IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 6, Issue 3, March 2017

Data Security Using Cramer – Shoup Algorithm in Cloud Computing

Deepak Jain

Rajasthan Technical University

Abstract: Cloud computing is an rising technology that has become today's blistering analysis space as a result of the advancement of inflated property and it's most attention-grabbing and magnetized technology that offers the on demand services to the users over the web. Since Cloud Computing stores the user knowledge and permits the user to figure on the cloud system so the protection has become the most concern that creates threat and tries to deploy the Cloud environments. Even supposing the Cloud Computing is economical, there area unit several challenges for knowledge security, which can deduct the users from mistreatment the cloud computing. To confirm the protection of knowledge, we have a tendency to planned a technique of RSA rule and Cramer – Shoup cryptosystem.

Keywords: Cloud Security; RSA; Cramer; Shoup; Cryptosystem.

I. INTRODUCTION

Cloud computing may be a term wont to describe the integrity of computing ideas that involve a huge range of computers connected through a period of time communication network like the net. Cloud computing is to explain the distributed computing over a network, that's intently meant for functioning on a unique machine to supply the convenience to the users. Cloud Computing is very useful for several little, medium and enormous sized corporations and as several cloud users get the services of cloud computing, the key concern is that the security of their information within the cloud.

Securing information is often of significant importance and since of the crucial nature of cloud computing and also the massive amounts of advanced information it carries, the requirement is even a lot of vital. thus forth, issues relating to information privacy and security area unit proving to be a barrier to the broader uptake of cloud computing services.

II. SECURITY ISSUES IN CLOUD COMPUTING

A. Privacy and Confidentiality

When a consumer is hosting some steer to the cloud there got to be some assurance that access to the data are restricted only to the approved persons. Inappropriate access of the personnel data is to boot a risk that will produce potential threat to cloud data. Assurances got to incline to the purchasers regarding the protection issues. the safety policies got to be plenty of protective. The cloud seeker got to be assured that data hosted on the cloud are confidential.

B. Data Integrity:

Along with providing the protection to the information, cloud service supplier ought to additionally make sure the knowledge integrity and observation the dataset is additionally obligatory. they must be able to tell what happened to the dataset, at any purpose. creating the users responsive to what specific knowledge is hosted on the cloud and also the integrity mechanism is accountable of cloud service supplier.

And additionally it's necessary to possess actual records what knowledge is placed within the cloud, once it's placed, at what virtual recollections (VMs) and storage it resided on, and wherever it had been processed. once such knowledge integrity details square measure supervised, it's simple to stop from meddling or sterilization the place wherever the information truly resides

C. knowledge location and Relocation:

The data that square measure hold on within the cloud can have the high degree of quality. probably it might float on the virtual machines time to time.

Small users might not want of knowing their knowledge, wherever will truly resides. however once some high-level corporations or enterprises desires their knowledge to be hold on during a exceedingly in a very specific earth science places then the cloud service supplier and enterprisers must place an agreement concerning the situation of information to be hold on. And additionally it's the responsibility of the cloud service supplier to confirm the protection of systems and providing strong authentication to safeguard customer's data. Since the data is been floating over the devices, the cloud providers has to been in some agreement with other cloud providers to use their storage devices.

D. Data Availability:

Customer knowledge is generally fragmented and keep on totally different servers often residing in several locations or in several Clouds. during this case, knowledge convenience becomes a serious issue because the convenience of uninterruptible becomes comparatively tough.

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 6, Issue 3, March 2017

1. Storage, Backup and Recovery:
When a user decides to maneuver the info to the cloud, the cloud service supplier needs to make sure the adequate knowledge storage devices. At a minimum they ought to be able to give RAID (Redundant Array of freelance Disks) storage systems though most cloud suppliers can store the info in multiple copies across several freelance servers.
In addition thereto, most cloud suppliers ought to be ready give choices on backup services that area unit definitely necessary for those businesses that run cloud based mostly applications so within the event of a significant hardware failure they'll roll back to AN earlier state.

III. KNOWLEDGE SECURITY

Data protection super the list of cloud considerations nowadays. merchandiser security capabilities area unit keys to establishing strategic price, reports the 2012 Computerworld "Cloud Computing" study, that measured cloud computing trends among technology call manufacturers. once it involves public, private, and hybrid cloud solutions, the likelihood of compromised data creates tremendous anxiety. Organizations expect third-party suppliers to manage the cloud infrastructure, however area unit usually uneasy concerning granting them visibility into sensitive knowledge.

Such problems give rise produce bring concerning make create to tremendous anxiety about security risks within the cloud. Enterprises worry whether or not they will trust their workers or ought to implement further internal controls within the personal cloud, and whether or not third-party suppliers will give adequate protection in multitenant environments which will additionally store rival knowledge. There's additionally current concern about the safety of moving data between the enterprise and the cloud, as well as how to ensure that no residual data remnants remain upon moving to another cloud service provider.

Private cloud involve new challenges in securing data, mixed trust levels, and the potential weakening of separation of duties and data governance.

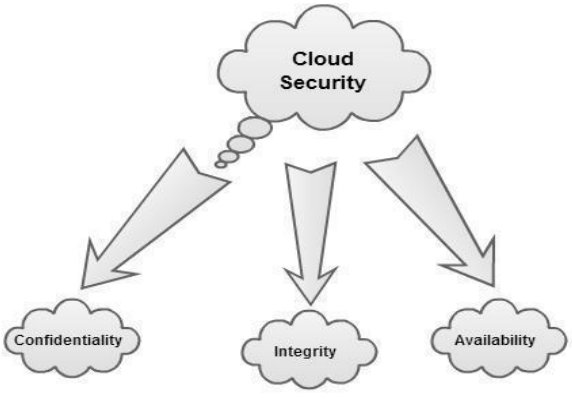


Fig. 1 Issues in cloud security

The public cloud compounds these challenges with data that is readily portable, accessible to anyone connecting with the cloud server, and replicated for availability. And with the hybrid cloud, the challenge is to protect data as it moves back and forth from the enterprise to a public cloud. Reliability in terms of a safe and secure environment for the personal data and info of the user is still required.

IV. DIGITAL SIGNATURE WITH RSA CRYPTOGRAPHY FORMULA TO BOOST INFORMATION SECURITY IN CLOUD

In Cloud computing, we've downside like security of knowledge, files system, backups, network traffic, host security .Here we have a tendency to square measure proposing an inspiration of digital signature with RSA formula, to encrypting the information whereas we have a tendency to square measure transferring it over the network. A digital signature or digital signature theme could be a mathematical theme for demonstrating the genuineness of a digital message or document. a sound digital signature provides a recipient reason to believe that the message was created by a legendary sender, which it absolutely was not altered in transit.
We have a tendency to planned digital signature with RSA formula theme to make sure the safety of knowledge in cloud. RSA is perhaps the foremost recognizable uneven formula. RSA was created by Ron Rivest, Adi Shamir, and Leonard Adleman in late 1970. Till now, it's the sole uneven (i.e. wants 2 totally different keys) formula used for private/public key generation and cryptography. we have a tendency to embrace each digital signature theme and public key cryptography to boost the safety of cloud computing.
In Digital Signature, code can crunch down the information, document into simply a number of lines by a victimisation "hashing algorithm". These few lines square measure referred to as a message digest. code then encrypts the message digest together with his personal key. Then it'll turn out digital signature .Software can decipher the digital signature into message digest with public key of sender's and his/her own personal key. we have a tendency to square measure victimization Digital signatures in order that we have a tendency to square measure ready to distribute code, monetary transactions, over the network and in different cases wherever it's vital to find forgery and change of state.

V. PROPOSED ALGORITHM TAKEN FOR RSA ALGORITHM

In this algorithm, n is known as the modulus. 'e' is known as the encryption exponent. 'd' is known as the secret exponent or decryption exponent.

Step 1. Key Generation Algorithm 1. Choose two distinct large random prime numbers p and q
2. Compute n = p q, where n is used as the modulus for

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 6, Issue 3, March 2017

both the public and private keys
3. Compute the totient: phi (n) = (p !1) (q !1)
4. Choose an integer e such that 1 < e < phi (n) , and e and phi(n) share no factors other than 1 , where e is released as the public key exponent
5. Compute d to satisfy the congruence relation d × e = 1 modulus phi(n); d is kept as the private key exponent
6. The public key is (n, e) and the private key is (n, d). Keep all the values d, p, q and phi secret.

VI. PROPOSED WORK

The Cramer–Shoup cryptosystem is associate degree uneven key coding formula, and was the primary economical theme tested to be secured against adaptation chosen cipher text attack exploitation normal cryptanalytic assumptions. Its security relies on the procedure trait (widely assumed, however not proved) of the decisional Diffie–Hellman assumption. Developed by Ronald Cramer and Victor Shoup in 1998, it's associate degree extension of the Elgamal cryptosystem. In distinction to Elgamal, that is very malleab le, Cramer–Shoup adds different parts to confirm non-malleability even against an imaginative wrongdoer. This non-malleability is achieved through the employment of a universal unidirectional hash perform and extra computations, leading to a cipher text that is double as giant as in Elgamal.

Cramer-Shoup System formula involves 3steps:
1. Key Generation
2. Encryption
3. Decryption
Consider a gaggle G of prime order letter of the alphabet, wherever letter of the alphabet is massive and presume that the first messages or the encoded messages area unit to be hold on because the component of G. ordinarily a method hash perform (SHA-1) is employed for cryptography and cryptography.

1. Key Generation
The key generation algorithm chose the random element g_1, g_2 € G and random elements x_1, x_2, y_1, y_2, z € Z_q are chosen. Next step is to compute the group element.
$C = g_1^{x1}.g_2^{x2}$, $d = g_1^{y1}.g_2^{y2}$, $h = g_1^{z}$
Then one-way hash function (SHA-1) is chosen. The public keys is (g_1, g2, c, d, h, H) and the private key is x_1, x_2, y_1, y_2, z € Z_q

2. Encryption
The secret writing rule encrypts the given message M € G. It conjointly chooses the worth r € Zq.
u1 = g1r, u2 = g2r, e = hrm, α = H (u1, u2, e,), v = crdr α. wherever H denotes the hash operate. and therefore the cipher text is (u1, u2, e, v) transfer through web to the receiver.

3. Decryption
The decoding formula decrypts the cipher text (u1, u2, e, and v). It computes α = H (u1, u2, e,) and checks, u1 x1+y1 α + u2x1+ y2α = v It the conditions in glad then message is decrypted by m = e/u1z

VII. CRAMER- SHOUP ALGORITHM EXAMPLES

1) Key generation
Consider the cyclic cluster G = and therefore the message transferred to be five (M = 5). contemplate g1 = three, g2 = 7. every which way chosen values ar, x1 = 2, x2 = 3, y1 = 4, y2 = 5, z = vi all belong to the set Zq.
Compute the cluster component,
c = 32*33 = 243, d = 34*35= 19683, h = 36= 729.
Public secret's (3, 7, 243, 19683, 729) and personal secret's (2, 3, 4, 5, 6)

2) Encryption
Choose any value for r from Z_q, Let us assume r = 3.
$u_1 = 3^3 = 9$, $u_2 = 7^3 = 343$, $e = 729^3(5) = 1.93 * 10^9$.
Then to compute α = H (9, 343, $1.93 * 10^9$).

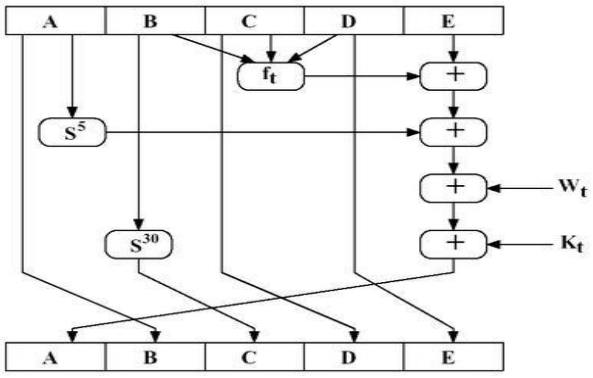
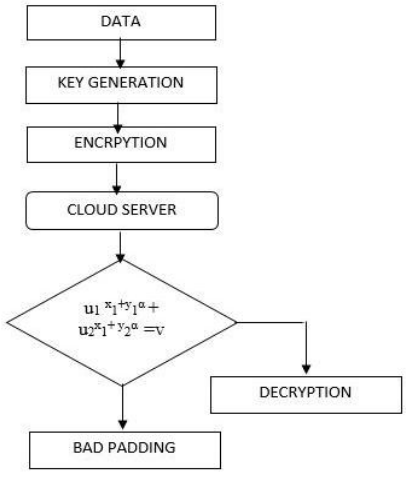


Fig.2. Elementary SHA Operation

3) Decryption
Receiver gets the cipher text as (9, 343, $1.93*10^9$, v). It computes the value of α = H (u_1, u_2, e,) and then checks whether $9^{2+3\alpha} + 343^{2+3\alpha}$ = v is equal or not. If they are equal then, $M = e/u_1^z$.

Execution Flow:



IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

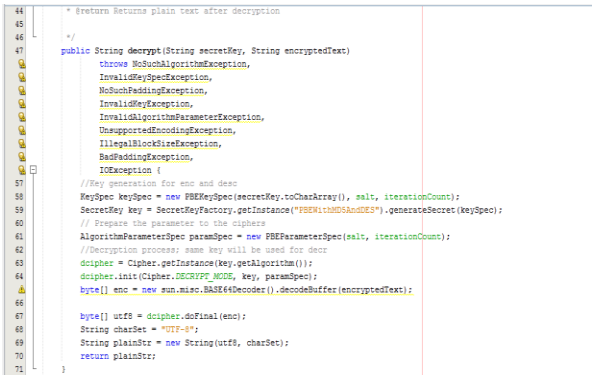
International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 6, Issue 3, March 2017

Expected outcomes:
Cloud Computing continues to be a brand new and evolving paradigm wherever computing is considered on-demand service. Once the organization takes the choice to maneuver to the cloud, it loses management over the information. Thus, the number of protection required tosecure knowledge is directly proportional to the worth of the information. Security of the Cloud depends on trusty computing and cryptography.

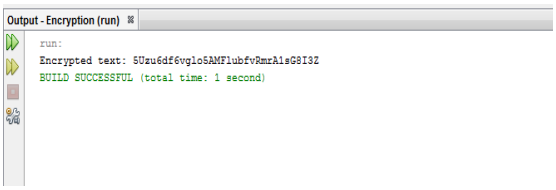
Thus, in our planned work, solely the licensed user will access the information. albeit some trespasser (unauthorized user) gets the information accidentally or deliberately if he captures the information additionally, he can't decipher it and find back the initial knowledge from it. therefore forth, knowledge security is provided by implementing Cramer
– Shoup cryptosystem.

Implementation:

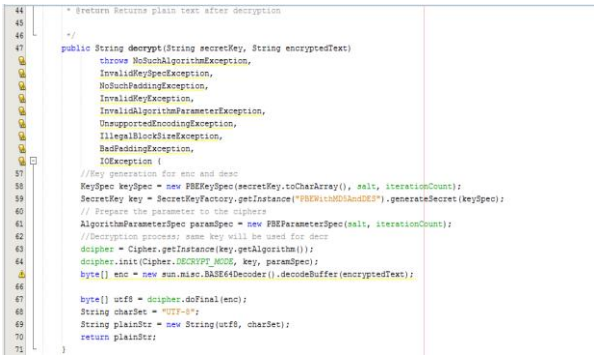
1) Encryption:



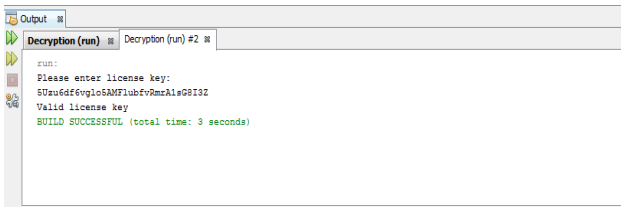
output:



2) Decryption:



Output:



VIII. CONCLUSION

From both side that means encryption and decryption key values are matching, hence Cramer Shoup algorithm is proved. It is a advance version of RSA algorithm. It is more accurate than RSA algorithm.

REFERENCES

[1] Carlsson, M. (2015). SICStus logic programing Users Manual. Kista, Sweden.
[2] C. Basile, A. Lioy, et al, "POSITIF: A Policy-Based Security Management System," in eighth IEEE International Workshop Policies for Distributed Systems and Networks, 2007, pp. 280-280, Italy.
[3] Committee of Sponsoring Organizations of the Treadway Commission. (2004). COSO ERM: Enterprise Risk Management - Integrated Framework. from http://www.coso.org/-ERM.htm
[4] Common Criteria for data Technology Security analysis (2009).