DATA SECURITY IN CLOUD COMPUTING

USING HONEY ENCRYPTION

***P RAGHAVENDRA REDDY1, S SHANTHI2***

***1 UG Student, Electronics and Communication Engineering, Saveetha School of Engineering, SIMATS, Chennai, Tamilnadu.*** [***raghavendrareddy515@gmail.com***](mailto:raghavendrareddy515@gmail.com)

***2 Professor, Electronics and Communication Engineering, Saveetha School of Engineering, SIMATS, Chennai, Tamilnadu.*** [***Shanthis.sse@saveetha.com***](mailto:Shanthis.sse@saveetha.com)

**Abstract: -Protecting one’s personal or an organisation or company’s data is absolutely critical – that’s why so many businesses use automated backup with their cloud storage. It’s scalable, flexible and provides peace of mind. Cloud storage gives easy back up of data. But there is a chance of hacking the cloud for the information. Our proposed method deals with how to provide security for the data by encrypting the data using Honey Encryption.**

Introduction: -

Cryptosystems utilize a lot of methods known as cryptographic calculations, or figures, to encode and decode messages to verify interchanges among PC frameworks, gadgets, for example, cell phones, and applications. A figure suite utilizes one calculation for encryption, another calculation for message validation and another for key trade. This procedure, implanted in conventions and written in programming that sudden spikes in demand for working frameworks and organized PC frameworks, includes open and private key age for information encryption/unscrambling, advanced marking and check for message validation, and key trade.

Types of cryptography:

Single-key or symmetric-key encryption calculations make a fixed length of bits known as a square figure with a mystery key that the maker/sender uses to encipher information (encryption) and the recipient uses to disentangle it. Sorts of symmetric-key cryptography incorporate the Advanced Encryption Standards (AES), a particular set up in November 2001 by the National Institute of Standards and Technology as a Federal Information Processing Standard (FIPS 197), to ensure delicate data. The standard is ordered by the U.S. government and generally utilized in the private area.

In June 2003, AES was endorsed by the U.S. government for characterized data. It is an eminence free determination actualized in programming and equipment around the world. AES is the successor to the Data Encryption Standard (DES) and DES3. It utilizes longer key lengths (128-piece, 192-piece, 256-piece) to forestall savage power and different assaults.

In June 2003, AES was endorsed by the U.S. government for characterized data. It is an eminence free determination actualized in programming and equipment around the world. AES is the successor to the Data Encryption Standard (DES) and DES3. It utilizes longer key lengths (128-piece, 192-piece, 256-piece) to forestall savage power and different assaults.

To keep up information respectability in cryptography, hash capacities, which return a deterministic yield from an info esteem, are utilized to outline to a fixed information size. Kinds of cryptographic hash capacities incorporate SHA-1 (Secure Hash Algorithm 1), SHA-2 and SHA-3.

**Literature Survey:**

Disseminated figuring is one of the standard purposes of the present world. Web has started driving all these new headways. There are various data security stresses in appropriated figuring. Mixed up revelation of a data used in associations in cloud to untouchables is one of the critical issues that has been found. Encryption should be properly used and the crypto figuring’s join AES, RSA, DES and 3 DES. Cloud Security can be ensured by data dependability, Secured data trade and by Cryptography. There are collections of cryptographic estimations which can be executed so as to ensure security in the cloud. The two sorts of estimations are Symmetric and Asymmetric encryption key counts. Symmetric contains counts like DES, AES, 3 DES and Blowfish figuring. Lopsided contains figuring’s like RSA, Diffie-Hellman Key Exchange. Symmetric key and disproportionate key figuring’s are used to encode and unscramble the data in cloud [1].

The work done by Mohamad Fadli, depend on it, and the phrasing and ideas related with it give critical knowledge. Writing on distributed computing has obscured the genuine importance of distributed computing. Be that as it may, a few organizations make their administration needs at the expression "distributed computing" starts from system topology. Cloud processing alludes to the direct of common-sense applications or administrations in an Internet. Distributed computing did not quickly rise; it might be followed back in some shape to when processing frameworks had registering assets, and down to earth applications that were remotely time-shared. Concerns have been raised with respect to the diverse assortments of uses and their administrations gotten by mists. In various cases, the gadgets and applications utilized in these administrations include no uncommon capacity. Numerous organizations benefit of administrations from the cloud. As in 2010, an example of organizations benefiting of distributed computing administrations created the accompanying: Microsoft has the Microsoft® SharePoint® online administration, which permits substance and business undertaking insight devices to be transferred into the cloud and makes office pragmatic applications accessible in the cloud. Google distributed storage conveying numerous administrations for formal clients, and vast framework I.T organizations [2].

Security episodes on open cloud information stockpiling had risen worries on cloud information security. Existing cloud information insurance arrangements that basically depending on the regular secret key-based encryption can't effectively oppose secret key speculating and secret word splitting assaults. To address this issue, this paper proposed an extended Honey Encryption (XHE) plot by including an extra insurance component the encoded information. At the point when the assailant endeavours to get to this scrambled information by entering the erroneous secret key, rather than dismissing the entrance, the HE calculation produces an unclear false information, in which the assault couldn't decide if the speculated secret key is working effectively or not. Thusly, expanding the multifaceted nature of secret phrase speculating and breaking assaults [3].

Despite the fact that numerous encryption calculations exist, all are for the most part dependent on secret phrase-based encryption and helpless against numerous digital assaults. An ongoing report reports that 1.08% of individuals picked a similar secret word. Because of increment in calculation speed of frameworks and appropriated processing, the time takes to split those encryption calculations is diminishing. Since delicate data is getting to be defenceless against assailants, there is a requirement for actualizing progressed cryptographic calculations. IoT is turning into a rising pattern where we can control all equipment gadgets with the assistance of programming. Since IoT is conveying more touchy data over the Internet, there is a requirement for better security. So, by executing cryptographic calculations, the client can speak with IOT gadgets in safe and anchored way. The issue of information encryption incited us to execute ad lobbed nectar encryption (HE). In PC security, nectar usually means a false asset intended to draw or dace [4].

The exchange off of database of passwords of Rock You, Yahoo, Adobe, LinkedIn revealed that basically taking care of the passwords in plaintext in unprotected against attacks. For tying down the passwords, the passwords are at present taken care of in database as cryptographic hash work as opposed to being taken care of as plaintext. Hashing is done by using a cryptographic hash work which is irreversible. Hash computations are single direction cryptographic limits which change any proportion of data into a settled length, unique finger impression that can't be turned around back to the main information. Hash estimations in like manner have a property that if the data changes by even a little total, the resulting hash changes absolutely from the first. Hash estimations in like manner have a property that if the data changes by even a little total, the resulting hash changes absolutely from the first. Following are a bit of the ordinary attacks which are used to part plain substance mystery word hashes [5].

The Encryption system ends up being adaptable against Brute force ambush. With the help of this Encryption structure, if ciphertext is decoded with the mixed-up key, it conveys a possible looking yet off base plaintext. The off-kilter key will make a fake plaintext when used while interpreting the data. The aggressors consider the fake plaintext as a legitimate message as doubtlessly a possible plaintext [6].

With the ultimate objective to improve the drawback of the ordinary mystery state-based encryption (PBE) with low-entropy passwords, Juels and Ristenpart introduced Honey Encryption (HE). The standard idea is that encryption of plaintext M is randomized with a mystery expression k, and unscrambling of ciphertext brings about possible looking plaintext M' with wrong mystery key k'. They build up a spread evolving encoder (DTE) for encoding and unravelling of message as bit string, implied DTE = (encode, unravel) [7].

To summarize things, when all is said in done process is

HE [DTE, SE] =(Hunched) where SE infers standard symmetric encryption. The ciphertext is C = Hence (k, M) and unravelling works M = HDec (k, C) or M = HDec (k, C).

Advantages:

1)A new secure chatting application robust to eavesdropping by applying the HE schemes, and call it as Honey Chatting.

2) Good Security.

3)Encrypted data.

4) Instant Messaging Security.

5)Good UI.

**PROBLEM IDENTIFICATION:**

Cloud can come in various kinds, and the administrations and the applications that conceivably run on mists might possibly be given by a cloud specialist co-op. There are two interesting gathering of models specifically arrangement models and administration models. Administration models comprises of IaaS, SaaS, PaaS. The Deployment or organization model comprises of Public Cloud, Private Cloud, Hybrid Cloud, Community Cloud. Distributed computing has bunches of particular properties that make it significant, protection is by all accounts an interesting worry in cloud. Different kinds of administration models under distributed computing encourage different degrees of security administrations. We will get the base security in IaaS (Infrastructure as a Service) and most with a SaaS supplier.

1)Problem Statement:

The encryption of information with the target that gathering and security can be effectively refined. Besides, some cloud security issues are one of the issues in dispersed preparing. Here the based utilized DES calculation, RSA estimation and whatnot.

**Problem Solving Strategies**:

1)Source of Information:

Must have detailed information about the source which is sending the information.

2)Data Collection:

Cryptography is considered as a social occasion of three estimations. These counts are Symmetric-key estimations, Asymmetric key computations and Hashing. In Cloud preparing, the essential issues are related to issue in data security, fortification data, sort out development, report amassing system, and security of host, and cryptography alone can understand these issues to degrees. For a protected and secure correspondence between the guest space and the host zone, or from hosts to organization systems, encryption advancements, for instance, Secure HTTP, encoded VPNs, TLS, Secure Shell, and so on should be used. Encryption will empower us to check such undertakings like man-in-the centre, mock ambushes, and session seizing.

**Methodology:**

The usage of Honey Encryption is to give acceptable security to the cloud information of clients.

**1)Hardware Specification:**

These specifications are not applicable.

**2)Software Specification:**

The execution of Honey Encryption is to give acceptable security to the cloud information of clients. The principle usefulness is that the passwords or any messages will scramble which prompts the client for security reason. This encryption is totally founded on the calculation or model, which is known as Honey Encryption Model. This encryption strategy is drifting than the DES, RSA and so forth.

In cloud-based application security is most significant factor than some other on the grounds that it stores the client's information in their particular servers or databases. Through the system, hacking or dangers may happen with the goal that the information which is moving by means of system ought to be secure and furthermore ought to be scrambled. Utilizing this calculation some security issues can conquer which are not done by conventional calculations, for example, RSA, MD5 and so forth. That is the principle highlight.

In part of specialized attainability, java is going to use to execute the Honey encryption model. The program multifaceted nature is moderate at which client's information as information and the scrambled information as yield.

**System Requirements: -**

1. DK- Version 1.90
2. Java compiler or IDE
3. System with 4 GB RAM
4. Windows OS

**Proposed Architecture:**

There are two methods need to be implemented

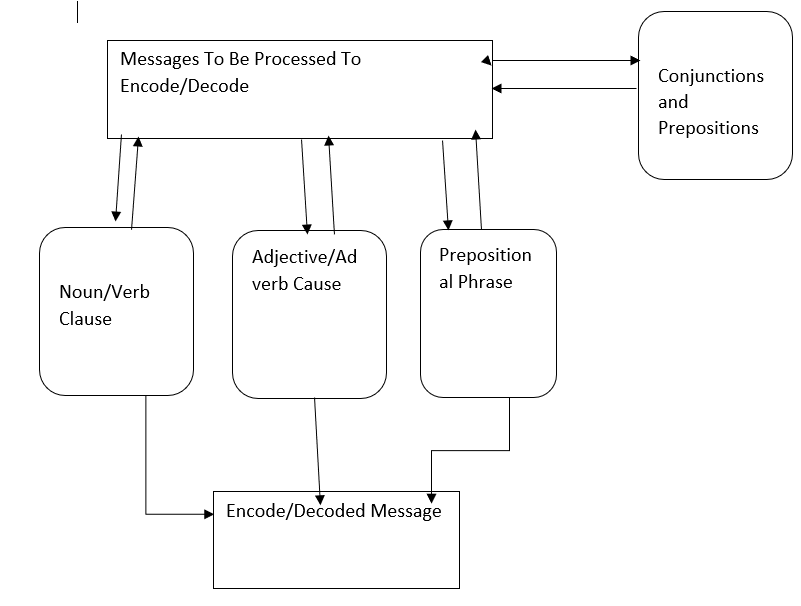
They are

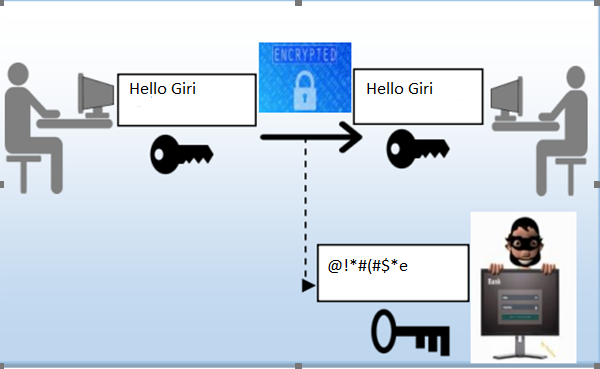
1. Encryption method

2. Decryption method

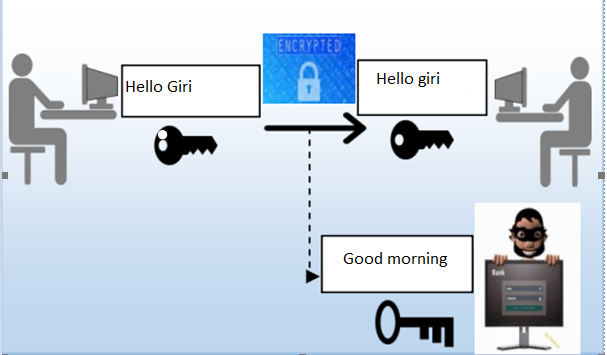
Both methods can implement using two classes that one for encryption and another one is for is decryption.

**Architecture Design:**





**Here hacker need to use a valid key otherwise he will get message like below**



**Defining Variables:**

m = key Seed ^ cipher;

cipher is cipher text

key seed is the key

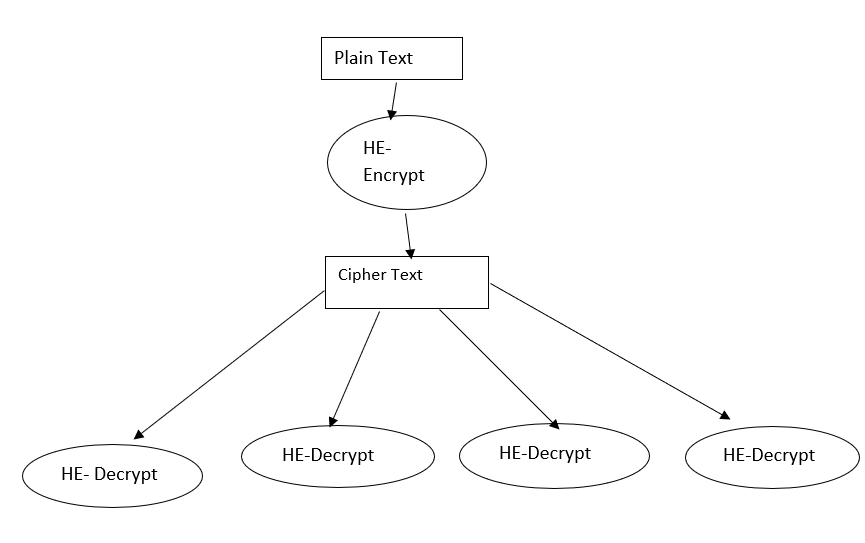
**Modules**:

Design module

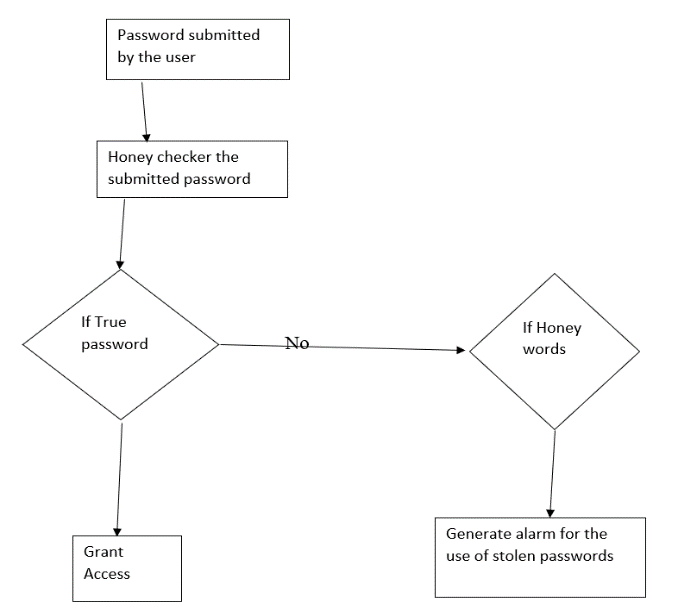
Encryption module

Decryption module

**(d) Data Flow Diagram:**

****

**Process Flow Diagram:**



1.Here the info brief from the client, which information should be verifying or scramble that is called Plain Text

2. For nectar encryption, plain content is the information and verifies the information, which implies the plain content and rationale of this calculation is referenced underneath.

3. Figure content is the verified information or message subsequent to applying nectar encryption calculation. It is an encoded message.

4. For nectar unscramble, figure content is the information. The plain content will be the yield which was quick from the client.

**Algorithm: -**

Pseudocode: -

HashMap<String, Integer> passwordToSeeds = new HashMap<> ();

HashMap<Integer, String> seedsToMess

ages = new HashMap<> ();

HashMap<String, String> states = new HashMap<> (); //U. S States as secret messages

assign States(states);

do {

ask ();

true Seed = rand. nextInt(27) + 1;

honeyWordGenerator (passwordToSeeds, seedsToMessages, states, trueSeed, userPass, message);

int cipher = (passwordToSeeds. Get(userPass)) ^ trueSeed;

displayPassword(passwordToSeeds);

crack(passwordToSeeds,seedsToMessages,cipher,trueSeed);

askExit(passwordToSeeds,seedsToMessages);

} while(status);

System.out.println("\nThank you for testing Honey Encryption.");

sc.close();

}

//ask user to crack the user

public static void crack(HashMap<String, Integer> passwordToSeeds, HashMap<Integer, String> seedsToMessages, int cipher, int trueSeed) {

System.out.print("Enter your password: ");

String query = sc.nextLine();

if(passwordToSeeds.containsKey(query)) {

int keySeed = passwordToSeeds.get(query);

int m = keySeed ^ cipher; //decryption key using XOR method

if (m != trueSeed) {

System.out.println("INTRUDER HAS BEEN FOUND!");

}

System.out.println(seedsToMessages.get(m));

}

else {

System.out.println("Password not found");

}

}

**Input Parameters:-**

1. Plain text(user’s data)

2. cipher text (encrypted data)

**Output Parameters: -**

1.cipher-text (encrypted data)

2.Plain-text (User’s data)

Conclusion: -

In this manner, the proposed encryption framework gives better Encryption guidelines in information security. The calculation of the Honey encryption gives better cloud information encryption. The information is isolated into figure content and plain content which gives information security when the beast power assault was made on the cloud. The encryption calculation shows some non-sense information rather than the first information.

References: -

1. Cryptography in Cloud Computing: A Basic Approach to Ensure Security in Cloud Rishav Chatterjee1, Sharmistha Roy2 UG Scholar1, Assistant Professor2 School of Computer Engineering KIIT Bhubaneswar, India.
2. Use of Cryptography in Cloud Computing, Aws Naser Jaber1 Faculty of Computer Systems & Software Engineering University Malaysia Pahang Kuantan, Malaysia aws\_z2010@yahoo.com, Mohamad Fadli Bin Zolkipli2 Faculty of Computer Systems & Software Engineering University Malaysia Pahang Kuantan, Malaysia [fadli@ump.edu.my](mailto:fadli@ump.edu.my).
3. Implementing the Honey Encryption for Securing Public Cloud Data StorageEdwin Mok1, Azman Samsudin2, Soo-Fun Tan3 {edwinmyp@gmail.com1, azman.samsudin@usm.edu.my2, soofun4818@yahoo.com3 School of Computer Sciences, University Saints Malaysia, Penang, 11800, Malaysia.
4. Implementation of Enhanced Honey Encryption, for IoT Security Dr. Shanthi Baskaran, S.V. L Sarat Chandra, Venkatesh, E. Silambarasan, M. Dinesh.
5. Honey Encryption beyond the Brute-Force Barrier, Ari Jules | Cornell Tech Thomas Ristenpart | University of Wisconsin.
6. Review on Honey Encryption Technique Nahri Syed Noorunnisa1, Dr. Khan Rahat Afreen2.3.
7. Security in Cloud Computing using Honey Encryption, Department of Management and Information Science, Rutgers Business School, Newark and New Brunswick, Corresponding Author: Fancy Arora.
8. HONEY CHATTING: A NOVEL INSTANT MESSAGING SYSTEM ROBUST TO EAVESDROPPING OVER COMMUNICATION Joo-Im Kim and Ji Won Yoon Centre for Information Security Technologies (CIST) Korea University, Seoul, Republic of Korea {jooimkim, jiwon yoon}@korea.ac.kr