ISSN: 0975-766X
CODEN: IJPTFI
Available Online through
www.ijptonline.com
Research Article

ENCRYPTING DATA AND SECURING IT WITH AN IMPREGNABLE COMPRESSION TECHNIQUE FOR CLOUD STORAGE

Eldhose M Joy*[1], Subhash Daggubati[2] and A.C Santha Sheela[3]
[1,2] Student,Department of Computer Science, Sathyabama University, Chennai-600119.
[3]Assistant Professor, Faculty of Computing, Sathyabama University, Chennai-600119.
Email: eldhose.maliyakel@gmail.com

Received on 25-04-2016 *Accepted on 20-05-2016*

Abstract

In the cloud computing environment privacy and data protection becomes a challenging task where many encryption schemes proposed to overcome this. When an intruder in a cloud environment with no authorized access tries intruding the traditional encryption schemes protect the cloud providers so that they cannot be hacked. They are forced to reveal the secret data present in storage encryption schemes. Thus current technologies involved in encryption of data and then store it in cloud. With the help of this only the authorized users with authenticating key can get the appropriate data by decrypting it. In our proposed method we deploy the enhanced security system by applying impregnable compression of data along with encryption system. Since the snooper cannot tell if obtained secrets are true or not, the cloud storage providers ensure that user privacy is still securely protected. Along with this the proposed impregnable compression technique which will overcome the extra data created by encrypted algorithm. After encrypting the data with potential ECC algorithm it is also compressed in archive files and then stored in cloud thus accomplishes both data privacy and efficient space saving.

Keywords: Cloud Storage Services, Impregnable Compression Technique, Elliptic Curve Cryptography (ECC) Encryption algorithm.

Introduction

In cloud common storage places the rapid changes or growth in storage development and its increasing familiarity leads to its insecure nature. Cloud is a common storage environment where the clients can store any kind of data and can access it anywhere at any network place. Each and every cloud clients have their own privacy login and protected data environment for storing their private data. Thus cloud storage services provide encryption and generate unique private and public keys to each user as protection on their side.

Most of the cloud databases use [7][13][14]Attribute Based encryption that is hack proof that handles number of cloud service providers along with third party encryption. It manage trusted key along with private and public key management that are more trusted and cannot be snooped by any intruder. [8][9][10][11]Sometimes the cloud storage providers enforced to reveal secret keys given to the user or they may be bribed for doing this thus there is no much security assured for our data stored in cloud storage. As the cloud providers are not so reliable many user data abducted by the external means and also intercept collaborations between clients and the storage providers of cloud. To avoid such situation cloud service providers used a trick that it reveals only the fake user id and key to the interloper. When the intruder uses the key they can access only the forged data which is not real so the original key will be secured at the same time intruder presumes to have the access towards the original data. Thus the user privacy is still protected by just providing them the cipher text that's of no use to the intruder.

[15]Deniable encryption is a concept that fakes the interlopers by faking counterfeit data which is capable of speculating the snoopers. They deny any data in the form of cipher text and endure its privacy by eliminating any suspicion to the snooper. But when the snooper realize about the uselessness of data then they got dejected automatically. This is more applicable in most of the audit less cloud storage service providers. As the cloud service providers have the chance of decrypting the entire encryption scheme yielded by them thus it is transparently insecure for maintaining entities in the cloud storage space.

In this paper we describe in detail about the protection of private data in the cloud storage and ECC encryption scheme used for securing data. Furthermore it inculcates private and public key to decrypt the cipher text obtained from encrypting algorithm. As in the proposed model it inscribes compression technique which is impregnable for the encrypted cipher text thus to accomplish the task of securing data in cloud storage services.

Related Work

Earlier researches for securing cloud database works precisely embeds attribute based encryption helps for data owners to get some kind of security according to [1][4][5]Sahai and Waters. Corresponding to the database storage security the decryption key has to match with the encrypted key only then they can have access towards the data. As cloud environment practices data sharing the cloud storage have to make privileges for attribute based encryption key. In the process of data encryption the data sharing in cloud storage service is common because of various encryption schemes for as many users engaged with cloud data storage place. Thus they practice multiplication of same key to different users and they need to decide what kind of users can share or access their data. When the same

kind of users satisfying the key for decryption then they could decrypt the cipher text data.

In the previously existing system of attribute based encryption it incurs key based and class based encryption that embeds users secret key within its embedded cipher text. The attribute set for securing the user key that is proposed by [2]Goyal with key based attribute encryption. It formally relates the user secret key policy with which they can have access towards cipher text that only checks the policy for unlocking such shared cloud data. This kind of similarity key based policy is expressed by [3]Bethencourt where it uses tree structure that uses formula to decrypt based on its attributes policy.

There exist some enhanced secret sharing schemes that use substantial set of schemas that uses random subset methods to determine the universal set of algorithms as explained by [12]Canetti. His model builds an exclusive permutation of set of public key encryption that denies set of both public and private key representation with encrypted bit of data. When such elements are represented as bit encryption it has substantial elements recognized as bit 1 and the non substantial sets recognized as bit 0. The simulation for encryption using public key encryption generates cipher text that sends encrypted bit along with set of encrypted data that claims public and private pairs of key pattern.

Encrypted Cloud Storage with ECC Algorithm

In the above cloud technology for secure model the [15]deniable encryption requires valid encryption scheme. Multi distributional and deniable encryption scheme there is no necessity to provide the normal set of algorithm. Thus to enhance the security model we use ECC that is Elliptical Curve Cryptography model to secure scheme for deniable algorithms. This is one of the most efficient algorithm that cannot break without authenticate key generated. A multilayered kind of security with public key based conventional algorithm that operates over binary field deploying Elliptic Curve Cryptography in applications such as multiple data sharing storage space like in cloud storage services.

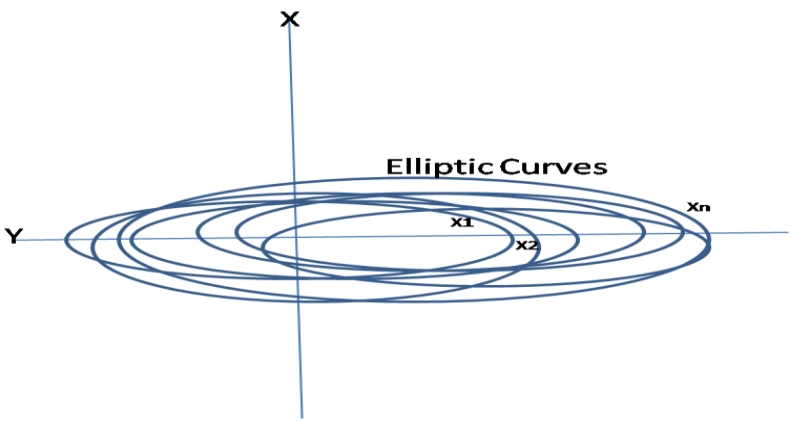

Figure.1 Representation of Key Generation using ECC Algorithm

Elliptic Curve Cryptography with digital signature is swift and reliable algorithm that secures data in public sharing spaces with high efficiency consuming less storage area and less power to accomplish encryption. They use public key algorithms that implements mathematical calculations with speculative set of instructions to software architecture in 32-bit processors. The feasible and reliable data protection implements the optimization of its performance oriented bits with protocols used such as public and private key algorithms termed as symmetric key.

ECC works by deriving random integers that derives precise values in parallel processors that computes random elliptic curves that is about 32 layered structures of elliptic curves that interlays within each other produces varying results. It produces uneven key that generates using live coding with different magnitudes of Elliptic Curves. Strategy based elliptic curves adopts strategies that has different curves each curve generates a key and encrypts so that it undergoes 32 levels of encryption as inscribed in Figure.1 so that the snooped data will not be of any use to the intruder.

In the key generation process minimization of key among all the curves in the cryptography algorithm generates the shortest possible probability to acquire the key generation process. The various cryptography algorithms are inversely proportional to its size of keys thus it consumes random generation of multiple keys that has probability of endless key generation for entire users sharing data in multi cloud environment. Its coordinates performs multiple inversion of integers that calculates algorithms and equations to outperform key generation.

Impregnable Data Compression Technique

Implementing Elliptic Curve Cryptography for generating key pairs to achieve 32 bit pairs of complete data encryption accomplishes high level of security for data to be stored. Enhanced level of security given to storage service for cloud data involves data compression technique which is impregnable by the snooper as he can able to get only the useless cipher text. Data compression is the archetype of computing mathematical formula and embodiment of linear calculations. The allowed adaptive model builds transmission model from the encrypted text and compress it without any loss in data. Any number of bits can be compressed and reduced to its size without having any knowledge about the source of the text. According to the complexity of computations the efficient hiding of data involves in coding in binary format. It helps shrinking of a document and accommodates less disk space than an uncompressed file. As these files are small it is easy to transmit as it has only less number of bytes thus it achieves efficient, swift and reliable data sharing in cloud storage space. Speed of data storage and retrieval is much easier with encoded data that has encrypted cipher text data.

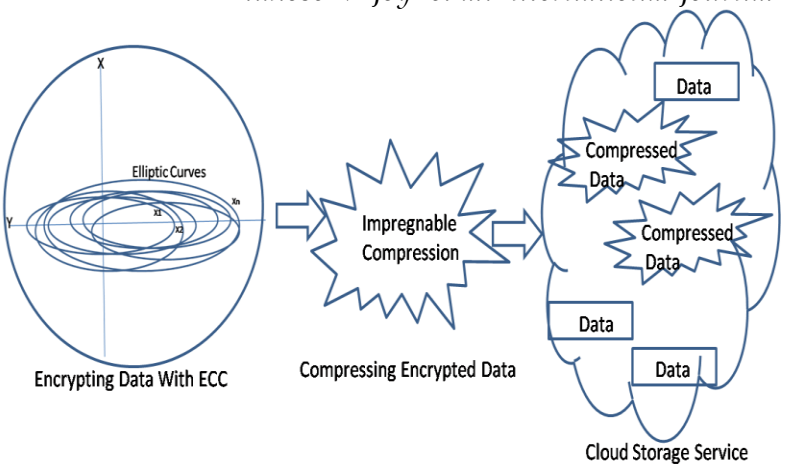

Figure.2 Compressing the Encrypted Data and Stored In Cloud Services.

Impregnable compression method involves the decoding or compression of the original data reduces the redundancy in data and repeated patterns are eliminated. It works more efficiently on text rather than image compression. Long string compression is achieved by finding out some repeated patterns pointing it with some code and making it repeated just by pointing it out. In real world applications the process of compression involves restoring or altering message context with approximate representation of data compression.

Shared data in cloud have same decompression and decrypting algorithm that is allotted for similar users of a particular data. The compressed form of typical data using deflator and inflator algorithm generates compressed and decompressed data. They form abstract of encrypted data whereas recursive data compression replace and maintain a secure data format that improvises the clarity of messages. In a sequence the encrypted data is compressed so that no bit is lost so no data will be lost in the encrypted form.

The encrypted data will be restored by decrypting it thus it also checks whether the whole data is decompressed properly. If any bit lost during compression or decompression then during decryption it cannot use appropriate key for performing that task. They will set upper and lower bounds towards the estimated probabilities of compressing algorithm deployed. Thus it ensures two level of scrutiny to get data security as well as data integrity towards the cloud stored data.

Experiment and Result Analysis

Using ECC algorithm the estimated storage security is enhanced by such strong and multilayered pairing key algorithm. Attributes of data secured by generating public and private key by using multi layered elliptic curve cryptography which provides pairing of keys using equations layered in 32 elliptic curves. This kind of secured equation in cloud storage it deploys encryption as a major securing technique and data compression to store in cloud.

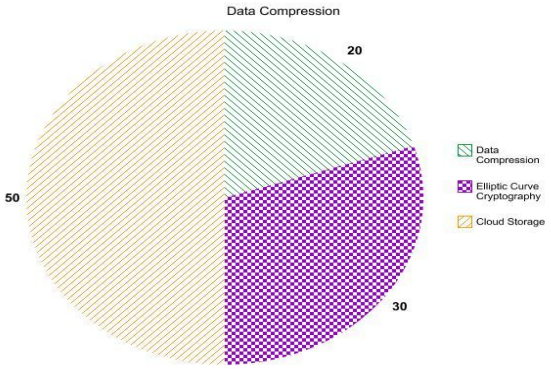

Figure.3 Compression and Encryption Distribution over cloud storage services.

In the above compression and encryption distribution for storage in cloud services the encryption of elliptic curves that deploys equations about multiple times as much as the random distribution of elliptic curves over the graph in random and definite manner. Thus its distribution is detailed as in the above distribution methodology. From the above analysis we could define how in the cloud storage the cryptography and compression of data to be stored is accomplished.

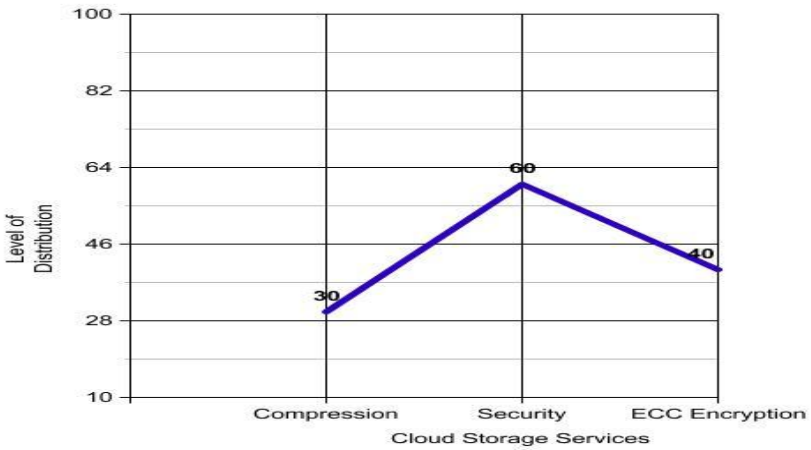

Figure.4. Graph representation on Distribution of Secure Storage.

As in the above graph we could able to denote how the compression and encrypted data stored in cloud for analyzing it in effective manner. The simultaneous problem of encryption where fake data in cloud storage services is efficient and the encrypted cipher text is efficiently compressed and stored in cloud. Thus it is safe and secure to protect data in the encrypted and compressed format. In various security based analysis over the storage they represents encryption and then compression made high security and less storage consumption. Thus this becomes an additional advantage over the cloud secure storage services.

Conclusion

In our proposed paper we implement Elliptic Curve Cryptography algorithm for enhanced encryption technique and with which the cloud storage will be strongly protected and the data stored will be transmitted as cipher texts. Along

with such a strong encryption the data stored will be compressed using data compression technique and thus it enable less bytes of cipher text data which is of no use to the intruder. When an intruder attacking the system they need to have key for decrypting the data along with decompression key which is not possible. Enhanced compression technique provides a possible way to fight against immoral interference with the right of privacy so herewith we provide strong encryption and compression technique to protect cloud storage service as a more protected environment. Its magnitude and infrastructure of cryptography algorithm generates live keys each and every time the user persists.

References

1. A. Sahai and B. Waters, "Fuzzy identity-based encryption," in Eurocrypt, 2005, pp. 457–473.
2. V. Goyal, O. Pandey, A. Sahai, and B. Waters, "Attribute-based encryption for fine-grained access control of encrypted data," in ACM Conference on Computer and Communications Security, 2006, pp. 89–98.
3. J. Bethencourt, A. Sahai, and B. Waters, "Ciphertext-policy attribute-based encryption," in IEEE Symposium on Security and Privacy, 2007, pp. 321–334.
4. B. Waters, "Ciphertext-policy attribute-based encryption: An expressive, efficient, and provably secure realization," in Public Key Cryptography, 2011, pp. 53–70.
5. A. Sahai, H. Seyalioglu, and B. Waters, "Dynamic credentials and ciphertext delegation for attribute-based encryption," in Crypto, 2012, pp. 199–217.
6. S. Hohenberger and B. Waters, "Attribute-based encryption with fast decryption," in Public Key Cryptography, 2013, pp. 162–179.
7. P. K. Tysowski and M. A. Hasan, "Hybrid attribute- and reencryption-based key management for secure and scalable mobile applications in clouds." IEEE T. Cloud Computing, pp. 172–186, 2013.
8. Wired. (2014) Spam suspect uses google docs; fbi happy. [Online]. Available: http://www.wired.com/2010/04/cloud-warrant/
9. Wikipedia. (2014) Global surveillance disclosures (2013present). [Online]. Available: http://en.wikipedia.org/wiki/Global surveillance disclosures (2013-present).
10. (2014) Edward snowden. [Online]. Available: http://en. wikipedia.org/wiki/Edward Snowden.
11. (2014) Lavabit. [Online]. Available: http://en.wikipedia. org/wiki/Lavabit.
12. R. Canetti, C. Dwork, M. Naor, and R. Ostrovsky, "Deniable encryption," in Crypto, 1997, pp. 90–104.

13. A. B. Lewko, T. Okamoto, A. Sahai, K. Takashima, and B. Waters, "Fully secure functional encryption: Attribute-based encryption and (hierarchical) inner product encryption," in Eurocrypt, 2010, pp. 62–91.
14. N. Attrapadung, J. Herranz, F. Laguillaumie, B. Libert, E. de Panafieu, and C. R `afols, "Attribute-based encryption schemes with constant-size ciphertexts," Theor. Comput. Sci., vol. 422, pp. 15–38, 2012.
15. M. D ¨urmuth and D. M. Freeman, "Deniable encryption with negligible detection probability: An interactive construction," in Eurocrypt, 2011, pp. 610–626.

Corresponding Author:

Eldhose M Joy*,

Email: *eldhose.maliyakel@gmail.com*