Multi owner based data security in cloud using threshold cryptography: A Survey

Sagar Rakshe, Rushikesh Suryawanshi, Sachin Tandale, Onkar Thorawade

***Abstract*– Cloud computing has become very trendy service which can offer number of online services as well as online storage of data at low price. Other than these highly advance service there are number challenges like data confidentiality, data integrity and access control of data. There are some approaches which are previously suggested for data security but they aren't that reliable and feasible as in there are chances of data violation due to collision attack and heavy computation. To minimize these issues a proposed system this uses threshold cryptography in which data owner Divides users in groups and gives a single key to each user group for decryption of data, and each user in the group shares the parts of the key. There are multiple owners of keys in this proposed system. There is a Onetime session password (OTP) which is shared between user group and data owner for authentication of users. The key is encrypted using Deffie-Hellman algorithm which provides us secure transaction of file.**

***Index Terms*— Capability list, Threshold Cryptography, S-Hash, Deffie-Hellman, Authentication**

I. INTRODUCTION

We live in a world of technology where every day we come across lots of intelligent or smart computer. As day by day the main frame computer are been reduced to small size and made affordable to common people. To tackle problem of storage and security for user data cloud computing was introduced .It provide basically services like IaaS (Infrastructure as a service), SaaS(Software as a service),PaaS (Platform as a service).Users have right to access data from any part of the world and store data over it. There are various type of service provide by cloud like public, private, personal or hybrid the user can choose according to its need. Due to security provided as service by cloud many of institute and companies are exploring cloud and moving their business over it. But the problem with cloud computing is that people don't trust cloud

for storing their data as leaking the data can result loss in confidentiality of the industrial data.Many data securing scheme were introduce but they are suffering from data collision of malicious user and heavy computation. To overcome this Problem of heavy computation and data collision Access Control List (ACL) has been introduced which specifies the user right and permit permission accordingly. Deffie-Hellman algorithm has been used in this to generate session key or one time password. S-hash algorithm has been used for Encryption and Decryption of data

II. LITERATURE SURVEY

1) *Genetic Algorithm and Error back Propagation Neural Network:*

Vikas Sagar and Krishan Kumar [1] explain the use of cryptography for secure file transfer over cloud. The paper has introduced use of two algorithm like AES (i.e. Advance Encryption Standard) is a Symmetric encryption algorithm and RSA which is an asymmetric cryptographic algorithm in RSA two different keys are used public key and private key where public key can be used by everyone. The paper provides a secure way of file transfer by giving rights and Encryption for every file rather than providing password.

2) Cryptography in Cloud Computing:

Kajal Chachapara and Sunny Bhadlawala [2] proposed that paper has introduced new way of Symmetric cryptography. This paper use two algorithm for Encryption and Decryption of data i.e. GA (Genetic Algorithm) and EBP-NN (Error Back Propagation-Neural Network) where GA algorithm has been used for encryption and EBP-NN algorithm are used for Decryption of data. The paper introduces a way of transfer of file over wired or wireless network without causing collision. The use of hybrid method of generating keys for encryption and decryption has result in fast and secure way of file transfer over network so by fast and easy key generation algorithm the time complexity has been reduced rather than using other algorithm.

3) *Symmetric Key Encryption:*

***Sagar Rakshe,** Computer Engineering, SKN SITS, Lonavala,Pune, India, 9552285837..*
***Rushikesh suryawanshi**, Computer Engineering, SKN SITS, Lonavala,Pune, India, 8149945977.*
***Sachin Tandale**, Computer Engineering, SKN SITS, Lonavala,Pune, India, 7350982872.*
***Onkar Thorawade**, Computer Engineering, SKN SITS, Lonavala,Pune, India, 9423502315.*

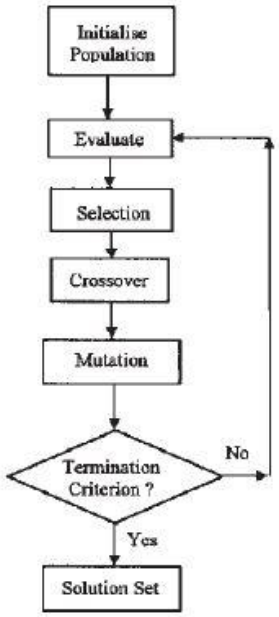
ISSN: 2278 – 1323

Mohammad Soltani [3] Suggests a new algorithm for Symmetric key generation the paper gives a new robust way of producing secure symmetric key. The paper proposes a way of cryptography where the file is divided in stages and each stage has five keys the part of the file is stored in one of the key. So during decryption the user has to choose the unique key at every stage if the user chooses the right key at every stage the user can be able to decrypt the file after decryption the part of the file are linked together and provide to user. This paper provides a secure way of file transfer but the problem with this algorithm is that the no of keys produce are too many which result in high time complexity.

I. STATISTICAL BASED CRYPTOGRAPHIC ALGORITHMS

1)*Error Back Propagation Neural Network(EBPNN) Algorithm***:**

One of most commonly used supervise artificial neural network is Error back propagation neural network (EBPNN). This model is very easy to understand, and can be easily implement as a software recreation.



Algorithm

1. Apply the inputs to the network and the initial weights that have been random numbers.
2. Then the input pattern is applied and calculates the output. If the output is completely not same to the target value, then calculate Error of each neuron.

The error is:
ErrorB=OutputB (1-OutputB) (TargetB – OutputB)

The term "Output *(1*-Output*)*" is a Sigmoid Function – if we were only using a threshold neuron it would be *(*Target –Output*)*.
3. We further change the weights.
Where, W+ AB be the new weight and WAB be the initial weight.

W+AB = WAB + (Error x Output). Update all the weights in the output layer similarly.
4. Calculate the Errors for hidden layer neurons. We can't compute these straight, so we back propagate them from the output layer. For this compute Errors from the output
Neurons and running them back during the weights to get hidden layer errors.
ErrorA= OutputA (1 - OutputA)(ErrorB WAB + ErrorC WAC)

This factor "Output *(1*–Output *)*" is present because of the sigmoid squashing function.
5. After calculating the Error for the hidden layer neurons now continue as in next stage to change the weights in hidden layer. By repeating this way we can prepare a network of any number of layers
The working can be easily shown in the following calculations:-
1. Calculate errors of output neurons
$\delta\alpha = out\alpha\ (1 - out\alpha)\ (Target\alpha - out\alpha)$

$\delta\beta = out\beta(1 - out\beta)\ (Target\beta - out\beta)$

2. Change output layer weights
$W+ A\alpha = WA\alpha + \eta\delta\alpha\ outA,$
$W+ A\beta = WA\beta + \eta\delta\beta\ outA$

$W+ B\alpha = WB\alpha + \eta\delta\alpha\ outB,$
$W+ B\beta = WB\beta + \eta\delta\beta\ outB$

$W+ C\alpha = WC\alpha + \eta\delta\alpha\ outC,$
$W+ C\beta = WC\beta + \eta\delta\beta\ outC$

3. Calculate hidden layer errors
$\delta A = outA\ (1 - outA)\ (\delta\alpha WA\alpha + \delta\beta WA\beta)$

$\delta B = outB\ (1 - outB)\ (\delta\alpha WB\alpha + \delta\beta WB\beta)$

$\delta C = outC\ (1 - outC)\ (\delta\alpha WC\alpha + \delta\beta WC\beta)$

4. Change hidden layer weights
$W+ \lambda A = W\lambda A + \eta\delta A\ in\lambda,$
$W+ \Omega A = W+ \Omega A + \eta\delta A\ in\Omega$
$W+ \lambda B = W\lambda B + \eta\delta B\ in\lambda,$
$W+ \Omega B = W+ \Omega B + \eta\delta B\ in\Omega$
$W+ \lambda C = W\lambda C + \eta\delta C\ in\lambda,$
$W+ \Omega C = W+ \Omega C + \eta\delta C\ in\Omega$
The constant η is put in to speed up or slow down the learning if required.

2)AES & RSA Algorithm:

A)AES Algorithm

AES is based on propose standard known as a substitution-permutation network, and it is fast in both software and hardware. Different its precursor AES, DES does not use a Feistel network. AES operates on a 4×4 column-major order matrix of bytes, term the state, even though some versions of Rijndael have a larger block size and have added columns in the state. Most AES calculations are done in special finite field.

1) KeyExpansion-: round keys are derived from the cipher key using Rijndael's key list
2) Initial Round:
    1. AddRoundKey—each byte of the state is combined with the round key using bitwise XOR.
3) Rounds
    1. SubBytes—Each byte is replaced with another according to a lookup table in non-linear substitution step.
    2. ShiftRows--Each row of the state is shifted cyclically a certain number of steps in a transposition step.
    3.MixColumns—Operates on the columns of the state, combining the four bytes in each column in a mixing operation.
    4. AddRoundKey
4) Final Round:
    1. ShiftRows
    2. SubBytes
    3. AddRoundKey

B) RSA Algorithm:

RSA involves a **private key** and a **public key**. The public key can be identified to everyone and it is used for encrypting messages. Messages encrypted with public key can only be decrypted using private key.

Key Generation:

1. Select two distinct prime numbers *q* and *p.*
2. Compute *n*= pq.
    n is used as the modulus for both the public and private keys
3. Calculate φ(*n*) = (*p* – 1)(*q* – 1), where φ is Euler's totient function.
1. Compute *n*= pq.
    n is used as the modulus for both the public and private keys
2. Calculate φ(*n*) = (*p* – 1)(*q* – 1), where φ is Euler's totient function.
3. Choose an integer *e* such that

1 < *e* < φ(*n*) and greatest common divisor of (*e*, φ(*n*)) = 1

Determine *d* as:

$$d = e^{-1}(mod\varphi(n))$$

Encryption:

$$c = m^e \pmod{n}$$

Where c is a cyphertext, M is file to be send, (n, e) is a public key.

Decryption:

$$m = c^d \pmod{n}$$

Given m it can retrieve the original file **M** by reversing the padding schemes.

SURVEY

TABLE

Project name	Year	Author	Algorithm	Advantages	Limitation	Application
Secure sharing with cryptography in cloud computing	2014	Kajal Chachapara Sunny Bhadlawala	Cryptography algorithms AES RSA	1)Use of Access Right List	1)Data intrusion easy due to Asymmetric and symmetric algorithm	Data compression, Data processing
A Symmetric Key Cryptography using Genetic Algorithm and Error Back Propagation Neural Network	2013	Vikas Sagar, Krishan Kumar	Symmetric key algorithm GA EBP-NN	1)Use of Hybrid algorithm 2)less time complexity	Collision of data can't be avoided	Stock exchange, Control systems
A New Secure Cryptography Algorithm Based on Symmetric Key Encryption	2014	Mohammad Soltani	Cryptography algorithms Public-key producing symmetric-key producing	1)Distribution of file and securing under a key	Large no of keys are created at each stage	Financial modeling, Data compression

ISSN: 2278 – 1323

CONCLUSION

The prime objective of our survey paper is to find out an efficient and effective way of transfer of file through server by using Symmetric or Asymmetric algorithm. The different algorithms used suffered from collision of data or high time complexity which result in failure of providing the basic necessity of security to file so to overcome this failure a hybrid algorithm should be introduce which would help in proper distribution of keys along the authenticate user

ACKNOWLEDGMENT

We take this opportunity to thank our project guide Prof. Pallavi Yevale and Head of the Department Prof. V.D Thombre for their valuable guidance and for providing all the necessary facilities, which were indispensable in the completion of this survey. We are also thankful to all the staff members of the Department of Computer of SKNSITS College of engineering, Lonavala, pune for their valuable time, support, comments, suggestions and persuasion. We would also like to thank the institute for providing the required facilities, Internet access and important books.

REFERENCES

[1] Sushil Kr Saroj, Sushil Kr Saroj, Aravendra Kr Sharma, and Sundaram Vats, "Threshold Cryptography Based Data Security in Cloud Computing" IEEE International Conference on Computational Intelligence & Communication Technology,2015

[2] Vikas Sagar and Krishan Kumar, "Symmetric Key Cryptography Using Genetic Algorithm And BPNN ANN IEEE Encryption ", 2015

[3] Kajal Chachapara and Sunny Bhadlawala, "Secure sharing with cryptography in cloud computing" Nirma University International Conference on Engineering (NUiCONE), 2013

[4]S. M. Metev and V. P. Veiko, Laser Assisted Micro technology, 2015.
2nd ed., R. M. Osgood, Jr., Ed. Berlin, Germany: Springer-Verlag, 1998.

[5] J. Breckling, Ed., *and* the *Analysis of Directional Time Series:*
Applications to Wind Speed and Direction, ser. Lecture Notes in
Statistics. Berlin, Germany: Springer, 1989, vol. 61.

[6]. S. Zhang, C. Zhu, J. K. O. Sin, and P. K. T. Mok, "A novel Ultrathin elevated channel low-temperature poly-Si TFT," *IEEE*
Electron Device Lett. vol. 20, pp. 569–571, Nov. 1999.

[7]Menezes, P. van Oorschot and S. Vanstone, "Handbook of Applied Cryptography". CRC Press, First ed., 1997J. Clerk Maxwell, A Treatise on Electricity and Magnetism, 3rd ed., vol. 2. Oxford: Clarendon, 1892, pp.68-73.

AUTHORS

Sagar Rakshe ,he is an engineering student of computer at SKNSITS, Lonavala , Pune , affiliated under Savitribai Phule Pune University.
His interest is in the field of Artificial intelligence. He has a great interest in Networking and Security. Also he has an interest in coding.

Rushikesh Suryawanshi, he is an engineering student of Computer at SKNSITS, Lonavala, Pune, affiliated under Savitribai Phule Pune University.
His interest is in the field if Artificial intelligence. He has a great interest in the field of animation.

Sachin Tandale , he is an engineering student of Computer at SKNSITS, Lonavala, Pune, affiliated under Savitribai Phule Pune University.
His interest is in the field if Artificial intelligence. He has a great interest in the field of home Automation. Also he has a great knowledge of SQL and database management.

