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

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 5, May 2017

Trusted Computing in Cloud Architecture

Neelam[1] , Ms.Rachna[2]

M.Tech Student, Department of CSE, New Green Field College of Engineering and Technology, Palwal , Haryana, India

Assistant Professor, Department of CSE, New Green Field College of Engineering and Technology, Palwal, Haryana, India

ABSTRACT: The concern of reliance in public cloud environment is depicted by examining the state of the art within cloud computing security and afterward addressing the problem of initiating trust relation between two or more resources between the cloud computing in public cloud environment. As a result, this paper proposes a hash based algorithm to ensure that the two or more resources communicating using the trust relation established using the digital certificates ensuring the secure communication among them and each request comprising of unique signatures to blind or poison the breach of data thus ensuring secured and trusted communication over a cloud resource.

KEYWORDS: Trusted Cloud Computing, Cryptography, Digital Signatures, Third Party Auditor.

I.INTRODUCTION

Cloud computing is the newest machinery that creates the convenience computing through easy and its service, consumption model are exceptionally delicately exertion for express suppleness and broad arrangement admittance over networks. The cloud computing implication and roles can be diverse and contrast from individuals or stakeholders. No qualm defence and seclusion policies they want a inclusive prominence on their submission area and resources punter that using public cloud application, a medium-scale establishment using a personalized collection of business applications on a cloud platform, and a government agency with a private cloud for internal database sharing. The reallocate of all grouping of client to cloud system bring a altered package of remuneration and risks. In this circumstances some real value that the user seeks to secure or protect the data. For an individual point of view, the value at risk can range from loss of public emancipation of the contents of bank accounts. For a business point of view the value runs from core trade secrets to continuity of business operations and public reputation. Much of this is hard to estimate and translate into standard metrics of value.

A.TRUSTED CLOUD COMPUTING DISTINCTIVENESS

Trusted cloud computing can be viewed as a network communication protection structural model that is premeditated to shield cloud systems from malevolent intrusions and attacks, and guarantee that computing wherewithal will act in a specific, conventional approach as projected. A trusted cloud computing system will protect data in use by digital certificates and applications, shield adjacent to unconstitutional access to information, provide for well-built verification, apply encryption to guard receptive data that resides on stolen or lost devices even, and support acquiescence throughout communication mechanisms using trust relationship. In a cloud computational classification, numerous processes might be running concomitantly. Each process has the potential to admittance definite reminiscence locations and to accomplish a subset of the computer's instruction set. The implementation and reminiscence space assigned to each process is called a trusted domain. This province can be extended to implicit remembrance to protect the information. The rationale of establishing a fortification province is to defend program from all unconstitutional amendment or executioners obstructions. A trusted computing foundation is the total amalgamation of fortification mechanism within a processor classification, which includes the digital certificates and firmware that are trusted to enforce a security policy. Because the projected digital signatures using hashing algorithm will form the mechanism which will conscientious for enforcing the security policy of a trusted resources, these apparatus must be sheltered from malevolent and un-trusted processes. The scheme must also provide for reminiscence shield and ensure that the processes from one domain do not access resources from another domain until trust relationship is not established. The safety measures perimeter is the state line that separates the distrusted as a residue

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

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 5, May 2017

of the arrangement. Frequent trust-related issues ought to be raised with, and contented by, a cloud contributor. They collection from concerns about security, recital, expenditure, organize, accessibility, resiliency, and merchant lock in. Following are some of the decisive questions that should be asked to address these concerns:

B.SECURED ECOSYSTEM

Forming computing platforms for protected implementation is a multifaceted assignment; and in several instances it is not performed appropriately because of the huge amount of parameters that are implicated. This provides opportunities for malware to exploit vulnerabilities, such as downloading cipher entrenched in in sequence and having the code executed at a elevated dispensation intensity. In cloud computing, the most important encumber of establishing a secure execution environment is transferred from the client to the cloud provider. However, confined data transfers must be reputable from beginning to end with well-built verification mechanisms, and the client must have practices in place to address the privacy and confidentiality of information that is exchanged with the cloud. In fact, the client's port to the cloud might present an battering conduit if not properly provisioned with security procedures. Therefore, the client needs declaration that computations and data relations are conducted in a sheltered atmosphere. This declaration is pretentious by conviction enabled by cryptographic methods. Also, study into areas such as compiler-based implicit equipment promises a more protected implementation upbringing for working systems in trusted clod computing.

C.SECURED COMMUNICATION

As contrasting to have managed, protected infrastructure surrounded by the computing assets inside to an association, faction of applications to the cloud requires a revaluation of interactions precautions. These communications be appropriate to both data in action and data at rest. Secure cloud communications involves the structures, communication mechanism, transportation formats, and safety procedures that grant privacy, veracity, accessibility, and endorsement for transmissions over private and public communications networks. Secure cloud computing communications should ensure the following:

Secrecy : Ensures to facilitate solitary individuals who are hypothetical to admittance facts can reclaim it. Thrashing of secrecy can transpire during the premeditated liberate of classified group information or throughout a misapplication of network rights. Some of the fundamentals of telecommunications used to guarantee discretion are as follows:

1. Network security protocols
2. Network authentication services
3. Data encryption services
4. Integrity
5.

Ensures that data has not been changed due to an catastrophe or malevolence. truthfulness is the agreement that the communication sent is the point acknowledged and that the communication is not deliberately or involuntarily misrepresented. Reliability also contains the perception of non-repudiation of a communication basis. Some of the constituent of veracity are as follows:

1. Firewall services
2. Communications Security Management
3. Intrusion detection services
4. Availability — Ensures that data is accessible

When and where it is required, and that connectivity is reachable when desirable, allowing authorized users to access the network or systems. Also included in that declaration is the agreement that security services for the security practitioner are usable when they are needed. Some of the fundamentals that are used to guarantee ease of use are as follows:

1. Liability lenience for data availability, such as backups and redundant disk systems
2. Tolerable logins and operating process performances
3. Reliable and interoperable security processes and network security mechanisms

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

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 5, May 2017

II. LITERATURE REVIEW

Consider all of the risks, threats, and vulnerabilities from a technical perspective, he could probably add approximately 500 different items. The respondent also stated that some threats are common to all public and online services, such as distributed denial of service (DDoS) attacks and thus, they are not specific only to the cloud. Hence, some of the identified threats are not specific to cloud computing. In addition, he believes that a more generic term needs to be used for DDoS in a cloud environment, which is 'service discontinuity' because this term will have much more vulnerabilities than DoS. According to him, "For example, there are more than ten types of DDoS attacks and you do not want to go deep into that and your job is to make sure the continuity of the connection", which is defining threat from a business perspective. Illustrating the case of a SQL injection attack, he said that he "may not have a SQL server on the cloud or the database at all, on that particular service that I am having on the cloud." Moreover, DDoS attacks are common to all public and online services, and thus, they are not specific to the cloud only. Therefore, the types of threats in cloud computing need to be redefined because the above 41 threats are not the concern of the company, but to the cloud service provider.

Denial of service attack : The aim of a denial of service attack is to deny legitimate users access to a specific resource [12]. Once the high employment on the flooded services notifies by Cloud Computing package then it'll begin providing a lot of machine power to address the extra employment. Thus, the server hardware boundaries for optimum employment to method do now not hold. Therein sense, the Cloud system is making an attempt to figure against the assailant (by providing a lot of machine power),but in some extent this may facilitate by enabling him to try to most potential injury on a service's handiness, ranging from one flooding attack entry purpose. Thus, the assailant doesn't need to flood all an server that give a definite service in target, however simply will flood one, Cloud based mostly address so as to perform a full loss of handiness on the meant service.[10]

Man-in-the-middle attack: The **man-in-the-middle attack** (often abbreviated **MITM).** As the name specifies, a man-in-the-middle attack occurs when someone between you and the person with whom you are communicating is actively monitoring, capturing, and controlling your communication transparently. It is additionally outlined as active eavesdropping wherever wrongdoer makes freelance connections between users and relays messages between them. Man-in-the-Middle attacks square measure usually cited as "session hijacking attacks", within which the entrant aims to realize access to a legitimate user's session.

Network Sniffing: A Network-snifferis a utility or device-application that can read, monitor, and scan network packets [11]. Knowledge packets with mal-intention measure transmitted from one network device to a different that causes the chance that outsider may see our knowledge or crucial information can be classified for any purposes. Sniffing is employed to examine what style of traffic is being passed on a network and to seem for things like passwords, master-card numbers, then forth.

Port Scanning: Port scanning can be defined as "hostile Internet searches for open 'doors,' or ports, through which intruders gain access to computers"[1]. The basic step is simply sends out a request to connect the goal host on each port in a order. It is a method used to recognize open ports and services accessible on a network host but it also used by hackers to target victim. If recurring port scan are complete, a denial of service can be created. Hackers typically use port scanning because they can easily identify services which can be broken. They conduct tests for open ports on private Computers that are linked to the web.

SQL Injection Attack: There is a big influence of web application on our life. Several business houses and governments and society in general depend on this. All these web applications are accessed through internet therefore security risks linked with it. Usually RDBMS (Relational Database Management Systems) is used for database by web applications [11]. They provide interface to the user to input the information in the form of SQL statements which are executed on the RDBMS. By using SQL-injections, malicious user can modify the secured and protected data, breach or intrude the sensitive or classified information or damage/crash/catastrophic the entire system

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

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 5, May 2017

XML Signature Element Wrapping: In cloud computing, customers are connected through a web browser or web service which increases the possibility of web services attacks in cloud computing. XML signature element wrapping is common attack for Web service. XML sign are designed to make easy integrity protection and source verification for a variety of documents types. It is use to protect a constituent identity, characteristic and value from unlawful festivity but unable to protect the position in the documents. (Jamil&Zaki, 2011b)[16]**An attacker** is capable to manipulate a

SOAP message by copying the target component and inserting whatever value the attacker would like and stirring the innovative constituent to somewhere else on the SOAP **message. Suppose** we use a signature to secure the transmit data then outsider can't be able to change that data. But this attack allows a malicious user to change the signed information what is being sent. Amalgamation of WS-security with XML signature to a particular component.

Browser Security: In a cloud computing system, the computational processes are done in the cloud server but the client side just send a request and wait for the result. Web browser is a common method to connect to the cloud systems. Before a client can request for services on the cloud system, the client is required to authenticate himself whether he has an authority to use the cloud system or not. . As a client sent the request to the server by web browser the web browser have to make use of SSL to encrypt the credentials to authenticate the user [16]. But SSL support point to point communication means the attacker may get the credentials of the user and use in these credentials in the cloud system as a valid user by installing sniffing packages on intermediary host.

Flooding Attacks: The most important feature of the cloud system is to give dynamically scalable resources. Once there are more requests from client, cloud system frequently increases its size. Flooding attack is basically distributing a large amount of non-sense requests to a certain service [16]. Once the attacker throws a batch of unused requests by providing more recourses cloud system will attempt to work against the requests, ultimately system all recourses are consumed by the system and it is distinguished to serve normal customer requests. These attacks charges additional cost to the consumer for the usage of resources

Cloud Malware Injection Attack : Cloud malware injection attack is to build attempt to insert a malicious service, application or even virtual machine into the cloud system depending on the cloud service models (SaaS, PaaS and IaaS) In order to perform this attack , the first step of intruder is to produce his private vindictive application[3]. Once the vindictive software is entered into the cloud structure the attacker had to trick the cloud system to treat the malicious software as a suitable instance. If successful user request for the vindictive service then malicious is implemented. Attacker can also upload the virus list in to the cloud system. Once the cloud system treats it as a valid service, the virus list is automatically executed and the cloud system infects the virus which can cause damage to the cloud system[10].

Incomplete Data Deletion: In cloud computing, replica's knowledge of information is placed in over totally different server owing to this data doesn't take away fully. This can be referred to as incomplete information Deletion [16]. once letter of invitation to delete a cloud resource is formed, most operational systems this may not take away accurately correct information deletion isn't potential as a result of copies of data are hold on another sever however aren't on the market.

Table 1: Different security threats and their countermeasures

Denial of Service:	Reduction of the human rights of the customer that connected to a server..
Man in the Middle Attack	Proper installation of SSL
Network Sniffing:	utilize of encryption methods for securing the information.
Port Scanning:	Use of firewall to secure the

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

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 5, May 2017

	data from port attacks.
SQL Injection Attack:	Web applications should not use one connection for all transactions to the database
Flooding Attacks	Intrusion detection system will filter the malicious requests and installing firewall.
XML Signature Element Wrapping:	Careful security policy specification and correct implementation by signed message providers and consumers.
Browser Security:	Use of WS-security concept on web browsers by vendors.

III.PROPOSED ALGORITHM

Proposed Trusted Hash based Algorithm for Trusting Computing Measures in Cloud Architecture

	Trusting		**Trusted**
Trusting and Trusted Resources publically share a generator and XOR value.	$g \wedge n$, $p \wedge n$	Common info	$g = x$, $p = x$
Each then secretly picks a number n of their own.	$n = 8$	secret number	$n = 6$
Each evaluate g^n mod p	$3^8 \bmod 17 = 16$		$3^6 \bmod 17 = 15$
They then exchange these resulting values.	$A = 16$ $B = 15$		$B = 15$ $A = 16$
Each then raises the value they received to the power of their secret nXor$p$.	$B^n \wedge p$ = XOR $15^8 \bmod 17 = 1$	mix in secret number	$A^n \wedge p$ =XOR $16^6 \bmod 17 = 1$
The result is the shared secret key.	XOR Value	shared secret key	XOR Value

IV. PSEUDO CODE

```
public String dosecret(String Message)
{   int lbound=8,ubound=4096; int magicValue; Random rand=new Random();
 int num=rand.nextInt(ubound-lbound+1)+lbound;int length=Integer.toString(num).length();
int[] arraygenerator=new int[length]; magicValue=num+length;
```

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

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 5, May 2017

```
int i=length-1,numeral=magicValue; for(int xx=0;xx<length;xx++){
arraygenerator[xx]=rand.nextInt(xx+8);}  int a0=0,a1=0,a2=1,a3=0;
for(int cnt=0;cnt<length;cnt++) { if((cnt%2)==0) a0+=arraygenerator[cnt];
else  a1+=arraygenerator[cnt];a2*=arraygenerator[cnt];}
a3=magicValue % 256;long b0,b1,b2,b3,b4,b5,b6;long[][] cipher=new long[6][6];
cipher[0][0]=T_HashCodeGenerator_0(rand.nextInt(ubound-lbound+1)+lbound*2,
rand.nextInt(ubound-lbound+1)+lbound*3and.nextInt(ubound-lbound+1)+lbound*4,rand.nextInt(ubound-
lbound+1)+lbound*2,rand.nextInt(ubound-
lbound+1)+lbound*2);cipher[0][1]=T_HashCodeGenerator_1(rand.nextInt(ubound-
lbound+1)+lbound*2,rand.nextInt(ubound-lbound+1)+lbound*3,
rand.nextInt(ubound-lbound+1)+lbound*4,rand.nextInt(ubound-lbound+1)+lbound*2,rand.nextInt(ubound-
lbound+1)+lbound*2);cipher[0][2]=T_HashCodeGenerator_2(rand.nextInt(ubound-
lbound+1)+lbound*2,rand.nextInt(ubound-lbound+1)+lbound*3,
rand.nextInt(ubound-lbound+1)+lbound*4,rand.nextInt(ubound-lbound+1)+lbound*2,rand.nextInt(ubound-
lbound+1)+lbound*2);cipher[0][3]=T_HashCodeGenerator_3(rand.nextInt(ubound-
lbound+1)+lbound*2,rand.nextInt(ubound-lbound+1)+lbound*3,
rand.nextInt(ubound-lbound+1)+lbound*4,rand.nextInt(ubound-lbound+1)+lbound*2,rand.nextInt(ubound-lbound+1)+lbound*2);
long msgparameter; Random rand1=new Random();  int num1=rand1.nextInt(9999-1024+1)+1024;
msgparameter=magicValue+num1+((a0+a1+a2+a3)/4)+((b0+b1+b2+b3+b4)/3)+((c0+c1+c2+c3+c4+c5)/4)+((c0+c1+c
2+c3+c4+c5)/4)+((c0+c1+c2+c3+c4+c5)/4);
String msg_secret1=Message; StringBuffer contents=new StringBuffer();  long msg_secret2, msg_secret3; String
msg_secret4;msg_secret1=new StringBuffer(msg_secret1).reverse().toString();
char[] c=msg_secret1.toCharArray(); int index1,index2;  Random rand2=new Random();  Random rand3=new
Random(); index1=rand2.nextInt(3);  index2=rand3.nextInt(3);String nl=System.getProperty("line.separator");  for (int
cnt = 0; cnt < c.length ; cnt++)  {  if(c[cnt]!='\n'&& c[cnt]!='\r')  {  if(c[cnt]!=' ')  {
msg_secret2=(long)c[cnt]^sbox[index1][index2];msg_secret3=msg_secret2^msgparameter;
msg_secret4=longFormation(msg_secret3);msg_secret4=new
StringBuffer(msg_secret4).reverse().toString();contents.append(msg_secret4); }
contents.append(sbox[index1][index2]); contents.append(':'); contents.append(msgparameter);
return contents.toString();
        }
```

V. SIMULATION RESULTS

Our objective in the scheme is to build a security service which will be provided with a trusted model between client (trusting resource) and server (trusted resource) and would lead to providing only security services and wouldn't store any malicious information and data in its system and even not passing the same.

Detailing it further.

1. To construct service or solution system which would provide data integrity verification? Provide encryption/decryption of the consumer data.
2. Defining access list for sharing data securely with specific band of individuals.
3. To construct thin client application which would call this service before accessing and rendering the data to and from cloud.

Machine	CPU Time in Seconds	Configuration	CPU Cache
1	1.227	I3-330 M	3MB
2	0.543	I5-330M	6MB

Table 1: CPU time used to execute the proposed algorithm in seconds with CPU Cache and Configuration

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

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 5, May 2017

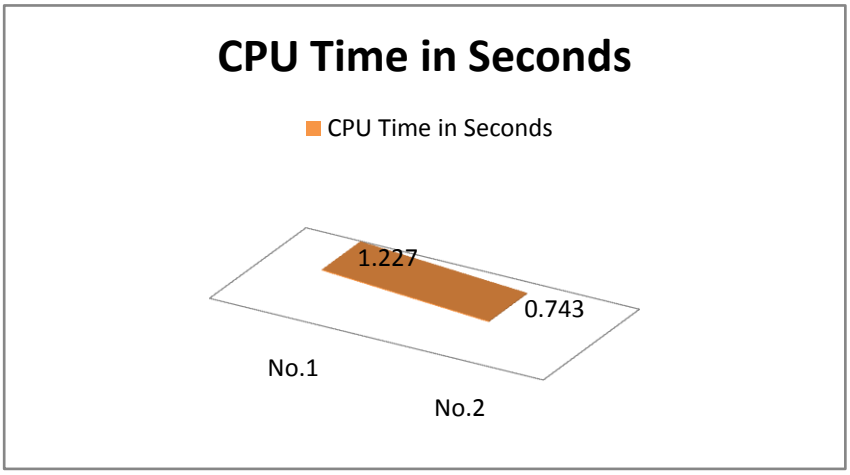

Chart 1: Surface Model depicting time utilized by proposed algorithm in seconds with CPU Cache and Configuration

VI. CONCLUSION AND FUTURE WORK

In the above scheme the users inside the cloud which hold the trust relationship as trusted or trustee resource will share the information under the secured umbrella of cloud security but also ensure that, the communication inside the cloud between two or more resources are secured using above mentioned algorithm thus, provide both proactive and reactive securities to the resources for better counterparts on security and such mal-intentions. However, this paper proposes a new trusted hash based algorithm to improve the encoding performance of trusted cloud computing

Additional future work is to put our new proposed scheme algorithm into a real storage system. Although we have analyzed how proposed algorithm improves the whole performance of storage systems, the data used in our analysis is synthetic and may not be representative the real world scenarios. We plan to implement a reliable storage system and use various scheduling algorithms in it to find how our scheduling algorithm can improve this system's performance and proposed scheme can be used in firmwares as augmented security for trusted cloud computing for security and auditing purpose.

REFERENCES

1. Abbadi, I.M. and Martin, A. (2011), Trust in the Cloud. Information Security Technical Report, 16,108-114. doi:10.1016/j.istr.2011.08.006
2. Agarwal, A. and Agarwal, A. (2011). The Security Risks Associated with Cloud Computing.International Journal of Computer Applications in Engineering Sciences, 1 (Special Issue on CNS),257-259.
3. Arshad, J, Townsend, P. and Xu, J. (2013).A novel intrusion severity analysis approach for Clouds.Future Generation Computer Systems, 29, 416–428. doi:10.1016/j.future.2011.08.009
4. Atayero, A.A. and Feyisetan, O. (2011). Security Issues in Cloud Computing: The Potentials ofHomomorphic Encryption. Journal of Emerging Trends in Computing and Information Sciences,2(10), 546-552.
5. Bisong, A. and Rahman, S.S.M. (2011). An Overview of the Security Concerns in Enterprise CloudComputing. International Journal of Network Security & Its Applications, 3(1), 30-45.doi:10.5121/ijnsa.2011.3103
6. Buyya, R., Yeo, C.S., Venugopal, S., Broberg, J. and Brandic, I. (2009). Cloud computing andemerging IT platforms: Vision, hype, and reality for delivering computing as the 5th utility. FutureGeneration Computer Systems, 25, 599–616. International Journal of Network Security & Its Applications (IJNSA), Vol.6, No.1, January 2014
7. Casola, V., Cuomo, A., Rak, M. and Villano, U. (2013). The CloudGrid approach: Security analysisand performance evaluation. Future Generation Computer Systems, 29, 387–401.doi:10.1016/j.future.2011.08.008
8. Celesti, A., Fazio, M., Villari, M. and Puliafito, A. (2012). Virtual machine provisioning throughsatellite communications in federated Cloud environments. Future Generation Computer Systems, 28,85–93. doi:10.1016/j.future.2011.05.021
9. Che, J. Duan, Y, Zhang, T. and Fan, J. ().Study on the security models and strategies of cloudcomputing. Procedia Engineering, 23, 586 – 593. doi:10.1016/j.proeng.2011.11.2551
10. Chen, D. and Zhao, H. (2012). Data Security and Privacy Protection Issues in Cloud Computing.International Conference on Computer Science and Electronics Engineering, 647-651. doi:10.1109/ICCSEE.2012.193