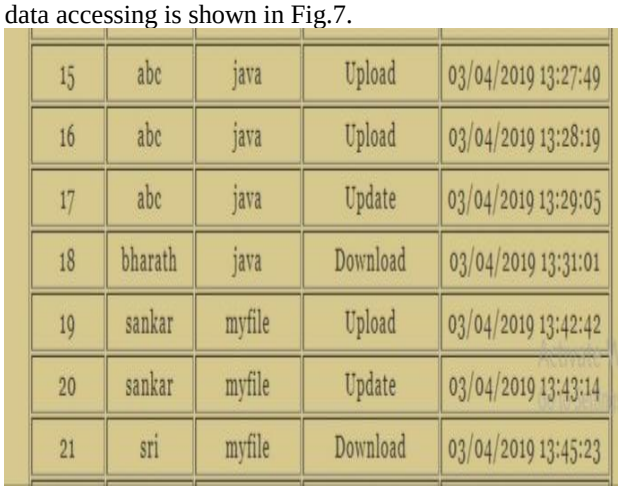


Fig.6. Results for uploaded ,updated and retrieved data.

The key authority will update the keys when user requests for data accessing is shown in Fig.7.



15	abc	java	Upload	03/04/2019 13:27:49
16	abc	java	Upload	03/04/2019 13:28:19
17	abc	java	Update	03/04/2019 13:29:05
18	bharath	java	Download	03/04/2019 13:31:01
19	sankar	myfile	Upload	03/04/2019 13:42:42
20	sankar	myfile	Update	03/04/2019 13:43:14
21	sri	myfile	Download	03/04/2019 13:45:23

Fig.7. Key authority functions.

If the revoked user tries to login, it shows the message you are under revocation as shown in Fig.8.

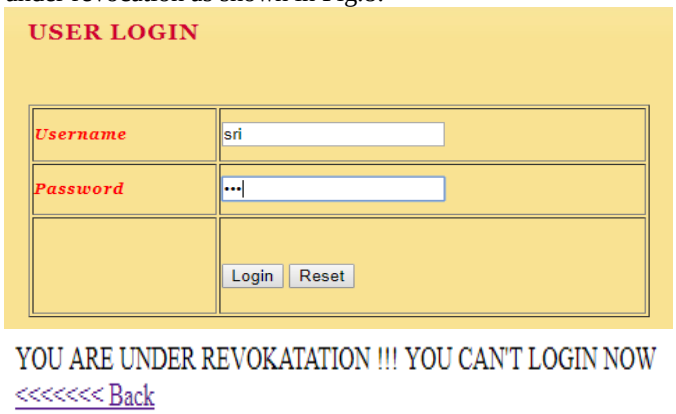


Fig.8. The user under revocation

REFERENCES

1. Jianghong Wei, Wenfen Liu, Xuexian Hu, "Secure Data Sharing in Cloud Computing Using Revocable-Storage Identity-Based Encryption", Journal Of Latex Class Files, Vol. 14, No. 8, August 2015.
2. Yuh -Min Tseng, Tung-Tso Tsai, Sen-Shan Huang, and Chung-Peng Huang, "Identity-Based Encryption with Cloud Revocation Authority and Its Applications", IEEE TRANS. CLOUD COMPUTING 2017.
3. A. Shamir, "Identity-based cryptosystems and signature schemes," in *Advances in cryptology*. Springer, 1985, pp. 47–53.
4. D.Boneh and M.Franklin, "Identity-based encryption from the weil pairing," *SIAM Journal on Computing*, vol. 32, no. 3, pp. 586–615, 2003.
5. Wang, B. Li, and H. Li, "Public auditing for shared data with efficient user revocation in the cloud," in INFOCOM, 2013 Proceedings IEEE. IEEE, 2013, pp. 2904–2912.
6. S.Ruj, M. Stojmenovic, and A. Nayak, "Decentralized access control with anonymous authentication of data stored in clouds," Parallel and Distributed .
7. Systems, IEEE Transactions on, vol. 25, no. 2, pp. 384–394, 2014.
8. X. Huang, J. Liu, S. Tang, Y. Xiang, K. Liang, L. Xu, and J. Zhou, "Cost-effective authentic and anonymous data sharing with forward security," Computers,IEEE Transactions on, 2014, doi: 10.1109/TC.2014.2315619.
9. C.-K. Chu, S. S. Chow, W.-G. Tzeng, J. Zhou, and R. H. Deng, "Key-aggregate cryptosystem for scalable data sharing in cloud storage," Parallel and Distributed Systems, IEEE Transactions.
10. R. Housley, W. Polk, W. Ford, and D. Solo, "Internet X.509 public key infrastructure certificate and certificate revocation list (CRL) profile," IETF, RFC 3280.
11. 10.W. Aiello, S. Lodha, and R. Ostrovsky, "Fast digital identity revocation," Proc. Crypto'98, LNCS, vol. 1462, pp. 137-152.
12. D. Boneh, X. Ding, G. Tsudik, and C.-M. Wong, "A Method for fast revocation of public key certificates and security capabilities," Proc.10th USENIX Security Symp., pp. 297-310.
13. Girishma, V., & Satyanarayana, K. V. V. (2016). Securing data stored in clouds using multi keys and proxy injection schemes. Journal of Theoretical and Applied Information Technology, 88(3), 553-557. Retrieved from www.scopus.com.
14. Paruchuri, V. L., Anantha, N. L., Konagala, V. L., & Bhattacharyya, D. (2016). Ciphertext-policy attribute-based encryption for access control of data in cloud. International Journal of Software Engineering and its Applications, 10(8), 13-22. doi:10.14257/ijseia.2016.10.8.02.
15. Ramya, K. R., Malleswari, D. N., Rani, C. R., Bhattacharyya, D., & Kim, H. -. (2016). Key aggregate based homomorphic encryption for efficient authentication for secure cloud storage. International Journal of Database Theory and Application, 9(11), 137-148. doi:10.14257/ijdta.2016.9.11.13.
16. Vurukonda, N., & Thirumala Rao, B. (2017). Secure sharing of outsourced data in cloud computing with comparison of different attribute based encryption schemes: A review. Journal of Advanced Research in Dynamical and Control Systems, 9(Special Issue 14), 680-698. Retrieved from www.scopus.com.

AUTHORS PROFILE

N.Sriyuktha pursuing Bachelor of Technology in Computer Science and Engineering from KLEF, Guntur, Andhra Pradesh. Research group is cloud computing.

P.Sai Sankar pursuing Bachelor of Technology in Computer Science and Engineering from KLEF, Guntur, Andhra Pradesh. Research group is cloud computing.

N.Sunanda working as Associate Professor in the Department of Computer Science and Engineering from KLEF, Guntur, Andhra Pradesh. She has her research areas of interests are cloud computing and security, network security.