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 7, July 2017

Evaluation of Secure Streaming of Files in Cloud Environment

Nemi Rishi

Assistant Professor, Dept. of IT, IITM, Janak Puri. New Delhi, India

ABSTRACT: The security of the messages being exchanged between two hosts on a network is of primary concern today for the internet community for secure transmission. The proposed work is aimed to provide a way to enhance the security of the text files stored in cloud environment. An authentication cloud server establishes trusted communication of files. Then the cloud stores chunks of files after RSA encryption. These messages are decrypted with the help of decryption keys provided by the Authentication Server to the client. These keys are passed to the receiver during the exercise to establish authenticated communication between the client and cloud server.

KEYWORDS: encryption, decryption, authentication server, digital signature, RSA etc.

I. INTRODUCTION

The security of the messages being exchanged between two hosts on a network is of essential concern today for the web group. The proposed work is plan to give an approach to improve the security of the content documents put away in cloud environment. A verification cloud server sets up trusted correspondence of documents. At that point the cloud stores pieces of documents after RSA encryption using an image to generate key and these messages are decrypted with the key generated by the same image provided by the client. These keys are gone to the recipient amid the activity to build up verified correspondence between the customer and cloud server.

For the most part encryption component utilizes the idea of RSA calculation with new hash work that produces alert and more productive and secure than different techniques. The proposed framework is performing secure by making chunks of the message, decrypting the chunks using a unique image and for decryption same image is needed. The image is utilized as the signature to get the document from the cloud server. The chunks are further recovered consolidated and came back to the client. The GUI based RSA 1024 bit encryption application has been produced in JAVA.

This application is equipped for producing the prime numbers all alone as per the quantity of bits determined by the client. Rest of the RSA encryption is led according to the storage of file from the client. An image is utilized to produce key for more secure gushing. This image is utilized to create key. The GUI based simulator is designed for sending and receiving text files between the cloud environment and server. The integration of the different components has been achieved by packaging them into different modules. The modularity achieved has been complete. The different modules can be used independent of each other. This is because of the Object Oriented nature of java.

A. Authentication server

An AS [1] provides a network service that applications use to authenticate the credentials, usually account names and passwords, of their users. When a client submits a valid set of credentials, it receives a cryptographic ticket that it can subsequently use to access various services

B.Password

A password [2] is a word or string of characters used for user authentication to prove identity or access approval to gain access to a resource (example: an access code is a type of password), which should be kept secret from those not allowed access.

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 7, July 2017

C. Kerberos

It is a network authentication protocol which works on the basis of 'tickets' to allow nodes communicating over a nonsecure network to prove their identity to one another in a secure manner. Its designers aimed it primarily at a client–server model and it provides mutual authentication—both the user and the server verify each other's identity. Kerberos [3] protocol message are protected against eavesdropping and replay attacks.

II. PROPOSED WORK

Cloud frameworks is basically a collection of interconnected servers that are provisioned alertly on interest, for execution of applications, to the client like electric grid. The cloud computing has increased awesome consideration from industry however there are still numerous issues that are in their primitive stage whining the development of Cloud. One of these issues is security of information put away in the servers of datacenters of Cloud service providers. Numerous plans have been created till date for guaranteeing security of information in Distributed Systems. These plans have been considered, investigated and new system has been proposed which infix the parameters of security like recuperation of information, classification of information and respectability of information such that it guarantee security of information put away in the servers of Cloud frameworks. The proposed plan is in view of two systems – Secure Streaming and creating key from an image. Data dispersal calculation helps in keeping up secrecy and honesty of information and key produced from image will helps in recovery of information. The property of proposed algorithm that makes it unique existing data storage schemes is that integrity is ensured by client. This property may help in picking up trust of client.

A. Platform independence and object-oriented nature were the two elements that made it the advancement environment of decision for the proposed work.

B. In the first step, File or message and an image are taken from client. In second track, for guaranteeing information repository security, handling of information happens. This incorporates part of record into shares, decoding of the shares with key produced by a picture document, of shares is performed in third step.

C. In fourth step, shares of the documents are saved on the distinctive servers. The ids of the servers and names of documents containing shares of record and its separate key are put away on the datacenter (cloud screen).

D. With a specific end goal to reproduce the document, client enters the id of servers containing the offer of record and picture key. The shares are decoded most importantly with the same picture key. *E.* On getting the shares, 'Remaking of record and message' calculation is actualized and the document (secret) and the message are recovered.

F. Message is sent to customer and customer checks if message acquired is same as the duplicate of message with him.

G. If message is right, then record is conveyed to customer.

N represent no. of shares of the File, K represents the no. of servers in cloud

1.Input File (to be Store on server) 2.Input Image File (to generate 16 bits key).

3. Implement TGS.
4. Divide the File into N shares and encrypt the shares.
5. Sending encrypted shares to K Serves Perform same steps to decrypt and return combined shares to the client on request. It is system Independent

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 7, July 2017

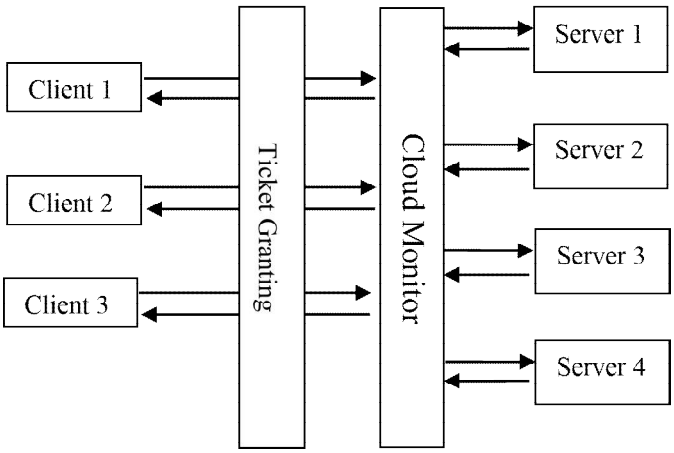

Fig: Architecture Of Proposed Work

III. LITERATURE STUDY

Security of information very still is the normal subject of research among researchers. There are diverse components reported till date to guarantee security of information very still and determination of any of these for any specific framework relies on upon different parameters like structural planning of framework where security is to be empowered, level of security obliged, measure of misfortune that may happen on loss of information and some more. The systems are talked about further in this section subsequent to presenting a few ideas of security. In today's reality secure transmission of vital or individual information is of enormous concern. The encryption of the information plays vital component of security while sending the data of information. Encryption of information means changing over plain content to figure content. There are numerous encryption methods accessible, however the central issue that emerges is which one is great one or which one is suitable according to requirements'

A. Authentication Protocol in Client – Server Application using Visual Cryptography. [4]

Kerberos [5] is a network authentication protocol and is designed to provide strong authentication for client/server applications by using Secret key cryptography for enhancing the security of transactions over a network. Kerberos Encryption Technique is used for authentication and transaction security in the network. An Authentication Server is created that used to derive a Steganography image from user's password. This Steganography image was used for verifying user's identity and gain access for sever. The generated image then was used by authentication server, to encrypt ticket granting ticket + session key.

EXISTING SYSTEM OF THE KERBEROS

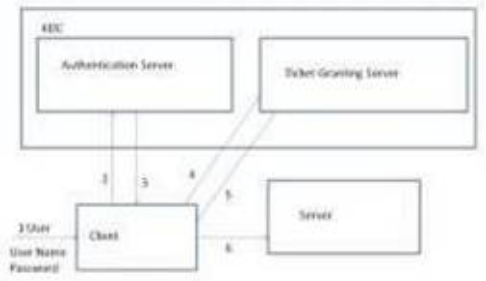

Fig1: Existing Kerberos Architecture

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 7, July 2017

1. Client's user name and password
2. Client providing the user name and password to authentication server
3. The authentication server generating ticket + session key gives to client
4. Client providing that ticket + session key to ticket granting server for granting ticket
5. Ticket granting server granting the ticket and sending it to client with timestamp
6. When all process is done in given timestamp then connection successful with client and server

*B.*Kerberos Working

Client to KDC (AS_REQ):The client sends its credentials to get authenticated by authentication server (AS), the part of Key Distribution Center (KDC) environment.

KDC to Client (AS_REP): AS replies to the request of the client with TGT and session key. TGT is encrypted using the TGS secret key and session key encrypted using user's secret key.

Client to KDC (TGS_REQ):Client sends request to TGS for service ticket. It contains TGT from the previous message and authenticator encrypted with the help of session key.

KDC to Client (TGS_REP):The TGS replies to the request of the client. It contains the service ticket encrypted using secret key of the service and session key generated by TGS and encrypted using session key generated in previous message by AS.

Client to Application Server (AP_REQ): In this client sends a request to access the service it requires. The request contains the service ticket, service name and the authenticator generated by client encrypted by service session key generated by TGS.

Application Server to Client (AP_REP): It's an optional reply to the client to prove authenticity of application server. It is generated when mutual authentication is required.

C. Encryption and Decryption Using Secure RSA [6]

1. **Cryptography**

Cryptography is a technique of converting plain text into cipher text. A cipher Text is a encoded form of plain text that is not readable or understandable by unauthorized user, the process of cryptography is also known as encryption and locking. RSA (Rivest, Shamir &Adleman) is asymmetric cryptographic algorithm developed in 1977. It generates two keys: public key for encryption and private key to decrypt message [7] .RSA algorithm consist of three phases, phase one is key generation which is to be used as key to encrypt and decrypt data, second phase is encryption, where actual process of conversion of plaintext to cipher text is being carried out and third phase is decryption, where encrypted text is converted in to plain text at other side.

As a public key is used for encryption and is well known to everyone and with the help of public key, hacker can use brute force method to find private key which is used to decrypt message.

2. **RSA file transmission**

The security of RSA comes from integer factorization problem. RSA algorithm is relatively easy to understand and implement RSA [8] algorithm is based on the theory of a special kind of reversible arithmetic for modular and exponent. RSA is used in security protocols such as IPSEC/IKE, TLS/SSL, PGP, and many more applications. The public and private keys are functions of a pair of large prime numbers and the necessary activities required to decrypt a message from cipher text to plaintext using a public key is comparable to factoring the product of two prime numbers.

RSA File Transmission Algorithm can be summarized as follows:

i)Generate the asymmetric keys with required digits. ii)Save and load the key, the key is saved as plain text.

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 7, July 2017

iii)Use specified key to encrypt any file with RSA algorithm. iv)Encrypted files can be loaded and decrypted with the specified key to restore the original file.

3.Implementation

Modified RSA for secure file transmission algorithm is divided in to four parts

i) Selecting file for transmission ii)Transmission of encrypted file iii)Encryption of file iv)Decryption of file at other end.

D. Secure Biometric Authentication Protocol. [9]

1. Biometric Authentication Authentication of a person is an important task in many areas of day-today life including electronic commerce, system security and access control. Kerberos present a client\server authentication protocol which can perform a secure communication over unsecured environments (internet) and solve the problem of authentication between client and server. When authenticating using Kerberos a series of messages is exchanged between principals and the authentication server, as well as between the principals themselves (the client and server). Tickets must be obtained from the authentication server and then exchanged between the client and server to perform authentication. Biometric authentication systems are gaining widespread popularity in recent years due to the advances in sensor technologies as well as improvements in the matching algorithms that make the systems both secure and cost effective. They are ideally suited for both high security and remote authentication applications due to the non-repudiate in nature and user convenience.

The biometric samples reveal more information about its owner in addition to the identity. Widespread use of biometric authentication also raises concerns of tracking a person, as every activity that requires authentication can be uniquely assigned to an individual.

Most biometric systems are assumed to be secure but there are chances of getting hacked. There are two places to be attacked: (i) one is on communication link and another (ii) on server's database.

The biometric authentication is being used for authenticating in most of the security required scenarios. If the biometrics used in plain, there are more chances for spoofing attacks by the imposters to gain illegal access to the server to get information about the client or to gain illegal access to the client to gain information about the server, which is not desirable. The network is not secure for the server as well as for the client. Hence this is a factor of motivation for any researcher to take up a research work on the enhancement of the security to address the problem.

Demerits of existing systems

i) The plain biometric can be easily accessed by the imposter.
ii) The plain biometric is sent to the server
For both enrolment and for
Authentication, there is a much chance for the leakage of information.
iii) If the user-specific key is compromised, the template is no longer secure imposter can recover the original biometric template using specific key.
iv) The network is insecure in the sense that the intruder is in the network then he can gain access to the server as well as to the client.

E.Cryptographic File System

In 1993, Cryptographic File System CFS was presented which empowers security of information very still in the framework. CFS has been accounted for in [10]. CFS pushes encryption administrations into the document framework. CFS backings secure capacity at the framework level through a standard UNIX record framework interface to encoded documents. Clients relate a cryptographic key with the indexes they wish to ensure. Records in these catalogs are straightforwardly scrambled and decoded with the predefined key without further client intercession; clear text is never put away on a plate or sent to a remote document server. One of the attributes of CFS is that it can utilize any accessible record framework for its hidden stockpiling without change, including remote document servers, for example, NFS. Framework administration capacities, for example, document reinforcement, work in an

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 7, July 2017

ordinary way and without information of the key. With a specific end goal to guarantee classified information in CFS, information is scrambled quickly before sending it to untrusted segments. CFS gives a straightforward UNIX document framework interface to registry chains of importance that are naturally encoded with client supplied keys. Clients issue a basic order to "join" a cryptographic key to a registry. Connected indexes are then accessible to the client with all the standard framework calls and instruments, however the documents are consequently encoded as they are composed and unscrambled as they are read. Clients control CFS through a little suite of devices that make, connect, confine, and generally manage scrambled registries. Every registry is ensured by a situated of cryptographic keys. These keys can be supplied by client passage by means of the console or, if equipment is accessible, through removable "savvy cards" joined with the customer PC. CFS utilizes DES to scramble document information. DES has various standard methods of operation [11], none of which is totally suitable for encoding records on-line in a record framework. In the least complex DES mode, every 8 byte square of a document is freely scrambled with the given key. Encryption and unscrambling can be performed haphazardly on any piece limit.

Valuable properties of CFS are as per the following:

1. CFS gives a basic component to secure information kept in disks and sent to network.

2. The execution of CFS on current workstations gives off an impression of being inside of a range that permits its standard utilization.

Deficiencies of this method are as per the following:

Cryptographic File System is custom-made toward single-client workstations and depend on client supplied passwords for information encryption [12]. This system is not positive for Cloud frameworks as Cloud frameworks include dispersed nature of system of servers where information is to be put away and these servers will be utilized by different clients. Also, utilization of passwords for information security is unequivocally restricted; in light of the fact that, most normal assault on such frameworks is animal power assault particularly because of clients' propensity of keeping passwords straightforward and essential [34,35,36]. Thus this system is not prescribed.

F.Secure Network Attached Disks (SNAD)

In [32], portrayal about SNAD is accounted for. SNAD is the framework for securing information on on network-attached disks. The fundamental system behind SNAD is to encode all information at the customer and give the server adequate data to validate the essayist and the per user adequate data to check the end-to-end honesty of the information. SNAD depends upon a few standard cryptographic devices for guaranteeing secrecy of information. The customer uses a standard algorithms, for example, RC5 [13] or Blowfish [13] to encode the information, guaranteeing that the information is confused by anybody until it is encrypted by the customer that understands it. Public key cryptography is utilized to permit disk to store data that can be utilized to unscramble their records; on the grounds that open key encryption is helter kilter, in any case, just a client with the fitting private key can utilize this data. SNAD additionally makes broad utilization of cryptographic hashes and keyed hashes for guaranteeing uprightness of information. Cryptographic hashes, for example, MD5 and SHA-1 [13] utilize a restricted capacity to figure a huge number (128 or 160 bits) from a square of information. Any alteration in the information will bring about the subsequent hash quality to change. Keyed hashes, for example, HMAC (hashed message validation code) [14] utilize a cryptographic hash in conjunction with a common mystery to check trustworthiness and confirm an essayist. On the off chance that the sender and beneficiary share a key, the key can be incorporated in the cryptographic hash, counteracting any individual who blocks the information from imperceptibly adjusting it unless they know the mutual key. At that point display three other security conspires, each suitable for diverse levels of customer and server CPU execution.

G.Secure group key administration for storage area network

In secure group key administration system has been presented for data security.Storage area networks are like ‘Distributed Systems’ where for security, data integrity and data confidentiality should be achieved. In this paper,

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 7, July 2017

a solution had been proposed that addresses these core security requirements. Characteristics of this system are as per the following:

1. Strong cryptographic systems have been utilized to accomplish information security and respectability.
2. A large portion of these storage frameworks give systems to productive gathering sharing of information. As it were, indistinguishable information access consents are given to gatherings of clients, and any client who can demonstrate bunch participation is approved to get to information in view of the gathering authorizations. Gathering sharing diminishes the aggregate number of keys to be put away and conveyed in the framework. These gathering keys are normally used to secure the symmetric keys utilized for information encryption.
   Cryptographically secure hashing and advanced marks have been utilized to give information uprightness. The SAN elements can effectively uphold information security arrangements by encoding and unscrambling on-the-fly squares of information that are composed to, or read from, the capacity subsystem.
3. To support secure sharing of information among a gathering of SAN substances without depending on any incorporated power, encrypt symmetric (mass information encryption) keys under a solitary group key known just to all approved SAN elements. This can be accomplished through the utilization of a safe group key assention instrument. TGDH is a group key understanding method joining Diffie-Hellman.

IV. EXPERIMENT AND RESULT

The proposed algorithm "An Empirical Study on Secure Streaming of Files in Cloud Environment" has been executed with the help of an example.

A.EXPERIMENT

For the simulation of experiment in CloudSim, certain parameters of Cloud have been set. These parameters are:
One user – There is only one user in this experiment who sends one file to the Cloud for data storage in its servers.
One Datacenter Broker – In this experiment, only one datacenter broker is included. One Datacenter – Generally, there are many Datacenters available with Cloud service provider and datacenter broker chooses one of these datacenters depending on the QOS requirements of the user. However, in this experiment, only one datacenter is included and it is assumed that this datacenter meets the QOS requirements of client's application. Fifteen hosts – Generally, there are thousands of hosts available with each datacenter of Cloud service providers; but, in this experiment only fifteen hosts are taken considering the size of file. Hardware characteristics of hosts – The hosts are of heterogeneous nature at Cloud service provider's organization. This feature is important in cases where compute service is provided by Cloud such that hosts are assigned according to the computing requirements of the application. But in storage servers, this feature is not important. Hence, for this experiment, fifteen hosts are taken that are identical to each other such that their characteristics are: System architecture – x86 Operating System – Linux
Virtual machine management – Xen
Time zone – 10.0, Storage space of each host – range (10GB to 100GB) ,Memory – 256 MB

The example executed in CloudSim is as follows: A file F has been taken whose contents are: "misha is a student of UIET. She studies in ME (cse) 2nd year. Her roll number is 433.She is a good girl."

Size of file is calculated as number of characters in file and in this case size of file = 106. Number of shares that the file will be divided into is decided by the programmer at Cloud service provider site. In this case, number of shares decided is 10.

Hence, n=10. k,no of shares is calculated as follows:- k=(Size (file) /10) if still some characters left then one more share is created. Since Size (file) = 106 and n = 10, therefore k = 10+1. There are 10 characters in 10 shares but 6 characters in last 11thshare.Such issues are kept in mind by the programmer at the Cloud service provider site. So message is break down into shares
Share 1-" misha is a"
Share 2-" student o"
Share 3-"f UIET. Sh"
Share 4-"e studies"
Share 5-" in ME (cs"
Share 6-"e) 2nd yea"

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 7, July 2017

Share 7-“r. Her rol”
Share 8-“l number i”
Share 9-“s 433.She”
Share 10-“ is a good”
Share 11-“ girl.”

These messages are saved on the servers of the cloud. Suppose there are five servers. The cloud monitor manage the IP addresses of the servers.

Table: Server Table in Cloud Monitor Servers Information Type_of_dataDescriptionServer_IDInt Unique Server ID Server_IP Character Server IP Address A database is maintained in the monitor of the cloud. Suppose here are five servers Server1, Server2, Server3, Server4, and Server5 in the cloud. Information related to the storage are stored in Storage table in Cloud monitor.

Table: Storage Table in Cloud Monitor Information Stored Type_of_data Description share_NameInt Share_NameServer_IP Character Server IP Address Key_value Character Key used for encryption Filename Character Filename FileNoInt Sequence of share Data is stored in the form of decrypted files in the server

Table: Files stored in servers after encryption using image key:

Server1 Server2 Server3 Server4 Server5
F1.dat F2.dat F3.dat F4.dat F5.dat F6.dat F7.dat F8.dat F9.dat F10.dat F11.dat

In Second Phase these shares are decrypted to get F1.txt,F2.txt,F3.txt,F4.txt,F5.txt,F6.txt,F7.txt,F8.txt,F 9.txt, F10.txt and F11.txt with same image key and combined to a single file F. The size of the file is after On Downloading ClousSim3.0, Hard storage Drive Class is in herited by Cloud Hard drive Storage.Cloud Hard drive Storage Class is calling the constuctors of Hard drive Storage Class.It is also using the functions of Hard Drive Storage Class to store the files on the cloud. Size of the message retrieved id 107 bytes. Determined as follows:-

Size (message) =number of characters in the message User is asked to send message of this size.

Simulation has been done in CloudSim3.0. Shares of file have been constructed in datacenter and these shares have been sent to hosts (servers) available in that datacenter. Ids of hosts (servers) and name of files which contain shares of file and image for encryption are sent to the user. Either, these ids and file names are sent to one client or set of employees working in the organization which is a client. It depends on the level of security, client organization desires. If client organization is large and control of data is to be distributed among a set of employees, then it is expected to distribute the information about shares of file and its image as signature among set of loyal employees. In order to get file/secret back from Cloud storage servers, users from client site send ids of servers and name of files. Cloud systems get these ids and extract information from the servers with the given ids and file names. Algorithm for reconstructing the file and message, is implemented in datacenter and file and message is returned to the user. If message is correct, then it assures client that file has not been modified during its stay in Cloud servers. In this case, client has information of all shares and none of the servers or shares of the file are damaged.

V. CONCLUSION

From the above comparison of different techniques of authentication and key-encryption,the best technique for information storage in the form of files on cloud is secure streaming using cloud environment using Kerberos algorithm . This technique provide confidentiality, integrity and authentication. The algorithm are tested for various sizes of messages and parameters. And provide high quality of service and security for cloud environment. RSA signature is first digital signature technique. This technique uses the concept of prime no. and cryptographic hash function. Prime no. is used for converting plain text into cipher text because it is difficult to factories the product of two large prime no. and the encryption become more powerful and not too easy to decrypt without the key. Mostly encryption mechanism uses the concept of RSA algorithm with new hash function that generates dynamic and more efficient and secure than other methods. The proposed system is performing secure streaming by creating chunks of the message, encrypting the chunks using image and for decryption same image is required. The image is used as the signature to get the file from the cloud server. The chunks are further retrieved combined and returned to the user. The technique is providing higher security for sending the files out of 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 7, July 2017

REFERENCES

[1]http://en.wikipedia.org/wiki/Authentication_server
[2] http://en.wikipedia.org/wiki/Password
[3] http://en.wikipedia.org/wiki/Kerberos_(protocol)
[4] Ms. Jasmin Bhambure, Ms. DhanashriChavan, Ms. Pallavi Band, Mrs.LakshmiMadhuri Department of Computer Engineering Dr. D.Y International Journal of Advanced Research in Computer Science and Software Engineering "Secure Authentication Protocol in Client – Server Application using Visual Cryptography" Volume 4, Issue 12, November 2014 Ms. Jasmin Bhambure, Ms. DhanashriChavan, Ms. Pallavi Band, Mrs.LakshmiMadhuri Department of Computer Engineering Dr. D.Y.Patil School of Engineering, Lohegaon, Pune, India (2014).
[5] Eman El- Emam, MagdyKoutb, HamdyKelash, and Osama
Farag Allah, "An Authentication Protocol Based on Kerberos5", International Journal of Network Security, Vol.12, No.3, PP.159{170, May 2011.
[6] Rajan.S.Jamgekar, Geeta Shantanu Joshi Manuscript received on February, 2013 "File Encryption and Decryption Using SecureRSA"International Journal of Emerging Science and Engineering (IJESE) ISSN: 2319–6378, volume-1, Issue-4, February 2013.
[7] Xin Zhou, Xiaofei Tang, "Research and Implementation of RSA Algorithm for Encryption and Decryption", IEEE, 6th International Forum on Strategic Technology, pp- 1118 – 1121.
[8] Gagan Dua1, Nitin Gautam2, DharmendarSharma3, Ankit Arora4, "Reply Attack Prevention in Kerberos Authentication Protocol Using Triple Password" International Journal of Computer Networks & Communications (IJCNC) Vol.5, No.2, March 2013.
[9] Shashidhar M S Student M.Tech, Dept of CSE Canara Engineering College, Mangalore
V.T.U university, Belgaum, India Suresha D Asst. professor, Dept of CSE Canara Engineering College, Mangalore V.T.U university, Belgaum , India. Rajan.S.Jamgekar, Asst.Professor, NBNSCOE, Solapur, India. Geeta Shantanu Joshi, Asst.Professor, MMCOEP, India. "Implementation of Secure Biometric Authentication Using Kerberos Protocol" International Journal of Advanced Research in Computer Science and Software Engineering. Volume 3, Issue 3, March 2013.
[10] M. Blaze, "A Cryptographic File System for Unix," 1st ACM Conf. Comp. and Commun. Sec., pp. 9–15, Nov. 1993.
[11] National Bureau of Standards, "Data Encryption Standard Modes of Operation," FIPS Publication #81NTIS, Dec. 1980
[12] Y. Kim, F. Maino, M. Narasimha, K. Rhee, andG. Tsudik, "Secure group key management for storage area networks," IEEE Commun. Mag., pp. 92–99, Aug. 2003. [13] W.C.Cheng, C.-F.Chou and L.Golubchik, Performance of Batch-based Digital Signatures, 10th IEEE International Symposium on Modeling, 2002.
[13] B. Schneier, Applied Cryptography, Wdey (New York), 1994
[14] H. Krawczyk, M. Bellare, and R. Canetti, "HMAC:Keyed-Hashing for Message Authentication," IETF Network Working Group RFC2104, Feb. 1997.