International Journal of Advanced and Innovative Research (2278-844)/

Volume 7 Issue 11

IF SECURE SESSION KEY BASED CLOUD ACCESS AND DISTRIBUTION SYSTEM

[1]Sumanjali Billi, [2]I Surya Sekhar

[1]Research Scholar, [2]Assistant Professor, Department of Computer Science & Engineering

KODADA Institute of Technology & Science For Women, Kodad

Abstract: Cloud computing is a new approach in the field of information technology based on the World Wide Web. It is new approach in the field information technology and also it satisfies a end users requirement for computing resources like services and applications etc. Security is one of the most challenging issue in the cloud computing. In cloud computing, services need to address the security during the transmission of sensitive information. Many organization, companies or banks have confidential information, this information is very essential. The cloud does not provide a fully guaranteed of data and it is compromised by the attackers. In this paper by providing a new method, we improve the security of data access in the cloud computing for a bank or any other particular location by using location-based encryption.

Keywords: - Cloud Computing, Services, Security, Geo-Encryption, Location-Based Encryption.

1. INTRODUCTION

In today's Information Technology epoch, processor networks are usually used to share information and to communicate with others. The chances of compromising the information being transferred over the networks are ever-increasing. Susceptible data is required to be protecting from unauthorized admittance from transmitting over insecure and timid networks for instance Internet. Safety measures during transmit of data has turn out to be one of the difficult challenge in excess of the networks. To deal with the data safety issues Cryptography is one of the techniques. It is based on encryption and decryption algorithms for secure transmission of data over the network. It is technique that has been used about thousands of years for keeping the data secure from others. These days modern cryptography techniques are used to provide safety measures which uses arithmetic techniques and based on two essential components: Algorithm and a key used to establish the algorithm operation. This modern cryptographic method objective is to attain the security goals such as data secrecy, data reliability, non-repudiation and verification. Using the computer networks for transferring the credit card information, transfer electronic credentials, online shopping, etc. every single one transmission require an well-organized security system. There is a possibility of interpretation the information by an unauthenticated third party. Cryptography is a proficient method that uses encryption and decryption to secure the data from illegal access.

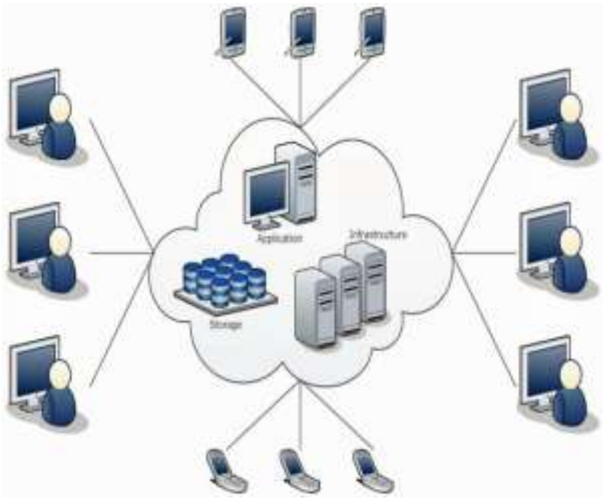

Figure 1.1: Cloud Computing Environment.

To conserve reliability and isolation of data, encryption and decryption methods are used. The plaintext is the original form of data and the cipher text is the encrypted form of data. Encryption techniques obtain pure content (original form of data) as an input and translate it into cipher text (encrypted form of data), based on input algorithm using a secret key. An input is a component on the basis of which information is encoded. Decryption technique obtain the encoded text (encrypted form of data) and convert it into plain text (original form of data) based on algorithm using a key input. Cryptography algorithms are classified into two categories based on the keys used: Bilaterally symmetric Key Coding algorithms and Unsymmetrical Key Coding algorithms. In Symmetrical Coding method solitary key input is required for encoding and decoding the data. A key input is transfer to both sender and recipient proceeding to connection. It is also best-known as surreptitious key cryptography algorithm. On the further side, Asymmetrical key Coding method put-upon a key input in couple well-known as private key and public key. The public key is utilized for encode the content but private key is utilized for decipher the content. They are also called public key cryptography techniques. Symmetric key encryption is faster than asymmetric key encryption.

Cloud computing is a current mechanical advancement in the processing field in which principally centered around outlining of administrations which can be given to the clients in same path as the essential utilities like sustenance, water, gas, power and communication. In this innovation administrations are created and facilitated on the cloud (a system intended for putting away information called datacenter) and afterward these administrations are offered to clients dependably at whatever point they need to utilize. The cloud facilitated administrations are conveyed to clients in pay-per-utilize, multi-tenure, versatility, self-operability, on-request and practical manner[3]. Cloud computing is turned out to be well known in light of above say administrations offered to clients. Every one of the administrations offered by servers to users are given by cloud specialist organization (CSP) which is working same as the ISP (Internet specialist organization) in the web figuring. In the web make some creative improvement in virtualization and dispersed figuring and getting to of fast system with minimal effort draw in center of clients toward this innovation. This innovation is composed with the new idea of administrations provisioning to clients without buying of these administrations and put away on their nearby memory [4].

2. LITERATURE REVIEW

This section describes the various researches carried out by researchers in the cryptography field for securing the data. Various IEEE transactions, journals are studied and the gaps are identified to develop an efficient and effective symmetric key encryption algorithm.

Some of the research papers reviewed to achieve the objectives are described as follows:

M. Yamuna [19] et.al proposed an algorithm that uses matrices for encrypting the message. A 26×26 matrix is taken in which the rows and columns of the matrix represents the alphabets from A-Z. The diagonal matrix A is created by entering the label value of the symbol in the word in the corresponding diagonal positions. In order to distinguish between two alphabets in a word ‘0’ is used. This process is iterated for remaining text. The other elements except the diagonal elements are filled in by randomly taken numbers and missing labels represents blank spaces. Then a key matrix B is chosen and multiplication is performed with this diagonal matrix A. The matrix C obtained after multiplication is sent to the receiver in the form of two dimensional arrays. To decrypt the data product of the inverse of the key matrix is performed with the encrypted matrix C at receiver side. As the method improves the security of the data but it encrypts only English alphabets that can be simply altered and the span of the matrix is limited to the sort of 26×26. The estimated procedure creates matrix dynamically depend on the length of the data and personal key is obtained based on the array of the matrix. It can encrypt any text. It is effective and efficient in protecting the data. It is difficult to guess the key because of the generation of random keys. The security further improved by using logical XNOR operation and the encoded matrix.

Devendra Prasad [20] et.al proposed a cipher algorithm for encrypting the message uses fundamental encoding cryptography of swapping and transposition and generate result with the help of logic gates and operation performed on the data. The arbitrary digit initiator function used makes cryptology more complex which decides the sequence of encoding rounds and keys to be used for encrypt the plain text. It uses random number and function to resolve the issues of overhead presents in fixed key. That arbitrary key is further added to the original text either at end of the message or the beginning of the message while transferring it to the receiver. If the size of data is multiple of two, key is to be supplementary at the outcome of the unique text and random figure the information will be placed at the starting of message. Otherwise, inverse operation is performed. The random keys generated are of fixed length, brute force attack can be performed. The proposed algorithm generates random keys of variable length so it is difficult to approximate the extent of the key input until the categorization of the obtained matrix is not identified. Thus keys are safe beside cryptanalysis intrude.

Udepal Singh [21] et.al projected a method depended on ASCII standards of data. The ASCII values of characters are in use and an arbitrary key of four characters is created from the data. Then data is encoded by applying different transformations with the help of key. The restriction is that it cannot encode sequential type of information and for all original data; a fixed key input of four characters is generated. The proposed system uses variable length key whose length varies as the length of the matrix changes. If anyone has to know key first of all it should know the matrix order then key length.

Charru [22]et.al proposed a symmetric key encryption algorithm overcoming the drawbacks of existing approaches that generates key of fixed length .In this algorithm ASCII values is used to translate the information and a key input of changeable size is generated depend on the length of the key data by means of various arbitrary cipher. The encoded data is then operated by XOR action to raise security point. The key characters should be known to decrypt the data. The execution time, key length value, security level, acceptance of sentence form and security issues are the parameters taken to compare the algorithm with the existing approaches. Although the algorithm shows less execution time as compared to other algorithms but the limitation is that the extent of key will be unchanged if the dimension of the essentials is bigger than ten bit. In the conventional algorithm the dimension of the key will not be unchanged if the length of the information increases as it depends on the order of matrix created which makes the cryptanalysis difficult. It enhances the security being dynamic in nature as well as the use of logical XNOR operation and the encoding matrix.

J Gitanjali [31] proposed an encryption technique based on ASCII values and a key is used to encrypt these ASCII values. The palindrome number and alphanumeric id used by the key are also converted into ASCII values. The palindrome number is generated by using the summation of the private key that makes the message difficult to decode for the attacker. Then to create encoding matrix this number is further used. The matrix multiplication used increase the security of the data. The proposed system convert the information into the matrix created dynamically and keys are generated randomly. The information is unknown to attacker until it knows the order of the matrix thus protecting the system from cryptanalysis attacks.

3. PROBLEM IDENTIFICATION

There are different techniques with the cloud computing data storage, its applicability over the data center, server and accessing is performed by different user. Multiple file upload and its usage make to access it from the cloud data storage and its server.

As the study is in use and performed with unusual technology and unusual consequence from the algorithms such as RSA , AES, Hash Based and other additional technique for information processing , safety approach over information accumulate . The methodology for safety over the cloud statistics is furthermore performed by dissimilar services to formulate it more protected and reachable.

In the lead verifying different state and the accessible method different tiny comes with the Existing algorithm AES-SHA2 with organizer based re-duplication which is in use as found for our investigate work.

The subsequent are the maintained points which recognized as trouble and supplementary analyzed and performed further with enhancements.

1. Prior method such as file based scheduling doesn't over count all its data parts , or internal division which can further be duplicate over the large amount of data . Thus an efficient monitoring is required which can further be monitor file duplicacy with data division.

2. AES algorithm takes an advantage of asymmetric encryption technique which is used by base paper , but still when we talk about the multiple tenant, multiple ownership and multiple user over the data. Thus an security of key sharing is still a challenging issue which is faced by authors.

3. The Key length taken for the purpose of security in previous research is not considerable today . Today's scenario required an efficient and long length key for security purpose.

4. The existing approach for security uses MD5 for the hashing for content matching, but the MD5 algorithm faces collision issue with value generation. Hashing algorithm is the best practice to have long hash value.

5. A permutation of MD5 and AES is use for the concern which is neigh more safe while discussion about key substitute, one more additional procedure is mandatory to do the input exchange. Consequently it exhibit further computational instance as well as computation rate for cloud server.

6. A box file intensity re-duplication algorithm by file hash MD5 is used, which be able to come under clash scenario and invention forged outcome when it conditions to huge quantity of server data files.

7. The existing algorithm take advantage over previous traditional techniques but still more refinements are required as per todays standard. Thus a better security, hashing mechanism can make it more reliable and executable to tackle with current security and cloud scenario in the world.

4. PROPOSED METHODOLOGY

As per our examination regarding the preceding method and their drawback in dissimilar terms and scenarios. Our vocation present a innovative approach which is extremely secure and consumes low computational time and thus computational cost over the huge number of prearranged accessible dataset. Our work suggest a innovative algorithm future algorithm with more safe algorithm blowfish is performed beside with SHA-2 and resemblance compute achieve as more secure hashing approach. Our algorithm also checks for appropriate redundancy by means of more protected and consistent parameters.

The projected algorithm is described below:

Algorithm Pseudo Code

Input: File F, Session Key Sk, UB ub, VM v

Output: Data processing, Encrypted Data Ed, Computation time, Bandwidth

```
Begin: Steps 1-
Initialize Cloud component (Vm, Ub, Sk, F)
{
VM setup i-n;
Ub Ui-n;
}
Processing File(F,K)
{
Processing File input F;
Session Key Sk;
LockBox (Sk,F);
Share LBox;
Data Encrypt();
DefineUsers(Share LockBox);
Data security & Sharing();
Return CCost & Bw;
}
End;
```

The figure below represent the complete flow of the proposed scenario which represent our work and computes parameters efficiently.

5. RESULT ANALYSIS

Performance Measures

Computation Time

A instruction time of a dataset in Java is computed with the help of initial and final time class variables distinct in the device and here as we load the dataset and verifies the eligibility and taking their features for consideration or not is the time taking process to recognize and to load the images and selection of password comes under training time of a dataset, extracting the properties and making them in process configure is training time.

TECHNIQUE APPROACH	EXISTING ALGORITHM (COMPUTATION TIME IN MS)	PROPOSED ALGORITHM(COMPUTATION TIME IN MS)
100 KB	400	372
500 KB	1340	1121
1 MB	3920	3600
2 MB	5730	4674
5 MB	9765	8788

Ct = Final Time Completion – Initial Time;

Bandwidth

A Bandwidth in cloud and network server is the total consumption of data amount in its process. All the data consumption including coding part, client end graphics and many other components which are related. They are being found the usage. All the combination data usage by all resources get to the bandwidth computation.

Bw = Summation Of (All Data Usage By Resources);

Traffic Volume

Traffic volume is also one of the important parameter of monitoring the parameter for comparison. It can be computed as total work performed by the available resources. It is the product multiplication of traffic intensity with time.

Tv = Traffic Intensity*Time;

Traffic Cost

An specific amount of financial unit which measure the volume and convert it into the traffic cost.

Tc = Tv* Basic Unit Cost Value;

Chunk Speed

A chunk speed can be defined in MBPS or KBPS, it is specifically the speed at which chunking is performed either at sender side or either at receiver side.

Table 1.1: Comparison Analysis Between Existing And Proposed Approach.

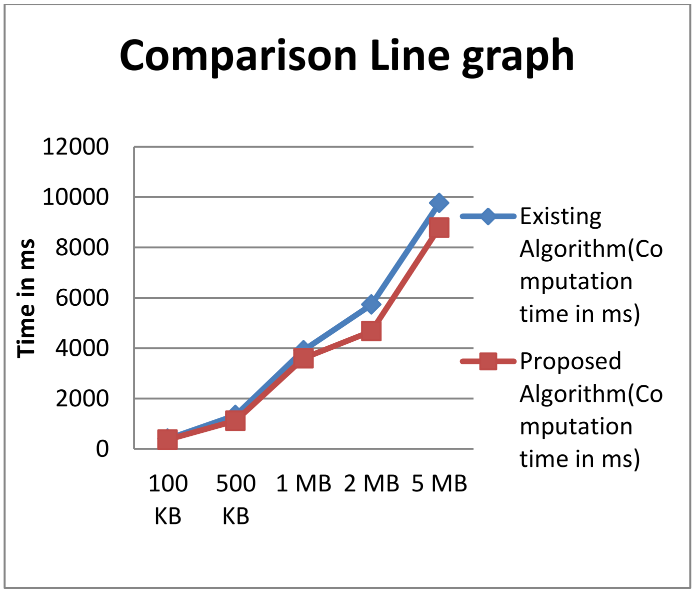

Figure 1.2: Comparison Graph Analysis Between Existing And Proposed Approach.

In the figure 1.2 above, a Line Graph is plotted between existing security algorithm and proposed algorithm. The experiment results show the efficiency of our proposed work over existing work scenario.

Table 1.2: Comparison Analysis Between Existing And Proposed Approach.

TECHNIQUE APPROACH	EXISTING ALGORITHM(BANDWITH KBPS)	PROPOSED ALGORITHM(BANDWITHKBPS)
100 KB	256	275
500 KB	226	259
1 MB	178	198
2 MB	156	173
5 MB	143	158

In the table 1.2 above, it shows the Bandwidth uploading different data and time taken to process them. The proposed algorithm executed shows the efficiency of our proposed approach over existing scenario.

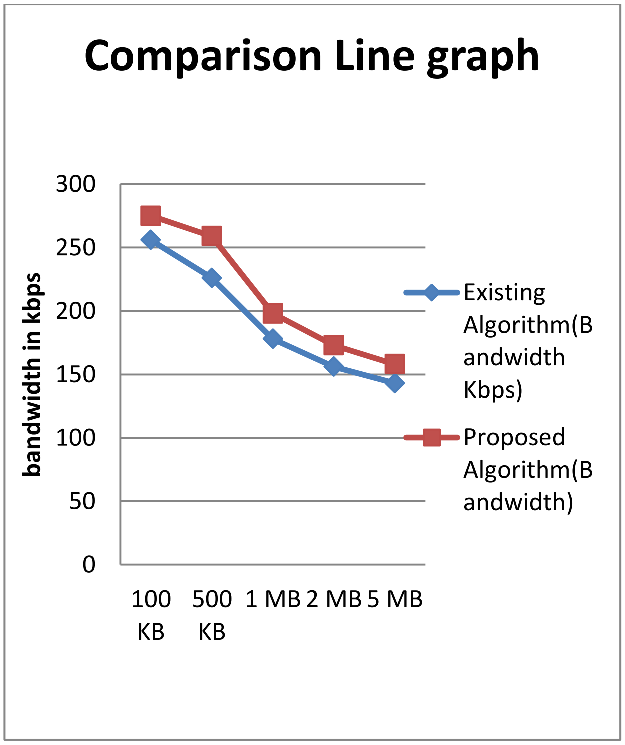

Figure 1.3: Comparison Graph Analysis Between Existing And Proposed Approach.

In the figure 1.3 above, an line graph is plotted between existing security algorithm and proposed algorithm. The experiment results show the bandwidth of our proposed work over existing work scenario.

5. CONCLUSION & FUTURE WORK

Our proposed algorithm makes use of comparison parameter as computation time as well as computation cost to compute the comparison analysis. The algorithm is developer in Java language with Java net-beans tool setup using intel i3 processor, 750 GB RAM. The comparison analysis and execution result shows that our proposed approach PROPOSED outperform best while comparing with existing algorithm.

A consistent proposed algorithm provides an high level security alongside de-duplication approach with data store. There are still further work can be done to prove our work in knowledge and for industry use. The following work is left for future work.

1. The real time execution can be finished, which be able to relate over the business level cloud infrastructure and to find it more protected, dependable than the other alternate existing over the web.
2. Further study over the Hashing can be completed, thus that an elimination of that part can be done, which can make it more fast easily reachable.
3. An study of system can be derived and performed with different operating system with other file format values.

REFERENCES

[1] Jianghong Wei,Wenfen Liu,Xuexian Hu"Secure Data Sharing In Cloud Computing Using Revocable-Storage Identity Based Encryption"-PKC 2015.

[2] Seo and Emura,"Towards black-box accountable authority IBE with short ciphertext and private keys,in Public Key Cryptography"–PKC 2009. Springer, 2009, pp. 235–255.

[3] J. H. Seo and K. Emura, "Revocable identity-based encryption revisited: Security model and construction,in Public-Key Cryptography"–PKC 2013. Springer, 2013, pp. 216–234.

[4] K. Liang, J. K. Liu, D. S. Wong, and W. Susilo, "An efficient cloud-based revocable identity-based proxy re-encryption scheme for public clouds data sharing," in Computer Security-ESORICS 2014.Springer, 2014, pp. 257–272.

[5] S. Ruj, M. Stojmenovic, and A. Nayak, "Decentralized access control with anonymous authentication of data stored in clouds," Parallel and Distributed Systems, IEEE Transactions on, vol. 25, no. 2, pp. 384–394, 2014.

[6] K. Yang and X. Jia, "An efficient and secure dynamic auditing protocol for data storage in cloud computing," Parallel and Distributed Systems, IEEE Transactions on, vol. 24, no. 9, pp. 1717–1726, 2013.

[7] B. Libert and D. Vergnaud, "Adaptive-id secure revocable identity-based encryption," in Topics in Cryptology–CT-RSA 2009. Springer,2015. pp. 1–15.

[8] L. M. Vaquero, L. Rodero-Merino, J. Caceres, and M. Lindner, "A break in the clouds: towards a cloud definition," ACM SIGCOMM Computer Communication Review, vol. 39, no. 1, pp. 50–55, 2012.

[9] K. Chard, K. Bubendorfer, S. Caton, and O. F. Rana, "Social cloud computing: A vision for socially motivated resource sharing," Services Computing, IEEE Transactions on, vol. 5, no. 4, pp. 551–563, 2012.

[10] iCloud. (2014) Apple storage service. [Online]. Available: https://www.icloud.com/

[11] Azure. (2014) Azure storage service. [Online]. Available: http://www.windowsazure.com/

[12] C. Wang, S. S. Chow, Q. Wang, K. Ren, and W. Lou, "Privacypreserving public auditing for secure cloud storage," Computers, IEEE Transactions on, vol. 62, no. 2, pp. 362–375, 2013.