A COMPREHENSIVE REVIEW ON HYBRID MECHANISM FOR DATA SECURITY IN CLOUD USING ECC AND SHA ALGORITHMS

SUNANDA MORAMPUDI[1], Dr.CH.G.V.N. PRASAD[2]

1.Research Scholar,CSE, Rayalaseema University, Kurnool,A.P,nsunandapratap@gmail.com

2. Professor & HOD CSE, Sri Indu College of Engg & Technology, Hyderabad, Telangana, India, prasadch204@gmail.com

Abstract:

With a specific end goal to meet the ongoing necessities and condition, the cloud processing turn out to be most imperative asset for both industry and individual use. Subsequently, cloud processing is the most quickly developing innovation of the previous couple of years. This quick development of cloud registering prompts extreme security concerns, since security has a basic issue in the cloud processing, as the client/the supplier is the outsider and numerous clients are sharing a same cloud. One essential plan issue in the cloud security system is space many-sided quality of the security model ought to be less with a specific end goal to meet the portable clients, in light of the fact that a large number of the clients getting to the cloud by the advanced hand held gadgets. The primary issues of cloud figuring are information security, respectability ,verification and secrecy .To give the answer for these security issues distinctive algorithm and strategies has presented by various specialists yet every algorithm and method having their own particular benefits and faults. In this paper we have done the survey of various algorithms are SHA AND ECC algorithm.

Keywords: ***Elliptic Curve Cryptography, Elliptic Curve Diffie-Hellman, Elliptic Curve Integrated Encryption Scheme, Elliptic curve Digital Signature Algorithm, Verifiable Delegation (VD), Hybrid Encryption, SHA.***

I. INTRODUCTION

Cloud processing is the one of the outstanding field, which is one of the key asset in online applications. Cloud figuring is the innovation which incorporates Virtualization, parallel processing and disseminated registering. Cloud registering is approach to give assets on request; any asset can be utilize proficiently. Each cloud display comprises of certain model, attributes and organization models. The cloud isn't simply innovation which gives not only one administration but rather bundle of such a significant number of administrations. Cloud processing is having one key segment which is Internet; any administration can be access with the assistance of program. Administration arranged engineering is framed for having the cloud based administrations. The innovation isn't simply kept to programming yet additionally to equipment, any equipment can be gotten to. The advantage related with cloud administrations is that mind-boggling expense gadgets can be effectively gotten to.

Cloud figuring is the way toward giving administrations to client in as indicated by their need. All the substantial undertakings are putting resources into expansive sum keeping in mind the end goal to give cloud administrations. Amazon, Google, Windows are having their own particular administrations which is accessible to all clients so as to have productive recovery. In our overview it is finding that homomorphism encryption is one of the better encryption strategies however the best of all encryption method is elliptic curve encryption. In this work, the correlation of the two calculations is performed and result is delineated keeping in mind the end goal to demonstrate the elliptic curve cryptography as better encryption system.

Cloud figuring is a sort of superior registering, which incorporates disseminated processing, network registering and cloud registering. Network figuring (AbrishamiET AL, 2012) is a worldview of asset sharing which offers wide and aggregate circulated processing. For as long as couple of years, the cloud registering is one among top 10 developing innovation, which demonstrates a huge effect on IT later on. Because of this total development of cloud processing, security ends up basic issue. The security of the cloud processing contrast from organize security, in light of the fact that the client/the supplier is the outsider to each other and furthermore numerous clients are sharing a same cloud. Additionally the cloud are gotten to by numerous clients through their portable and handheld gadgets, subsequently the proposed cryptography ought to possess lesser memory space. Thusly, littler sizes of security keys are tremendously favored for encryption algorithm.

In the ongoing open key cryptography, factors deterioration issues in light of extensive numbers are generally utilized, for instance, RSA. With the advancement of PC equipment and elite figuring innovation, RSA has experienced a few troubles. In the circumstances, the cryptography in light of elliptic curve discrete logarithm issue shows up, whose open key is short, arrange data transmission is pretty much nothing and capacity to oppose to assault is solid.

Cloud registering understands the significance of information sharing and along these lines makes the segment keeping in mind the end goal to have greater possibility. Cloud is divided as open, private and hybrid cloud. Associations which need the private access which implies the capacity inside the surroundings are private cloud while if the capacity and administrations are permitted all through the encompassing then it is called as open cloud. There are sure business regions where there is need of administrations in both Environment which are in and out, subsequently for them hybrid cloud is utilized.

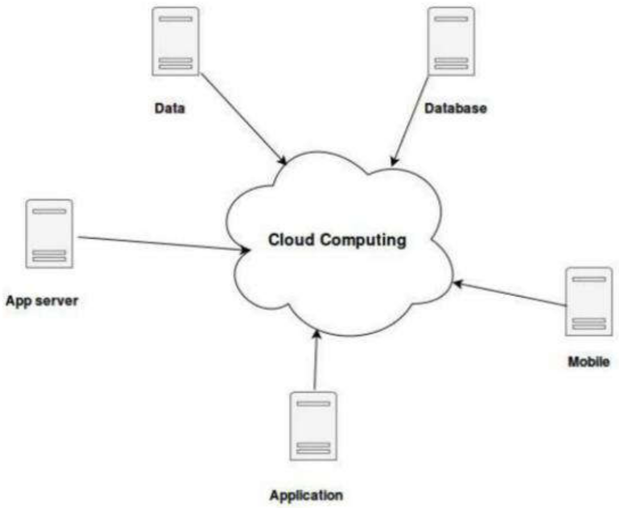


Figure 1. Cloud Computing

II. SECURITY ISSUES OF CLOUD COMPUTING

Cloud processing is a colossal accumulation of entomb associated organize. . There are such a significant number of hazard related with the cloud organize like information can be hacked by an unapproved individual. Information can be changed by outsider while exchanging [4]. The real issues identified with information security incorporate information uprightness, information accessibility, information classification, protection, straightforwardness of information [2] and control over information where information dwells. There are different viewpoints for giving information security, for example, by giving access controls and encryption strategies. The specialist co-op must guarantee that their foundation that giving is secure and customer's information stay ensured [3].On the side of customer, they should investigate the safety efforts identified with information that what are the security strategies are given by cloud supplier.

Some Security Policies in Cloud:

1. Authentication: Authentication is a vital worldview for cloud processing which can not change ever; here validation is critical to affirm the personality of client and framework through which client conveying. Outsider specialist organizations which are once in a while assailants, so the confirmation of character of the supplier is vital to check whether the specialist organization is aggressor or confided in seller. Verification oversees security hazard.

2. Confidentiality: Confidentiality is equivalent to security. A few measures are taken to anchor the data conveyance to wrong individual and ensuring that perfect individual will get the message. Approved individual has the privilege to get to the information. On the off chance that it falls under the hand of unapproved individual then the sum to harm can't be envisioned. Best case of secrecy is information encryption in which verification is a standard factor. For the transmission of delicate data client id and secret word is vital for confirmation and encryption of that information makes privacy.

3. Availability: Maintenance of equipment is additionally essential so to play out the right working of working framework. Repair of equipment not working great will spare time when the equipment is required. Security against information misfortune is essential and interference in association can be prompt calamity occasion like fire. Which is the motivation behind why support of equipment is imperative?

4. Integrity: Integrity remains for precision, implies information can't be modified at the season of transmission by unapproved individual. Modification of information is the action done by unapproved individual when information transmits. They make mistake or erase some essential information.

III. Literature of review

Vast number of algorithms and strategies are in the writing and gives a vibe that Cloud stockpiling security is standard research subject among the analysts. Hybrid encryption algorithm utilizing symmetric encryption with inserting low regular codec[1].Data end up arbitrary code in nature when it is out, the main path from which the data proprietor can recuperate the same. As cloud framework stockpiling more inclined to data spillage at inward division in this way the creators proposed to utilize checksum + square size to isolate information from client work force data. This not just limits maintenance of data in the meantime it guarantees information security by isolating some key data. The entire work process is contains two sections. They are putting away stage and information sending out stage, Checksum 1 and the Timestamp would be kept in customer condition of framework. After that second checksum is figured and added to square size. Next, the irregular vector is included in this manner Random code with Checksum 2 and Block measure is transmitted to transmission module. Next, session id is added to send transferring solicitation to server. Server gives new storage room utilizing capacity controller. For recovery information is decoded first and tried for Checksum 1 and Timestamp. On the off chance that it coordinates at that point advance decoding happens utilizing private key [2].

Cloud stockpiling classification insurance framework with cloud encryption and muddling strategy. Obscurity strategy to enhance the information secrecy in cloud framework stockpiling. They have demonstrated that encryption and jumbling strategy should be possible at customer closes. They proposed database outsourcing model which will assist client with utilizing information effectively as a bring together capacity. Checking DBMS is hard as it is conveyed among various hardware's. In this manner, security turns out to be enormous worry in numerous virtual machines as we can get to database without anybody seeing or setting off any alert[3].Malicious individual can utilize circumstance on his hand and damage necessary database framework in danger. Every one of the information must be scrambled or muddled before it is sent to the cloud database. For the customer, it is giving consent by giving the required data unscrambling/disentangles keys [4].

Security show for processing reason utilizes diverse servers and each server performs same calculation in the network[5].To get trustworthiness of data server will register SHA-1" lastly server scrambles the information utilizing AES to keep up secrecy of information. At long last information is scrambled utilizing AES to guarantee privacy.

To ensure information on the cloud utilizing meta-information [6, 7] the proposed method gives age of figure utilizing Meta information. It relies upon number of qualities in meta-information and algorithm utilized. There are two principle highlights: Generated key can't be settled without relationship of client and Meta information stockpiling server and Key created utilizing holiday arrange hold useful for the torrential slide impact. It requires investment to create figure key.

With this daily paper, a great many people gave an outline in regards to scrambled shield in regards to resemble the other alike utilizing AES in addition to vision cryptanalysis [8]. The samara has been purchased from the entire picture attributes in addition to the AES-256 convention was used to have the capacity to make the fundamental gainful for your realistic encoded shield as per the expelled key. The convention is extremely a symmetric block figure in which consume basic measurements in regards to 128, 192 in addition to 256 pieces, together with data oversaw inside 128-piece clog[9]. The specific pixel knows significance from the photos to for the most part be secured has been ensured utilizing n-share vision cryptographic procedure. The specific scrambled shield strategy experienced for all intents and purposes no takeoff with respect to pixel goals through the whole procedure. The 128 little gravestone will then be enlarged a few 44 blog entries with respect to 32 lumps Guide 4 unique terms program like a flyer fundamental for each around; basic motivation influences utilization of your S-to box. The procedure is made of 3 layers? Straight line Diffusion, Non-direct Diffusion .The 128 minimal basic will at that point be broadened a few 44 blog entries with respect to 32 pieces terms; 4 unique terms be an around basic for any around; basic motivation would depend about the S-box. AES just leaks deter almost no help each blend of data in addition to basic sizes in regards to 128, 192, in addition to 256[10] sums.

All things considered, AES essentially empowers the 128 little data time-traverse which can be part straightforwardly into various standard business mind hinder Each blend is created by AES and make utilization of different circuits in regards to foreordained campaigns to accomplish perfect profitability which thusly can help decide it has the insurance degree that is unquestionably tried inside expression with respect to scattering (strict deluge prerequisites (Sac)) in addition to bewilderment consequently the quantity of circuits have a tendency to be picked inside a your convention gives the Theca esteem. The basic style in addition to muscle of the encryption convention this kind of with respect to example AES will be reliant about dispersion in addition to mind disarray. This included utilization of Innovative File encryption convention in addition to vision cryptography inside getting criminological biometric pictures.

The proposed game plan recommends an alternate strategy for how the records are put away from the swarm by utilizing the current en-tomb particle technique and swarm processing framework [11]. Most medication client is positively not happy by realizing that their amazingly private or classified records could be gotten to for grouped purpose with the cloud Waiter supplier. This might be for support purposes, authentication string claims or just general document reinforcement physical procedures. Typically, these grounds are finishing legitimate with an end goal to ensure the cloud Waiter status and execution. In any case, clients are frequently unwilling to transfer their classified records into cloud servers [12]. This proposed framework intends to fill this leap forward giving an abnormal state level of record security. RSA is known to be the best openly accessible encryption strategy. This algorithm blends with both private key and open key. The main strategy for decoding the documents which have been scrambled with the populace key is to utilize the non-open key. Clients record may be encoded just before the transfer procedure towards the cloud Server. Precisely the scrambled document may be transferred towards the Server. This proposed framework aim to fill this hole by giving an expert measure of single file organizer security. RSA is known to be the best prevalently accessible encryption strategy acting. This algorithm works with both private key and open key. To get of decoding the records which have been encoded with the general population key is with the individual key [13, 14]. Exploiter document may be encoded just before the transfer activity on the cloud Waiter. The scrambled document may be transferred on the host.

Security show that contain three parts: cloud controller, client and associated hubs. Postpone estimation was performed based on the demand and reaction time amid document transfer. Framework they proposed is based on online record handling framework comprises of web application [15]. They utilized 128 piece AES encryption, where encryption comprises of 10 rounds for 128-piece keys. The records are part into various lumps which rely upon document estimate. At that point specific squares are scrambled independently and afterward after square shrewd encryption each square are transferred to cloud at various areas with various id and square id. In the event that somebody like cloud supplier, endeavor to achieve composed records totally from the server, they won't get entire information, since it put away at various areas and in addition are in scrambled shape [16]. Thus the person who knows mystery key can recover information back. Web based altering is permitted in the proposed framework, information can be changed without downloading the contain. Nature of administration is kept up to decrease postpone in the transferring [17]. The postponement is immeasurably unique in accordance with the span of web information being prepared. Over that, kinds of variables which influence delay inside the framework: organize speed is critical yet one basic viewpoint amid real time execution. 128 piece AES cryptographic encryption is utilized as a part of these to give genuineness, classification, and access control. At that point execution of proposed approach was dissected in light of postponement [18], there's intense surge in delay with surge in record estimate. Client is validated utilizing secret key check.

K.Sekar and M.Padmavathamma et al proposed investigation of encryption in enormous information in cloud environment[19]. The key security issues of huge information are close verification level, information level, arrange level and bland level issues. Of these levels, we have chosen you're the outcomes level issue. In huge information, insights is very fundamental part. Information facilitated via web-based networking media destinations is extremely fundamental for a venture which is frequently inside people in general utilize or private zone. Information Con-fidentiality, Security, honesty and accessibility is really a noteworthy test as of this degree[20]. It changes over information into mystery message utilizing encoding algorithms. There are bunches of algorithms like AES, RSA, and DES. These algorithms utilize private insider facts to scramble information and decode information. Encryption is led for the information sent from supply and decoding is led before the information is gotten. For encryption and decoding process, two instance of algorithms are broadly utilized i.e., symmetric and unbalanced algorithms. Information En-cryption Standard algorithm utilizes the nothing Francis Scott Key called feistily square mystery code. The capacity connected to tolerating the plain content and key plan decides the sort of figure. It utilizes "64-bit square figure" for encoding and decipherment which is in this way known as Symmetric. Encoding and unscrambling symmetric key subtle elements are moderately easy to do.Encrypting and decrypting symmetric key details are relatively simple to do. Many of the solid state drives use symmetric key encryption for internal reposting of data. This algo-rithmic program performs a lot better than unencrypted traditional hard drives.

Dta storage techniques for efficient and intelligent storage using data replication. Several new techniques are adapted to optimize the present generic architectures for developing softwares are as explained by the authors [21].

SHA ALGORITHMS

SHA and MD5 is used for message digest algorithm same as the older MD4.SHA and MD5 both use for calculate hash value. In proposed system we are using SHA algorithm with blowfish algorithm. Blowfish algorithm for encryption and decryption and SHA use for calculating hash value of file which is uploading by user on cloud server.

The Secure Hash Algorithm takes a message of less than 264 bits in length and produces a 160-bit message digest which is designed so that it should be computationally expensive to find a text which matches a given hash. ie if you have a hash for document A, H(A), it is difficult to find a document B which has the same hash, and even more difficult to arrange that document B says what you want it to say.

SHA-1 produces a 160-bit hash value which is renders in a 40-digit-long hexadecimal form. It has a message digest strength of 80-bit [2], [4]. Several examples are given to understand how actual data is encrypted. For example, the statement for SHA-1 is given as “The quick brown fox jumps over the lazy dog” then hexadecimal form will be “2fd4e1c67a2d28fced84fced849ee1bb76e7391b93eb12”. Any kind of string less then size of 2□□-1 bits size can be converted into a hexadecimal form of 40 digits. Even a blank string can also be converted into a 40-digit hexadecimal form.

- Each variable are unsigned 32-bit.
- Message length is 64-bit and message digest is 160-bit.
- Constants are assumed in Big-endian format.
- H0, H1, H2, H3, H4 are variables which are initialized with some hex value.
- msgL = message length.

The process for the Algorithm is given below, which describes the bit process of the SHA algorithm in general form: SHA – 1 and SHA – 2. SHA – Analysis Expanding nature and compression functions are different or Both SHA-1 and SHA-2 hash algorithms. This makes difference in their efficiency, vulnerability to attacks as well as block size. Highest message size which can be encrypted is also different. SHA-1 uses more number of packets with short number of operation than SHA-2. This makes SHA-2 more efficient than SHA-1.

SHA ANALYSIS

Bits provided for security purpose are less than 80 which makes attacks easy in SHA-1. It is also easy to break it using brute force attack and collision attack [2]. SHA – 2 has more than 80 security bits, especially in SHA – 384 and SHA – 512.

SHA – 512 has a packet size of 1024 bits and 80 packets, and the Rotation and Shift operations are also different from other

SHA – 2 algorithms. The bits for security are less than any other SHA – 2 algorithm in SHA – 512. On the other hand, it has maximum efficiency with comparatively high vulnerability [2], [3], [5].

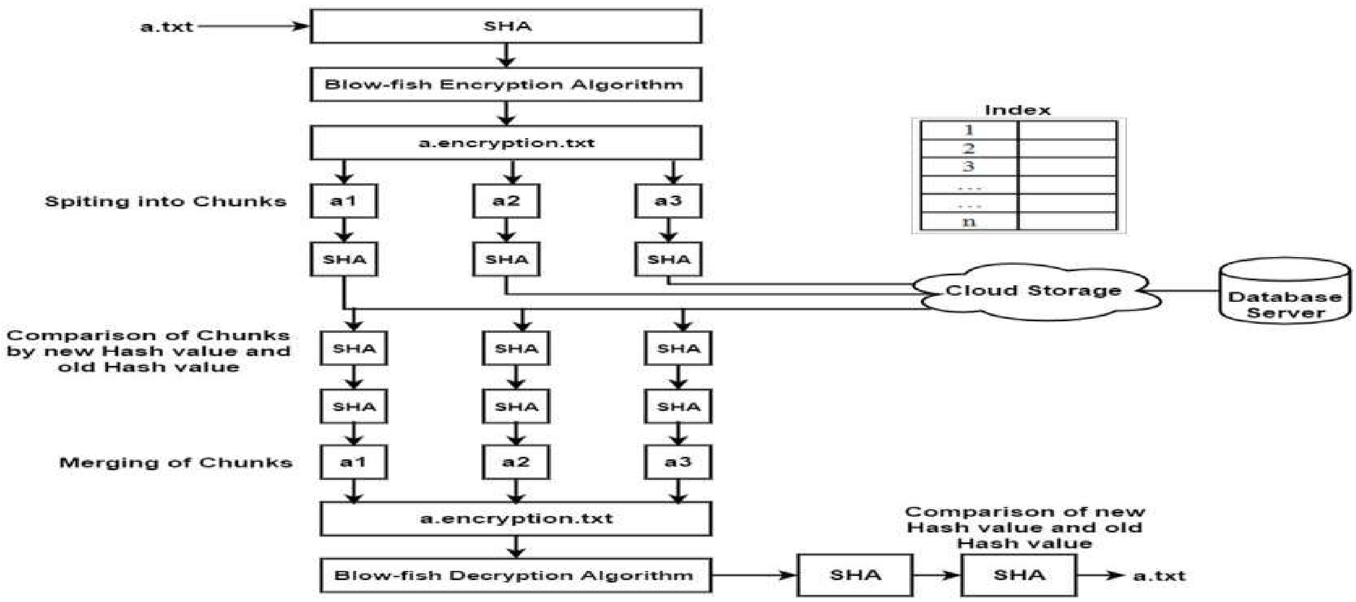


Figure 2 System using Blowfish and SHA

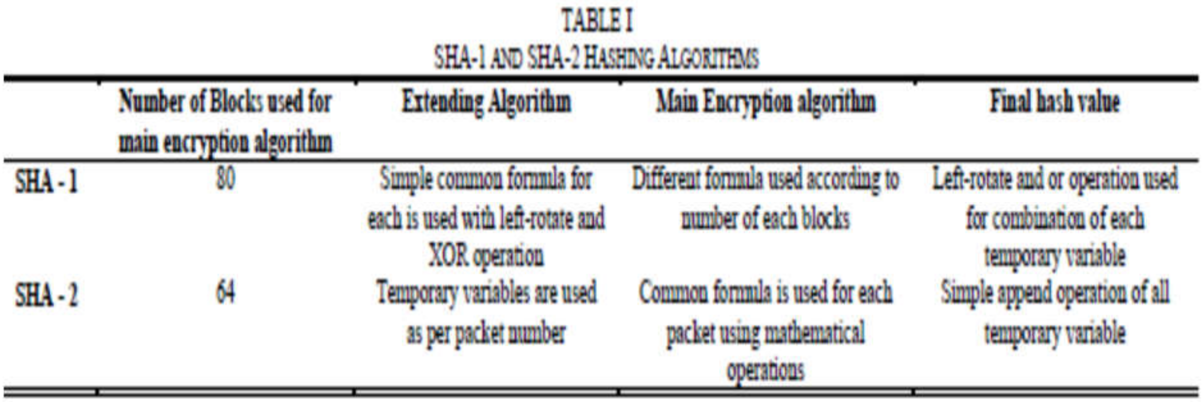
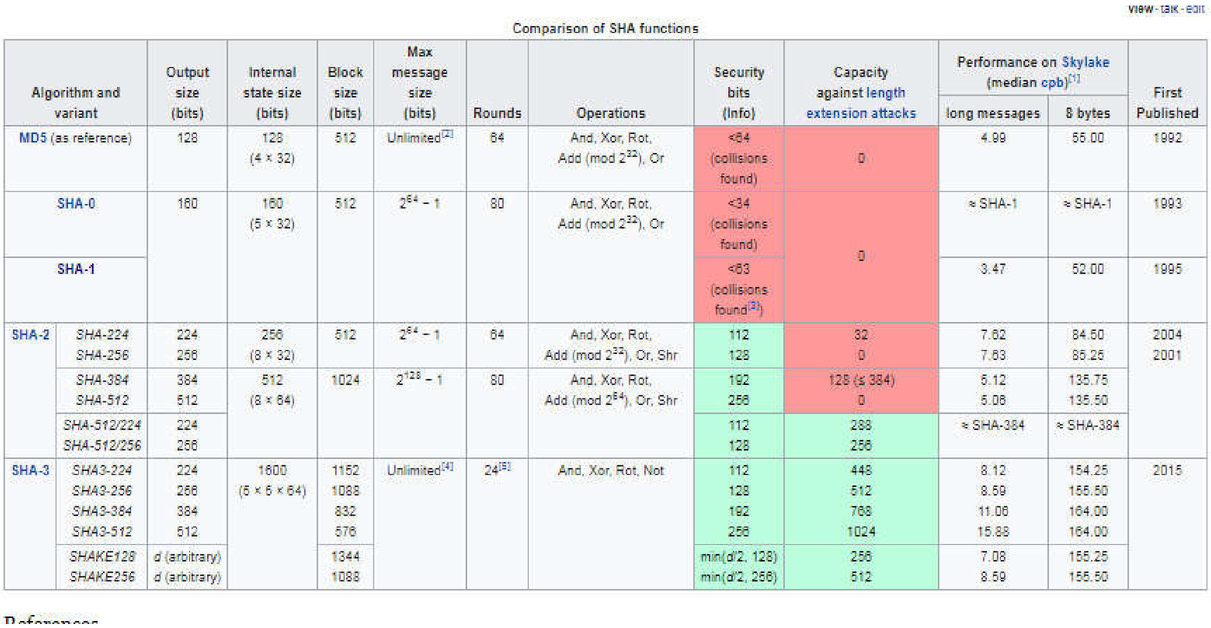


TABLE I
SHA-1 AND SHA-2 HASHING ALGORITHMS

	Number of Blocks used for main encryption algorithm	Extending Algorithm	Main Encryption algorithm	Final hash value
SHA - 1	80	Simple common formula for each is used with left-rotate and XOR operation	Different formula used according to number of each blocks	Left-rotate and or operation used for combination of each temporary variable
SHA - 2	64	Temporary variables are used as per packet number	Common formula is used for each packet using mathematical operations	Simple append operation of all temporary variable

TABLE II:COMPARISION SHA FUNCTIONS



view · talk · edit

Comparison of SHA functions

Algorithm and variant		Output size (bits)	Internal state size (bits)	Block size (bits)	Max message size (bits)	Rounds	Operations	Security bits (Info)	Capacity against length extension attacks	Performance on Skylake (median cpb)[1]		First Published
										long messages	8 bytes	
MD5 (as reference)		128	128 (4 × 32)	512	Unlimited[2]	64	And, Xor, Rot, Add (mod 2^{32}), Or	<64 (collisions found)	0	4.99	55.00	1992
SHA-0		160	160 (5 × 32)	512	$2^{64} - 1$	80	And, Xor, Rot, Add (mod 2^{32}), Or	<34 (collisions found)	0	≈ SHA-1	≈ SHA-1	1993
SHA-1								<63 (collisions found[3])		3.47	52.00	1995
SHA-2	SHA-224 SHA-256	224 256	256 (8 × 32)	512	$2^{64} - 1$	64	And, Xor, Rot, Add (mod 2^{32}), Or, Shr	112 128	32 0	7.62 7.63	84.50 85.25	2004 2001
	SHA-384 SHA-512	384 512	512 (8 × 64)	1024	$2^{128} - 1$	80	And, Xor, Rot, Add (mod 2^{64}), Or, Shr	192 256	128 (≤ 384) 0	5.12 5.06	135.75 135.50	
	SHA-512/224 SHA-512/256	224 256						112 128	288 256	≈ SHA-384	≈ SHA-384	
SHA-3	SHA3-224 SHA3-256 SHA3-384 SHA3-512	224 256 384 512	1600 (5 × 5 × 64)	1152 1088 832 576	Unlimited[4]	24[5]	And, Xor, Rot, Not	112 128 192 256	448 512 768 1024	8.12 8.59 11.06 15.88	154.25 155.50 164.00 164.00	2015
	SHAKE128 SHAKE256	d (arbitrary) d (arbitrary)		1344 1088				min(d/2, 128) min(d/2, 256)	256 512	7.08 8.59	155.25 155.50	

IV. ECC ALGORITHM

The emerging expansion of the information systems has made revelatory advances in the cryptographic systems to provide the data confidentiality and integrity. Elliptic Curve Cryptographic (ECC) technique is emerging as an alluring public-key cryptosystem. Unlike familiar cryptosystems like RSA, ECC ensures same level of security with smaller keys. Thus, it provides faster computation, less memory and bandwidth savings.

The proposed work uses Secure Hybrid Encryption using ECC to overcome the limitations of Xu et al. scheme. ECC is a public-cryptosystem defined over finite fields on the basis of algebraic structures of the elliptic curves. The Elliptic curve cryptography is defined on the supposition that the elliptic curve discrete logarithm problem (ECDLP) is very difficult. ECDLP is determining the integer k, given a rational point P on the elliptic curve E and the value of ‘k*P’[4][5]. Elliptic curve cryptosystems rely on the hardness of solving the ECDLP.

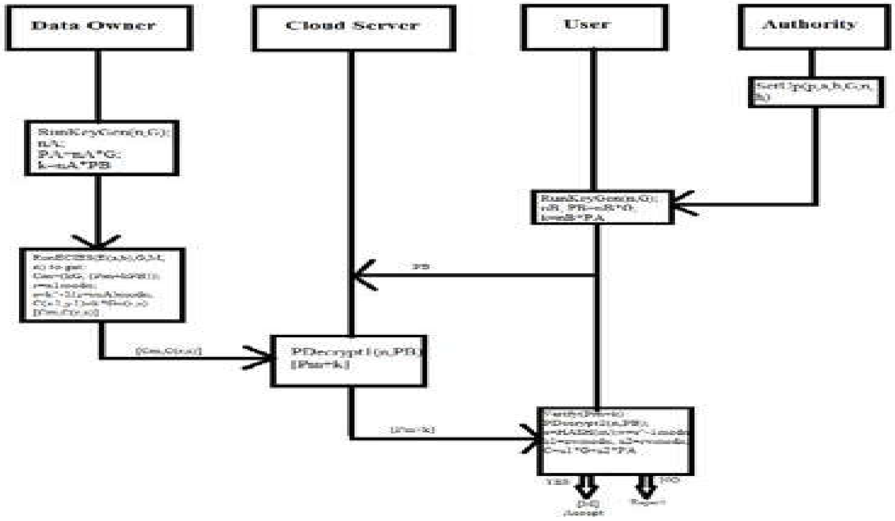


Fig: Architecture of Secure Hybrid ECC scheme

The ALGORITHM work consists of the following 5 phases:

A. *SetUp phase*

To work with ECC, all the users must agree upon the elements defining the curve. These are called as "Domain Parameters"[6]. They are 6 distinct values : (p, a, b, G, n, h) defined as:

p : Prime numbers defining the field in which curve operates

a, b: Integer co-efficients of the curve

G : Generator

n : Order of G (Curve Generator Point)

h : Co-factor of curve

Authority ensures that all the users agree on the domain parameters.

B. *Key Generation Phase*

After agreeing on the domain parameters, a shared Secret key is produced using Elliptic Curve Diffie-Hellman (ECDH) to form a secure communication channel. ECDH is the elliptic curve analog of the Diffie-Hellman key exchange. It is an anonymous key agreement protocol used to form a shared secret through an unsecured channel. This shared secret is shared across two parties who have elliptic curve public-private key pair [4]. The sender will encrypt the messages using public key of receiver and the receiver will decrypt it using his/her private key.

The shared secret between the data owner and the user is formed as follows [6] [8]:

(i) A selects an integer ' an<n '. This will be A's private key. Then, he generates public key as "PA = nA * G ".
B similarly selects private key 'nB' and computes public key "PB".

(ii) Now, A generates the secret key as:
" K = nA * PB ". And, B generates the secret key as: " K = nB * PA ".

The shared secret is then used for further communication. This is proven to be secure as no party can derive the private key unless they can solve ECDLP.

C. *Encryption Phase*

Elliptic Curve Integrated Encryption Scheme(ECIES) is used for encrypting and decrypting the messages. ECIES combines elliptic curve asymmetric encryption and AES symmetric encryption algorithm with SHA-1 hash algorithm as such to provide ease of using encryption scheme along with authentication support[5]. The plain text 'M' is converted as a point 'Pm' on the elliptic curve Ep(a, b) so that 'nG = O' is a large prime number for the smallest value of n. The Generator G and Ep are made public[8]. To transmit a message 'Pm' to B, A selects a random positive integer 'k' and yields the cipher text comprising of a pair of points

"Cm = (kG, (Pm + kPB)) ".

D. *Decryption Phase*

To decrypt the message, B first multiplies the foremost point of cipher text by B's secret key and then deducts the result from the second point. This gives the original message 'M'.

"M = ((Pm+kPB) – (nB (kG))) "

The decryption phase comprises of two partial decryptions i.e., PDecrypt1 at the cloud server and PDecrypt2 at the user to obtain the original message. A has concealed the message Pm by adding kPB to it. As the value of k is unknown, even though PB is a public-key, it is hard to unmask 'kPB'.

E. *Authentication Phase*

Elliptic Curve Digital Signature Algorithm (ECDSA) is used to provide authentication. It is a variant of the Digital Signature Algorithm using the elliptic curve cryptography. The signatures are created and verified using it. To provide a security of 80 bits, ECDSA would require a 160-bit public key whereas other DSA would require at least 1024-bit public key[5][9]. This shows that an attacker have to perform 2^80 operations to find out the private key. ECDSA comprises of Signature generation and verification algorithms to provide the authentication.

(i)*Signature Generation:* Suppose A wants to transmit a signed message to B, first they must coincide on the curve parameters (E, G, n). Now, for A to sign a message, it proceeds as follows[6][7]:

a. Calculate e = HASH (m).
b. Assume 'z' to be the Ln leftmost bit of e where Ln is the bit length of group order n.
c. Select a random integer 'k'.
d. Calculate the point on the curve C(x1, y1) as C = k * G.
e. Calculate "r = x1modn". If r = 0, then select another 'k' and repeat.
f. Calculate "s =k^-1(z + r.nA)modn".
 If s = 0, choose another 'k' and try anew.

The pair " (r, s) " is the signature Using this signature pair, A signs the message.

(ii)*Signature Verification:* To check the validity of the signature, B first checks that[6]:

- Public key (PA) is not equal to O.
- PA lies on the curve.
- n * PA = O.

This is done to confirm that the public key of A is a valid curve point or not. Then to verify the signature, B does the following[6][7]:

a. Verify that 'r' and 's' are integers in [1,n-1].
b. Calculate e = HASH (m).
c. Assume 'z' to be the Ln leftmost bit of e.
d. Calculate w = s^{-1} modn.
e. Calculate u = (zw) mod n and
 u2 = (rw) mod n .

f. Calculate the point on the curve C(x1, y1) as C = u1*G + u2*PA.
g. The signature is a valid one if r = x1modn i.e., if

C = k*G.

Thus signing a message and verifying it using the points on the curve makes it hard to break it.

The scheme (Fig:) works as follows:

1. First of all, Authority runs SetUp algorithm so that all the parties agree on the same domain parameters.
2. Then, KeyGen algorithm is run at the data owner and the user to form a shared secret key for further communication.
3. If the data owner wants to upload a file, he runs the encryption algorithm and the signature generation algorithm to encrypt the data and to provide authentication.
4. The user who wants to access the data, sends a request for data along with his public key to the cloud server.
5. Then, the cloud server partially decrypts (PDecrypt1) the data using the user's public key. The decrypted message with signature is sent to the user.
6. The user then decrypts (PDecrypt2) the data and verifies the signature using signature verification algorithm. If the user is authenticated, then he has the access to the data.

CONCLUSION

Security of information and trust downside has perpetually been an essential and troublesome pickle in cloud figuring. The proposed show enhances the security issues identified with cloud models and insurance of record trading is explained. The previously mentioned show is productive in information as an administration, which can be reached out in their administration models of cloud. Issue of existing algorithm has been fathomed by ECC and Secured Hash Algorithm (SHA).Implementation of proposed utility, which processes hash estimations of documents at the information proprietor feature, can dispense with the need of third event inspectors. The ensuing hash esteems from this utility are put away at secure territorial hash store. The data document can be recovered again every time required and checked for any contentions among occasions stressed by utilizing re-processing and coordinating the hash impact with the pre-registered hash esteem.

REFERENCE:

1. Patel and M.B.Chaudhari,' DATA SECURITY IN CLOUD COMPUTING USING DIGITAL SIGNATURE', International JournalFor Technological Research In Engineering Volume 1, Issue 10,PP.1177-1180, June-2014 .
2. B. Nayak, Sudhansu Ranjan Lenka,'Enhancing Data Security in Cloud Computing using RSA Encryption and MD5 Algorithm ',,IJCST,Volume 2 Issue 3, pp.60.-64,June-2014
3. Deepika Verma, K. Mahajan,' To Enhance Data Security in Cloud Computing using Combination of Encryption Algorithms',International Journal of Advances in Science and Technology (IJAST), Vol 2, Issue 4 ,pp.41-44,December 2014
4. . R. Pal Singh,' Enhanced Cloud Computing Security and Integrity Verification via Novel Encryption Techniques', SSRG InternationalJournal of Mobile Computing & Application , volume 2, Issue 3 ,pp.38-44,June 2015
5. Jie Xu, Qiaoyan Wen, Wenmin Li and Zhengping Jin, " Circuit Cipher-text-Policy Attribute-Based Hybrid Encryption with Verifiable Delegation in Cloud Computing" in Proc. IEEE Transactions on parallel and distributed systems, 2016. [2] K. Kurosawa and Y. Desmedt,"A New Paradigm of Hybrid Encryption Scheme," in Proc. CRYPTO, pp.426-442, Springer-Verlag Berlin, Heidelberg, 2004.
6. Vishwanath S Mahalle, Aniket K Shahade," Enhancingthe Data Security in Cloud by Implementing Hybrid(Rsa&Aes) Encryption Algorithm", 2014 IEEE.
7. Syed rizvi, Katie cover, Christopher gates, "A trustedthird party(TTP) based encryption scheme for ensuringdata confidentiality in cloud environment", ProcediaComputer Science 36 (2014) 381 – 386, Elsevier**.**

8. Deyan Chen and Hong Zhao “Data Security and Privacy Protection Issues in Cloud Computing” 2012 IEEE International Conference on Computer Science and Electronics Engineering.
9. Tumpe Moyo and Jagdev Bhogal “Investigating Security Issues in Cloud Computing” 2014 Eighth International Conference on Complex, Intelligent and Software Intensive Systems.
10. Babitha.M.P and K.R. Ramesh Babu,” *Secure Cloud Storage Using AES Encryption*” published in International Conference on Automatic Control and Dynamic Optimization Techniques (ICACDOT),International Institute of Information Technology (I²IT), Pune 2016**.**
11. Alexa Huth and James Cebula ‘The Basics of Cloud Computing’, United States Computer Emergency Readiness Team. **(2011)**.
12. Anitha Y, “Security Issues in cloud computing”, “International Journal of Thesis Projects and Dissertations “(IJTPD) Vol. 1, Issue 1, PP :(1-6), Month: October 2013.Maurich Ingo, Heberle Lukas, G¨uneysu Tim, ”IND-CCA Secure HybridEncryption from QC-MDPC Niederreiter”, 7th International Workshopon Post-Quantum Cryptography, Vol.9606, (2016), pp.1–17.
13. Usman Muhammad, Ahmed Irfan, Aslam M Imran , Khan Shujaat, Shah Usman Ali, ”SIT: A Lightweight Encryption Algorithm forSecure Internet of Things”, arXiv preprint arXiv:1704.08688, (2017).
14. MDawahdeh Ziad E , Yaakob Shahrul N ,bin Othman, Rozmie Razif,”A New Image Encryption Technique Combining Elliptic Curve Cryptosystemwith Hill Cipher”, Journal of King Saud University-Computerand Information Sciences, (2017).
15. Kumar S.K.S. and P. Balasubramanie. 2012. Dynamic scheduling for cloud reliability using transportation problem. J. Comput. Sci. 8: 1615-1626, DOI:10.3844/jcssp.2012.1615.1626.
16. Marc Stevens (June 2012). "Attacks on Hash Functions and Applications" - PhD thesiS