Simulated Cryptography Algorithm for Enhanced Security of Cloud Data

Susant Kumar Dash
Associate Professor
Department of CSE
MITS,Rayagada,Odisha

Chidananda Panigrahy
Assistant Professor
Department of CSE
KIT,Berhampur,Odisha

ABSTRACT
Today Service Providers are achieving ever-increasing transmission over networks due to Cloud and Web services bang. But information security of user as well as provider is a main apprehension whenever we talk about the implementation of network services. In this paper the proposed work has developed a new cryptography algorithm which is based on concept of block cipher. In this algorithm I have used logical operation like XOR and shifting operation. Experimental results illustrate that proposed algorithm is more efficient and secured than existing techniques.

From the service provider's point of view, a typical simulated optimal algorithm handles various significant issues such as standard communication infrastructure, distributed network graph and language transparency. This paper shows the work in progress on this particular feature introducing a practical development, giving an outline on the subject, security management using cryptography algorithm presenting a view on further research. The proposed algorithm has the batter speed compared with the comparing encryption algorithm. However, the proposed algorithm expands encryption security by introducing the symmetric layer. The planned algorithm will be beneficial to the applications which require the same procedure of encryption and decryption. The cryptography techniques used in current research also applied in stenography applications.

Keywords
Encryption, Cryptography, Symmetric layer, XOR operations and Network Security Graphs.

1. INTRODUCTION
The Cloud Computing is a flexible IT service over internet. However it also causes to a high level of risk of data loss or hacking. In cloud essential services are always outsourced to a third party that makes fir it a threat to its security and privacy. This research is about the key encryption technique used by data owner in clouds. The existing system carries hierarchical variant in which entity node form a tree structure called hierarchy [1].

In the proposed system of this research a simulated cryptography algorithm scheme is implemented in which keys are linked to root nodes as well as neighbor nodes. In this simulated cryptography algorithm, any data owner has its own identity and a master key; it can also provide secret keys to other delegate nodes.

In the results of this research we will show the enhancement work using graphs and comparison analysis. The graph analysis represents the comparison among existing and extended cryptography technique. Through this research we reported that proposed encryption technique is more secured technique for any cloud network.

With Cloud implementation, the user's trust margin will develop into dynamic and will move beyond the control of any application provider. The system, structure, and application margin of an organization will enlarge into the Cloud Service Provider domain. The trust governance and control model will continuously establish and enhances the loss of control. That is where we need Federated Identity; it allows end users to keep their own directories and confidential exchange information from them [2]. Federated trust and identity management enables:

- Cloud resources access become easy
- Advanced end-user knowledge through SSO and just-in-time account provisioning
- Enhances authentication and permission By reducing cost and time
- Exclusion of non-scalable proprietary SSO applications

Cryptography is the methods that allow information to be sent in a secure from in such a way that the only receiver able to retrieve this information. Presently continuous researches on the new cryptographic algorithms are going on. However, it is a very difficult to find out the particular algorithm, since we have already identified that they must reflect many factors like: security, the time complexity and space complexity. Figure 1 is representing conventional encryption.

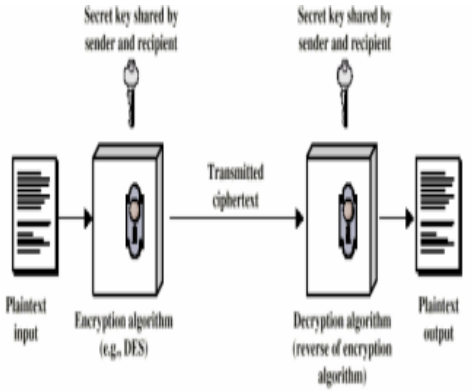

Fig. 1: A Simplified Model of Conventional Encryption [2]

Security Services: If we are compelling about security of information then subsequent services come in mind.

- Confidentiality (privacy)
- Authentication (who created or sent the data)
- Integrity (has not been altered)
- Non-repudiation (the order is final)
- Access control (prevent misuse of resources)
- Availability (permanence, non-erasure)

To write this paper I hadstudied about data security using cryptography technique. After the thorough study of Network security using cryptography, I presented my proposed work through this paper. This paper is mainly divided in four sections. Section-I consists of just basic introduction about Cloud data Security using cryptography, section-II includes detailed description of Information security using cryptography and their various algorithms, section-III consists of proposed algorithm and experimental results, and in section IV summary and references of research.

2. RELATED WORK

The research work of encryption simulation will be based on the model of memory and side-channel attacks, reported by Akavia [3].

According to the above mentioned study we can learn authentic information about the secret state of a system, by selecting polynomial time function:

$$f_i : \{0, 1\}^* \rightarrow \{0, 1\}^{\lambda i} \qquad (1)$$

and knowing the values of fi applied to the inner state of the system.

There are two main variants of the memory attacks model, known as the bounded-leakage and the continual-leakage models. Both are different in sense of life-time existence and similar in sense of having secret keys and public keys [4].

To define an example of cryptography technology used in security system Bishop [5] identifies military security policies and commercial security policies as two discrete types of policies that underline the difficulty in developing an all-purpose security model.

Military security strategies are characterized as essential concerned with protecting data privacy while business security approaches basically concentrate on ensuring data trustworthiness. The dichotomy between administrative and business needs prompted the improvement of two unique access control instruments, Mandatory Access Control (MAC) and Discretionary Access Control (DAC).

Velte et al. [6], give a general outline of distributed computing. These researches covers the definitions, profits, security, agreeability, administrations, and the various ranges and viewpoints identified with distributed computing. Other extra sources were utilized to supplement the idea of distributed computing and its security.

All material on each page should fit within a rectangle of 18 x 23.5 cm (7" x 9.25"), centered on the page, beginning 2.54 cm (1") from the top of the page and ending with 2.54 cm (1") from the bottom. The right and left margins should be 1.9 cm (.75”). The text should be in two 8.45 cm (3.33") columns with a .83 cm (.33") gutter.

3. EXISTING CRYPTOGRAPHY TECHNIQUES

3.1 Identity based Encryption

An identity based encryption system based on a public-key crypto system that allows users to encrypt messages knowing only the recipient’s identity and some public parameters. It includes four main parameters [3]:

- Setup
- KeyGen
- Encrypt
- Decrypt

Function: Decrypt (Encrypt (M, I) KeyGen (M, K’, I)) = M

If the identifying key‘I’ is used through the encryption of message M is same as the identity of secret key K used during the decryption.

3.2 Hierarchical Identity-based Encryption

In this system, entities form a structured hierarchy: a user can delegate keys to its subordinate identities, and thus decrypt any message encrypted to them. It handles identity vectors I= (I_1…..I_j) and define children of I as I_z. It includes five main parameters [4]:

- Setup
- KeyGen
- Encrypt
- Delegate
- Decrypt

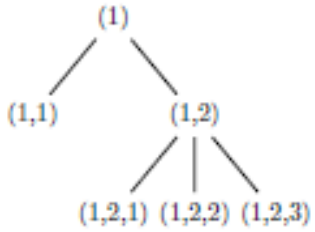

Fig. 2: Vector identities in a hierarchy [4]

3.3 Spatial Encryption

In spatial encryption scheme, the secret keys are linked to sub-nodes of tree and the delegation relation is defined by sub-node inclusion. From HIBE we got identity vector and if we apply secret keys as Z^n_N, and n ranges to 0 to N. We can associate it in double space manner like I_1…….I_j, I_{j+1}……..I_n Є Z_N.

It includes five main parameters [6]:

- Setup
- KeyGen
- Encrypt
- Delegate
- Decrypt

This is based on cipher text technique. However this scheme still has a drawback of not handling leakage of data though cloud networks.

4. EXISTING WORK

The security of existing framework is dependent upon simulation, called Masterleakspatial. In this simulation, the challenger first makes a call to Setup, to get a mystery key for the entire space, and open parameters that it can provide for the enemy [7]. In a first stage, the recipient can make a polynomial number of questions, in any request:

- Create queries to store keys in an display;
- Leak queries to apply a release capacity of his choice on any key (as long as the aggregate number

of released bits for a certain key does not surpass LSK-Leaky System Key);

- Or Reveal questions to recover an entire key (as long as it is not a key partnered to the entire space, evidently).

At the end of this Final stage, the opponent picks a test vector u* such that none of the uncovered spaces and two messages m0, m1 hold it. It offers them to the challenger, which picks an irregular bit β and returns Ct* = Encrypt (mβ, u*).

It consists of just four main parameters:

- Setup
- Delegate
- Encrypt
- Decrypt

The formal meaning of the amusement Master leak spatial, which is depicted in as below steps comprises of the accompanying stages:

Setup: The challenger makes a call to Setup (1_λ) and gets a key SK for the entire space and people in general parameters PP. It offers PP to the enemy [7, 8].

- **Stage 1:** In this stage, the enemy can make any of the accompanying inquiries to the challenger, in any conceivable way: Create Leak, Reveal, and Delegate. These calculations are recorded in form of key data.
- **Challenge:** The enemy picks a test vector u* such that no component of R holds it, and two messages m0, m1 of equivalent size. It makes a call to LR (u*, m0, m1) and acquires a ciphertext Ct*.
- **Stage 2:** This is the similar as Phase 1, with the exception of the main permitted inquiries to Create and Reveal for mystery keys whose space does not contain u*.
- **Guess:** The adversary chooses a bit β' and calls Finalize (β'). If the output is true, it succeeds.

5. PROPOSED METHODOLOGY

Here we are using symmetric encryption approach. We havealready know that symmetric encryption approach is divide in two type one is block cipher symmetric cryptography technique and another is stream cipher symmetric cryptography but here we are choosing block cipher type because its efficiency and security. In the proposed technique we have a common key between sender and receiver, which is identified as private key.

Basically private key concept is the symmetric key concepts where plain text is converting into encrypted text known ascipher text using private key where cipher text decrypted by same private key into plane text. The encryption key is trivially related to the decryption key, in that they may be identical orthere is a meek transform to go among the two keys. The keys, in practice, denote a shared secret between two or more parties that can be used to preserve private data. Elementary concept of symmetric cryptography is shown in Fig.3.

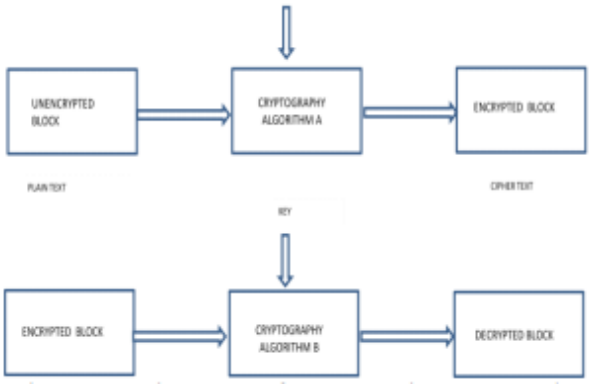

Fig. 3: Basic Concept for Symmetric Cryptography

4.1 Drawback in Existing Technique

- Low-power "Sensor Nodes (SN)" with partial functionality;
- The existing techniques are based on Leaky System Key in which lots of database requirements in key management.
- The user and server connection is necessary in dispatch and receiving of information.
- The techniques used are applicable only in cloud data.

The existing techniques are less efficient and secured than our proposed block based encryption.

5.1 Steps of Proposed Algorithm

- Firstly select plane text of 16 bytes to 64 bytes depending on requirement.
- Secondly insert key of size 16 bytes to 64 bytes depend on plane text value
- Apply XOR operation between key and plane text block. Result will store in Cipher_Block1.
- Apply right circular shift with 3 values. Result will store in new Cipher_Block2.
- Repeat step 1 to 7 till (Encryption Number / 4).
- Exit.

6. SIMULATION RESULTS

Simulation results have demonstrated the efficiency of simulated cryptography techniques.

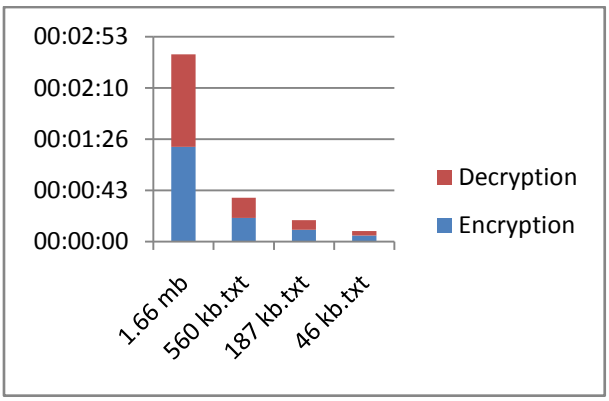

Fig. 4: Efficiency increment of cloud data security using block based cryptography

The above fig.4 presented that using the implementation of simulated cryptography technique the efficiency increment values are 2-20 per units of time as considered.

6.1 Comparison Results

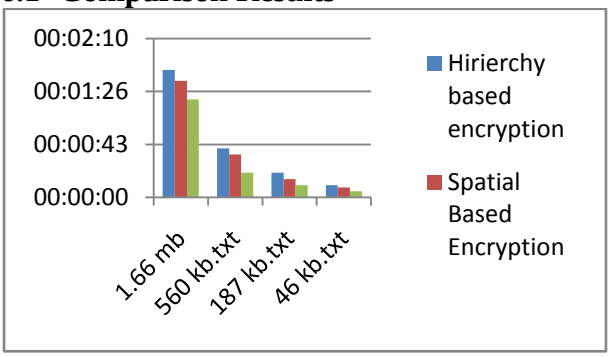

Fig. 5: Comparison graph between existing and simulated Cryptography technique

The graph represents the comparison among encryption techniques through analysis of attack number in presence of particular encryption technique.

7. CONCLUSION

Security in cloud computing must be approached carefully. Numerous associations are moving to the Cloud, so the effect of potential ruptures gets ever more elevated. Multi-inhabitant architectures and virtualization innovations permit cloud administration suppliers to get the most adequacy of their foundations, additionally empower another ambush vector not show in the recent past. The hypervisor/VMM is available at the virtualization layer overseeing and controlling the cooperation of the distinctive virtual machines and the host OS/equipment. The research work done or simulations used in block based cryptography enhances security in cloud data.

The center of future works ought to mean to solidify the security of virtualization in multi-inhabitant situations.

8. REFERENCES

[1] Jill-Jenn Vie, Michel Abdalla, Crypto Team, "A Leakage- Resilient Spatial Encryption scheme", August 23, 2011.

[2] Rosado DG, Gómez R, Mellado D, Fernández-Medina E (2012) Security analysis in the migration to cloud environments. Future Internet 4(2):469–487.

[3] Akavia. C., On the power of simple branch prediction analysis, IACR Cryptography, report/ 2006.

[4] Marinos A, Briscoe G (2009) Community Cloud Computing. In: 1st International Conference on Cloud Computing (CloudCom), Beijing, China.

[5] Bishop, S. Kim, M. Okajima and P. Rämö, Multitenant Utility Computing on IBM Power Systems Running AIX, IBM Redbooks, February 2009, http://www.redbooks.ibm.com/redbooks/pdfs/sg247681.pdf

[6] Velte. They want froot loops: Why industry will continue to deliver multi-level security. In SACMAT'01, pages 145–146. SACMAT, May 2001.

[7] Li W, Ping L (2009) Trust model to enhance Security and interoperability of Cloud environment. In: Proceedings of the 1st International conference on Cloud Computing. Springer Berlin Heidelberg, Beijing, China, pp 69–79

[8] Marsha, The Center for Internet Security, Security Configuration Benchmark for VMware ESX 3.5, December 2009, http://benchmarks.cisecurity.org/tools2/vm/CIS_VMware_ESX_Server_3.5_Benchmark_v1.2.0.pdf

[9] A.Nath, S.Ghosh, M.A.Mallik; Symmetric key cryptography using random key generator, Proceedings of International conference on SAM-2010 held at Las Vegas(USA) 12-15 July,2010, Vol-2,P-239-244

[10] A.Nath, S.Das, A.Chakrabarti; Data Hiding and Retrieval, Proceedings of IEEE International conference on Computer Intelligence and Computer Network held at Bhopal from 26-28 Nov, 2010.

[11] Neal Koblitz "A Course in Number Theory and Cryptography" Second Edition Published by Springer-Verlag.

[12] By Klaus Felten "An Algorithm for Symmetric Cryptography with a wide range of scalability" published by 2nd International Workshop on Embedded Systems, Internet Programming and Industrial IT.