International Journal of Recent Technology and Engineering (IJRTE)
ISSN: 2277-3878 (Online), Volume-8, Issue-1, May 2019

A Novel Method for Secure Distributed Computi using Honey Encryption Approach

Gowtham Mamidisetti, Ramesh Makala

Abstract: ***BIG DATA and mists creation is occurring in the present age, it is getting extremely hard to store such a huge measure of data. The most ideal approach to store these immense measures of information is to store it on the cloud. As individuals and enormous associations are moving towards cloud to store their information, security remains the essential concern. Is the information sufficiently verifying on the cloud? One of the approaches to furnish security in distributed computing is with '(HECC-OTP) ECC Honey Encryption with OTP'. Nectar encryption creates figure content, which whenever gave an inaccurate decoding key, delivers an authentic plaintext. Henceforth, by giving false plaintext Honey Encryption gives affirmation against Brute power assault and if a right decoding key it creates OTP to enrolled portable number and EMAIL. Moreover, after the information encryption, SRM (Secure Repository Manager) partitions the information into lumps of little information and transfers it to cloud servers. This paper talks about the present issue looked in the distributed computing with respect to safeguarding the protection in sharing the information. Distributed computing offers set of administrations and assets using web. These administrations are given from server farms which are situated all through the world. Contemporary plans of action for associations to send IT administrations are offered by distributed computing with no forthright speculation. Distributed computing disentangles giving the virtual assets from anyplace on the planet to anyplace on the planet by means of web. . The proposed framework gives an answer for saving the information in cloud with the guide of ECC Honey encryption convention and OTP age.***

Index Terms: Distributed computing, Honey encryption.

I. INTRODUCTION

A cloud commonly includes a virtualized critical pool of figuring assets, which might exist reallocated towards various intentions inside brief instance periods. The whole procedure of mentioning as well as accepting assets is normally computerized and is finished in minutes. The cloud in distributed computing is the arrangement of equipment, programming, systems, stockpiling, administrations and interfaces that joins to convey parts of registering as an administration. Offer assets, programming and data are given to PCs and different gadgets on interest. It enables individuals to would belongings they like towards do on a PC devoid of the requirement in favour of them to purchase along with assemble an I/T foundation or to comprehend the hidden innovation. During distributed compute customers container get to institutionalized IT assets en route for send latest applications, administrations or else registering assets rapidly exclusive of reengineering their whole foundation, consequently creation it active. The center idea of distributed computing is diminishing the preparing load on the clients incurable by always getting better the dealing with capacity of the cloud. The majority of this is accessible through a straightforward web association utilizing a standard program. On interest administration cloud is substantial asset and administration pool that you can get administration or asset at whatever point you need by paying sum that you utilized. Omnipresent system get to cloud gives administrations. Wherever however standard terminal like cell phones, PCs and individual computerized collaborators Easy use: the most cloud supplier's offers web based interfaces which are more straightforward than application program interfaces so client can without much of a stretch use cloud administrations. Plan of action cloud is a plan of action since it is pay per utilization of administration or asset. Area autonomous asset poling: the suppliers figuring possessions are pooled to dish up a variety of clients utilizing multitenant exhibit among various physical moreover practical property progressively doled out furthermore reassigned by interest.

II. CLOUD SECURITY CHALLENGES

Cloud computing separation the information hooked on supportive classes or else grouping is among no previous knowledge. This is a basic method in the field of processor data removal in addition to it has curved into an indispensable element in lots of previous manufacturing areas counting cloud computing. This survived exertion purports a novel clustering procedure based on the submission of krill herd Efficient Stud Krill Herd—Clustering (ESKH-C) procedure. It is an optimization move towards for cloud computing trouble in which a swarm of krill (candidate solutions) shifts to converge to detailed positions as ending cluster centers through minimizing the strength function. The correctness of the purposed method is blazed on dissimilar well recognizable bench mark data sets. Analyzed among the ordinary clustering scheme such as k-means clustering algorithm, cloud computing using particle swarm optimization algorithm, ant colony optimization based data clustering, also clustering system using bacterial foraging algorithm, simulation results proof to facilitate the existed procedure is an effectual cloud computing scheme.

Revised Manuscript Received on 30 May 2019.
***** Correspondence Author
Gowtham Mamidisetti*, research scholar of Acharya Nagarjuna University. Guntur, A. P. India
Dr. Ramesh Makala, Associate Professor of RVR&JC College of Engineering, Guntur, A. P. India

The existed cloud computing method container be working to influence vast data sets among dissimilar cluster sizes, multi-dimensional as well as densities

III. EXISTING METHODS

A. Elliptic curve cryptography

The elliptic bend crypto system is at first projected through Koblitz as well as after that Miller in 1985 to plan open input cryptosystem as well as by and by, it turns into an indispensable piece of the cutting edge cryptography. A concise presentation of E-C-C is known beneath: Let E/Fp means an elliptic bend E more than a prime limited pasture Fp, which preserve be characterized through

$$Y=X+ a X +b$$

Distributed storage space is the mainly noticeable administration in distributed calculating, among distributed storage, clients preserve store in addition to admission their information whenever/anyplace, it conveys much comfort to the clients, anyway since the information is put away over the cloud and course through the system in plaintext position, clients stress over the security of the information, in spite of the fact that the cloud suppliers guarantee information put away in the cloud is much security [1]. We give a casing work, there are two sections for each client's information, the private information division moreover the common information element. In the confidential information fraction clients can stock up their private as well as delicate information which is utilized just independent from anyone else; in the common information part, clients can impart information to numerous validated clients. Client's tasks are portrayed as following:

Private/data/part/operation: In the private information division, client initially scrambles the information at the customer elevation among the assistance of the P/E/A, moreover afterward transfers it to the confidential information piece of the cloud, while he requirements the information, and initial downloads along with afterward unscrambles the information among his session input

Shared-data-part-operation: In the common information part, customer preserve accumulate the information which they need to impart in the direction of different clients. At the point when client needs to impart information to other validated clients, he initially scrambles the information with his session input as well as encodes the session key among the confidential solution of the key couple which is certificated through the C/A. In the wake of completing the encryption, client transfers the link of the 2 sections' scrambled information to the mutual information division of the cloud. Commencing the endorsement record, previous verified clients preserve verify the open solution of the client who transfers the information moreover utilize this open input unscramble the encoded session key, in the wake of getting the session/key, clients be capable of utilize it to decode the scrambled information.

In mutually private information moreover collective information divisions, client encode information utilizing symmetric encryption calculations among various session keys, moreover just in collective information division, clients scramble the assembly key utilizing E/C/C open key calculation among their private key, moreover furthermore decode the scrambled assembly input utilizing E-C-C open type calculation among relating client's open solution. Also, clients deal with every one of the tasks through C/A moreover cloud boundary from side to side PEA. This plan not just permits clients stock up as well as admission their information safely yet in addition permits clients share information with numerous validated clients safely through the unbound web.

Hybrid security in Cloud by using Ensemble Algorithm

In our proposed structure following with this ECC Encryption, SHA-512 is utilized as Identification Agent (IA) and focus on IA. in the presentation of framework sort out , SHA-512 flooded in the framework while IA to see each asserted customer to keep on handshake[2]. In the Later before a social occasion of people, the SHA-512 is used as a piece of light of the way that TA for affirming the part and keeping up a vital separation from non-part.

Consequently there are four parts in the proposed system.

Member: an associate can be a substance who is one of the social event. U€G interprets that U is one of the part in the social event G.

Non-party: A non-member can be a substance would you not value the social event G.

SHA-512 IA is responsible for adding individuals to the get-together.

SHA-512 TA is responsible for uncovering clients what's more looking handshake players value his own particular get-together. The execution of the engaging situation is cleared up here under:

a) Set up: the customary parameter time allotment figuring. Given a security parameter k, set up yields the general people parameters that are typical to all or any parties.

b) KeyGen: the get-together open key age figuring. KeyGen is regularly work by SHA-512 IA and SHA- 512 TA. Given param, KeyGen yields a social event general masses key gpk, a key of SHA-512-IA isk and a key of SHA-512 TA tsk.

c) Add: the part advancement calculation. Fuse is executed just by non segmentAn and SHA-512 – IA. Given param ,gpk, and isk put yields a help guaranteeing (certA) , a confuse focal (skA) , and ID of A(IDA).

d) Group Trace: A handshake player's get-together take subsequent to figuring .givengpk, tsk and a transcript TA, B, gather take after yields yes if A,B€G; ordinarily collect take after ouputs Zero.

e) Demand Reveal: the handshake part following calculation, gave gpk,tsk, certA,skA , a transcript TA , B also interior data with the aim of are found by handclasp through another player. A demand uncover yields the part B.

B. An efficient way to preserve privacy on cloud

Information Owner registers with the CSP and CSP sends the introduction key to the Data Owner to his enrolled email id. After fruitful enrolment Data Owner transfers the scrambled information to the cloud. The Data User who is an enlisted client question's for information to the CSP. The CSP at that point gives a rundown of Data Owners to the Data User who has the mentioned information. The Data User demands for information from the regarded Data Owner. Presently, it totally relies upon the Data Owner to share the way to the Data User.

When the Data User has gotten the key, the Data User can download and unscramble the record from the CSP .Here, the benefits of the CSP has been diminished.

IV. PROPOSED METHOD

Honey Encryption is a structure that winds up being exceedingly adaptable against Brute power attacks. With the help of this Encryption structure, if figure content is unscrambled with the mixed up key, it conveys a possible looking yet off kilter plaintext. The incorrect key will create a fake plaintext when used while unscrambling the data. The aggressors consider the fake plaintext as a real message as no doubt a possible plaintext. In the occasion that accept decoded key is appropriate, by then HECC-OTP estimation make 2-OTPs to resister flexible and Email separately finally using these OTPs we are get to the cloud viably.

Huge DATA and fogs creation is happening in the present age, it is getting astoundingly difficult to store such a gigantic proportion of information. The best way to deal with store these tremendous proportions of data is to store it on the cloud. As people and gigantic affiliations are moving towards cloud to store their data, security remains the basic concern. Is the data adequately confirming on the cloud? One of the ways to deal with outfit security in appropriated figuring is with '(HECC-OTP) ECC Honey Encryption with OTP'. Nectar encryption makes figure content, which at whatever point gave an off kilter translating key, conveys a solid plaintext. From now on, by giving false plaintext Honey Encryption gives affirmation against Brute power attack and if a correct disentangling key it produces OTP to enlisted versatile number and EMAIL. In addition, after the data encryption, SRM (Secure Repository Manager) isolates the data into chunks of little data and exchanges it to cloud servers. This paper analyzes the present issue looked in the dispersed registering as for sparing the security in sharing the data. Conveyed figuring offers set of organizations and resources utilizing web. These organizations are given from server ranches which are arranged all through the world. Contemporary plans of activity for relationship to pass on IT organizations are offered by appropriated registering with no frank hypothesis. Dispersed figuring improves giving the virtual resources from wherever on the planet to wherever on the planet by methods for web. . The proposed structure gives a response for shielding the data in cloud with the guide of ECC Honey encryption tradition and OTP age.

A cloud customarily surrounds a virtualized basic pool of figuring possessions, which might be reallocated to dissimilar reasons inside brief occasion designations. The whole strategy of referencing also getting possessions is regularly motorized as well as is done in proceedings. The cloud in circulated processing is the course of action of gear, programming, frameworks, storing, organizations and interfaces that combines to pass on parts of figuring as an organization. Offer resources, programming moreover in sequence are given to PCs also diverse contraptions on intrigue. It empowers persons to might things they desire to do on a PC devoid of the prerequisite in favour of them to pay money for also fabricate an I/T establishment otherwise to fathom the essential development. from side to side appropriated registering customers canister get to organized I-T advantages for send new requests, organizations or figuring capitals rapidly devoid of reengineering their whole establishment, along these lines making it dynamic.

The inside thought of conveyed processing is reducing the planning load on the customers terminal by consistently improving the dealing with limit of the cloud. Most of this is open through a clear web affiliation using a standard program. On intrigue organization cloud is far reaching resource and organization pool that you can get organization or resource at whatever point you need by paying aggregate that you used. Ubiquitous framework get the opportunity to cloud gives organizations. Wherever anyway standard terminal like PDAs, PCs and individual propelled helpers Easy use: the most cloud provider's offers online interfaces which are less troublesome than application program interfaces so customer can without quite a bit of a stretch use cloud organizations. Plan of activity cloud is an arrangement of activity since it is pay per usage of organization or resource. Region independent resource poling: the providers preparing resources are pooled to serve various customers using multitenant appear with different physical and virtual resources capably assigned and reassigned by intrigue.

A. CLOUD SECURITY CHALLENGES

The cloud administrations present numerous difficulties en route for an association. At the point whilst an organization alleviate to expend cloud administration, along with mostly unlock cloud administrations, a large division of the figuring structure basis determination now beneath the manager of cloud authority association. A substantial batch of these problems ought to be tended to from side to side management performance. This organization performance will necessitate unmistakably outlining the proprietorship as well as compulsion jobs of together the cloud contractor along with the organization operational in the job of customer. Safety chiefs should almost certainly shape out what criminologist also protection joystick survives to obviously typify security posture of the alliance. Albeit legitimate safety wheels are should be actualize dependent on resource, danger, moreover powerlessness hazard appraisal frame works. Circulated computing sanctuary hazard evaluation statement predominantly beginning the merchant's standpoint concerning security capacities scrutinize security dangers seem by the cloud. At this time are refuge dangers register.

- Regulatory consistence: disseminated computing provider who refuses to outer surface reviews moreover security accreditations.
- Privileged client get to: touchy in order handled exterior the organization carries among it a natural dimension of hazard.
- Data area: whilst you use cloud, you most probable won't know accurately where your in sequence make possible. Information isolation: information in the cloud is jointed situation
- Alongside data commencing dissimilar customers. Recuperation: despite of whether you don't have the foggiest idea where your in sequence is, a cloud contractor must disclose to you what will occur to your in order with administration in the occasion of a fiasco.
- Investigative help: investigative shocking or illicit exploit strength be unimaginable in dispersed computing.

Extended haul feasibility: you should create sure your in sequence will stay reachable even following such an instance.

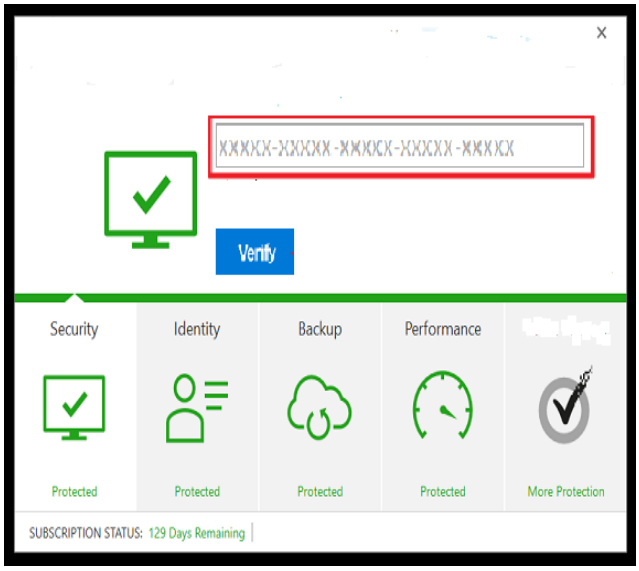
B. PROPOSED HECC-OTP METHOD

Honey Encryption Encryption is a framework that ends up being very flexible against Brute power assaults. With the assistance of this Encryption framework, if figure content is unscrambled with the mistaken key, it delivers a conceivable looking yet off base plaintext. The off base key will create a phony plaintext when utilized while unscrambling the information. The aggressors think about the phony plaintext as a lawful message as it would seem that a conceivable plaintext. On the off chance that assume decoded key is right, at that point HECC-OTP calculation produce 2-OTPs to resister portable and Email individually at long last utilizing these OTPs we are get to the cloud productively.

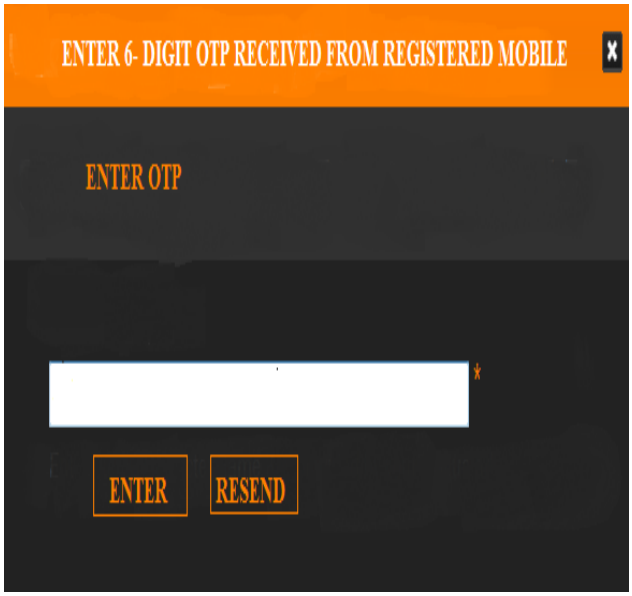
ALGORITHM

START: when user wants access allows this algorithm

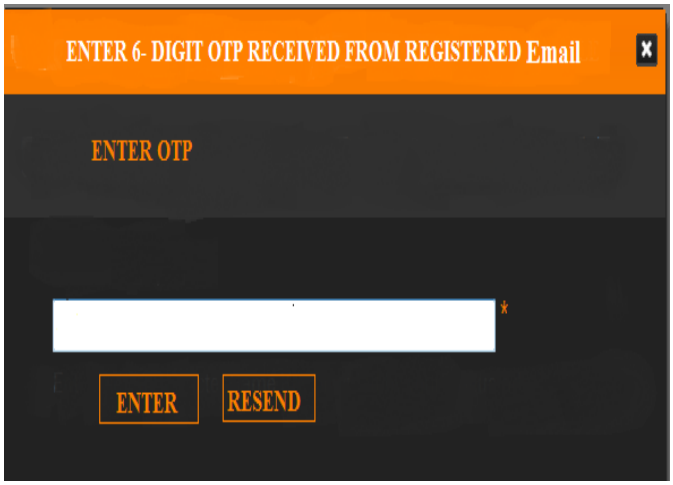
STEP:1 at decrypted side ask the pop like **ENTER KEY**



STEP: 3 if entered password is correct it generates two OTPs to registered mobile and Email respectively



STEP: 4 entered OTP is correct then open the new window like below

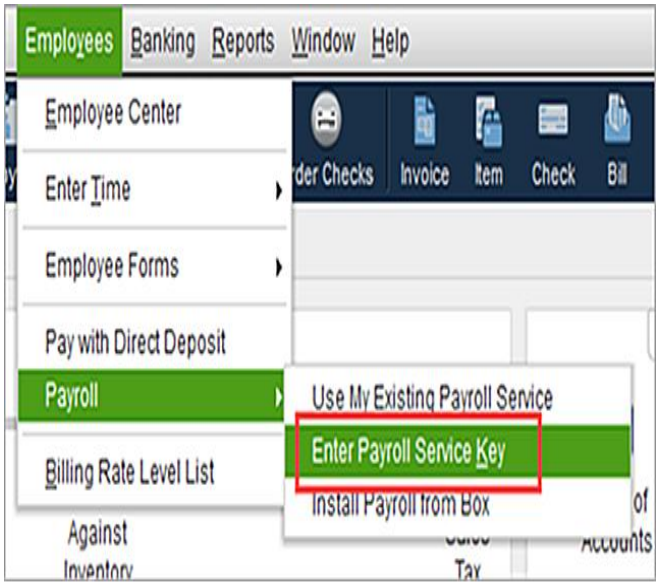


A one-time password (O/T/P A one-time clandestine word (O-T-P) is a consequently created numeric or alphanumeric sequence of lettering to facilitate verifies the customer for a solitary replace otherwise conference. This is utilized by HECC online stages to approve client exchanges and character. Client Authentication while making exchange is the most noteworthy factor for any business. Phonon gives a standout amongst the most secure verification strategy by making a token or irregular code and sends OTP by means of. SMS, Email and Voice Calls to the clients. When client gets the token or arbitrarily produced code, at that point client can enter those subtleties and approve himself/herself. Amid OTP conveyance to the client, Phonon keeps up exacting TRAI and NDNC consistence while sending messages and making calls to the enlisted telephone numbers. For email conveyance, Phonon utilizes Amazon SES Integration with SPF and DMAC/DKIM verification to guarantee that the mail is conveyed to the Primary inbox of the client.

OTP (One Time Password) security is kept up through a single direction hash dependent on the HECC-OTP with the assistance of HMAC SHA calculation.

STEP: 5 finally cloud give the access to user

STEP: 6 when **e**nter key is wrong in the 1st step simply cloud shows false data and the access not approved.



This strategy HECC-OTP technique is additionally pursues the robbery client ceaselessly and gather the information from client distinguishes HACKER.

In Software as an administration, clients can utilize the application given by the Cloud administration merchant running on the Cloud framework. SaaS applications mostly incorporate business applications, for example, ERP, CRM, SCM, and so forth. Associations, which don't have the assets to build up their very own applications, more often than not purchase the applications from cloud-based merchants for their business purposes. The information that is utilized by the applications for handling is generally put away in the cloud itself. Besides, this information is put away as plaintext, which makes it progressively powerless against various sorts of assaults. Clients have minimal power over the security for this situation, as both the application and the information are put away in the Cloud and it turns into the essential obligation of the merchant to give security in Software as a Service (SaaS) office.

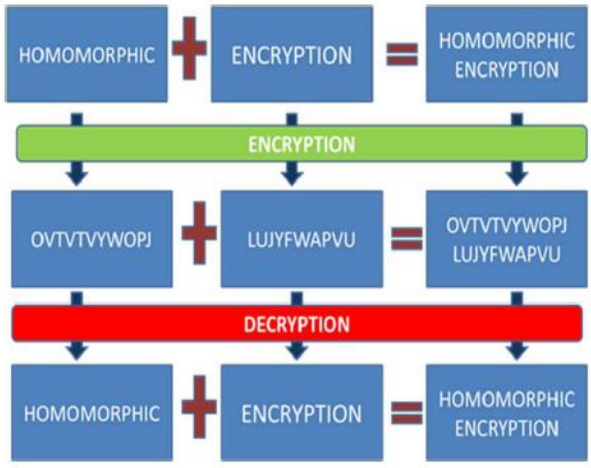


Fig 1 Encryption Model

In the above model gave in Figure 1, we can see that it was not important to decode the figure message before playing out the link task. Consequently, we can say that HECC is homomorphism on connection activity. As we found in the above model, Homomorphism connection lands at a similar outcome, as does the non homomorphic link. Be that as it may, this isn't generally the situation. Thus, we need a Homomorphic encryption, which can unravel every one of the activities in the cloud. The encryption, which can play out every one of the tasks on the ciphertext (NOT, AND, OR and XOR), is known as completely homomorphic encryption.

C. KEY-GENERATION

1) User (U) choose an integer dU. This is User's private/key.
2) User then produces a public/key PU=dU*R
3) Cloud Vendor (V) likewise picks a private\key dV as well as computes a public\key
a) PV= dV *R
4) User (U) generates the secret key K= dU *PV. B generates the secret key K=dV *PU.

ENCRYPTION

Suppose User U wants to retrieve an encrypted message from Vendor V.
1) Vendor V takes plaintext message M and encodes it onto a point, PM, from the elliptic group.
2) Vendor chooses another random integer, k from the interval [1, p-1]
3) The cipher text is a pair of points PC = [(kR), (PM + kPU)]
4) Send ciphertext PC to User U.

DECRYPTION

User U will take the following steps to decrypt cipher text PC.
1) User U computes the product of the first point from PC and his private key dU, dU * (kR)
2) User U then takes this product and subtracts it from the second point from PC, (PM + kPU)– [Du (kR)] = PM + k (dU*R) – dU (kR) = PM
3) User then decodes PM to get the message, M.

D. EXTRA SECURITY BLOCKS

In mutually private information also shared information divisions, client encodes information utilizing symmetric encryption calculations among various session keys, as well as just in joint information division, clients scramble the assembly key utilizing E/C/C open input calculation through their private solution, moreover furthermore unscramble the encoded sitting key utilizing ESKH-F open key calculation with relating client's open key. In addition, clients deal with every one of the tasks through C/A as well as cloud boundary from side to side ESKH-F. This plan not just permits clients accumulate also admission their information safely yet in addition permits clients share information with numerous confirmed clients safely through the unbound

V. RESULTS

In this paper, the usage is finished by utilizing NETBEANS 8.0.2 and JDK 1.8 and Mysql 5.7 for the better outcomes. Here a portion of the functionalities are accommodated the getting to of information and offering authorization to download the information. Validation (information proprietor, client and key expert), Key Generation for the information, Encryption, Decryption and to get to the information by the client the verified key ought to be given by the information proprietor. This will be finished by the inside key generator which gives the consent through the key expert.

The key ought to be send by the cloud administrator (key expert) to get to the needful information or records.

VI. CONCLUSION

At long last this '(HECC-OTP) ECC Honey Encryption with OTP framework can be important in business circumstances as it catches functional access arrangements dependent on jobs in a versatile manner and gives secure information stockpiling in the cloud maintaining these entrance methodologies. Likewise Confidentiality of client access to profit and client mystery key duty can be cultivated. Formal security proofs exhibit that this arrangement is secure under standard cryptographic models.

REFERENCES

1. Ora, P.,& Pal, PR(2015, September)Data security and integrity in cloud computing based on RSA partial homomorphic and MD5 cryptographyIn Computer, Communication, and Control (IC4), 2015 International Conference on (pp1-6)IEEE
2. Chen, D.,& Zhao, H(2012, March)Data security and privacy protection issues in cloud computingIn Computer Science and Electronics Engineering (ICCSEE), 2012 International Conference on (Vol1, pp647-651)IEEE
3. Khan, MSS.,& Deshmukh, MSS(2014)Security in cloud computing using cryptographic algorithmsIJCA
4. Kamara, S.,& Lauter, KE(2010, January)Cryptographic Cloud StorageIn Financial Cryptography Workshops (Vol6054, pp136-149)
5. Zargari, S.,& Benford, D(2012, September)Cloud forensics: concepts, issues, and challengesIn Emerging Intelligent Data and Web Technologies (EIDWT), 2012 Third International Conference on (pp236-243)IEEE
6. N. Ram Ganga Charan, S. Tirupati Rao, Dr . P. V. S Srinivas Deploying an Application on the Cloudll International Journal Advanced Computer Science and Applications, Vol. 2, No. 5, 2011
7. DeyanChen , Hong Zhao -Data Security and Private Protection Issues In Cloud Computingl12012 International Conference on Computer Science and Electronics Engineering
8. Qi Zhang· Lu Cheng . RaoufBoutaball Cloud computing: state-of the-art and research challenges II InternetServ Appl (20 I 0) 1: 7-18
9. EmanM.Mohamed, Hatem S. Abdelkader, Sherif EI-Etriby, Enhanced Data Security Model for Cloud Computing The 8th International Conference on Informatics and System (IN FOS20 12)- 14-16 May
10. Michael Annbrust etc.,Above the Clouds: A Berkeley View of Cloud Computing, http: //eecs.berkeley.edu/Pubs/TechRpts/2009 /EECS 2009-28.pdf:2009.2 .

AUTHORS PROFILE

Gowtham Mamidisetti is a research scholar of Acharya Nagarjuna University. His research includes Cryptography and Information security.

Dr. Ramesh Makala is an Associate Professor of RVR&JC College of Engineering, Guntur .His research interests include Information security, Data mining and image processing. He published papers in various reputed journals, national and international conferences.