International Journal of Recent Technology and Engineering (IJRTE)
ISSN: 2277-3878 (Online), Volume-8 Issue-4, November 2019

Secure Text Transfer using Diffie-Hellman Key Exchange Based on Cloud

D Komali, Vamsi, Tejsai, Ganga Bhavani

Abstract- Web based life are one of the slanting medias through which the clients speak with one another utilizing messages. Messages are sent from the source to the goal without breaking a sweat. Yet, what is the assurance that the message isn't meddled by the gate crasher in the middle of the source and the goal? To fathom this issue, the protected content exchange utilizing Diffie Hellman Key Exchange dependent on cloud application is presented. Encryption is one of the procedures for giving security to the information that has been sent by the sender. There will be various calculations utilized so as to accomplish the encryption of the information.

This application will enable the client to send the plain content to the goal. Prior to sending the message, the client needs to choose the calculation like AES, DES and so on. At that point the message will be scrambled utilizing such calculations. The key will be sent to the goal so as to decode the message. This will be one of the intriguing applications that one can chip away at and execute continuously world without hardly lifting a finger. Individuals can depend on this application without any difficulty utilizing this application. The UI will be straightforward and straightforward even by the basic man. The data that is private may be taken through such assaults.

Keywords-Crypto graphical key,communication parties, Diffie–Hellman, MiM attack; Plain – text attack.

I. INTRODUCTION

Distributed computing is a rising innovation in the present time. It very well may be portrayed as a huge course of action of assets offered to the customer through the web by cloud administration suppliers according to their solicitations. Distributed computing is for the most part related with use registering, diverse VM and so forth. It very well may be utilized in instructive field to give record-breaking access of the information documents to the understudies just as teachers. A cloud-based model is recommended for engineering instructive space in which

educators can transfer their exploration work can share their discoveries and so on. What's more, understudies can download the information records for their study. This architecture supplies the above mentioned facilities in SaaS(Software as a Service). Also, storage space is given to users to upload their repository.

Cloud computing has many security challenges such as data integrity, unlicensed access, DoS etc. The traditional cryptographic algorithms are used to prevent user's sensitive data from data tempering and unauthorized access. There are two type of cryptographic algorithms: Symmetric

Key algorithms and Asymmetric Key algorithms. In symmetric key algorithms, same key is used for encoding/decoding the data. While in Asymmetric Key algorithms, different key is used. Now, to transmit the keys securely, Diffie-Hellman key exchange algorithm is used. But it is vulnerable to MiM attack and plain-text attack. In this paper, an improved version of the Diffie–Hellman key exchange algorithm is suggested. In this version, one mathematical model is used and this model is based on arbitrary numbers and logarithm, In addition, this algorithm

can prevent the user data from the MiM attack and plain-text attack. need to shield the information from various dynamic assaults and unaccredited access.

In the paper various difficulties in the territory of security is considered. The most significant difficulties are noxious inner individual from the cloud, defence less API, different, VMM (Virtual Machine Manager) risk, hold onto the administration and so forth. Cryptography is gained by the ventures which are increasingly stressed over information security. Cryptography can fix the examined issues at some level. The main thoughts considered in paper are useful to evacuate numerous issues in the information security region.

A cloud with cryptographic abilities is exhibited. It enables client to supply the secret information on people in general cloud. It scrambles the information utilize advanced mark of the client and ensure that nobody come to think about information area and access rights. In the event that information holder is changed, just cloud client translates the information.

On the off chance that there is any approved untouchable's information dwells in the cloud, it is at risk to get security. Due to this office, cloud client can store the information at remote area. In the paper

Diffie–Hellman key exchange strategy is proposed among the CSP and the cloud part to disperse symmetric key. This convention settles the issue of key regulation and support. Two level validation systems are utilized in this convention. In the paper a moderator premise singular validation portrayal is proposed to grow the unwavering quality and security of cloud client uniqueness the executive's framework. An unmistakable extension is recommended to perceive the holder of the individual contraption and to list the conditions among the cloud part and CSP.

Manuscript published on November 30, 2019.
* Correspondence Author
D.Komali*, Koneru Lakshmaiah Education Foundation, Guntur, India. Email: komali@kluniversity.in
A.Vamsi, Koneru Lakshmaiah Education Foundation, Guntur ,India. Email: ibm.145164104@gmail.com
R.Ganga Bhavani, Koneru Lakshmaiah Education Foundation, Guntur, India..Email: gangabhavani.ryali@gmail.com
Ch.Tejsai, Koneru Lakshmaiah Education Foundation ,Guntur ,India. Email:tejsai123@gmail.com

In this paper, an improved Diffie–Hellman key trade calculation is displayed which uses discretionary number to deliver particular figure content for comparable plain-content. Furthermore, it applies logarithms on the conveyed key with private number. This number is utilized as a fundamental belief which individualize the cloud part to the imparting party what's more, to make it secure against MiM assaults and plain-content assaults.

A. MiM(Man-in-the-Middle) Attack

This is a functioning assault wherein, the trespasser forestalls the message from proceeding to the goal. Likewise, he can change the message by avoiding himself as a one of the imparting parties.

B. Plaintext Attack

An intruder has plain-message just as encoded message in this sort of assault. If the conveyed key is a consistent key, the it will create the equivalent unscrambled content for a similar plain-content. This data is utilized by a trespasser to get the relationship between the plain-message and scrambled content.

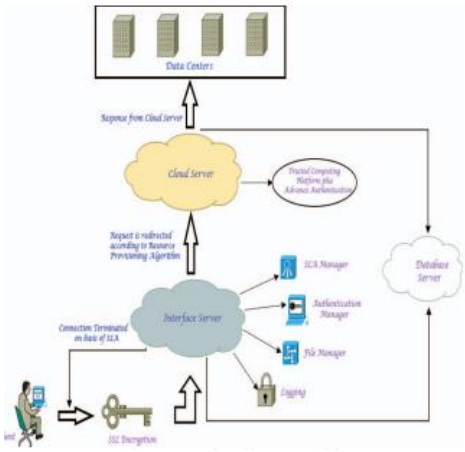
II. PROPOSED ARCHITECTURE MODEL

A cloud system is recommended for an instructive area particularly for engineers. It is utilized by the resources to share their examination work and thoughts and to get to the IT asset according to their benefit. It gives following administrations:

1. Teachers can transfer and share their exploration work, various applications.
2. Educators can control their information and distribute it.
3. A colossal measure of capacity
4. Brought together access and individualization
5. Single sign-on administration
6. Understudies can download the required research information.
7. Numerous specialized authorities meet up into one normal stage.
8. If any intruder tries to make any change into user data then one notification goes to the Admin.
9. Cloud user data are safe. As we are using security algorithm for the security of user data.
10. Revised version of Diffie-Hellman algorithm is used to secure the common key transportation in public channel.

Here, Service Level Agreement (SLA)[7] is created as per traditional way of creating SLAs. In this, different user roles and their access rights are mentioned. One database server is created to preserve the database of the user activity. When any user comes to use the portal, his request first go across the interface server [9]. SLA manager and Authentication manager check the identity of the user and pass the request as per the Resource Provisioning algorithm to the cloud server. We have applied 3-way defence strategy as described below:

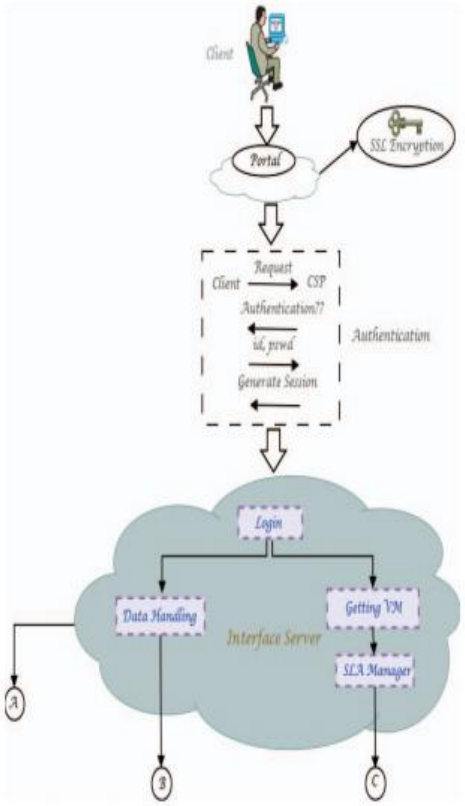
1. Use improved Diffie-Hellman algorithm to produce the key for key exchange.
2. Use DES encryption algorithm to encrypt and decrypt the data.
3. Compress and de-compress the data on the cloud server.



III. WORK FLOW OF THE SYSTEM

The succession of the exercises for the above design is shown in following figures

1. Client visit the entrance which is encoded by applying SSL Encryption.
2. Client get 'Read Only' get to authorization at first. Too, client can get compose get to on the off chance that he/she get himself/herself enlisted in the cloud utilizing the gateway.
3. CSP individualized the cloud client and diverted him to the interface server. Access rights and capacity limit is inspected according to the SLA.
4. When client is signed in, there are two alternatives accessible. One is for Data dealing with and second one is for Getting Virtual Machine.



5. New clients don't get the main alternative which is information taking care of. This alternative is accessible just for the enlisted client who are diverted to cloud framework. Additionally, client can share the information documents by utilizing this foundation.

Retrieval Number: D9978118419/2019©BEIESP
DOI:10.35940/ijrte.D9978.118419
Journal Website: www.ijrte.org

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication

6. Client will be diverted to the open stack on the off chance that he/she picks second (Getting VM) choice.

7. One Common key is created by improved Diffie Hellman calculation and it is utilized for safe

Correspondence between two gatherings.

8. A trustful registering stage is given to encode client information utilizing normal key between them.

9. We use pressure strategy to store the decoded information on to the cloud server. It utilizes less extra room on the server.

10. Just decoded information is put away on the cloud server.

11. At the point when client demands for the record then it will be downloaded from the cloud server.

12. Prior to this, decompression of the record is done and at that point DES calculation is utilized to disentangle the record so that client can get to the equivalent.

13. We keep another server for reinforcement reason. Due to this we can accomplish adaptation to internal failure.

14. At the point when client demand for logout, VM shutoff and one alarm is sent to the server to end the session.

15. CSP produce the cost articulation as indicated by SLA.

IV. EXSISTING MODEL

Whitefield Diffie and Hellman proposed one answer for the verified key trade in 1976. It permits two imparting gatherings to trade the keys safely. These keys are utilized to encode consequent interchanges. Its proficiency relies upon the trouble of assessing discrete logarithms.

In the proposed arrangement, two openly realized numbers are utilized a prime number 'q' and a crude root 'n' to such an extent that n < q. As 'n' is a crude base of 'q' at that point the numbers n mod q, n^2 mod q, …., n^x mod q will create all numbers from 1 to q-1.

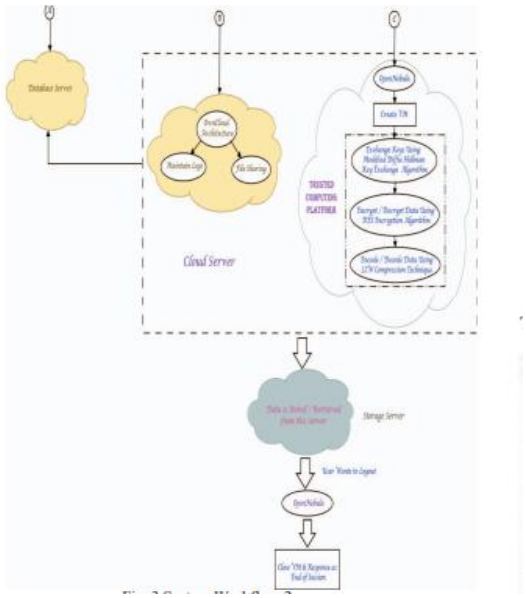
Algorithm:

Give Alice and Bob a chance to be two conveying parties:

1. Both can concur on two open components which are referenced previously.

2. Alice chooses her private key as 'x' where x < q and figure open key as A= n^x mod q.

3. Bounce chooses his private key as 'y' where y < q and figure open key as B= n^y mod q.



4. The two gatherings shared the open keys An and B with each other.

5. Alice ascertains the mystery key as K1 = B^x mod q and Sway does likewise as K2 = A^y mod q.

6. Both are having a similar mystery key now, which will be utilized in further correspondence.

The two gatherings can compute a similar mystery key as they are the one in particular who knows the numbers n and q. This calculation is powerless against MiM assault as they don't have any instrument to confirm the gatherings. Additionally, the keys stay same for the session so it will result into the equivalent unscrambled content for the plain content. By utilizing this data, a trespasser can discover the connection between the plain-content and figure content.

V. REVISED DIFFIE-HELLMAN KEY EXCHANGE ALGORITHM

To shield the key from the above assaults, we changed the Diffie-Hellman key trade calculation as pursues:

1. In this additionally, we are utilizing the centre Diffie-Hellman calculation pursued by the discretionary numbers for additional security.

2. 5 stages are same as the current Diffie-Hellman key trade calculation.

3. Presently, the two of them are having a similar mystery key. They select the discretionary numbers 't' and 's' with the end goal that 0 <t,s<q.

4. Another open key is created by applying logarithm on the keys and having one mystery number 'm' as a base of the logarithm. The estimation of the 'm' is known by both the gatherings. 5. At that point another open key for Alice is determined as C = log(t,K1).

6. Likewise open key for Bob is determined as D = log(t,K2).

7. Both trade the key which will be considered in further encryption of the messages.

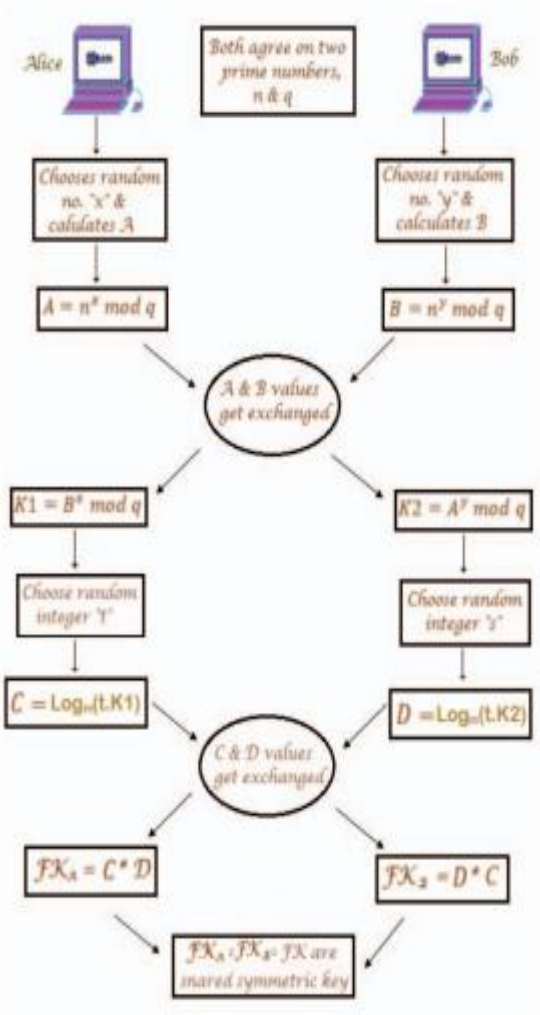
A .Removal of MiM attack:

A mystery number 'm' is utilized as a base of the logarithm by the conveying parties. In the event that a trespasser attempted to get the key, it is hard to get a similar base. Clients are validated by

utilizing this number as it is known distinctly by the gatherings. It forestalls a calculation from MiM assault.

B. Removal of Plain-text attack:

A self-assertive component is considered in key trade convention which produces unique figure content for a similar plain-content. A similar piece of content is scrambled utilizing various keys each time. Thus, unique figure content is created for the equivalent plain content. On the off chance that an intruder gets.



the message, he won't have the option to know the real content.

VI. EXAMINATION OF PROPOSED ALGORITHM

The investigation of the exhibited calculation depends on various security components like privacy, confirmation and honesty of information.

A. Confidentiality:

Information is encoded, when client transfer it, by applying the equivalent keys. These keys are created by amended Diffie-Hellman key trade calculation. Along these lines, Confidentiality of the information is ensured by putting away the keys. These keys are known just to the information proprietor. This make the information progressively classified as CSP can't get the entrance of the information.

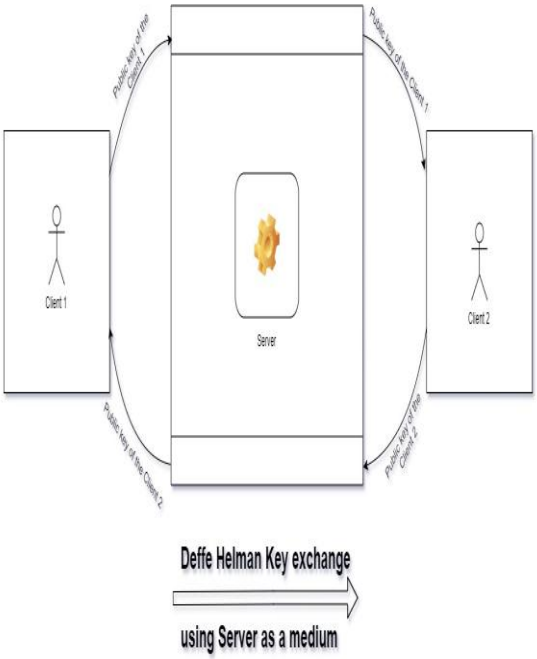
B. Authentication:

The logarithmic worth is registered for the regular mystery key utilizing the base worth 'm'. It is accessible for both the gatherings what's more, it guarantees individualization. On the off chance that an assailant endeavours to convey in the middle of, the estimation of 'm' won't be same mandatorily.

C. Integrity:

Information Integrity is accomplished by the different encryption procedures which are using a similar key created by the calculation. It will ensure that information is secure over the cloud stage.

VII. IMPLEMENTATION



Algorithm:

Step 1: when client connected to the server sends global values to connected client

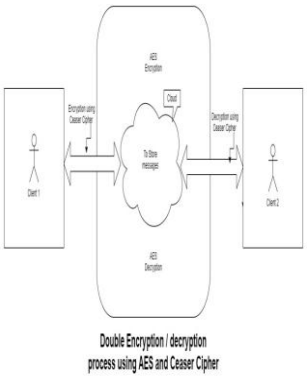
.Step 2: At client-side private key will be generated randomly and with the help of global values public key will be created

.Step 3: Created public key will be send to the server and server will store and send it to other Users .

Step 4: By using the public key of receiver and private key of sender, sender will generate a secret key using Diffe-Hellman key exchange algorithm.

Step 5: Receiver also generate the secret key by using public key of sender and his own private Key. With the same secret key at sender and receiver we can encrypt the message and decrypt the message with ease. It will be secured from the other people.

Process 2:



Double Encryption / decryption process using AES and Ceaser Cipher

Algorithm:

Step 1: After generating secret key sender will encrypt the message by use an encryption algorithm like Caesar Cipher.

Step 2: That encrypted message will be send to the other client with the help of the server.

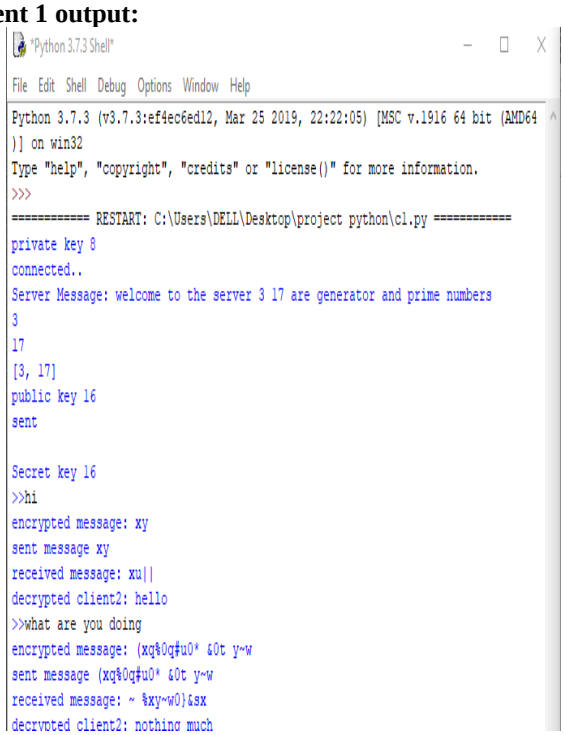
Step 3: In the server it will be encrypted and stored using highly secure algorithms like AES, DES etc. To send the message to the receiver it will be decrypted and send to the receiver using algorithm decryption.

Step 4: Server will send the messages to the receivers and receive the messages from the senders and acts as a medium.

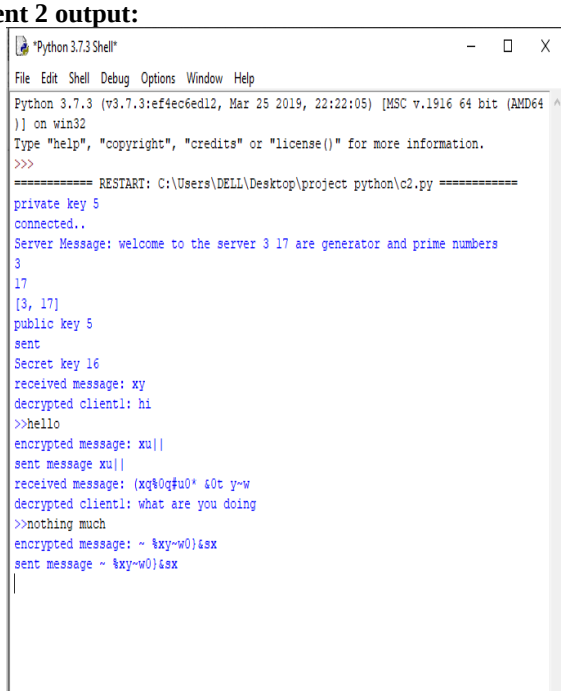
Step 5: After decrypting the message server will send the message to respective receiver. With the Caesar Cipher encryption users can create end to end encryption to ensure the security from the server provider. By using AES encryption model, we can ensure the security from the non-authorized people.

VIII. RESULTS

Client 1 output:



Client 2 output:



Server output:

IX. CONCLUSION

Distributed computing has numerous security issues regarding secrecy, information integrity, individualization. There is a necessity for viable and methodical calculations which can be utilized to give greater security to the cloud information. Diffie-Hellman calculation is commonly utilized in key exchange methodology over the defence less channel. We attempted to give greater security by considering the arbitrary component in the normal key. It is extraordinary for each message that will be encoded. By utilizing this, plain-content assault can be limited.

This diminishes the plaintext assault and MiM assault in Diffie – Hellman calculation. Be that as it may, to structure 100% secure key trade calculation isn't simpler. Quite possibly mystery number picked by gate crasher can be same as 'm'. At that point there is a few odds of Man-in-the-Middle assault in it. Introduced calculation considers a basic numerical approach which is clear and simple to actualize. Secrecy, information integrity, individualization is accomplished by applying this calculation.

REFERENCES

1. FengZhao,ChaoLi,andChunFengLiu,"ACloudComputingSecurity Solution based on Fully Homomorphic Encryption," 16thIEEE International Conference on Advanced Communication Technology (ICACT-2014), pp.485-488.
2. Ian F. Blake and Theo Garefalakis, On the complexity of the DiscreteLogarithm and Diffe-Hellman problems.
3. Willian Stallings, Network Security Essentials: Applications and Standards, 2nd ed, Beijng: qinghua press, 2004.1, pp.75–77.

4. Galbraith and Victor Rotger, Easy decision Dffe-Hellman groups, LM Sai kiran Journal of Computation and Mathematics 7 (2004).
5. Steven Galbraith and Victor Rotger, Easy decision Dffe-Hellman groups, LM Sai kiran Journal of Computation and Mathematics 7 (2004).
6. Ueli Maurer and Stefan Wolf, On the complexity of breaking the Diffe-Hellman protocol, Advances in Cryptology - CRYPTO'96, Lecture Notes in Computer Science, vol. 1109, Springer-Verlag, 1996, pp. 268–282.

AUTHORS PROFILE

Ms D Komali is pursuing M.Tech in department of Computer Science and Engineering, working as Asst.Professor in CSE department of Koneru Lakshmaiah University.Her research area is cloud computing .

A.Raghu Vamsi is pursuing B.Tech in department of Computer Science and Engineering in Koneru Lakshmaiah University. His research area is cloud computing. he is robotic process automation developer. Intrested subjects are C, DBMS, computer networks.

R.Ganga Bhavani is pursuing B.Tech in department of Computer Science and Engineering in Koneru Lakshmaiah University. Her research area is cloud computing. She is salesforce trainer and currently working on many salesforce projects. Her interested subjects are DBMS,OS,OOPS through Java.

CH.Tejsai is pursuing B.Tech in department of Computer Science and Engineering in Koneru Lakshmaiah University. His research area is cloud computing he is ui path developer .His interested subjects are DBMS, C, Python, Machine learning.