Hybrid Security System over Banking Transaction Maintance by a Meta Key

R.Rajavarman[a], Dr. T. Vetriselvi[b], S.Shiyamala Devi[c], R.Rithanika[d], and S.Saidharshini[e]

[a]
Assistant Professor, K.Ramakrishnan College of Technology, Trichy.
[b]Associate Professor, K.Ramakrishnan College of Technology, Trichy
[c,d,e] U.G Student, K.Ramakrishnan College of Technology, Trichy

Article History: Received: 10 January 2021; Revised: 12 February 2021; Accepted: 27 March 2021; Published online: 16 April 2021

Abstract: The cloud security is to get to the data by approved clients by anyplace and whenever idea. Here, the data encryption and key encryption procedures are utilized to get the data. Where, the data encryption will work under ECC (elliptical curve cryptography) algorithm, to lessen the data bits. It stores in public cloud. The key encryption method conveys by the honey encryption algorithm. This honey encryption algorithm stores the double encrypted key in the fog cloud and the garbage value returns to the unapproved personates. Here the private key will create to the receiver's E-mail ID associated with the registration. Indeed, even the sender won't know about the key which was created. On the off chance that the receiver side issue happens, the exchange get come up short and self-transaction happens.

Keywords: ECC(elliptical curve cryptography)algorithm, honey encryption algorithm, public cloud, fog cloud, data encryption, key encryption.

1. Introduction

Prior to arising the cloud computing, there was Client/Server processing which is fundamentally a unified stockpiling in which all the product applications, all the information and all the controls are lived on the worker side. Cloud security concern arises which both customer data and program are residing in provider premises[5]. In the event that a solitary client needs to get to explicit information or run a program, he/she need to associate with the worker and afterward acquire suitable access, and afterward he/she can do his/her business. Contrasted with conventional computing model, the cloud computing model appropriates computing undertakings on an enormous number of computers because of dangerous development of web information today [4].At that point after, appropriated registering came into picture, where all the PCs are arranged together and offer their assets when required.

In a cloud computing framework, there is a huge responsibility move. The test results demonstrate that the card level security utilized is safer and exceptional[9].Cloud storage innovation has been focused closer as an arising network storage innovation which is broadened and created by cloud computing ideas [1]. Nearby computers have no longer to do all the hard work with regards to run applications. Analysts everywhere on the world contribute colossally for the domain of keenness with the adage of whenever anyplace worldview[10]. This developing innovation is at the danger of safety necessities, for example, confirmation, secrecy, trustworthiness and non-renouncement [2].Authentication key arrangement protocols may employ either private or public key cryptography [7]. The lone thing the client's computer needs to have the option to run is the distributed computing interface programming of the framework, which can be just about as basic as a Web program and the cloud's organization deals with the rest.

2. Exsisting System:

In the development of security the user equipped with devices like mobile with mobile services from service provider in a efficient way. In this scheme, prove that you can control an adversary. The target user primary device he can incorporate to send the user server authentication. To avoid these problems we proposed scheme of key arrangement and protection of key.As particularly secure common verification plot between a portable client and the worker is likewise required. It is a double gadget confirmation plot (KAKP) .In KAKP the client furnished with two cell phones and the one is called ace gadget and another is called helper gadget. To execute a common confirmation with a worker, the client needs to use both two gadgets to produce a verification code. The security necessitates that an enemy can't pass the confirmation of the worker regardless of whether control both of the gadgets. It is known as two factor security yet KAKP neglects to accomplished that and it likewise bombs the two factor security. What's more, we demonstrate who an enemy is control whether the objective client essential gadget can create a substantial confirmation code to send validation of the administrations. At

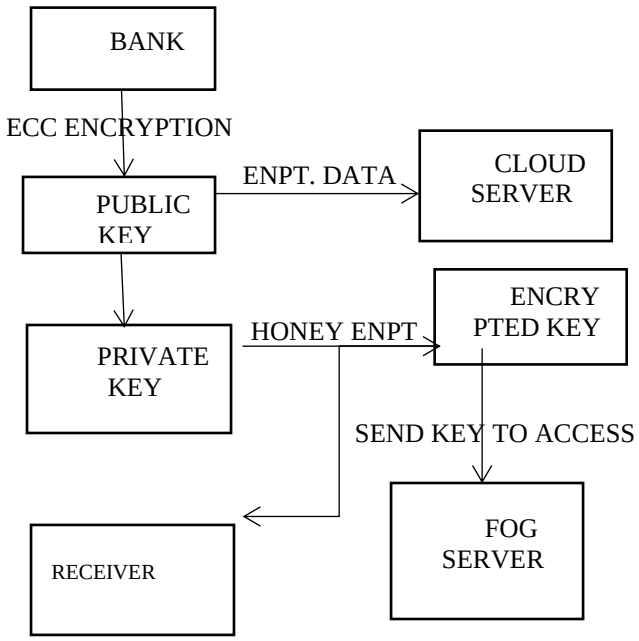
long last we have examined KAKP and exhibit that it neglects to accomplish the two factor security, an enemy who just controls client's lord gadget can imitate the client to pass the worker validation.The different smart card security issues are certification spillage assault, refusal of administration assaults, falsification assaults, shared validation, replay assaults, equal meeting assaults, reflection assaults, keen card misfortune assaults, client namelessness [10], disconnected secret word speculating assaults, taken verifier assaults, alteration assaults, worker parodying assaults, forward mystery and insider assault[6].

2.1 DISADVANTAGES:

- It fails to achieve two factor security.
- Unsecured data.
- Online transaction is insecure due to the hacking of customers data.
- Less efficient.
- Multiple login attack.

3.PROPOSED SYSTEM:

In banking system there are so many security measure to enhance them this hybrid cloud security system is used. The data is encrypted using two methodologies: Elliptical curve cryptography and honey encryption cryptography.



3.1 MODULE LIST:

- creation of an account.
- Filling up the details.
- Cloud storage.
- Transaction flow.
- Key encryption.
- E-mail connectivity

3.2 MODULE DESCRIPTION:

3.2.1 CREATION OF AN ACCOUNT:

In this system the user wants to register an individual account with the strong password. After the completion of registration the user have to login the individual account. Every bank creates an account to maintain the user data.

Registration of an account takes place to the user and bank. Here the login page for individual users with their password is created initially. Every bank creates an account to maintain the user data.

3.2.2 FILLING UP THE DETAILS:

User details are collected in the form and an individual account is created toevery user. Bank stores their details, which combines with the database.

The registered user details ate collected in the form and an individual account is created to every user by the bank. Bank stores their detail which combines with the database for further and future references.

3.2.3 CLOUD STORAGE:

Hybrid clouds are blend of public and fog (private) clouds. Here the public cloud is used for the storing of transaction data which can be view for both bank and the user and the private cloud is used for the storing of key values. This is a most complex clouding arrangement for the unauthorized users.

In this cross breed cloud the match of administrations from public cloud and private cloud greater chance to possess server farm it can without much of a stretch consolidate the advantages of all frameworks is a planned an explicitly for a necessities, it's adaptable and versatile as the business develops. The public cloud gives your moderate help while the private cloud part gives the undeniable degree of control and security.

3.2.4 TRANSACTION FLOW:

Bank needs the user's basic data like account number, name, IFSC code for secure transaction using elliptical curve cryptography encryption techniques. The transaction details are stored in the public cloud. The user can also view the transaction history for their reference.

The bank requires the user's basic data such as account number,name,IFSC code for secure transaction using Elliptical Curve Cryptography encryption techniques.In Elliptical Curve

Cryptography which means data to encryptso that lone approved gatherings can unscramble it .This has a few clear use cases yet is regularly used to scramble web traffic.Transaction details are stored in the public cloud. Users can view the transaction history for their reference.

3.2.5 KEY ENCRYPTION:

Here the key encryption takes place where the encrypted key is once again encrypted using the honey encryption algorithm to make that as private key. This algorithm used to return the garbage value to the impersonate users.

Here the encryption takes place for the secure transaction using Elliptical Curve Cryptography where the encrypted key is once again encrypted using honey algorithm (which will be stored in the local fog server) to make that as the private key . This algorithm ensures that is used to return garbage value to the impersonate users to the server. Key encryption purpose is to secure the user's transaction by using the private key.Here the encryption takes place for the secure transaction using Elliptical Curve Cryptography where the encrypted key is once again encrypted using honey algorithm (which will be stored in the local fog server) to make that as the private key . This algorithm ensures that is used to return garbage value to the impersonate users to the server. Key encryption purpose is to secure the user's transaction by using the private key.

3.2.6 E-MAIL CONNECTIVIY:

Private key generates a secret code to the receiver which is stored in the local fog server where the generated code is connected to the receiver's e-mail. This kind of transaction is highly secured where the encrypted secret code is sent only to the receiver for their safety and the code is stored in the fog cloud. If authentication is failed then self -transaction takes place.

3.3 ADVANTAGES:

- Easy to access their individual user account login
- It maintains high secure transaction between sender and receiver
- Only the users can login their individual account because of avoiding the multiple logins
- Customer data will be highly secured
- More efficient compared to the other systems

4. Algorithm:

- Elliptical curve cryptography
- Honey encryption algorithm

4.1 Elliptical curve cryptography:

Elliptic-curve cryptography is an approach to manage public-key cryptography subject to the arithmetical plan of elliptic curves over restricted fields. ECC allows more humble keys appeared differently in relation to non-EC cryptography to give indistinguishable security.To relieve the security issues and to improve the security highlights of keen card, the scientists accept that the joining of shrewd cards with biometrics and elliptic curve cryptographic calculations will convey various critical advantages to associations and all areas which require secure ID framework[3].Elliptic curve cryptography (ECC) is a public key encryption strategy dependent on an elliptic curve hypothesis that can be utilized to make quicker, more modest, and more proficient cryptographic keys. The innovation can be utilized related to most open key encryption strategies, like RSA and Diffie-Hellman.

Elliptic curve cryptography is an advanced public-key encryption procedure dependent on numerical elliptic curves and is notable for making more modest, quicker, and more productive cryptographic keys. For instance,

Bitcoin utilizes ECC as its asymmetric cryptosystem due to its lightweight nature.Elliptic-curve cryptography (ECC) is an approach to manage public-key cryptography reliant on the numerical plan of elliptic curves over restricted fields. ECC allows more humble keys appeared differently in relation to non-EC cryptography (considering plain Galois fields) to give indistinguishable security.

In light of the qualities given points, this will decide the state of the curve. Elliptical curve cryptography utilizes these curves over limited fields to make a mysterious that solitary the private key holder can open. The bigger the key size, the bigger the curve, and the harder the issue is to tackle.

4.2 Honey encryption:

In network security key distribution is major facing problem [8]. But here, honey encryption is a sort of information encryption that "delivers a cipher text, which, when unscrambled with an erroneous key as speculated by the aggressor, presents a conceivable looking yet off base plaintext secret phrase or encryption key."

It is a security instrument that makes it hard for an attacker who is doing a brute force attack to know whether they had accurately speculated a secret phrase or encryption key.

The working of the advancement of honey encryption is the design of the distribution transforming encoder. It maps the message to a seed range in a seed space. At that point it arbitrarily selects a seed from the reach and xor's it with the way in to the code text.

5. Result:

6. Conclusion:

The hybrid security system over banking transaction maintenance approach gives the next level on security in the bank transaction sector. This collaboration on the fog cloud and the public cloud gives the immense change in the security sector.

The double encryption method secures the data abundantly. This methodology is useful for both the user side and to the bank side. the garbage value generates to the third party is a dummy value where there will not be any belonging users.

Reference:

1. Yi-Wu;Xingjun-Wu, Implementation of efficient method of RSA key-pair generation algorithm, IEEE International Symposium on Consumer Electronics (ISCE), 2017
2. SarehAssiri, Key Exchange using Ternary system to Enhance Security, IEEE 9th Annual Computing and Communication Workshop and Conference (CCWC), 2019
3. Daisy PremilaBai T, Elliptic Curve Cryptography based Security Framework for Internet of Things and Cloud Computing, 2015
4. DiaoZhe ; Wang Qinghong ; Su Naizheng ; Zhang Yuhan, Study on Data Security Policy Based on Cloud Storage, ieee 3rd international conference on big data security on cloud (bigdatasecurity), ieee international conference on high performance and smart computing (hpsc), and ieee international conference on intelligent data and security (ids), 2017
5. EmanMeslhy, Data Security Model for Cloud Computing, 2013
6. AmitHendre ;KarunaPande Joshi, A Semantic Approach to Cloud Security and Compliance, IEEE 8th International Conference on Cloud Computing, 2015
7. Ari Juels, Honey Encryption: Encryption beyond the Brute-Force Barrier, IEEE Security and Privacy Magazine 12(4):59-62 • July 2014

8. Ningbo Li ; Tanping Zhou ; Xiaoyuan Yang ; Yiliang Han ; Wenchao Liu ; GuangshengTu, Efficient Multi-Key FHE With Short Extended Ciphertexts and Directed Decryption Protocol, IEEE Access, Vol:7, 2019
9. Wenjie Yang ; Shangpeng Wang ; Wei Wu ; Yi Mu, Top-Level Secure Certificate less Signature Against Malicious-But-Passive KGC, IEEE access, Vol:7, 2019
10. Zhen Wang ; Zhaofeng Ma ; ShoushanLuo ; HongminGao, Key Escrow Protocol Based on a Tripartite Authenticated Key Agreement and Threshold Cryptography, IEEE Access (Volume: 7), 2019