ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 10, October 2016

Design and Analysis of New Cryptographic Algorithm for Trust as a SERVICE (TaaS) in Cloud Computing

Dushyant Singh, Shalini Agarwal

HOD, Dept. of Computer Science, Chandravati Group of Institutions, Bharatpur, India

M.Tech Pursing RTU, Dept. of Computer Science& Engineering, Chandravati Group of Institutions, Bharatpur, India

ABSTRACT: Cloud computing is the good technology for computing. In this computing era the cloud computing technology and services are the most promising & valuable model for compute, storage, on demand services and software. It provides user to complete development environment, virtualization, allocation and reallocation of storage resources and sharable services like "as-a-services". The cloud network security issue is main concern because the data send and receive between the user and cloud service provider totally depends upon the data centers and these data centers are managed by third party, so it is required to encryption and decryption mechanism or secure algorithm on that data transmission. We design an algorithm that enhanced the cloud based systems and network security that will base on symmetric cryptographic algorithm.

KEYWORDS: Cloud computing, encryption and decryption, cryptography.

I. Introduction

In this computing era the cloud computing technology and services are the most promising & valuable model for compute, storage, on demand services and software. It provides user to complete development environment, virtualization, allocation and reallocation of storage resources and sharable services like "as-a-services". The cloud network security issue is main concern because the data send and receive between the user and cloud service provider totally depends upon the data centers and these data centers are managed by third party, so it is required to encryption and decryption mechanism or secure algorithm on that data transmission. We design an algorithm that enhanced the cloud based systems and network security that will base on symmetric cryptographic algorithm. [1]

Cloud computing combines the data-sharing model and service statistical model. From a technical point of view, cloud computing has the following three basic characteristics. Hardware infrastructure architecture is based on the clusters, which is large-scale and low-cost. The infrastructure of cloud computing is composed of a large number of low-cost servers, and even the X86 server architecture. Through the strong performance, the traditional mainframe's prices are also very expensive. Collaborative development of the underlying services and the applications is to achieve maximum resource utilization. By this way, application's construction is improved. But for traditional computing model, applications to be complete dependent on the underlying service. The redundant problem among multiple low-cost servers is solved by the software method. Because of using a large number of low-cost servers, Failure between nodes cannot be ignored, so the issue of fault tolerance among nodes should be taken into account, when designing software.[2] Our research works towards design a new cryptosystem follows the sequence of steps identifies the methodology adopted in this work.

II. Related Work

We will discuss about the trust management in cloud computing. The Security is a principal concern when entrusting an organization's critical information to geographically dispersed cloud platforms not under the direct control of that organization. If we discuss about our conventional IT information system security procedures, designing security into cloud software during the software development life cycle can greatly reduce the cloud attack surface. With cloud computing providing SaaS, secure software is a critical issue. From the cloud consumer's point of view, using SaaS in

DOI: 10.15680/IJIRCCE.2016. 0410061

the cloud reduces the need for secure software development by the customer. The requirement for secure software development is transferred to the cloud provider.Trust plays a role only when the environment is uncertain and risky.

- Trust is the basis based on which certain decisions are made.
- Trust is built using prior knowledge and experience.
- Trust is a subjective notion based on opinion and values of an individual.
- Trust changes with time and new knowledge while experience will have overriding influence over the old ones.
- Trust is context-dependent.
- Trust is multi-faceted.

III. Cloud Computing Security

When we say any system is more secure and reliable then security is prime constrain. Security is a major worry when entrusting an organizations critical information to geographically spread cloud raised area not under the direct control of that organization means others take charges to provide third party service, so that our platform should be perfectly secure and more powerful no attacker easily access the data of others or confidential information . We can also include here in the conventional Information Technology system security procedures, designing security into cloud software during the software development life cycle can really trim down the cloud attack surface. With cloud computing providing Software as a Services (SaaS), secure software is a critical issue. From the cloud consumers point of view, using Software as a Services (SaaS) in the cloud reduces the need for secure software development by the customer. The requirement for secure software development istransferred to the cloud provider.[3]

IV. Trust As A Service(Taas)

Trust in cloud computing is major concerned and valuable for both cloud service providers and cloud customers, because adoption and growth of cloud computing is depend on Trust management. Although several solutions have been proposed recently in managing trust feedbacks in cloud environments, how to determine the credibility of trust feedbacks is mostly neglected. Cloud Armor, a reputation-based trust management framework that provides a set of functionalities to deliver Trust as a Service (TaaS). Trust as a Service (TaaS) framework to improve ways on trust management in cloud environments. The approaches have been validated by the prototype system and experimental results.[4]

Here, it provides some drawbacks are, It is not unusual that a cloud service experiences malicious behaviors from its users, It is not sure whether they can trust the cloud providers, It not convincing enough for the consumers, SLAs are not consistent among the cloud providers even though they our services with similar functionality, Customers are not sure whether they can identify a trustworthy cloud provider only based on its SLA. In particular,the system introduce an adaptive credibility model that distinguishes between credible trust feedbacks and malicious feedbacks by considering cloud service consumers capability and majority consensus of their feedbacks. The approaches have been validated by the prototype system and experimental results.[5]

V. Algorithm For sequence generating The Sequence Encryption And Decryption

In our present work an algorithm is developed. The First algorithm uses a matrix key which on multiplication with a quaternary vector and applying a sign function on the product generates a sequence. This sequence will be used to generate three different models of substitution technique. Thus the algorithm is considered to be a substitution algorithm which uses a single key to be shared by both the sender and receiver, and the cipher processes the input element continuously, producing output one element at a time. The new encryption algorithm is based on the concept of Poly alphabet cipher which is an improvement over mono alphabet.

DOI: 10.15680/IJIRCCE.2016. 0410061

VI. PROPOSED ALGORITHM

A. *ALGORITHM FOR GENERATING THE SEQUENCE:*

- STEP#1. Consider the sequence for 0 to N values where N is a positive integer.
- STEP#2. Convert each element of the sequence into Quaternary form of a given digit number.
- STEP#3. Represent the values of STEP#2 in a matrix form of 256X4.
- STEP#4. Subtract 1 from each element of the matrix specified in STEP#3.
- STEP#5. Consider a random matrix key of size (4X4).
- STEP#6. Multiply the output of STEP#4 with the output of STEP#5.
- STEP#7. Convert all positive values of matrix to 1, negative values to -1and zero by 0.
- STEP#8. Add 1 to each element of output of STEP#7.
- STEP#9. Convert Quaternary values of STEP#8 into decimal form. A sequence is generated.

B. *ALGORITHM FOR ENCRYPTION:*

- STEP#1. Consider any random sequence as plain text.
- STEP#2. Calculate the total characters say WC.
- STEP#3. Convert each element of the sequence into ASCII Equivalent code.
- STEP#4. Consider the Public key that we generate in Algorithm A.
- STEP#5.Generate Sub keys using addition of ASCII Equivalent elements from STEP#2 and public key from STEP#3.
- STEP#6. Perform MOD operation of output of STEP#5, if WC is ODDthen follow the Mod64 operation else Mod 128.
- STEP#7. Generate the ASCII Equivalent values if ASCII Code between 0 and 32 then and if WC is EVEN then add prefix and suffix of (dot, full stop ASCII CODE 46=.) is used else WC is ODD then add prefix and suffix of (Question mark ASCII CODE 63 =?) create Cipher Text .

C. *ALGORITHM FOR DECRYPTION:*

- STEP# 1.Consider Cipher Text in algorithm B.
- STEP#2. Load the ASCII Even and ODD table. Convert each element ofthe sequence into ASCII Equivalent.
- STEP#3. Consider the Sub key that we generate in Algorithm B.
- STEP#4. Consider the Public key that we generate in Algorithm A.
- STEP#5. Perform Subtraction operation between sub key and Public key.
- STEP#6. Write the equivalent ASCII code from ASCII Table. We get plain text is ODD then follow the Mod64 operation else Mod 128.

VII. FEATURE AND ADVANTAGES OF ALGORITHM

1. A set of poly alphabetic substitution rule is used.
2. A new block cipher is developed.
3. A Random matrix is being used as key.
4. Generated sequence being used as sub key.

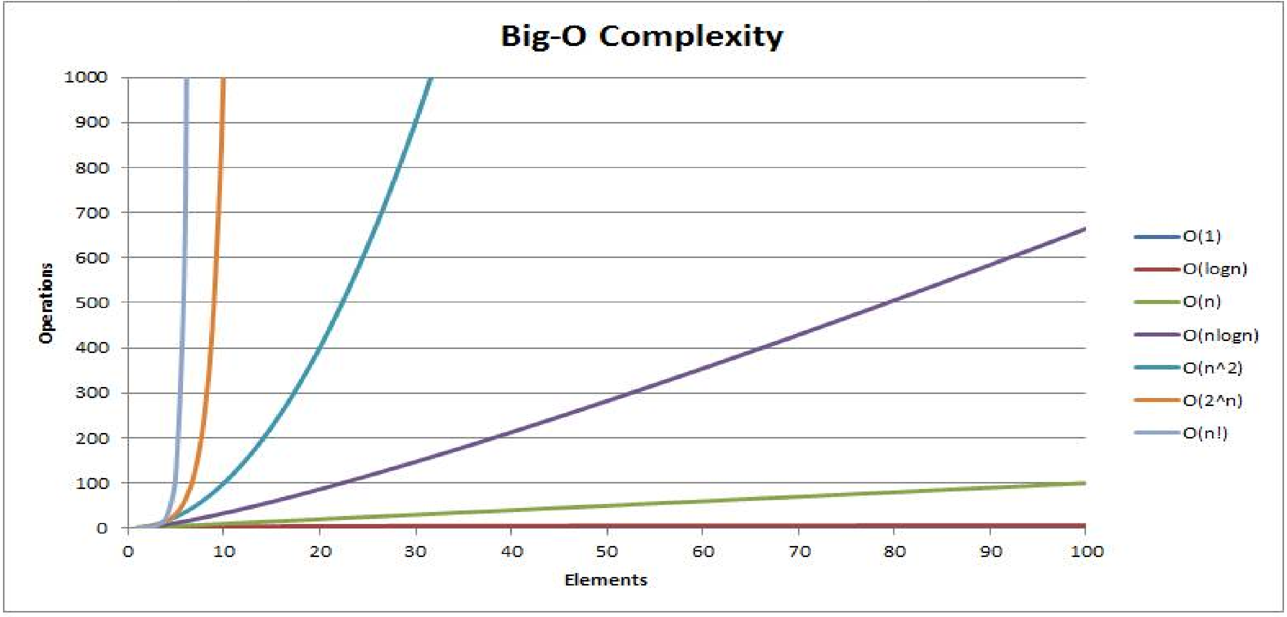
VIII. COMPLEXITY OF THE ALGORITHM

Complexity by Construction:
I Computation: Converting n=0:256 to Quaternary vector. Let it be QVR.The complexity is in multiples of n.
II Computation: Calculating QVR-1. The complexity is in multiples of n.
III Computation: Multiplying QVR with the key considered. The complexityis in multiples of n
IV Computation: Applying sign function on the product. Store it in QVR.The complexity is in multiples of n
V Computation: Calculating QVR+1. The complexity is in multiples of n
VI Computation: Converting output Quaternary vector to integer form. Let this be SEQ,the sequence Generated.

The complexity is in multiples of n
VII Computation: Converting plain text to ASCII value. The complexity isin multiples of n.

IX. Simulation Result

I The complexity of my research work is O(n) and O(n) is fair condition for complexity.



X. COMPARISON TABLE FOR ALGORITHM

S. No	FACTORS	AES	3DES	DES	RC2	BLOWFISH	Proposed Algorithm
1	**KEY LENGTH**	128,192 OR 256	(K1,K2,K3)168 BITS (K1 AND K2 IS SAME)112 BITS	56 BITS	8–1024 bits, in steps of 8 bits; default 64 bits	32-448 bits	256 BITS
2	**CIPHER TYPE**	SYMMETRIC ALGORITHEM	SYMMETRIC ALGORITHEM	SYMMETRIC ALGORITHEM	SYMMETRIC ALGORITHEM	SYMMETRIC ALGORITHEM	SYMMETRIC ALGORITHEM
3	**BLOCK SIZE**	128,192 OR 256	64 BITS	64 BITS	64 BITS	64 BITS	256 BITS
4	**DEVELOPED**	2000	1978	1977	Leaked in 1996,designed in 1987	1993	2016
5	**KEY(s)**	SINGLE	SINGLE(LATER DIVIDED IN 3 PARTS)	SINGLE	PUBLIC	PUBLIC	SINGLE
6	**POSSIBLE KEYS**	2^{128},2^{192} and 2^{256}	2^{112} OR 2^{168}	2^{56}	2^{64}, 2^{128}	2^{32},2^{448}	2^{256}

REFERENCES

1. Ruichuan Chen, Xuan Zhao, Liyong Tang, Jianbin Hu, and Zhong Chen, "CuboidTrust: A Global Reputation-Based Trust Model in Peer-to-Peer Networks," in Autonomic and Trusted Computing. Berlin / Heidelberg: Springer, 2007, vol. 4610, pp. 203-215.
2. Sepandar D Kamvar, Mario T Schlosser, and Hector Garcia-Molina, "The EigenTrust Algorithm for Reputation Management in P2P Networks," in Proceedings of the 12th international conference onWorld WideWeb (WWW '03), Budapest, Hungary, 2003, pp. 640-651.
3. Yong Wang, Vinny Cahill, Elizabeth Gray, Colin Harris, and Lejian Liao, "Bayesian network based trust management," in Autonomic and Trusted Computing. Berlin / Heidelberg: Springer, 2006, pp. 246-257.
4. Huirong Tian, Shihong Zou, Wendong Wang, and Shiduan Cheng, "A Group Based eputation System for P2P Networks," in Autonomic and Trusted Computing. Berlin / Heidelberg: Springer, 2006, pp. 342-351.
5. Abawajy, J. (2009). Determining service trustworthiness in intercloud computing environments. 2009 10th International Symposium on Pervasive Systems, Algorithms, and Networks. doi:10.1109/I-SPAN.2009.155.
6. NIST Special Publication 800-14, “Generally Accepted Principles and Practices for Securing Information Technology Systems,” September 1996
7. Almulla S, Chon YeobYeun. (March 2010) 'Cloud Computing Security management ', 2nd International Conference On Engineering Systems Management and Its Applications , 1-7..
8. Security Guidance for Critical Area of Focus in Cloud Computing,. 2009.
9. R.Chow, et al. Controlling Computation without Outsourcing Control. in CCSW'09, ACM workshop on Cloud computing security. 2009.
10. S.Hanna, A security analysis of Cloud Computing. Cloud Computing Journal.
11. TRUST SERVICES PRINCIPLES AND CRITERIA, EXPOSURE DRAFT, Prepared by the AICPA Assurance Services Executive Committee Trust Information Integrity Task Force, September 30, 2013.
12. Shalini Agarwal et al, / (IJCSIT) International Journal of Computer Science and Information Technologies, Vol. 6 (5) , 2015, 4568-4570.

BIOGRAPHY

Dushyant Singh has been serving as HOD of Computer Science Department in Chandravati Group of Institutions, Bharatpur affiliated to Rajasthan Technical University, Kota ,India. He received Master of Technology (M.Tech) from SKIT,Jaipur affiliated to Rajasthan Technical University, Kota, India. She is more interested in Cloud Computing and Information System and Security.

Shalini Agarwal is passed B.tech in computer science and engineering from Govt. Mahila Engineering College, Ajmer affiliated to Rajasthan Technical University, Kota(Rajasthan) and currently pursuing Master of Technology(M.Tech) in Computer Science & Engineering from Chandravati Group of Institutions, Bharatpur affiliated to Rajasthan Technical University, Kota(Rajasthan),India.She is more interested in Cloud Computing and Information System and Security.