NC as a Security Services for Data Security in Cloud

Hetal Patel
Master Engineering, Silver Oak College of Engineering & Technology
Ahmedabad-Gujarat

ABSTRACT

Cloud Computing is trending in today's technology driven world. With the advantages of flexibility, storage, sharing and easy accessibility, Cloud is being used by major players in IT.Apart from companies, individuals also use cloud technologies for various daily activities. From using Google drive to store, to Skype to chat and pica web albums, we use cloud computing platforms extensively. We proposed a design for cloud architecture which ensure secure data transmission for the client organization to the server of the cloud network. We have use combined approach of network coding and steganography because it will be provide a security to the data being transmission on network. First Data get converted in to coded format through the use of network coding algorithm and coded format data again converted into Stegno images through steganography.

Keyword: - *Network Coding, Security, Cloud Computing*

Paper 1: A Novel Cryptographic and Steganographic Approach for Secure Cloud Data Migration.

The flexibility to store unlimited data without any worry about storage limitations available at our disposal and the freedom to use it as and when required from anywhere in the world makes cloud computing the most preferred technology & platform to store and transfer data. Organizations and individual users are now very much comfortable to let their all-important data and software reside on the cloud servers and make themselves free from all the concerns of storage and security. However, every flexibility or benefits comes at a price and cloud computing too is not an exception. The threat of user's privacy, data confidentiality & integrity and data safety are always looming around. Among all of these, the secure transfer of data from organization's premises to the cloud servers is of utmost importance. So many encryption techniques and algorithms have been proposed by researchers in recent times to move data securely from their end to the servers. In this research paper, we propose a design for cloud architecture which ensures secure data transmission from the client's organization to the servers of the Cloud Service provider (CSP). We have used a combined approach of cryptography and steganography because it will provide a two way security to the data being transmitted on the network. First, the data gets converted into a coded format through the use of encryption algorithm and then this coded format data is again converted into a rough image through the use of steganography. Moreover, steganography also hides the existence of the message, thereby ensuring that the chances of data being tampered are minimal.

Keywords:-cryptography; steganography; cloud; encryption; private; key; stego; compliment;

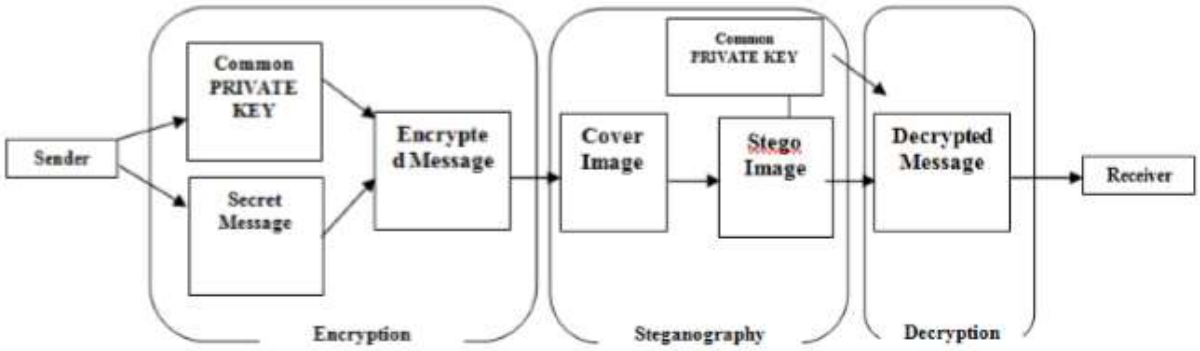

Fig-1: Sequence diagram of cryptography and steganography Process

Figure above shows the sequence diagram where we have categorized the cryptography process into encryption and decryption part and in between these, the steganography works. We propose to use symmetric key cryptography or Private Key Cryptography in the approach where both sender and the receiver share a common secret key. The beauty of this approach is that the value of this Private Key will not remain static or constant all the time, it will be different or dynamic for every calculation and thus, it proves to be a secure method of performing cryptography. The sender and receiver both agree on using a common Private Key. The sender, while sending the secret message encrypts the message using commonly agreed Private key. The message now gets encrypted and then, through the use of a cover image, the encrypted message or data is hidden behind that cover image which we call now a stego image. This stego image travels across the network and on the receiving side; the actual receiver firstly removes the cover image from the stego image and then again uses the commonly agreed Private Key to bring back the message in its original form.

Benefits of the proposed work

The proposed approach provides a secure way of migrating data on to the cloud servers. It makes use of cryptography and steganography techniques which provide a multilayered protection to the client's sensitive data files. For Cryptography, it uses the symmetric approach which is not much costly when compared to the Asymmetric approach. It also takes dynamic values every time for calculations which make it even better. For Steganography, it uses LSB method of embedding bits in the pixel elements of the image.

Conclusion:

In this paper, we proposed an innovative approach to migrate data on cloud servers through the combined use of cryptography and steganography. In cryptography process, we make use of very simple yet effective technique for data encryption using one's complement method which we called as SCMACS. It used symmetric key method where both sender and receiver share the same key for encryption and decryption. The strength of the approach lies in the fact that the symmetric key method generates a dynamic value for the private Key which makes it very safe because no one can have the private key and even some one gain access to it, it gets changed for each data that needs to be transferred. In Steganography part, we used the LSB method that is used and mostly preferred. As for future work, we'll put efforts in implementation part of this approach and will try to make comparison of our approach with similar other approaches proposed by fellow researchers.

Paper-2 Secret Data Sharing in Cloud Environment Using Steganography and Encryption Using GA

Cloud Computing is the next step in the evolution of on-demand network access to a shared pool of configurable resources that can be rapidly provisioned and released with minimal management effort or service provider interaction where Infrastructure, Platform and Software can be accessed as a service. The clients accessing the service, pay for what they use. Cloud Computing provides benefits in terms of low cost and accessibility of data, but its unique aspect is its security. Sharing of data is an important functionality in cloud storage. In cloud computing environment data sharing and transfer has increased exponentially. Security, integrity, non-repudiation, confidentiality, and authentication services are the most important factors in data-security. Maintaining Confidentiality and Security for critical data are highly challenging, especially when these data are stored in memory or send through the communication networks. The confidential data are embedded steganography. Data encryption

technique tries to convert data to another data that is hard to understand. In this paper, a crypto-stego methodology has been proposed where image steganography and a new method of cryptographic technique is used. The steganographic technique embedded confidential data using Pixel Mapping Method (PMM), but in a chaotic sequence generated by chaotic map technique. The encryption and decryption uses Genetic Algorithm (GA) which is used to produce a cryptographic method with the help of the powerful features of the Crossover and Mutation operations of GA. Both the encryption and steganography process use secret session key which are generated using the combination of some universal feature of cover image and the users user's secret key.

Introduction:

cloud computing is acquiring great deal of attention in users, markets, education and publications. Cloud computing technology is a group of servers that provide highly scalable cloud services like SaaS (Software as a Service), PaaS (Platform as a Service), IaaS (Infrastructure as a Service) to transform computing in business. Information stored in clouds is accessible from anywhere at any time. Cloud providers have storage, software and infrastructure facilities to run businesses effectively, more connective, scalable, collaborative, real-time and productive. It is an internet based computing, whereby shared resources, software and information are provided to computers and outer devices on demand.Cloud computing is based on the concept of virtualization and hence eliminates the need of a powerful configuration deployment by providing services at a reasonable price and hence this technology is very helpful for small organizations that cannot afford the cost of infrastructure and storage space.

Proposed Method:

In the proposed method we use Symmetric-key Encryption technique where some properties of the Stream cipher's properties used, i.e. for each block, a different "key" is generated in case of data encryption, but the encoding of each block is not depend on previous blocks. We use the PMM technique but the embedding blocks are dependent on the session key.

Conclusion & Future Work:

In this paper, we propose a genetic algorithm based secret key image encryption method and data position scrambling PMM. After the examinations of the proposed method, it is clear that this encryption method is satisfied the goals that are required in any encryption method for encrypt text or images. Our proposed method exceeds the embedding capacity of GLM method but was less than PVD technique. The PSNR value is at par with the other two methods.

In this paper, Genetic algorithm based secret key data encryption method is presented. In the future work, there is a planning to design a public key data encryption method based on this technique which will targeted to use in highly secure multimedia data transmission applications but that method must have low computational complexity and overcome the database overload headache.

Paper-3 Secure Cloud Storage Meets with Secure Network Coding

This paper reveals an intrinsic relationship between secure cloud storage and secure network coding for the first time. Secure cloud storage was proposed only recently while secure network coding has been studied for more than ten years. Although the two areas are quite different in their nature and are studied independently, we show how to construct a secure cloud storage protocol given any secure network coding protocol. This gives rise to a systematic way to construct secure cloud storage protocols. Our construction is secure under a definition which captures the real world usage of the cloud storage. Furthermore, we propose two specific secure cloud storage protocols based on two recent secure network coding protocols. In particular, we obtain the first publicly verifiable secure cloud storage protocol in the standard model. We also enhance the proposed generic construction to support user anonymity and third-party public auditing, which both have received considerable attention recently. Finally, we prototype the newly proposed protocol and evaluate its performance. Experimental results validate the effectiveness of the protocol.

Keyword: Cloud storage auditing, network coding, security, user anonymity, third-party public auditing

Introduction:

CLOUD storage is being widely adopted due to the popularity of cloud computing. However, recent reports indicate that data loss can occur in cloud storage providers (CSPs). Thus, the problem of checking the integrity of the data in cloud storage, which we referred to as secure cloud storage (SCS), has attracted a lot of attention. On the other hand, networking coding, which was proposed to improve the network capacity, also faces the problem of integrity checking. An intermediate router may intentionally pollute codewords, which results in decoding failures at the endpoints. Checking the integrity of codewords is referred to as the secure network coding problem. Different researchers have studied secure cloud storage and secure network coding independently.

Secure cloud storage. This problem was first proposed by Juels and Kaliski and Ateniese et al. Two main entities are involved in these protocols: a user and a cloud storage provider. A user outsources the data to the cloud who promises to store the data. The user then confirms the data integrity by interacting with the cloud using a secure cloud storage protocol. The motivation of data integrity checking lies in several factors. First, due to the poor management of the cloud, the user's data could be lost due to system failures (hardware or software). To cover the accident, the cloud may choose to lie to the user. Second, the cloud has a huge financial incentive to discard the data which is rarely accessed by the user. Ignoring some part of the data helps the cloud to reduce its cost. Third, a cloud could also be hacked and the data could be modified. Fourth, a cloud may behave maliciously because of various possible government pressures. Without a secure cloud storage protocol, the occurrence of these incidents may be hidden by the cloud and gone unnoticed.

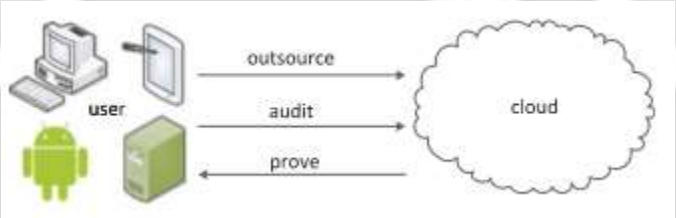

Fig -2: Secure cloud storage system

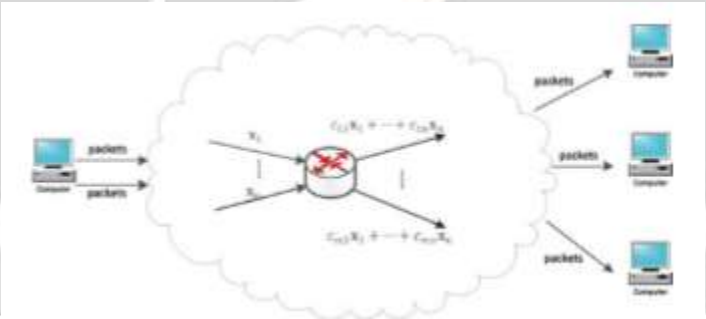

Fig 3-: A Secure Network Coding System

Fig. 3 shows a typical system that employs the network coding technique. There are three types of entities: sender, router, and receiver. A sender wants to broadcast some data to a group of receivers. The sender divides the data into packets and sends a linear combination of the packets via the network. A router in the network also sends a linear combination of the received data packets to its next hops. When a receiver obtains sufficient encoded data packets, it can decode them to recover the original data by solving a system of linear equations. To prevent a malicious router from modifying a packet, the sender attaches some authentication information with each data packet. When a router receives a series of packets, the router first checks their correctness, then combines the received correct packets, and finally sends out the combined packet together with the combined authentication information. The combined authentication information is computed according to the details of a specific protocol.

Conclusion & Future Work

We reveal a relationship between secure cloud storage and secure network coding for the first time. Based on the relationship, we propose a systematic way to construct a generic secure cloud storage protocol based on any secure

network coding protocol. As a result, we obtain the first publicly verifiable secure cloud storage protocol which is secure without using the random oracle heuristic. Further, we enhance our generic construction to support user anonymity and third-party public auditing. We hope our opensourced prototype can make a step towards practical use of secure cloud storage protocols. For future work, it is interesting to design new and efficient secure cloud storage protocols based on our generic construction and existing/ future researches on secure network coding protocols. It is also interesting to study the reverse direction, i.e., under what conditions a secure network coding protocol can be constructed from a secure cloud storage protocol. This possibly requires the latter to have some additional properties

Paper-4 A Novel Privacy and Security Framework for the Cloud Network Services

We reveal a relationship between secure cloud storage and secure network coding for the first time. Based on the relationship, we propose a systematic way to construct a generic secure cloud storage protocol based on any secure network coding protocol. As a result, we obtain the first publicly verifiable secure cloud storage protocol which is secure without using the random oracle heuristic. Further, we enhance our generic construction to support user anonymity and third-party public auditing. We hope our open sourced prototype can make a step towards practical use of secure cloud storage protocols. For future work, it is interesting to design new and efficient secure cloud storage protocols based on our generic construction and existing/ future researches on secure network coding protocols. It is also interesting to study the reverse direction, i.e., under what conditions a secure network coding protocol can be constructed from a secure cloud storage protocol. This possibly requires the latter to have some additional properties.

Keyword: Cloud Computing, Security, CCMP, Services

Introduction:
Cloud computing is the Internet-based computing where the application software, infrastructure, and platform are exposed as software and the end users can access it through a distributed cloud, as a client. Cloud is a step on from utility computing and provides a convenient on demand network access to a shared pool of configurable computing and communication resources. Here, resources refer to computing applications, network resources, platforms, software services, virtual servers, and computing infrastructure. Cloud computing is being widely adopted across many industrial sectors. Security, availability, and performance are the three biggest problems in cloud adoption. The serious challenge is how it reports security and privacy issues which occur due to movement of data and application on networks, loss of control on data, dissimilar nature of resources, and several security policies. Data storage, processing and movement outside the controls of an organization poses an inherent risk and making it vulnerable to various possible attacks. Cloud computing poses privacy concerns because the cloud service providers may access the data that is on the cloud that could accidentally or knowingly be changed or even removed, creating serious business trust and legal consequences.

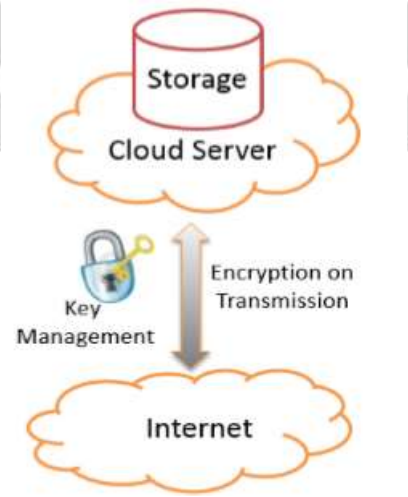

Fig -4: Encryption Mechanism on Cloud Network

Fig -5: Security Mechanism on Cloud Network

Conclusions:

There are several advantages of cloud computing such as high level computing, scalability and pay-as-you use. Cloud service provider has less transparency than other information security policy. As a result, it may create clash with the enterprise's information. The enterprise needs to have detailed understanding of the service level agreements that requires desired level of security provided by the cloud service and cloud networks must enhanced the performance when a user moves to cloud computing infrastructure. The computing performance is normally measured by capabilities of applications running on the cloud system. However, this paper discusses the insight computing of CCMP payload with excess AAD, and without excess AAD and designed a novel secure framework for cloud services, as well as presented a critical analysis of CCMP protocol for secure data management of cloud network ITS services. We present a novel privacy and security scenario user and cloud network management ITS services.

Paper-5 Securing Cryptographic Keys in the IaaS Cloud Model

Infrastructure-as-a-Service (IaaS) is a widespread cloud computing provisioning model where ICT infrastructure, including servers, storage and networking, is supplied ondemand, in a pay-as-you-go fashion. IaaS cloud providers give their clients virtual machines (VMs) that are controlled by cloud administrators who can run, stop, restore and migrate the VMs. A typical threat to IaaS is unauthorized access of untrustworthy administrators to cloud users' sensitive information residing in VMs' memory. In this paper we focus on the threat of users' cryptographic keys being stolen from the RAM of the VM they provision. We propose a decrypt scatter/gather-decrypt technique that allows users to carry our encryption/decryption while protecting keys from unauthorized peeks on the part of cloud administrators. Our technique does not require modification to the current cloud architecture, but only the availability of a Trusted Platform Module (TPM) capable of creating and holding a TPMprotected public/private key pair. It lends itself to security-asa-service scenarios where third parties perform encryption/decryption on behalf of data owners.

Keyword: Cloud Computing, encryption key, code obfuscation, VM RAM security, memory protection.

Introduction:
In the Infrastructure-as-a-Service (IaaS) cloud model, encryption/decryption operations take place on a virtual resource, i.e. a Virtual Machine (VM) provisioned by the cloud provider. Protecting the content of VMs' RAM from unauthorized peeks is therefore an important step toward providing a secure CaaS in the IaaS model. Techniques for achieving such protection depend, in turn, on the type of virtualization used for IaaS provisioning.For this reason, many cloud providers are currently offering Cryptography as a Service (CaaS) to their clients. In principle, a cloud-based CaaS should allow cloud users to keep some control over the encryption/decryption operations performed on the cloud on their behalf, preventing disclosure of the users' cryptographic keys to other cloud tenants as well as to the cloud administrators/provider.

Motivation:
Attacks to encryption keys in the cloud are welldocumented in the field. For example in a cross side channel attack has been used to retrieve private keys from a co-located VM. Vulnerability number "CVE-2015-3340" allows certain remote service domains to obtain sensitive information from user memory, including cryptographic keys. Despite those examples of vulnerabilities targeting VM RAM, this issue has not received much attention in the technical literature. One of the main features of symmetric encryption is key randomness. This suggested to attackers a way to detect encryption keys in RAM based on the higher entropy of their value compared to surrounding data. With AES, the encryption round keys are usually generated and saved next to each other in RAM before starting data encryption and are an easy target for detection.

Conclusion:

In this work we presented a novel solution to secure the cryptographic keys in the RAM of VM provisioned according to the IaaS model. Our solution can run on any cloud environment that can provide a TPM, without modifying the infrastructure. It will provide data owners with full control over encryption key and decryption services in the IaaS model. Inevitably, our solution will incur in a performance overhead that we plan to measure in our future work. We will also deploy our implementation in a real cloud environment to measure its security effectiveness and performance overhead.

CONCLUSIONS

In the cloud computing many process available for the data security for the data transmission. In the cloud server using network coding and steganography we can provide more and reliable security in cloud. In the network coding process we can make very simple and effective technique use for data security. We proposed a design for cloud architecture which ensures secure data transmission for the client organization to the server of the cloud network. We have use combined approach of network coding and steganography because it will be provide a security to the data being transmission on network. First Data get converted in to coded format through the use of network coding algorithm and coded format data again converted into Stegno images through steganography.

ACKNOWLEDGEMENT

I, hereby, take an opportunity to convey my gratitude for the generous assistance and cooperation, that I received from the **PG Coordinator Mr. Vikash Tulshyan** and to all those who helped me directly and indirectly.
I am sincerely thankful to my Guide, **Mr. Darshil Shah** for their constant help, stimulating suggestions and encouragement helped me in completing my Literature Review work successfully.
I am also thankful to **Mr. Jaimin Dave, Head of the Department** and other faculty members who have directly or indirectly helped me whenever it was required by me.
Finally, I am also indebted to my friends without whose help I would have had a hard time managing everything on my own.

REFERENCES

[1] Abdulzahra H et al, "Combining Cryptography and Steganography for Data Hiding in Images" ACACOS, Applied Computational Science ISBN 978-960-474-368-1

[2] Sherekar et al, Critical Review of Perceptual Models for Data Authentication,Emerging Trends in Engineeringand Technology (ICETET)2nd International Conference, 2009, pp. 323-329. IEEE.

[3] Usha, S., Kumar, G. A. S., and Boopathybagan, K., A secure triple level encryption method using cryptography and steganography, Computer Science and Network Technology(ICCSNT), International Conference, Vol.2, No.2.11, 2011 ,pp. 1017-1020.IEEE.

[4] Bharti,P.,andSoni, R.,A New Approach of Data Hiding in Images using Cryptography and Steganography,InternationalJournalofComputer Applications,Vol.58,No.18,2012,pp1-5

[5] Marwaha, P., Visual cryptographic steganography in images,Computing,Communication and Networking Technologies(ICCCNT), International Conference , 2010,pp 1-6. IEEE.

[6] Umamaheswari, M., Sivasubramanian, S. and S. Pandiarajan S., Analysis of Different Steganographic Algorithms for Secured Data Hiding,IJCSNS International Journal ofComputer Science and Network Security, Vol.10, No.8, 2010, pp 154-160.

[7]Domenico Daniele Bloisi, Luca Iocchi, "Image based Steganography and cryptography", Computer Vision theory and applications volume I, pp. 127-134 .

[8] Souvik Bhattacharyya, Lalan Kumar and Gautam Sanyal, "A novel approach of data hiding using pixel mapping method (PMM)"

[10]Spillman R,Janssen M, Nelson B and Kepner N, "Use of Genetic Algorithm in Cryptanalysis of Simple Substituion Cipher" Cryptologia, Vol.l7, No.4, pp. 367- 377, 1993.

[11] Spillman R,"Cryptanalysis of Knapsack Ciphers using Genetic Algorithms", Cryptologia, VoU7, No.4, pp. 367-377, 1993.

[12]Y. News. (2013). Cloud computing users are losing data, symantec finds [Online]. Available: http://finance.yahoo.com/news/ cloud-computing-users-losing-data-205500612.html

[13] P. Hernande. (2013). Byod, data loss top list of cloud computing challenges [Online]. Available: http://www.datamation.com/ cloud-computing/byod-data-loss-top-list-of-cloud-computingchallenges.html

[14]C. Wang, S. S. M. Chow, Q. Wang, K. Ren, and W. Lou, “Privacypreserving public auditing for secure cloud storage,” IEEE Trans. Comput., vol. 62, no. 2, pp. 362–375, Feb. 2013.

[15] N. Cai and R. W. Yeung, “Secure network coding,” in Proc. IEEE Int. Symp. Inf. Theory, 2002, p. 323.

[16] C. Gkantsidis and P. R. Rodriguez, “Cooperative security for network coding file distribution,” in Proc. IEEE Int. Conf. Comput. Commun., 2006, pp. 1–13.