2023 Third International Conference on Artificial Intelligence and Smart Energy (ICAIS) | 978-1-6654-6216-7/23/$31.00 ©2023 IEEE | DOI: 10.1109/ICAIS56108.2023.10073781

A Secured Method for Authentication of Data Security using Public Key Cryptography

Srisailapu D Vara Prasad [1]
GITAM Deemed to be University, Hyderabad, Telangana
sdvprasad554@gmail.com

J.Kavitha [2]
BVRIT HYDERABAD College of Engineering for Women, Hyderabad, Telangana
j.kavitha5555@gmail.com

Rokesh Kumar Yarava [3]
Chalapathi Institute of Engineering and Technology (Autonomous),Lam,Guntur, Andhra Pradesh.
rokeshy12@gmail.com

Arumalla Nagaraju [4]
Koneru Lakshmaiah Education Foundation, Vaddeswaram, Andhra Pradesh.
anagaraju@kluniversity.in

G.Charles Babu [5]
GRIET, Hyderabad, Telangana
charlesbabu26@gmail.com

P.Gopala Krishna [6]
GRIET, Hyderabad, Telangana
charlesbabu26@gmail.com

ABSTRACT- This study suggests that the cloud is an internet storage tool mostly used to store papers, media, and different types of material. However, because cloud storage is so widespread and accessible, there are a number of security concerns, including data theft and problems with authentication when sharing data on public platforms. Attribute-based encryption allows for the fine-grained exchange of encrypted data. This is done by utilizing a methodology to combine key creation, encryption, and decryption to guarantee data confidentiality and integrity. Data sharing in the cloud can be done using a variety of methods, each of which uses a unique set of stages or processes to get the job done. One of those methods is public key encryption, a type of asymmetric key encryption in which the data or document is protected by both the public and private keys. Our challenge is to create an efficient public-key encryption scheme which enables flexible delegation in the sense that any subset of the cypher texts (made by the encryption scheme) is decryptable by a constant-size decryption key (issued by the owner of the master-secret key). By utilizing a unique form of public-key encryption, which is referred as the key-aggregate cryptosystem to resolve this issue.

Keywords: *Data Security, encryption techniques, cryptography, Privacy*

I. INTRODUCTION

Resources and applications are delivered over the Internet as services in a cloud computing environment. The term "cloud" refers to an environment made up of hardware and software resources in data centres that enable a variety of services to be provided across a network or the Internet to suit consumer needs [1]. Concerns about cloud data security have been raised by recent security incidents involving public cloud data storage. Users can employ scalable on-demand services by maintaining their information on the cloud. Specifically for small and medium-sized businesses with tight budgets, cloud-based project management services enable significant cost savings and productivity improvements [2]. They also facilitate cross-team cooperation. Techniques based on encryption: A significant amount of research on using encryption-based techniques to protect sensitive data on the cloud has been published. Password-based encryption is used by the majority of encryption schemes [6]. These systems are vulnerable to assaults using brute force guessing. The well-known password-based encryption technique produces strong cryptographic keys. The basis of PBE cryptography is the hashing algorithm.

In order to produce random data through the application function process and to be processed by the iteration count, a password and salt will be mixed. Once the mixing procedure is complete, the data will be transmitted in the assemble of cypher text. Using the users' provided passwords, it enables the user to find strong secret keys. It is assumed that the generated key bytes are as random and unreliable as feasible. PBE techniques are vulnerable to brute-force assaults since user-generated passwords are frequently used or weak. It is a weak defense against attacks and does not provide safe data storage. Data Encryption A standard secret key encryption and decryption method has been looked at [7].

Because it is inexpensive, requires no upkeep, and is simple to access from anywhere, the cloud is a popular place to store data and files. Government agencies, in addition to commercial and public businesses, are looking for cloud-based storage and services for their sensitive data storage. Each cloud provider has given their own method to encrypt and decrypt the data, including Microsoft Azure, IBM, Amazon Web Services (AWS), and many others. Many business and public service firms utilize cloud computing to store vast amounts of data that are accessible from any location. Industry, military colleges, and private entities all use the cloud. User authentication is required to access data stored in the cloud, but additional layers of security are in place for confidential access. The level of privacy affects the algorithm used by this multiple layer security. Cryptography and steganography techniques are frequently used to address issues with various levels of security. Incorporating many methods is necessary to increase data storage security. This article suggests a novel technique that makes use of symmetric key cryptography and steganography.

II. PROPOSED MODEL

The Advanced Encryption Standard algorithm, which is regarded as the most well-liked symmetric cryptographic technique, has been examined [10]. High performance development is highly important. Because it uses 128, 192, or 256-bit keys, the AES algorithm has a high level of security. It demonstrates resilience to a variety of techniques, including differential, square, key, and key recovery attacks. AES takes less time to encrypt data than DES. It follows that AES's performance is significantly superior to that of DES. There is currently no proof that this algorithm can be broken. This encryption algorithm is quite safe. Additionally, data can be safeguarded from potential assaults like smash strikes. While other symmetric algorithms have flaws and variances in performance and storage space, AES encryption algorithm offers minimal storage requirements and high performance without any limitations. As AES encryption is utilized for data transport, there is no chance that the system will occasionally be unavailable during the arrival of large data. Denial of access to the third party prevents the potential of hackers impersonating the third party and breaking into the network. When compared to alternative methods, the use of the Advanced Encryption Standard for data security offers advantages of faster calculation and less memory usage.

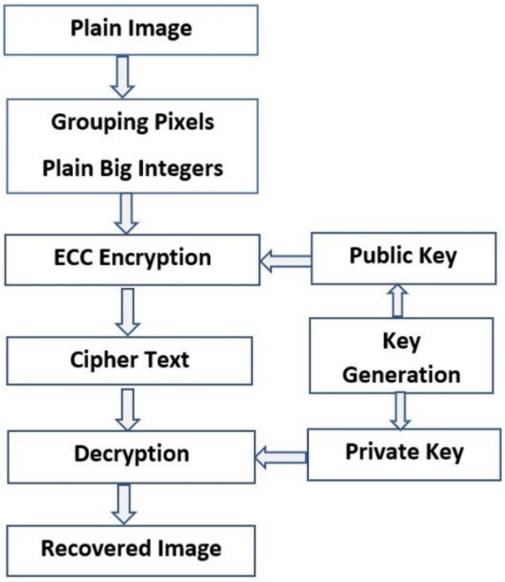

Figure 1: Flowchart

Plain image

Source or original image is fed as an input and that input is termed as a plain image.

Figure 2: Input Image

Image Shuffling

Once, the image is read then it is subjected to image shuffling is done i.e., grouping of pixels so that equi-distributed collections of pixels are formed by sub intervals of the pixel progression or shuffle.

Pixel Grouping inside Single Integer

Images have much number of pixels. Whenever an image's cryptographic operation occurs on a single pixel, it takes more time because of enormous number of pixels in the image. These issues, such as grouping pixels into one group, should be addressed thoroughly. However, no. of pixels captured for each group must be determined by the elliptic curve's parameters.

Plain Big integer

Pixel value of the coordinate must be within the bit size range favored for the ECC operation. To create the cipher images, scale the image down to the ECC coordinate range (0 - 255) and apply mathematical functions to the Integer Digits [large integer value, 256]. As a result, insert the value of an integer that is more than the base value, which are 256.

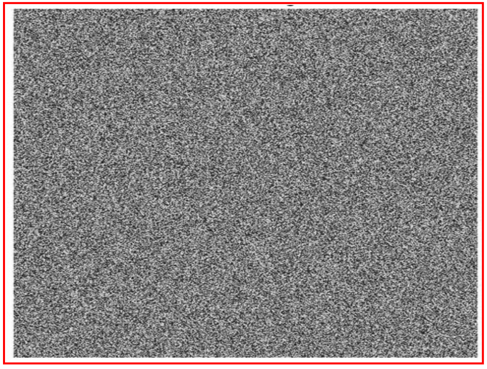

Figure 3. Shuffled Image Histogram

III. METHODOLOGY

a. ECC Encryption

1. Encryption is the process of converting a plain image into a cipher image.
2. If not, throw away the signature from step1.
3. Next e= H (M)is the equation to use.
4. Compute the value of w=s—1modn.
5. Compute u1ase·w modn and u2asr·w modn.
6. Compute the point on the curve Q (xq, yq) asu1·G+u2·XA.
7. Get the value of vas xq modn.
8. Verifythatvr. To accept the signature, you must agree else reject that. One is used to sign messages, and the other is used to verify signatures.

If the sender is willing to sign on a message M to the receiver after two sides will agree on parameters, generated by ECC key pairs, and exchanged public keys.

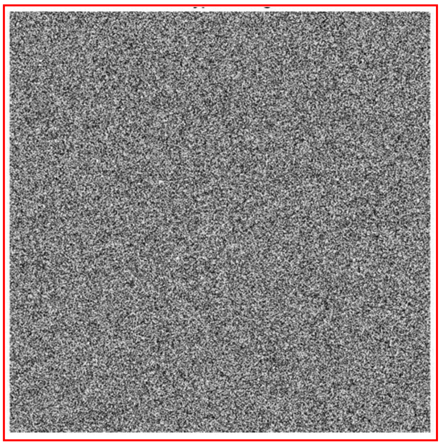

Figure 4: Encrypted Image Histogram

K1 k2 = KDF k1 and k2 are identical to the two keys sent out by the sender(S).

It rejects the message if MAC (M) k2t, so check if that’s the case.

Using the next derived key, message M=DCk1, is used to decrypt the message.

Decryption is the process of recovering the plain image from a cipher image.

Figure 5: Decrypted Image

b. Types of Cryptographic Algorithms SKC (Secret Key Cryptography)

SKC (Secret Key Cryptography) is a symmetric encryption that uses only a single key for both encryption and decryption. Mostly for the sake ofensuring the privacy.One of the most significant drawbacks of symmetric keyencryption is the issue of key transmission.Since there is only single key in symmetrical encryption, both sender and receiver must be aware of it, and then this key is sufficient to decode the coded message. Before transmitting the actual message, the secret key must be sent to the receiving system. Everykind of digital communication is unsafe since no one can ensure that lines of communication will not be tapped.

c. PKC (public key cryptography)

PKC (public key cryptography) is also known as asymmetric encryptionsince it uses one key to encrypt the data and another for recovery. Authorization and crypto keys exchange are the most common uses.

d. Symmetric Cryptography

Asymmetric cipher is one that uses the same or a similar key for both encrypting and decrypting information.[12] That key is referred to as asymmetric key, and it is also referred to as a secret key. Symmetric encryption is a method of establishing a secure channel of communication between two parties.

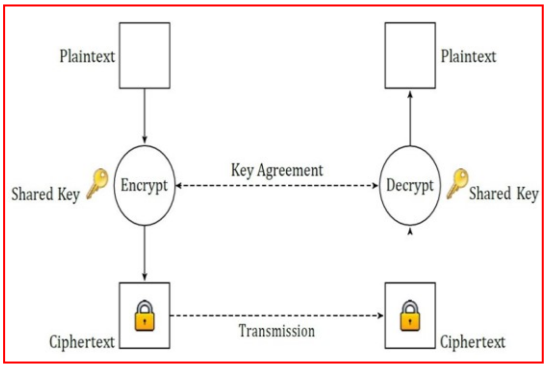

Figure 6: Symmetric Cryptography

For example, if Sender wishes to communicate information to Receiver but does not wish for anyone else to be aware of it, she can encrypt the plain text message using her secret key and then send the cipher text message to Receiver. When he receives the cipher text, he can decode it using the same secret key that he used to decrypt it in order to recover the plain text.

The biggest disadvantage of symmetric key cryptography is that all sides should definitely hare these keys used to encrypt the content before decrypting it.

e. Asymmetric Cryptography

Synthetic or public-key cryptography are terms used to describe a crypto- graphic approach that uses distinct keys for encryption and decoding. Asym- metric cryptography is also known as key separation cryptography (PKC).[12] Each of the two keys has a different intended function, with one being kept private by the owner and referred to as the secret key, and the other being referred to as the public key and accessible to anybody. A key pair is the union of a public key and the private key that is linked with it. Utilizing secret key to encrypt as well as the public key to decrypt, or inversely., encryption and decryption can be done in either order. Public-key encryption is the term used to describe the use of an asymmetric cryptographic cypher (PKE).

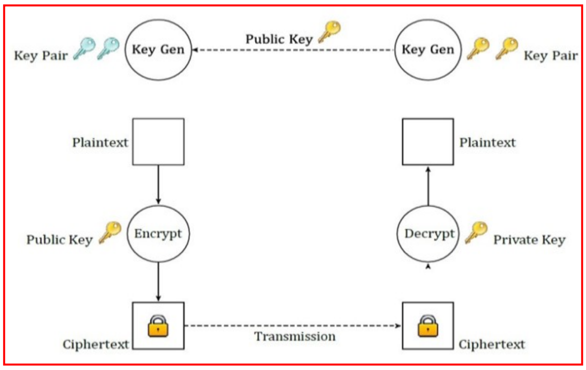

Figure 7: Asymmetric Cryptography

When compared to [13] symmetric encryption, asymmetric encryption is a relatively new technological development. Comparatively speaking, asymmetric encryption takes a considerable time compared to symmetric encryption.

f. Hybrid Cryptosystems

A hybrid scheme combines public-key and symmetric-key cryptography principles. To use public-key encryption, no shared secret must be computed between the two parties, and the storage of the asymmetric keys once the secret has been computed is not mandatory. Instead of using two separate symmetric key pairs for encryption and decryption, a hybrid cryptosystem uses one shared secret for both encryption and decryption, generating a shared secret for each communication and encrypting and decrypting it with the recipient's public key before including it as cipher text.

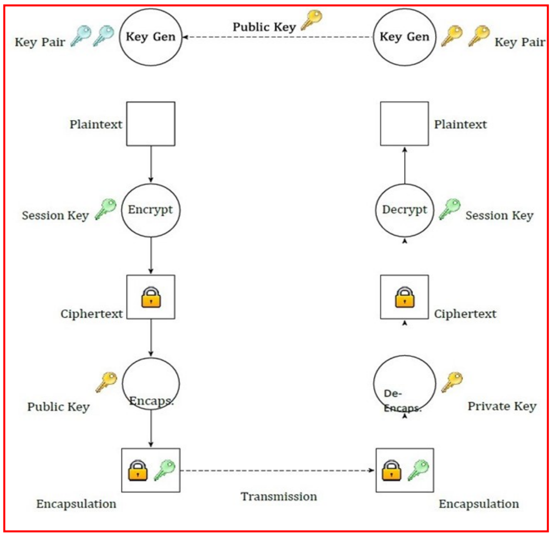

Figure 8: Hybrid Cryptosystems

Key encapsulation is the term for this kind of asymmetric encryption. The Transmitter (blue keys symbols) and the Recipient (yellow keys symbols) generate the keys, and then the public key of the Receiver is exchanged, and finally the Sender generates the session key (green keys symbol). A new message is then sent to the recipient, which includes a cipher text of the original message and the session key. Receiver's public key is subsequently used to encrypt the message. Encryption is performed using the receiver's private key to de encapsulate and extract the session key and decode the encrypted message back to its original plain text.

In this way, the hybrid cryptosystem combines the advantages of both types of encryption. It only needs O(n) keys, yet it can quickly encrypt plain text of anysize.

g. Elliptic Curve Cryptography (ECC)

Elliptic Curve Cryptography (ECC) mechanism is a type of public-key cryptography that uses the algebraic elliptic curves (ECs) structures as the basis for cryptographic functions. [14] Keys are created using ECC, to Encrypt and Decrypt the message, key pairs generated by ECC are essential [14].

ECC is a revolutionary public-key encryption technique that is more eco-nominal, quicker, and shorter than its predecessors. Due to its lightweight nature, ECC is used for Bitcoin's asymmetric cryptosystem.

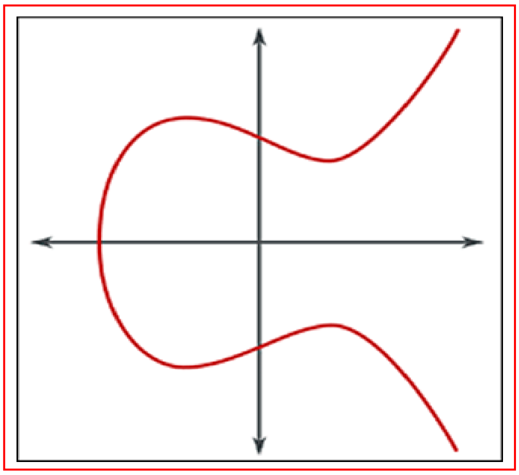

Figure 9 : ECC

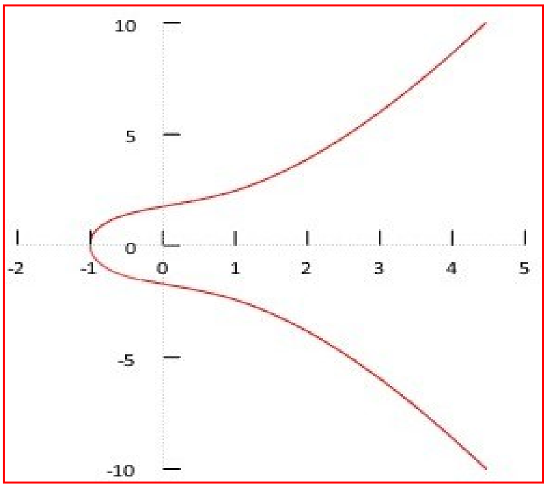

Figure 10 : Plot of the elliptic curve

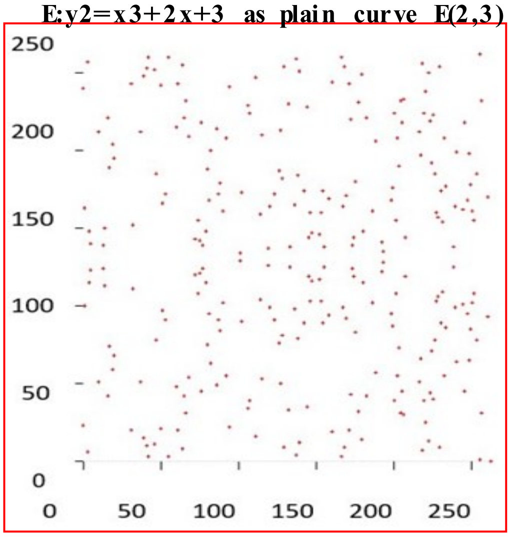

Figure 11: Plot of the elliptic curve

E: y2 = x3 + 2x + 3 as over a field as E263(2,3) is difficult, exactly as with the DLP. An elliptic-curve DLP (ECDLP) is used to generate the trapdoor function that ECC is built upon. A more general definition of the ECDLP is as follows: Then, determine k [1,p 1] such that the two EC points Q and G have a distance k [1,p 1].
Q = k G

Where on an EC over a finite field Fp, the points Q and G are located as with the DLP mentioned, the calculations for brute force must be performedat least k times:

$$k \cdot G \bmod q = G + G + G + \ldots + G$$

mod q — k times Owing to the fact that perhaps the numerical group operations are performed to EC points, they must be specified especially for the group of points on an elliptic curve (point addition and scalar multiplication). It is possible to define point addition as thus: Two EC points P and Q (xp and yp) on the elliptic curve E will always cross at a third point—R—if the line traced through them intersects E. (this is a property of elliptic curves). In other words, P + Q = R, or the negative of this point, i.e. R(xr, yr), is defined as the point addition of these two points. Officially, this is known as λ = yq — yp/(xq — xp)
xr = λ2 — xp — xq

yr = λ(xp — xr) — yr To visualise this computation on a curve y2 = x3 — 2x, consider the graphic shown in Figure .

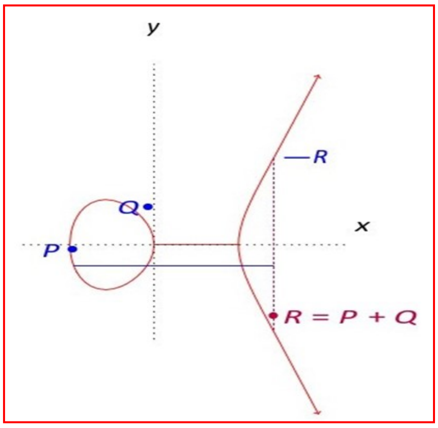

Figure 12: Point addition on elliptic curves for R=P+Q

Similar to point additions, point doubling utilizes a unique point that is added to itself, resulting in 2 P. In contrast to point addition, when a line is created between 2 points, the tangential of the position P(xp,yp) is usedVto determine the intersection of R and E. As a consequence of point doubling, R(xr,yr) becomes negative, such that R= 2P. The following equations summarize the essential computations mathematically.

$=3x2a+a/2yp$

$xr=\lambda_2—2xp$

$yr=\lambda(xp—xr)—yp$

The figure illustrates the geometric representation of this calculation, which is also based on the curvey 2= x32x. Point multiplication is the repeated application of point doubling and addition, and it is expressed by the formula multiplication between a point P and a scalar k,where PE and kN+, for example, R = 5 P, where P E and k N+ are positive integers. There is no distinct group operation for point multiplication; rather, the factor k is divided into multiple sets of 2, plus1for even value of k and zero for odd value of k.

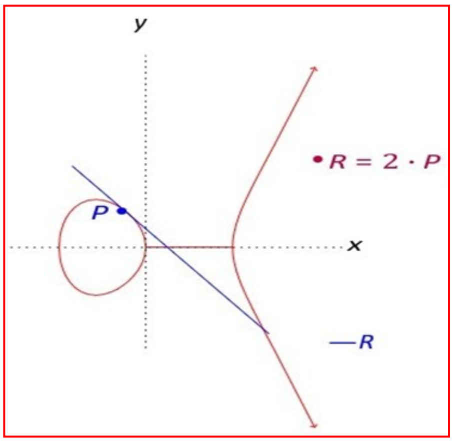

Figure 13: Point multiplication on elliptic curves for R=2·P

As an example, consider the following: 5 P would thus be computedas 2 2 P + P, which is equivalent to doing a double-point multiplication of P followed by a point addition with the result and P. Component group Xiamu Niu, Li Li, and A.Abdl El-Latif proposed an encrypted image system based on Elliptic Curve El Gamal technology, which allows for the sharing of secret images by playing a homogeneous image together. However, the y picked a different parameter for the elliptic curve based on Pohling Hellman and Rho Pollard's attack resistance theories. The outcome was superior tothe encryption scheme based on ElGamal and RSA. Scott Vanstone, Alfred Menezes, and Don Johnson discussed the implementation phase of the Ellipticcurve technique for digital signatures in terms of interoperability and security. While Walid Aljoby, MoadMowafi, and Lo'aiTawalbeh contributed two ECC algorithms based on encryption pictures, such as selective bit plane and selective quantization of DCT coefficients. Furthe rmore, Dr.Mamfred Lochter discussed set parameters for elliptic curve cryptography in a finite prime field.

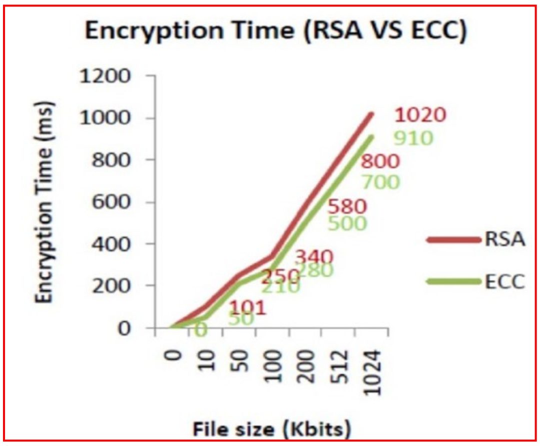

Figure 14: Encryption Time RSA vs ECC

IV. RESULTS AND DISCUSSIONS

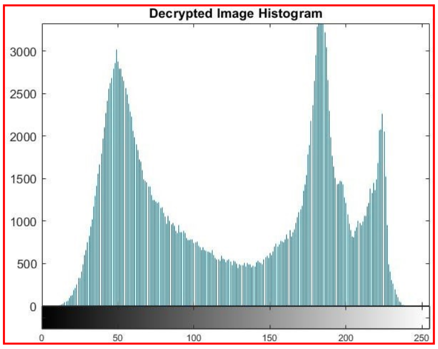

Figure 15: Input Image Histogram

Source or original image is fed as an input and that input's corresponding histogram of the plain image is shown here.

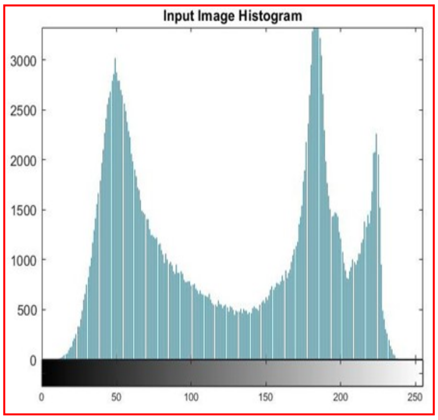

Figure 16: Shuffled Image Histogram

Image pixels are grouped to ease the cryptographic operations hence the Shuffled image Histogram is shown and is similar to the plain image as no cryptographic operation is performed till this step.

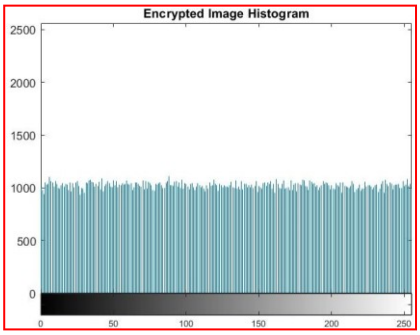

Figure 17: Encrypted Image Histogram

The image is subjected to encryption after the shuffling the image. Corresponding image's histogram is shown here.

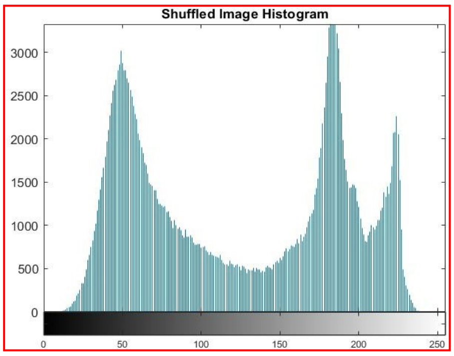

Figure 18: Decrypted Image Histogram

Decryption operation is then performed and its histogram is shown above.

V. CONCLUSION

This study has suggested an effectively implementable variant of the fundamental key-aggregate cryptosystem that makes use of asymmetric bilinear pairings, low overhead cipher-texts, and aggregate keys. For a number of cloud-based data sharing applications, such as collaborative data sharing, product license distribution, and medical data sharing, our design offers an effective solution. Under reasonable security presumptions, we have demonstrated that our structure is completely collusion resistant and semantically secure against a non-adaptive adversary. Then, we showed how this design might be altered to obtain CCA-safe construction. As far as we know, this is the first CCA secure KAC construction to be published in the cryptographic literature. Furthermore, we have shown how the fundamental KAC architecture can be effectively expanded and generalized for safely disseminating the aggregate key among numerous data consumers in a practical data sharing scenario. This offers a vital route for developing a scalable fully public-key based online data sharing system for large-scale cloud deployment. To verify the criteria for our scheme's space and temporal complexity, we have produced simulation results. The findings demonstrate that, in terms of performance and scalability, KAC with aggregate key broadcast beats other current secure data sharing systems.

References

[1] IDC Enterprise Panel. It cloud services user survey, pt. 3: Whatusers want from cloud services providers, august 2008.

[2] Sherman SM Chow, Yi-Jun He, Lucas CK Hui, and Siu Ming Yiu.Spice–simple privacy-preserving identity-management for cloud environment. In Applied Cryptography and Network Security, pages526–543. Springer, 2012.

[3] Cong Wang, Sherman S.-M. Chow, Qian Wang, KuiRen,andWenjing Lou. Privacy-preserving public auditing for secure cloud storage. Cryptology ePrint Archive, Report 2009/579, 2009.http://eprint.iacr.org/.

[4] Sherman SM Chow, Cheng-Kang Chu, Xinyi Huang, JianyingZhou,and Robert H Deng. Dynamic secure cloud storage withprovenance. In Cryptography and Security: From Theory to Applications,pages 442–464. Springer, 2012.

[5] Erik C Shallman. Up in the air: Clarifying cloud storage protections.Intell. Prop. L. Bull., 19:49, 2014.

[6] Ruixuan Li; ChenglinShen; Heng He; ZhiyongXu; Cheng-ZhongXu, "A Lightweight Secure Data Sharing Scheme For Mobile Cloud Computing" IEEE Transactions on Cloud Computing, Vol.PP, Issue.99, 2017. doi: 10.1109/TCC.2017.2649685

[7] JianShen , Tianqi Zhou, Xiaofeng Chen, Jin Li, and Willy Susilo, "Anonymous And Traceable Group Data Sharing In Cloud Computing" IEEE transactions on information forensics and security, Vol.13, Issue.4, 2018.

[8] Joseph K. Liu, Man Ho Au,Xinyi Huang, Rongxing Lu, andJin Li, "Fine-Grained Two-Factor

Access Control For Web-Based Cloud Computing Services" IEEE Transactions on Information Forensics and Security, Vol.11, Issue.3, 2016.

[9] Bernardo Ferreira, Joao Rodrigues, Joao Leitao, Henrique Domingos, "Practical Privacy-Preserving Content-Based Retrieval In Cloud Image Repositories" IEEE Transactions on Cloud Computing, Vol.PP, Issue.99, 2017. doi: 10.1109/TCC.2017.2669999

[10] SikharPatranabis, YashShrivastava, DebdeepMukhopadhyay,"Provably Secure Key- On InformationForensics And Security, Vol.10, Issue.7, 2015.