ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com

International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 4, Special Issue 11, March 2017

Blowfish Algorithm with Verifiable Outsourced in Cloud Computing

[1]Bawya.M,
PG scholar/CSE,
Tagore Institute of Engineering and Technology,
Salem, India.
aglya08@gmail.com

[2]Raja.K,
Assistant Professor/CSE,
Tagore Institute of Engineering and Technology,
Salem, India.
ckrajacse@gmail.com

[3]Dr.Tholkappia Arasu.G,
Principal,
AVS College of Technology,
Salem, India.
tholsg@gmail.com

Abstract — Cloud Computing is an emerging paradigm in our day to day globe As good as it is, this technique also bring forth many new trails for data security and access control when users outsource sensitive data for distribution on cloud. Attribute-based encryption (ABE) is a promising strategy for fine-grained access control of scrambled information in a distributed storage, nonetheless, unscrambling included in the ABEs is generally for asset compelled front-end clients, which incredibly blocks it's down to earth fame. Keeping in mind the end goal to decrease the decoding overhead for a client to recuperate the plaintext were outsourced most of the unscrambling work without uncovering really information or private keys. Here a novel technique is future to make an ABE with Verifiable outsourced decryption based on a blowfish encryption. It provides a unified model, which can be considered in both key-policy (KP) and cipher text-policy (CP) settings. In verifiability, it guarantees the suitability of the transformation done between the original cipher text and the simplified cipher text. A major issue is the absence of access control rights. So, it considers an access key structure for improving the security and performance by specifying access rights for the authorized user. Access control rights, restrictions and rights for an individual are established. The access control rights is validated and results shows increased security level.

Index Terms: Outsourced decryption, verifiability, access control.

I.INTRODUCTION

Traditionally, it have to seen encryption as a method for one user to encrypt data to a new specific targeted party, such that only the target addressee can decrypt and read the message. However, in more than a few applications a user might often request to encrypt data according to some policy as opposed to specified set of users. Demanding to appreciate such applications on top of a traditional public key mechanism provides a number of difficulties. For example, a user encrypting data will need to have a tool which agrees him to look up all parties that have access recommendation or attributes that match his policy. These difficulties are compounded if a party's credentials themselves might be complex (e.g., the set of users with a top secret clearance) or if a party gains credentials well after data is encrypted and stored.

II-PROPOSED WORK

In cloud environment if a data owner wants to share data with users he/she will encrypt data and then

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com

International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 4, Special Issue 11, March 2017

upload to cloud storage service. Complete the encryption

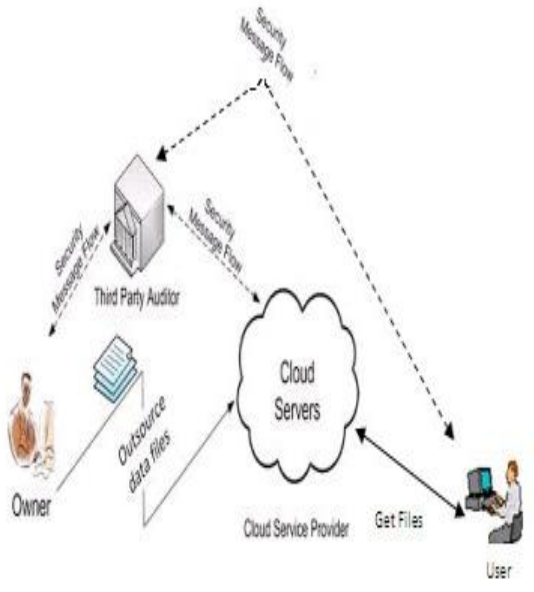


Fig. 1 Architectural Diagram

the cloud cannot know the information of the encrypted encrypted data in the cloud, a data owner uses encryption scheme for access control of encrypted data. In existing schemes several encryption schemes can achieve and provide security assure data confidentialy and prevent collusion attack scheme

IV.EXISTING SYSTEM

In fixed public-key cryptography, a message is encrypted for a specific receiver using the receiver's public-key. Identity-based cryptography and in particular identity-based encryption (IBE) changed the common understanding of public-key cryptography by allowing the public-key to be an arbitrary string, e.g., the email address of the receiver. Attribute-based encryption (ABE) with outsourced decryption not only enable fine-grained sharing of encrypted data, but also overcomes the efficiency drawback (in terms of cipher text size and decryption cost) of the standard ABE schemes.. In ABE scheme with outsourced decryption allows a third party (e.g., a cloud server) to transform an ABE cipher text into a (short) El Gamal-type cipher text using a public transformation key provided by a user so that the final can be decrypted much more efficiently than the former data. Besides to avoid the unauthorized user editing the user. That is, an end user could be cheated into accepting a wrong or maliciously transformed output. ABE goes one step further and defines the identity not atomic but as a set of attributes, that someone should only be able to decrypt a cipher text if the person holds a key for "matching attributes" where user keys are always issued by some trusted party.

III. PROPOSED ALGORITHM

cloud server's transformation cannot be verified by the

Blowfish was considered in 1993 by Bruce Schneier as a fast, free alternative to existing encryption algorithms. It takes a variable-length key, from 32 bits to

448 bits, making it ideal for both domestic and exportable use. Blowfish provides a good encryption rate in software and no effective cryptanalysis of it has been found to date. Blowfish as a general-purpose algorithm, intended as an alternative to the aging DES and is free of the problems and constraints associated with other algorithms. Blowfish algorithm is a simple design, a high speed algorithm, with low memory costs. The same key is used to encrypt and decrypt the message.

There are two parts to this algorithm;

A part that handles the expansion of the key.

A part that handles the encryption of the data.

The expansion of the key: Split the original key into a set of subkeys. Specifically, a key of no more than 448 bits is separated into 4168 bytes..

The encryption of the data: 64-bit input is denoted with an x, even as the P-array is denoted with a Pi (where i is the iteration).

Blowfish has a 64-bit block size and a key length of anywhere from 32 bits to 448.It is a 16-round Feistel cipher and uses large key-dependent S-boxes. It is similar in structure to CAST-128, which uses fixed S.

Since Blowfish is a Feistel network, it can be inverted simply by XORing P17 and P18 to the ciphertext block, then using the P-entries in reverse order.

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com

International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 4, Special Issue 11, March 2017

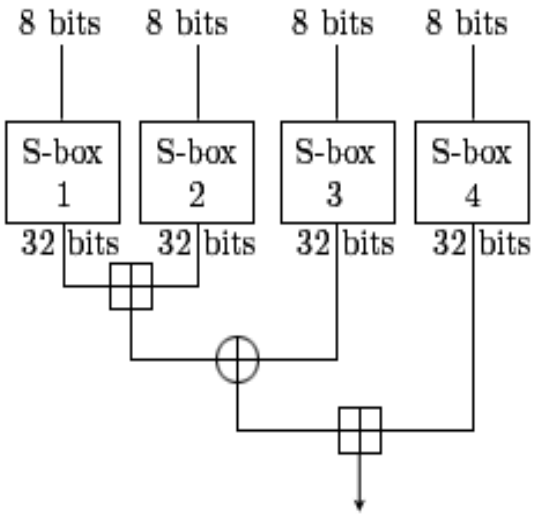


Fig.2 Blowfish's F-function Diagram

The diagram to the right shows Blowfish's F-function. The function splits the 32-bit input into four eight-bit quarters, and uses the quarters as input to the S-boxes. The outputs are added modulo 2^{32} and XORed to produce the final 32-bit output.

Uploading Files by Owner

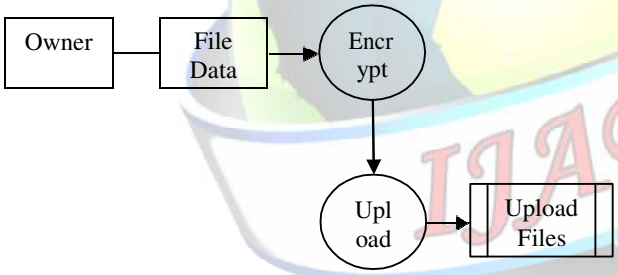


Fig.3 Uploading Files by Owner

It have the encryption algorithm, Encryption is the process of converting a plaintext message into ciphertext which can be decoded back into the original message. There are several types of data encryptions which form the origin of network security. Encryption schemes are based on block or stream ciphers. In this module the data owner give request to TPA(Domain) and get the username and password from TPA through mail. Data owner login with that user name and password, finally data owner upload the text file with encryption algorithm and also generate secret key.

Uploading Files by User

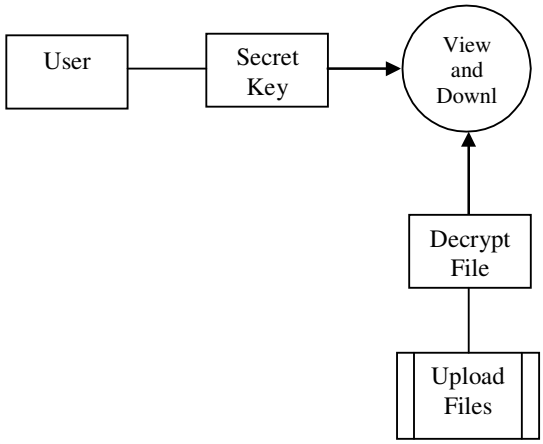


Fig.4 Uploading Files by User

User give a request to TPA(Domain) and get the username and password from TPA through mail. Data user login with that user name and password, Data user request to data owner and get the secret key from data owner, Finally data user to give the secret key and get the decrypt text file.

TPA Gives a Authority to Owner

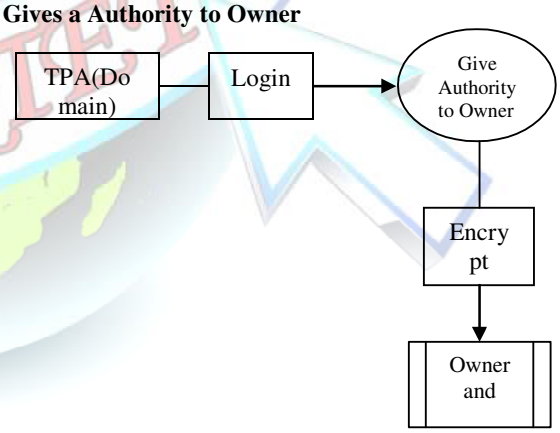


Fig.5 TPA Gives a Authority to owner

TPA(Domain) can be used to provide the authority for both user and owner. Its means data owner and user request to TPA for creating account. The TPA create data owner and user account with encrypt password. In this module advantages is the TPA not knowuser and owner password. The password automatically generate with encrypt algorithm.

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com

International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 4, Special Issue 11, March 2017

overturn process, decryption, to make the encrypted information readable again.

Admin Gives Authority to Domain

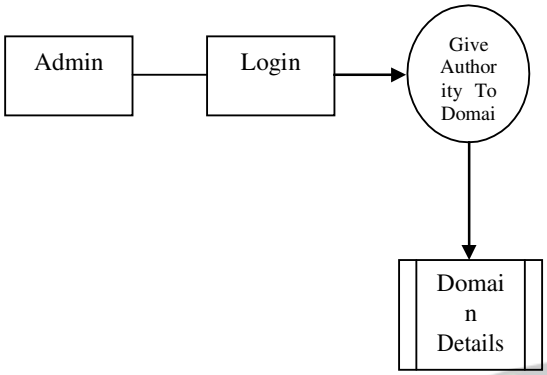
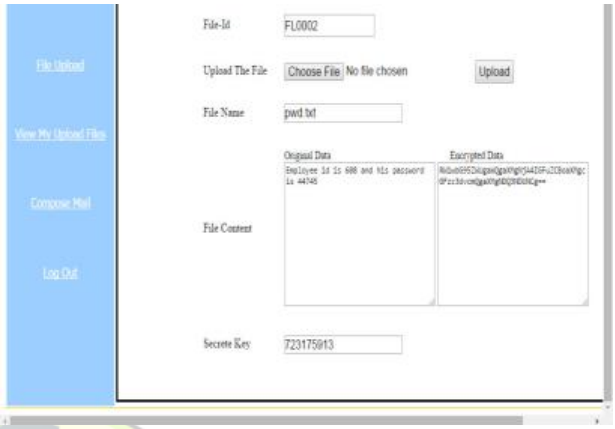


Fig.6 Admin Gives Authority to Domain

The authorization bar, a gray bar located below the main menu on each organizational module screen, contains the authorization number and symbol for your First Search account. Changes made in the administrative module affect the use of that account. If you have multiple First Search accounts, the authorization number in the bar reminds you of the account for which you are viewing settings. To view or change the settings for another account, you must log on to the administrative module using the authorization number and administrative password for that account. In this module the admin give to authority to domain and also view the domain details, owner details and user details. [5] discussed about Reconstruction of Objects with VSN. By this object reconstruction with feature distribution scheme, efficient processing has to be done on the images received from nodes to reconstruct the image and respond to user query. Object matching methods form the foundation of many state- of-the-art algorithms. Therefore, this feature distribution scheme can be directly applied to several state-of- the-art matching methods with little or no adaptation.



EXPERIMENTAL RESULTS

It provides security using Cryptography is the practice and study of hiding information.

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com

International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 4, Special Issue 11, March 2017

V- CONCLUSION

In this paper encryption algorithms have been proposed to make cloud data protected, vulnerable and gave concern to security issues, challenges and also comparisons have been made between AES, DES, Blowfish and RSA algorithms to find the best one security algorithm, which has to be used in cloud computing for making cloud data secure and not to be hacked by attackers data security on cloud and by association of different parameters used in algorithms, it has been found that AES algorithm uses least time to execute cloud data. Blowfish algorithm has least memory requirement. DES algorithm consumes least encryption time. . This secure attribute based cryptographic method for data security that's presence a shared in the cloud .It enhances the data security manner by ABE outsourced decryption technique using Blowfish algorithm.

REFERENCES

[1] Suqing Lin, Rui Zhang, Hui Ma, and Mingsheng Wang, ―Revisiting Attribute-Based Encryption With Verifiable Outsourced Decryption‖, IEEE Transactions On Information Forensics And Security, vol. 10, no. 10, october 2015.

[2] Attrapadung, J.erranz, F. Laguillaumie, B. Libert, E., ―Attribute-based encryption schemes with constant-size ciphertexts,‖ Theoretical Comput. Sci., vol. 422, pp. 15–38, Mar. 2012.

[3] Balamurugan B, Nirmala Devi M, Meenakshi R, Abinaya V, ―Cipher-text Outsourced Decryption with Enhanced Access Rights‖ , ICMCE – 2013.

[4] Bethencourt, A. Sahai, and B. Waters, ―Ciphertext- policy attributebased encryption,‖ in Proc. IEEE Symp. Secur. Privacy, May 2007,

[5] Christo Ananth, M.Priscilla, B.Nandhini, S.Manju, S.Shafiqa Shalaysha, "Reconstruction of Objects with VSN", International Journal of Advanced Research in Biology, Ecology, Science and Technology (IJARBEST), Vol. 1, Issue 1, April 2015, pp:17-20

[6] C.Gentry, ―Fully homomorphic encryption using

[7] Cheung and C. Newport, ―Provably secure ciphertext policy ABE,‖in Proc. ACM Conf. Comput. Commun. Secur., 2007.

[8] Chevallier-Mames, J.-S. Coron, N. McCullagh, D. Naccache, and M. Scott, ―Secure delegation of elliptic- curve pairing,‖ in Smart Card Research and Advanced Application vol. 6035,2014.

[9] Chung, Y. Kalai, and S. Vadhan, ―Improved delegation of computation using fully homomorphic encryption,‖ in Advances in Cryptology, vol. 6223, T. Rabin, Ed. Berlin, Germany: Springer-Verlag, 2010.

[10] Gennaro, Gentry, and B. Parno, ―Non-interactive verifiable computing: Outsourcing computation to untrusted workers,‖ in Advances in Cryptology vol. 6223, 2010.

[11] Green,Hohenberger, and B. Waters, ―Outsourcing the decryption of ABE ciphertexts,‖ in Proc. 20th USENIX Secur. Symp., 2011.

[12] Jin Li, Jingwei Li, Xiaofeng Chen, ChunfuJia and Duncan S. Wong, ―Secure Outsourced Attribute-based Encryption‖, , ICMCE-2015.

[13] Lai, R. H. Deng, C. Guan, and J. Weng, ―Attribute-based encryption with verifiable outsourced decryption,‖ IEEE Trans. Inf. Forensics Security, vol. 8, no. 8, pp. 1343–1354, Aug. 2013.

[14] M. Bellare and P. Rogaway, ―Random oracles are practical: A paradigm for designing efficient protocols,‖ in Proc. CCS, 1993.

[15] Matthew Green, Susan Hohenberger, Brent Waters, ―Outsourcing The Decryption Of ABE Ciphertexts‖, 2013.

[16] Pandey, A. Sahai, and B. Waters, ―Attribute-based encryption for fine-grained access control of encrypted data,‖ in Proc. ACM Conf. Comput. Commun. Secur., 2006..

[17] Ruby raju ,J.JerinJeysh,‖ Secure and Authenticated Group Data in Clouds Using ABE ―, Vol.2, No.2, February 2014.

[18] Sahai and Waters, ―Fuzzy identity-based encryption ‖ in Advances in Cryptology (Lecture Notes