International Journal of Engineering & Technology, 7 (4.19) (2018) 186-188

International Journal of Engineering & Technology

Website: www.sciencepubco.com/index.php/IJET

Research paper

Hyper Elliptic Curve Cryptography (HECC) to Ensure Data Security in the Cloud

K.Nagendran[1*], N.Thillaiarasu[2], P.Chandrika[3], R.Chethana[4]

[1 3 4] Assistant Professor, Sri Krishna College of Engineering and Technology, Coimbatore - 641008
[2]Assistant Professor,SNS College of Technology Coimbatore,India-641107
**Corresponding Author E-mail: [1]knagendrancse@gmail.com*

Abstract

In today's technological world, cloud computing is emerging as a trendsetting information technology service for storing data and resources and retrieving them from the Internet rather than direct server connection. This technology also enables users to save them in a remote database. But the main concern with this technology is about the security of data stored in the cloud. Since users rely on third party services for data storage, they are highly vulnerable to attacks and data exploitation. Cloud services offer a multitude of security tools to safeguard user data but they face some disadvantages like data leakage, denial of service, eavesdropping, lack of safety standards etc., This paper proposes a efficient method for safeguarding cloud data through Hyper elliptic curve cryptography (HECC). The proposed cryptographic technique offers effective encryption and decryption of data in the cloud.

Keywords: *Data Security, Hyper elliptic curves, Encryption and Decryption.*

1. Introduction

Cloud computing is an approach of sending mechanical administrations in which the information and assets are recovered from the web through online apparatuses and applications, as an option in contrast to an immediate server association. Cloud-based capacity makes it conceivable to spare them to a database remotely as opposed to keeping documents on a restrictive hard drive or a nearby gadget for capacity. For whatever length of time that an electronic gadget can get to the web, it can access to the information and the product projects to run it. With the utilization of distributed computing, we can dispose of the obstacles looked in introducing, designing, anchoring, testing, running, refreshing and keeping up the equipment and programming that accompany putting away our own information, since we're not keeping up the equipment and programming. It swings to be the duty of a cloud benefit merchant. It gives a mutual foundation which implies it fills in as an utility, where the client needs to pay just for what they require and the updates are programmed which likewise empowers scaling up or down is simple.

2. Cloud Based Services

Some of the cloud services offered are "Infrastructure as a Service(IaaS), Platform as a Service (PaaS), Software as a Service (SaaS) and Storage as a Service (SaaS)"[5-9].

2.1. Infrastructure as a Service

Infrastructure as a Service provides an instant infrastructure service which helps us to avoid complexities in buying physical servers and datacenters. An IaaS can offer support for Testing and development, hostingwebsites, backup storage and recovery, Web applications, High-performance computing and big data analysis.

2.2. Platform as a Service

Platform as a service (PaaS) includes the entire deployment service in the cloud, which includes resources that can deliver everything from simple cloud-based applications to enterprise applications. PaaS provides services like middleware, Business Intelligence tools and database systems in addition to infrastructure.

2.3. Software as a Service

Software as a Service refers to the method of accessing software provided by the cloud service provider which manages the software according to the service agreement. SaaS provides benefits such as cross device compatibility, no hardware setup cost, scalable usage and automatic updates.

2.4. Storage as a Service

Storage as a Service is a model of providing storage infrastructure for managing backups, hardware and physical space. Storage as a Service is used by organizations to diminish risks in disaster recovery, to provide long-term adaptability and to increase business availability and continuity.

3. Challenges in Cloud Security

Cloud computing is emerging as a growing technology widely implemented in most of the organisations and companies. But it also puts forth a number of security challenges which jeopardize

user's sensitive data and resources. Some of the major challenges are

3.1. Distributed Denial of Service Attack

Distributed denial of service attacks are mainly targeted on SaaS cloud services where the website servers are altered to be irresponsive to user requests. This results in revenue loss, loss of customer trust and brand status

3.2. Vulerable Access Points

The main feature of cloud computing is that it can be accessed from any place from any device. This requires the APIs and the interfaces to be compatible with all environments. Hackers often exploit cloud services through loopholes in APIs and interfaces which act as a access point.

3.3. Contingency Planning

Having cloud services as the primary source of storage of critical and sensitive data, the possibilities of data breach and compromises in data availability are of high chance. Companies and users need to be aware of the security services provided by the cloud provider and should be prepared to face such circumstances to retrieve data without compromisation.

4. Hyper Elliptic Curve Cryptography in Cloud Security

Hyper elliptic curves are similar elliptic curves and are well suitable for cryptography. These algebraic curves are a generalisation of elliptic curves. The equation of a hyper elliptic curve C of 'g' genus over k field is given by

C: $y^2 + h(x)y = f(x)$

where

h(x) - a polynomial of degree $\leq$ g over F

f(x) - a monic polynomial of degree 2g+1 Over F

The proposed model implements the encryption of the document in the side of the data owner by using hyper elliptic Curve Cryptography (HECC)

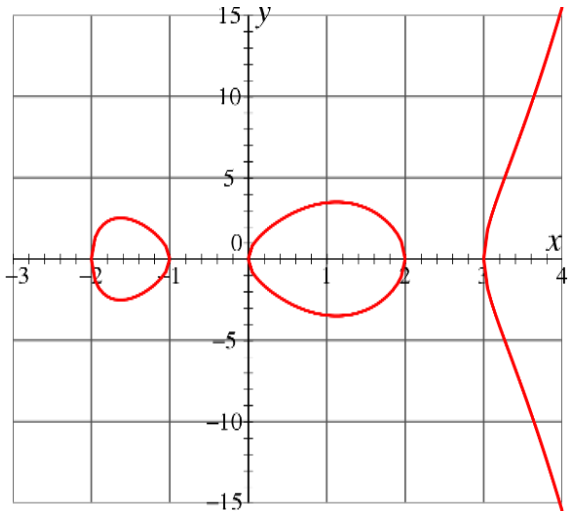

Fig. 1: Hyper elliptic curve

Hyper elliptic curve cryptographic technique [HECC] is an asymmetric public-key cryptographic technique which involves the usage of a public key and a private key. Every user has a public-private key pair. Private Key is used for decryption or signature generation whereas Public key is used for encryption/ verification of signature.

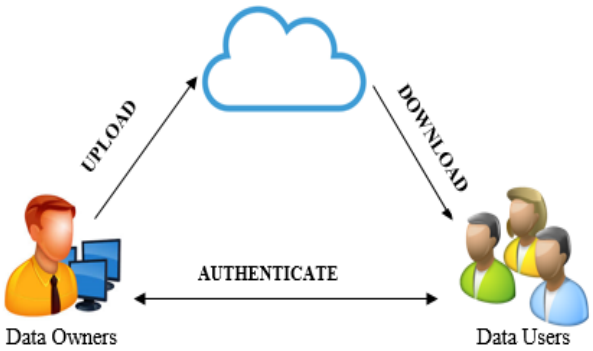

Fig. 2: Security model in the cloud

There are "three types of schemes based on hyperelliptic curve cryptography - key agreement, encryption and signature schemes".

4.1. Key Agreement

The client implements the HECC algorithm to generate the public and private keys. The key pair is defined as {pk, d} where pk - public key and d -private key. The Diffie-Hellman key agreement technique was designed for the multiplicative group of numbers, but it can adjusted easily to general groups. Let us consider G be a group whose elements can be efficiently represented the group operation scan be efficiently evaluated as well. The group is jacobians of hyper elliptic curves.

The following public parameters are considered

- The group 'G'.
- An element R $\in$G of large prime order r.

4.2. Encryption/Decryption

The data owner will encrypt the files to the cloud before sending with the public key pk - -> E. The hash value generated is stored for further verification process and the data encrypted is uploaded to the cloud. If A wants to send data message M to B, it does the following

- It obtains the public key pk of receiver B.
- It chooses a secret number a$\in$ [1,r-1]
- Computes the value C1 = aR.
- Compute the value C2 = M + a(pk).
- Send (C1, C2) to B.

When the data user needs to access the file, a download request will be sent to the cloud and a decryption key is used to decrypt the retrieved content. After retrieval of content, the hash value will be calculated again. The file integrity can now be verified upon comparison. As the file is stored in the cloud, the comparison of hash value will be helpful to identify whether the file is perfect while it is stored in the cloud. The "receiver B can decrypt the cloud data by doing the following:

- Receive the encrypted message (C1, C2) from sender A
- Compute the message value M = C2 − bC1".

4.3. Signature Schemes

The Digital Signature Algorithm can be used for any group G signature generation and verification. If sender A needs to sign a message M, it has to do the following.

- Choose a random integer k $\in$[1, r − 1], and compute Q = kR.
- Compute s from H(M) and a.

Now the signature is (M, Q, s).

In order to "verify this signature at the receiver end, the verifier B has to do the following"

- Compute v1 and v2 from H(M) and ∅(Q)
- Compute V = v1R + v2P
- Accept the signature if V = Q". Otherwise, reject it.

5. Performance Analysis

The Hyper elliptic curve cryptosystem is a successor of Elliptic curve cryptosystem. The ECC method involves defining the set members over which the group is defined. An operation on any two elements in the set will result in a element of the group itself. In ECC the time required for encryption and decryption increases as the timestamp (t) increases whereas in HECC the encryption/decryption time decreases with increases in timestamp. The Figure.3 depicts the decrease in encryption time in HECC and in ECC the curve increases with increasing timestamp.

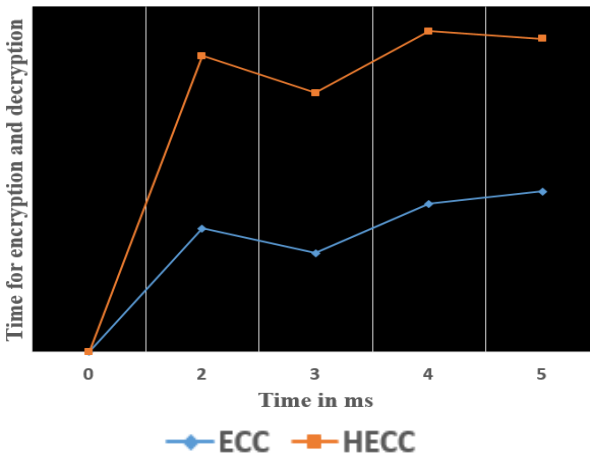

Fig. 3: Comparison of HECC and ECC in terms of Encryption and Decryption time

The analysis of performance between ECC and HECC shows that the HECC system is more efficient in terms of performance. The graph in Figure 4 shows the time for encryption and decryption in the x-axis and the key size of the cryptosystem in the y-axis. The ECC system with 160-bit key size is found to take more time for encryption and decryption than the HECC system. The HECC system requires only 80-bit key size for cryptographic processing. Here the time required for encryption and decryption is said to be lower than ECC as the key size decreases. Hence it is evident that the key size is directly proportional to the time required for encryption and decryption and the HECC system with lower key size offers secure processing of resources in the cloud.

The HECC system also offers less computational cost since the key size is minimum. This algorithm is also resistant to various types of intruder attacks. It involves lesser time in the stages of operation and it is well suited for an efficient and scalable environment in the cloud. It provides the security provided by ECC system with a minimum key size.

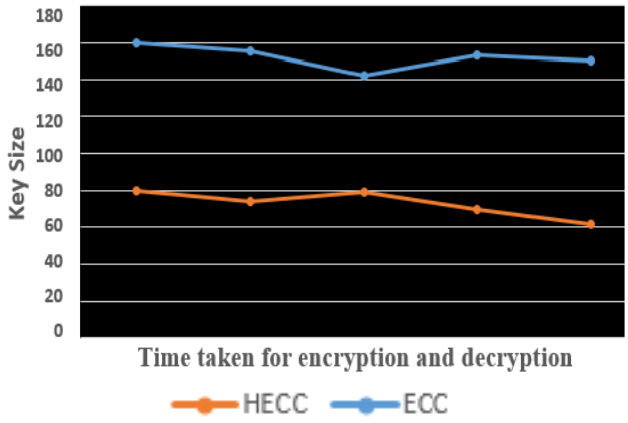

Fig. 4: Comparison of HECC and ECC in terms of Key size

6. Conclusion

Cloud computing is facing a lot of challenges concerned with security. User's data must remain confidential and must be authenticated whenever it is accessed. The proposed system of hyper elliptic cryptography provides a secured key agreement, encryption, decryption and signature scheme. The HECC system requires less storage, bandwidth and power when compared with other cryptosystems. HECC also uses lesser key sizes of about 50-80 bit size and is also efficient to reduce complexity of the algorithm.

References

[1] Joshi, J.B.D., Gail-JoonAhn. Security and Privacy Challenges inCloud Computing Environments.IEEE Security Privacy Magazine,Vol 8, IEEE Computer Society, 2010, p.24-31.

[2] DebajyotiMukhopadhyay,AshayShirwadkar,PratikGaikar, TanmayAgrawal. Securingthe Data in Clouds with Hyperelliptic Curve Cryptography.13th International Conference on Information Technology, IEEE Computer Society, 2014, p.201-205.

[3] R.Maheswari, S.Sheeba Rani, V.Gomathy and P.Sharmila, "Real Time Environment Simulation through Virtual Reality" in International Journal of Engineering and Technology(IJET) , Volume.7, No.7, pp 404-406, April 2018

[4] Bouayad, A., et al. "Cloud computing: Security challenges." Information Science and Technology (CIST), 2012 Colloquium in.IEEE, 2012.

[5] Thillaiarasu, N. and ChenthurPandian, S., 2017. A novel scheme fosafeguading confidentiality in public clouds fosevice uses of cloud computing. Cluster Computing, pp.1-10.

[6] Shyamambika, N. and Thillaiarasu, N., 2016, January. A survey on acquiring integrity of shared data with effective user termination in the cloud. In Intelligent Systems and Control (ISCO), 2016 10th International Conference on (pp. 1-5). IEEE.

[7] Thillaiarasu, N. and ChenthurPandian, S., 2016, January.Enforcing security and privacy over multi-cloud framework using assessment techniques. In Intelligent Systems and Control (ISCO), 2016 10th International Conference on (pp. 1-5). IEEE.

[8] Shyamambika, N. and Thillaiarasu, N., 2016. Attaining integrity, secured data sharing and removal of misbehaving client in the public cloud using an external agent and secure encryption technique. Advances in Natural and Applied Sciences, 10(9 SE), pp.421-432.

[9] Ranjithkumar, S. and Thillaiarasu, N., 2015.A Survey of Secure Routing Protocols of Mobile AdHoc Network.SSRG International Journal of Computer Science and Engineering (SSRG-IJCSE)–volume, 2.

[10] S. Balakrishnan, J. Janet, K.N. Sivabalan, "Secure Data Sharing In A Cloud Environment By Using Biometric Leakage resilient Authenticated Key Exchange", Pak. J. Biotechnol. Vol. 15 (2) 293-297 (2018).

[11] J. Janet, S. Balakrishnan and E. Murali, "Improved data transfer scheduling and optimization as a service in cloud," 2016 International Conference on Information Communication and Embedded Systems (ICICES), Chennai, 2016, pp. 1-3. doi: 10.1109/ICICES.2016.7518895.

[12] Balakrishnan S., Janet J., Spandana S. "Extensibility of File Set Over Encoded Cloud Data Through Empowered Fine Grained Multi Keyword Search". In: Deiva Sundari P., Dash S., Das S., Panigrahi B. (eds) Proceedings of 2nd International Conference on Intelligent Computing and Applications. Advances in Intelligent Systems and Computing, vol 467. 2017. Springer, Singapore.

[13] J. Janet, S. Balakrishnan and K. Somasekhara, "Fountain code based cloud storage mechanism for optimal file retrieval delay," 2016 International Conference on Information Communication and Embedded Systems (ICICES), Chennai, 2016, pp. 1-4. doi: 10.1109/ICICES.2016.7518901.

[14] J. Janet, S. Balakrishnan and E. R. Prasad, "Optimizing data movement within cloud environment using efficient compression techniques," 2016 International Conference on Information Communication and Embedded Systems (ICICES), Chennai, 2016, pp. 1-5.doi: 10.1109/ICICES.2016.7518896.