IMPROVED ALGORITHM FOR BETTER AUTHENTICATION AND SECURITY IN CLOUD ENVIRONMENT

Gopi VinyasMusunuru[1]

[1] Graduate Student, Department of Computer Science, Northern Illinois University, USA

ABSTRACT

Cloud Computing is a Service Delivery Mechanism. Computing resources are delivered as a service over the network. These services are Scalable, Autonomous, and Cost effective in nature. Cloud Computing is responsible for the exponential growth of IT Industry. In spite of having so many advantages it has various security challenges that cannot be ignored. In order to make the Cloud Computing all the more secure and reliable some steps has to be taken against the threats of Cloud Computing model. Although cloud computing environment is viewed as a promising Internet-based computing platform, the security challenges it poses are also equally striking. Despite the rapid advancement of cloud computing technologies, security issues in cloud environments have to be addressed to a greater extent. Cloud security is one of the major issues that hinder the adoption of cloud computing and slow down its acceptance in many sectors. The security concerns that should be addressed to realize the maximum benefits of cloud computing. Security patterns allow cloud developers to use security measures without being security experts. Also, a cloud environment can be reengineered by using security patterns to add missing security features.

Keywords: -Cloud security; Cloud threats; Data privacy; Security framework

1. INTRODUCTION

Cloud Computing is the use of computing useful things inclusive of hardware and software that are added as a carrier over a community. In other words Cloud computing can be defined as a new style of computing in which dynamically Scalable and often virtualized sources are furnished as a offerings over the net. It can also be defined as “the idea that data and programs can be stored centrally, in the cloud and accessed anytime from anywhere through thin clients and lightweight mobile devices. It provides many features like data ubiquity and resilience. Cloud computing provides more options to users because the data storage and processing are primarily handled by the cloud vendors. Therefore the data is stored in remote location which leaves the user without an exact understanding of the storage location.With the cloud computing generation, users use a variety of devices, such as desktops, laptops, smartphones, and PDAs to get admission to packages, storage, and application- development systems over the net, through offerings provided by cloud computing companies. This type of environment involves multiple stakeholders like clients, software developers, security experts and cloud vendors. Cloud Computing is labeled in approaches, one is with deployment version and the opposite is carrier transport version.

1.1.Deployment fashions of the cloud are:

A. Private Cloud: Personal Clouds are provided by means of an agency or their distinct provider company and offer a single-tenant (committed) operating environment with all the advantages and functionality of elasticity and the duty/utility version of Cloud.

B. Public Cloud: Public Clouds are furnished by using a designated service issuer and can offer both an unmarried-tenant (dedicated) or multi-tenant (shared) running surroundings with all the blessings and capability of elasticity and the accountability/application model of Cloud.

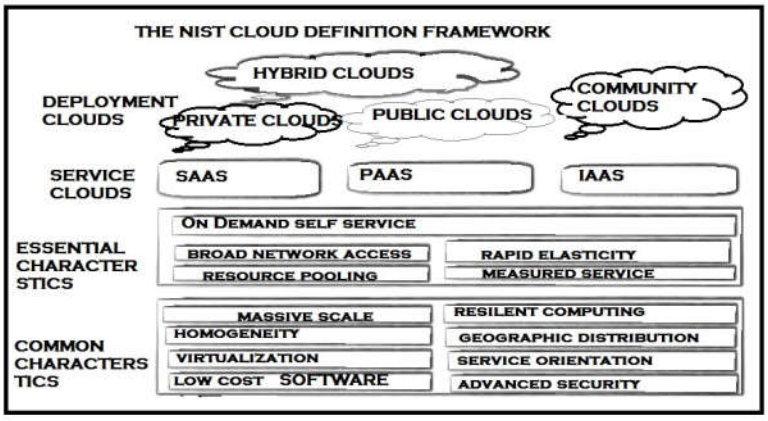
C. Network Cloud: Community Clouds are furnished by way of a chosen carrier provider related to a specific network and may also offer either a single-tenant (dedicated) or multi-tenant (shared) working surroundings with all the advantages and functionality of elasticity and the responsibility/application model of Cloud.

D. Hybrid Cloud: Hybrid Clouds are a mixture of public and non-public cloud offerings that permit for transitive statistics alternate and in all likelihood utility compatibility and portability across disparate Cloud service services and carriers utilizing wellknown or proprietary methodologies irrespective of possession or location.

1.2. Provider shipping version of the cloud are

A. Software as a service (SaaS): The capability furnished to the consumer is to use the company's packages going for walks on a cloud infrastructure and reachable from diverse consumer devices through a thin consumer interface inclusive of an internet browser (e.g., web-based e-mail).

B. Platform as a provider (PaaS): The capability provided to the customer is to install onto the cloud infrastructure customer- created packages the use of programming languages and gear supported by the provider (e.g., java, python, .internet). Infrastructure as a carrier (IaaS): The functionality supplied to the consumer is to lease processing, storage, networks, and different fundamental computing resources in which the purchaser is capable of deploy and run arbitrary software, that may consist of operating structures and packages.



2. LITERATURE SURVEY

A. RYAN (Protection challenges based on encryption strategies):-

He stated the following factors of cloud computing safety troubles:

1) Cloud, being a shared environment lets in any sharer to end up an attacker,
2) Cloud-primarily based statistics access is feasible from insecure protocols across any public networks
3) facts saved inside the cloud might also be lost or by chance/deliberately changed by using the cloud dealer,
4) Any worker, sub-contractors or the cloud company hasget admission to the records stored within the cloud.

The author claims that the primary three troubles aren't very specific to cloud computing however stresses that vendors'/employees' facts get admission to possibility poses a extreme safety risk on statistics confidentiality. Cloud provider may not manipulate the statistics, but the very fact that the company can view the facts without authorization is a severe safety breach. Ryan proposed 4 unique encryption techniques from the literature as ability solutions to block the unauthorized records access by using a cloud provider. This paper basically targeted at the confidentiality viewpoint of the facts. on this look at, authors mentioned the confidentiality problems by means ofthinking about cloud-computing-basedconvention control structures like EDAS and Easy Chair as case studies, which might be exceedingly small-sized clouds. From the scalability viewpoint, the proposed encryption strategies won't fulfill the safety requirements, and the author confirms it through stating, "the query of ways relevant it's miles to real cloud computing problems isn't always clean."

B. POPOVIC AND HOCENSKI (challenges to hold private-ness in clouds):

They highlightedtop ten cloud security worries in their examination. They emphasized the lack of know-how or manage of wherein the sources run, who controls the encryption/decryption keys, law violation of information seizure (via foreign governments) as foremost security challenges. Authors also claim records integrity, some government guidelines on a few touchy financial or PII (non-public Identifiable records) statistics to be remained of their home us of a as a severe protection difficulty cloud computing generation is dealing with. Their observe concentrates on the difficulty in making sure the auditability and consistency of information due to the dynamic and fluid nature of digital machines. After an analysis on modern safety countermeasures used in cloud computing, Popovic and Hocenski defined twenty advocated security control models that have to be maintained by means of cloud service vendors. Essentially, those control models are targeted on protection requirements from vendors than a supporting model for customers. in line with the survey conducted by global information corporation (IDC), among 263 IT executives to gauge the demanding situations concerned in using cloud offerings, safety turned into ranked as the largest assignment Jensen et al. recognized XML signature, browser safety, cloud integrity, binding troubles and flooding assaults as large cloud computing security issues. XML Signature detail Wrapping assaults, commonly called wrapping attacks, is an assault on protocols using XML signatures to break the integrity and authentication policies of a gadget. This assault takes place at the same time as the use of internet services, and cloud computing uses web services. for this reason, wrapping assaults are feasible in cloud computing as well. Jensen et al. kingdom that "current browser-based authentication protocols for cloud computing are not relaxed whilstthe

browsers cannot trouble XML-based totally protection tokens by itself." Jensen et al. discussed how cloud malware injection assault and Metadata spoofing assault can introduce integrity threats to the facts saved within the cloud. The authors investigated the effect of flooding attacks in cloud environments, which occur when a hacker sends a bulk quantity of beside the point or useless requests to a carrier to launch a Denial of service (DoS) assault to the server hardware.

C. KUYORO ET AL(protection demanding situations based on cloud kinds):

He studied the cloud computing safety problems and challenges by way of focusing on the cloud deployment and service delivery types. Clouds can be deployed as three exceptional models, non-public, Public or Hybrid clouds. Authors said that the personal clouds are a great deal more secure than public clouds considering all cloud sources are managed by way of the corporation that maintains the cloud. Public clouds, generally a pay-in step with-use model poses a protection threat, because the information is shared with an off-website online third-birthday celebration company. Hybrid cloud is a aggregate of personal and public clouds that offer extra control over the records, and additionally numerous users can get entry to those records via the net. on this type model, authors failed to evaluate the cost fashions in keeping those deployment fashions and security change-offs.

D. RAMGOVIND ET AL (protection challenges based totally on cloud deployment models):

He defined three huge deployment fashions: Infrastructure as a provider (IaaS), software as a provider (SaaS) and Platform as a carrier (PaaS) and highlighted safety issues that are specific to every deployment version. Upon selecting a cloud delivery model (non-public, Public or Hybrid) and deployment version (IaaS, SaaS or PaaS), authors enumerated the security concerns that protection experts and users have to be privy to in the cutting-edge cloud computing environment. The authors integrated several safety troubles emphasized via Gartner into their investigations on records security issues whilst managing cloud computing, which might be privileged get right of entry to, regulatory compliance (outside audits, security certifications, and so forth.), information vicinity (purchaser's control over the vicinity), information segregation (is encryption to be had in any respect tiers to all clients?), restoration (catastrophe management), investigative guide (potential to analyze illegal/beside the point sports), long term viability (if a supplier goes out of business), and records availability (if the supplier moves to a unique environment).

E. ZISSIS AND LEKKAS (severe threats faced by means of cloud computing environments):

They enumerated the safety challenges in cloud computing and recognized the important thing functions of cloud computing as flexibility/elasticity (quick and clean access), broad network access (used from heterogeneous platforms – cellular phones, pcs, Laptops, etc.), area independence, reliability (use of a couple of redundant websites), economies of scale and price effectiveness (no protection required) and sustainability. Zissis and Lekkas additionally argued that the adoption of this progressive architecture and its extensive key features opened up the window of many uncategorized threats.

Subhashini and Kavitha's paintings surveyed the cloud security troubles related to provider delivery fashions. along with all the protection demanding situations, the authors highlighted the

need for network safety even as deploying SaaS model. In a SaaS model, records is acquired from the user, processed through the SaaS utility, and the statistics/records is stored in the cloud. on this system, a huge amount of information switch takes region inside the community, and the authors emphasized the want for network security. Even as cloud computing safety demanding situations were mentioned by means of many researchers,Morsy et al. diagnosed a few root reasons and key participating dimensions for protection problems in cloud computing. Their studies diagnosed multi-tenancy and elasticity to be the key characteristics that would have serious protection implications in a cloud. Their proposed solution to accomplish comfy multi- tenancy is to preserve isolation amongst tenants' facts by using the cloud supplier. the field of cloud computing is not completely mature, not to mention that the safety aspects of cloud computing remains beneath exploration. In maximum instances, protection is taken into consideration as an afterthought and nearly constantly comes as a Band-useful resource answer as soon as the attack takes vicinity.

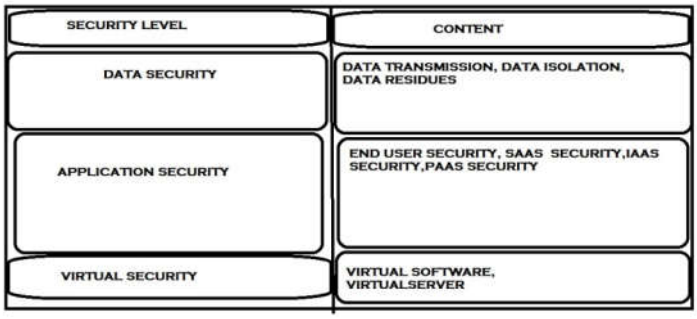
The contribution of this paper is especially focused on to enhance the security of the cloud surroundings so one can make the cloud all the extra comfy and dependable. via this paper we have tried to deliver the idea that the security of the cloud is the responsibility of both company and customer depending upon the layer and architecture of the cloud below attention. we've got referred to diverse threats of the cloud and their solutions as well. The unique contributions of this paper are as follows:

- Implementationof Isolation and Segmentation techniques of computing resources can triumph over the problem of multi-tenant structure that stocks the equal example of sources with a couple of customers.
- Introduction of devoted application on the area of net browsers can overcome the problems of phishing attacks and different statistics breaches threats. Defining the extra particular service level agreement (SLA) will resolve the troubles of maintenance of exceptional of carrier (QoS), information loss and other related cloud threats.
- Use of strong two aspect authentication strategies can save you the problems of account hijacking and associated threats.
- Implementation of honeypot device will prevent the cloud from Denial of carrier assault and the abuse of cloud offerings.

3. SAFETY ATTRIBUTE FOR CLOUD SERVICE

The version of cloud computing has changed the manner we use the IT sources. The development of the cloud provider model provides commercial enterprise-supporting era greater efficaciously than ever before. Cloud computing has concurrently converted commercial enterprise andgovernment andcreated new protection challenges. The CSA (Cloud safety Alliance) has recognized the pinnacle nine cloud computing threats for 2013. Those threats are the most essential threats that may be feasible in the contemporary cloud surroundings.

Cloud security content:-



4. RESEARCH METHODOLOGY

Those threats are as follows in keeping with their rank of severity:

A. **Data breaches:** The idea of records breach is that any malicious character or unauthorized character enters right into a corporate network and stoles the sensitive or private records.

B. **Data Loss:** The every other serious threat is the ability incapacity to prevent statistics loss because most of the corporations treat their information as a treasured asset.

C. **Insecure API:**If the utility Programming Interfaces which might be utilized by the customers to speak with the cloud services are vulnerable or no longer sufficiently secured, unintentional or malicious try to violate them may reveal the cloud information to many security threats associated with rigid access control, scalability and restricted monitoring and lots of other troubles.

D. **Account Hijacking:**In Account Hijacking a malicious intruder can use the stolen credentials to hijack cloud computing services and they are able to input on different transactions, insert fake statistics, and divert users to abusive net sites which led to criminal problems for cloud service vendors.

E. **Denial of provider:**DoS have emerged as very severe chance when the groups are depending on the offerings for 24/7. It quickly denies the get admission to of data saved within the cloud to the authorized customers by using make an attack on the server by using sending heaps of requests to it end up unable to respond to the regular clients.

F. Malicious Insiders: A person who enters the cloud network to damage the agencies personal data and property, harm precious manufacturers, penalize economic harm, prevent productivity is known as a malicious insider.

G. Abuse of Cloud offerings: This hazard is more of an issue for cloud provider companies than cloud purchasers, however it does increase some of severe implications for those providers.Itmighttake an attacker, a year to crack an encryption key the use of his very own constrained hardware, however using an array of cloud servers, he might be capable of crack it in minutes.

Cloud companies and client each are liable for the safety of cloud surroundings. In 2011 Sony PlayStation community became hacked the usage of the Amazon Elastic ComputeCloud as a result, Sony turnedinto forced to close thePlayStation network. in this attack, Attackers stole account information belonging to more than 100 million Sony PS customers. This incidence is the great example of “data Breaches” and “Abuse of Cloud offerings”.

In October 2012 large Flooding Damages numerous NYC records facilities and convalescing from a catastrophe is by no means easy.In October 2014 almost 7 million Dropbox usernames and passwords were hacked, apparently from third-celebration appsthat users allowed to get right of entry to their money owed these days in October 2015 TalkTalk Telecommunication group turned into attacked and personal and banking details of as much as 4 million clients may additionally were accessed inside the "giant" attack.

The analysis of danger is very critical in cloud environment, because of the numerous demanding situations of cloud computing. the security and privacy of both provider and purchaser may be compromised with the specific present threats of cloud. within the next segment contains the concept and certain answer of these problems and threats.

5.METHODS USED

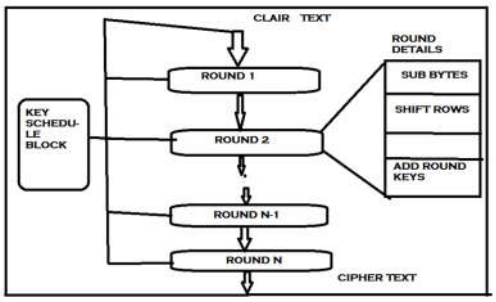
5.1.AES ALGORITHM

The advanced Encryption wellknown (AES), also acknowledged by means of its original call Rijndael,is a specification for the encryption of digital records installed by means of the U.S. countrywide Institute of requirements and generation (NIST) in 2001.For AES, NIST selected three members of the Rijndael own family, every with a block size of 128 bits, however three one of a kind key lengths: 128, 192 and 256 bits.

AES is now used worldwide. It supersedes the records Encryption standard (DES), which turned into published in 1977. The algorithm described by AES is a symmetric-key algorithm, which means the identical secrets used for both encrypting and decrypting the information.AES has a fixed block size of128bits, and a key size of 128, 192, or 256 bits. The key size used for an AES cipher specifies the number of repetitions of transformations rounds.

The number of cycles of repetition is as follows:

1. 10 cycles of repetition for 128-bit keys.
2. 12 cycles of repetition for 192-bit keys.
3. 14 cycles of repetition for 256-bit keys.

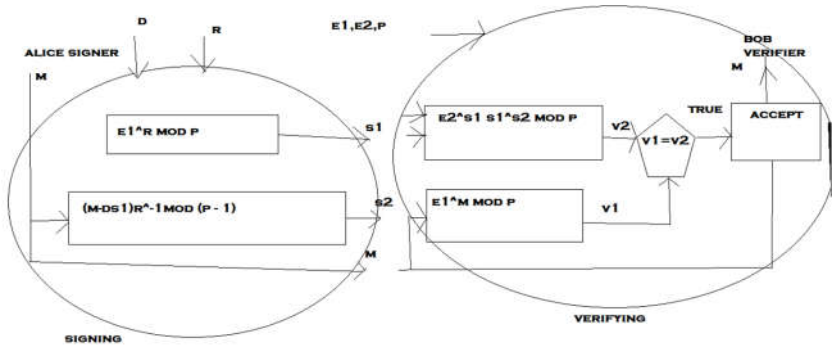


5.2. ELGAMAL ALGORITHM

In cryptography, the ElGamal encryption system is an uneven key encryption set of rules for public-key cryptography that is primarily based at the Diffie–Hellman key alternate. The machine offers an extra layer of safety by means of asymmetrically encrypting keys previously used for symmetric message encryption. It turned into described with the aid of Taher Elgamal in 1985. ElGamal encryption is used inside the free GNU private-ness defend software program, current variations of PGP, and other cryptosystems. The digital Signature set of rules (DSA) is a variant of the ElGamal signature scheme, which should no longer be harassed with ElGamal encryption.

Elgamal Scheme(..)

M: Message	R: Random secret
S1, S2: Signature	D: Alice's private key
V1, V2: Verifications	e1, e2, p: Alice's public key



Input: public key kpUb= (p, A, B) and message m
Output: ciphertext c
l. Function ENCRYPT(m)
2. Choose k E {2, .. .p-2}
3. x =cx:k mod p
4. Y = Bk * m mod p
5. Return c = (x, y)
6. End function
Input: private key kpr = a and ciphertext c = (x, y)
Output: message m
l. function DECRYPT(c)
2. Calculate m = x-ay mod p
3. return m
4. end function

6. ALGORITHM

6.1. File Upload Algorithm:

1.Encrypt_File (F) {
2. /* algorithm to encrypt file onto cloud storage */

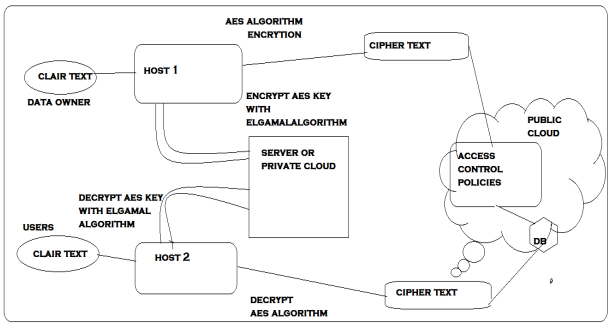
3. /* to transform Clair text in file F into Cipher text in file F' */

4. /* Phase 1: Encrypt Clair text with AES Algorithm */
5. for B+-1 to numberOfBlock(F) do
6. {
7. B'=ENC_AES (B, K)
8.}
9. send_to_cloud(F')
10. /* Phase 2: Encrypt AES key with Elgamal Algorithm */
11. for k+-1 to SizeOf(K) do
12. {
13. k'=ENC_Elgamal(k)
14.}
15. Save_in_server(K')
16.}

6.2. File Download Algorithm

1.Decrypt_File (F') {
2. /* algorithm to decrypt file downloaded from cloud storage*/
3. /* to transform Cipher text in file F' into Clair text in file F*/
4./* Phase 1: Decrypt AES Key with Elgamal Algorithm */
5.for k' +-1 to SizeOf(K') do {
6.k=DEC_Elgamal(k')}
7. return(K)}
8. /* Phase 2: Decrypt Cipher text with AES Algorithm */
9. for B'+-1 to numberOfBlock(F'} do {
10. B=DEC_AES (B', K)
11. return(F)
12.}

Proposed Model of Data Storage in Cloud Computing: -



CONCLUSION

Although Cloud storage has many advantages there are still many actual problems concerning security that need to be solved. If we can eliminate or master this weakness of security, the future is Cloud storage solutions for large as well as small companies. We have also proposed a solution to improve the security of the storage of data, data security is provided by implementing our algorithm. Only the authorized user can access the data. Even if some

intruder (unauthorized user) gets the data accidentally or intentionally if he captures the data, he can't decrypt it and needs two keys coming from two different locations. In the next papers, we will try to offer solutions to protect against DDOS attacks in cloud computing.

REFERENCES

1. Kolodner, Elliot K., TAL, Sivan, KYRIAZIS, Dimosthenis, etal. Cloud environment for data-intensive storage services. In : Cloud Computing Technology and Science (CloudCom), 2011 IEEE Third International Conference on. IEEE, 2011. p. 357-366.
2. P. Arora, R. C. Wadhawan, and E. S. P. Ahuja, « Cloud Computing Security Issues in Infrastructure as a Service », into J. Adv. Res. Comput. Sci. Softw. Eng., vol. 2, n° 1, 2012.
3. A Platform Computing Whitepaper. -Enterprise Cloud Computing: Transforming IT. Platform Computing, pp6, 2010
4. Cloud Security Alliance 'Top Threats to Cloud Computing" Version 1.0 (20 10). <http://www.c1oudsecurityalliance.org.>.
5. 9 top threats to cloud computing security <http://www.infoworld.com/article12613 560/c1oud-security/9-topthreats- to-c1oud-computing-security.html>.