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

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 6, Issue 2, February 2018

Group Message Privacy and Data Sharing

Ritu Dharmik [1], Pooja Likhar [2] , Kaustubh Deshmukh[3] ,Madhuri Dubey [4]

U.G. Student, Department of Information Technology Engineering, S B Jain Institute of Technology Management and Research Engineering College , Katol Road Nagpur, India[1]

U.G. Student, Department of Information Technology Engineering, S B Jain Institute of Technology Management and Research Engineering College , Katol Road Nagpur, India[2]

U.G. Student, Department of Information Technology Engineering, S B Jain Institute of Technology Management and Research Engineering College , Katol Road Nagpur, India[3]

Associate Professor, Department of Information Technology Engineering, S B Jain Institute of Technology Management and Research Engineering College , Katol Road Nagpur, India[4]

ABSTRACT: This paper is all about services and various functionality that are provided in the project. The various services like time constraint , key , history ,group security that all are services provided in the project .
Each service has different work who help to do various operations on the data. The data and the file is present in the group or in any chat box then that data will be access by whom that all are comes under this various services.
The working of each services and the implementation of each module will be describe here. This shows the overall implementation and the working of modules. The services like time constraint , history , group security , key , and another all services that all comes under it.The services that are provided in this project like encryption / decryption so on what technques and on which function that all are working that all are explains here. Various function or inbuilt functions are used here. Similary,This paper presents a various techniques and algorithms that was proposed earlier by researchers for the better privacy-preserving data access.This key is anonymous in that the message received are known to the selected members of the group and then encryption and decryption technquies will be applied on the message. In this key assignment of serial numbers allow much complex data to be shared and has application to other problem in privacy reserving data mining, collection avoidance in the communication and distributed without using the trusted fundamental authority.

KEYWORDS: Encryption, Decryption, Polynomials,Time constraint, privacy preserving data access

I. INTRODUCTION

In this paper the whole working of our project is presented .Our project is all about , the communication between selected members are established by selecting some member from group. When sender sends any message, attachments and any multimedia messages in a group before clicking on the send button there will be the list of member show. From that list sender select the member those who want to send the message and that message will be visible to the selected members only. But the visible message is present in encrypted from for other members and the secret key will be provided to specific member for decryption. In the past, authentication was almost synonymous with password systems, but today's authentication system must do more. For instance, in a distributed client server environment, a user might have several client programs running on her desktop, which access server programs on remote computers across a network which is not trusted. In such an environment the server must authenticate that the client run on behalf of a legimate user. Further the authentication system should provide "single logon" so that the user does not have to repeatedly enter passwords. An authentication service for computer networks, is an increasingly popular system for meeting these coals. While authentication provides proof of identity, it does not describe the privileges an entry processes. So for instance, you are authenticated before you access a database system, but this does not tell the database system which data you are entitle to access. This later function is known as the authorization or access control.

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

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 6, Issue 2, February 2018

II. LITERATURE SURVEY REVIEW

1.Encryption/Decryption

Cryptography plays major roles to fulfilment these demands. Nowadays, many of researchers have proposed many of encryption and decryption algorithms such as AES, DES, RSA, and others. But most of the proposed algorithms encountered some problems such as lack of robustness and significant amount of time added to packet delay to maintain the security on the communication channel between the terminals. In this paper, the security goals were enhanced via "A New Approach for Complex Encrypting and Decrypting Data" which maintains the security on the communication channels by making it difficult for attacker to predicate a pattern as well as speed of the encryption / decryption scheme.Network Security & Cryptography is a concept to protect network and data transmission over wireless network. Data Security is the main aspect of secure data transmission over unreliable network. Data Security is a challenging issue of data communications today that touches many areas including secure communication channel, strong data encryption technique and trusted third party to maintain the database. The rapid development in information technology, the secure transmission of confidential data herewith gets a great deal of attention. The conventional methods of encryption can only maintain the data security. The information could be accessed by the unauthorized user for malicious purpose. Therefore, it is necessary to apply effective encryption/decryption methods to enhance data security.In network security, cryptography has a long history by provides a way to store sensitive information or transmit it across insecure networks (i.e. the Internet) so that it cannot be read by anyone except the intended recipient, where the cryptosystem is a set of algorithms combined with keys to convert the original message (Plain-text) to encrypted message (Cipher-text) and convert it back in the intended recipient side to the original message (Plain-text) [1]. The first model proposed by Shannon on the cryptosystem [2].The decryption process involves converting the encrypted data back to its original form for the receiver's understanding. The same process is performed at the beginning of the encryption and decryption process (connection established) as described in the encryption part at the sender side to generate the same private position at the receiver side to eliminate the key from the cipher text.

2.Key Sharing

Due to the tremendous growth of the Internet and huge amount of online transactions taking place over it, opportunities exist for joint computations requiring privacy of the inputs. These computations occur between parties which may or may not have trust in one another. In literature, this subject of information security is called Secure Multiparty Computation (SMC). This type of computation is aimed at privacy of individual inputs and the correctness of the result. Formally, in SMC the parties P1, P2, …, Pk want to compute some common function f(x1, x2,…, xk) of inputs x1, x2,…, xk such that a party Pi can know only its own input xi and the value of the function f . The SMC problems use two computation paradigms; ideal model and real model paradigm. In ideal model there exists a Trusted Third Party (TTP) which accepts inputs from all the parties, evaluates the common function and sends result of the computation to the parties. Diffie–Hellman Key Exchange establishes a shared secret between two parties that can be used for secret communication for exchanging data over a public network. The following conceptual diagram illustrates the general idea of the key exchange by using colors instead of very large numbers. The process begins by having the two parties, Alice and Bob, agree on an arbitrary starting color that does not need to be kept secret (but should be different every time[3]); in this example the color is yellow. Each of them selects a secret color that they keep to themselves. In this case, red and aqua. The crucial part of the process is that Alice and Bob now mix their secret color together with their mutually shared color, resulting in orange and blue mixtures respectively, then publicly exchange the two mixed colors. Finally, each of the two mix together the color they received from the partner with their own private color. The result is a final color mixture (brown) that is identical to the partner's color mixture.If a third party listened to the exchange, it would be computationally difficult for them to determine the secret colors. In fact, when using large numbers rather than colors, this action is computationally expensive for modern super computers to do in a reasonable amount of time. (In cryptology publications, the eavesdropper is usually named Eve.)

3.Access control

Access control is a security technique that can be used to regulate who or what can view or use resources in a computing environment.

There are two main types of access control: physical and logical. Physical access control limits access to campuses, buildings, rooms and physical IT assets. Logical access limits connections to computer networks, system files and data.The four main categories of access control are:

Mandatory access control

Mandatory access control (MAC) refers to a type of access control by which the operating system constrains the ability of a *subject* or *initiator* to access or generally perform some sort of operation on an *object* or *target*.

Discretionary access control

Discretionary access control (DAC) is a type of access control defined by the Trusted Computer System Evaluation Criteria[4] "as a means of restricting access to objects based on the identity of subjects and/or groups to which they belong. The controls are discretionary in the sense that a subject with a certain access permission is capable of passing that permission (perhaps indirectly) on to any other subject (unless restrained by mandatory access control)".

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

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 6, Issue 2, February 2018

Role-based access control

Role-based access control (RBAC) is a method of regulating access to computer or network resources based on the roles of individual users within an enterprise. In this context, access is the ability of an individual user to perform a specific task, such as view, create, or modify a file. Roles are defined according to job competency, authority, and responsibility within the enterprise.

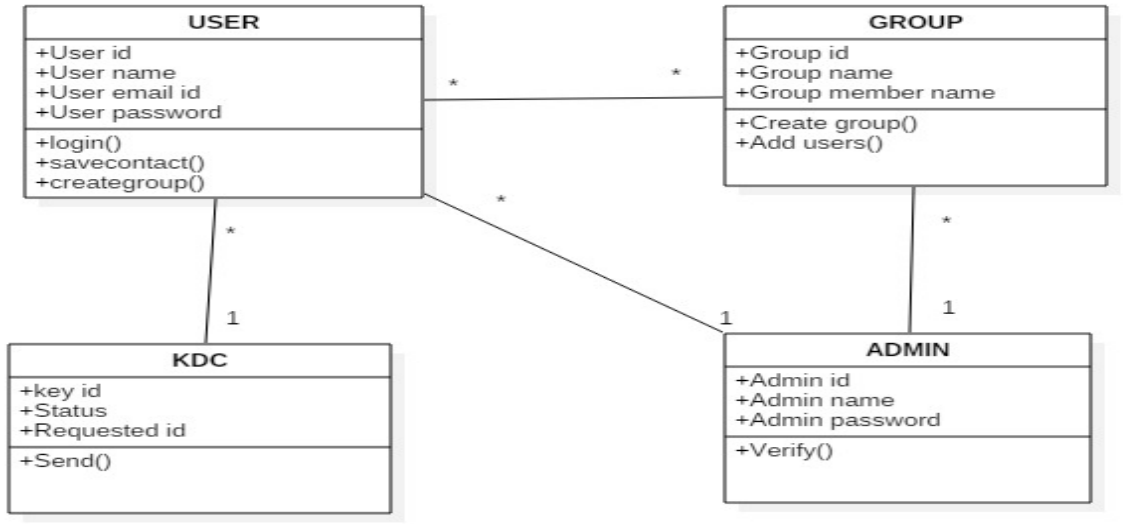
Rule-based access control

Rule Based Access Control (RBAC) introduces acronym ambiguity by using the same four letter abbreviation (RBAC) as Role Based Access Control. Under Rules Based Access Control, access is allowed or denied to resource objects based on a set of rules defined by a system administrator.

Access control systems perform authorization identification, authentication, access approval, and accountability of entities through login credentials including passwords, personal identification numbers (PINs), biometric scans, and physical or electronic keys.The purpose of access control is to limit the actions or operations that a legitimate user of a computer system can perform. Access control constrains what a user can do directly, as well as what programs executing on behalf of the users are allowed to do. In this way access control seeks to prevent activity that could lead to a breach of security. Access control relies on and coexists with other security services in a computer system. Access control is concerned with limiting the activity of legitimate users. It is enforced by a reference monitor which mediates every attempted access by a user (or program executing on behalf of that user) to objects in the system. The reference monitor consults an authorization database in order to determine if the user attempting to do an operation is actually authorized to perform that operation. Authorizations in this database are administered and maintained by a security administrator. The administrator sets these authorizations on the basis of the security policy of the organisation. Users may also be able to modify some portion of the authorization database, for instance, to set permissions for their personal files. Auditing monitors and keeps a record of relevant activity in the system.It is important to make a clear distinction between auhentication and access control. Correctly establishing the identity of the user is the responsibility of the athentication service. Access control assumes that the authentication of the user has been successfully verified prior to enforcement of access control via a reference monitor.

III. SYSTEM DIAGRAM

1.Class Diagram



This system diagram is all about various modules that present in system this are shown by various classes which contain the combination of attributes and behaviour that performs various operation related to the classes. How that classese are connected to each other that all are shown in this system design.

This system design contains the combination of four classes that are user ,group,kdc and admin which performs different different operations.

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

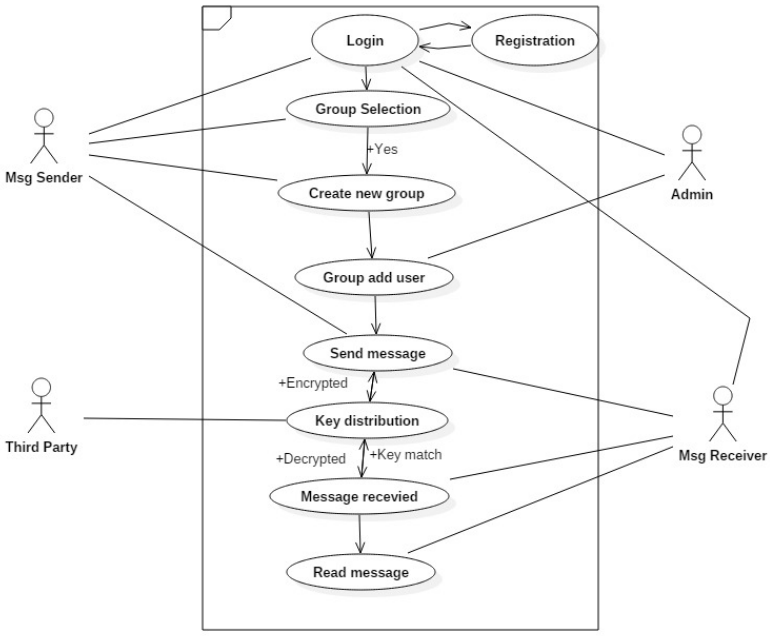
International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 6, Issue 2, February 2018

2.Use Case Diagram



This system design is all about the process of working the how and when the various operations are performed that comes under this system.The sequence of processes are shown in this system.Each process done one by one and whom access to this process and when it access that all are shoen in this system design.

IV. IMPLEMENTATION MODULE

1.Time Constraint

Time constraint is nothing but the the duration in which the message will be visible and present in the group. Time Constraint is present for the message that shows the time period of the message. Time constraint is the most important part which shows the time related functionality.Time constraint refer to the limitations on the start and end times of each task in a project critical path, which is the sequence of task that cannot be delayed without delaying the entire project .Timestamp is used for storing the message in chatbox. A **timestamp** is the current time of an event that is recorded by a computer. Through mechanisms such as the Network Time Protocol (NTP), a computer maintains accurate current time, calibrated to minute fractions of a second.

2.Group Security

Group Security is one in which only authorized members who registered and present in the group only those members are able to read and send the message . Group security is important service which add and remove the members from the group. A group of people are present in the group who are present under the unique name. Every attachment any file that all are present in the group.Access to security group is controlled by the permissions.

3. Encryption/Decryption

Encryption and Decryption Service is one which provide the unreadable message to the members of the group and that message will be decrypted by the key that one is another service which helps to decrypt the message. Encryption and decryption is the most important service. Cryptography plays major roles to fulfilment these demands. Nowadays, many of researchers have proposed many of encryption and decryption algorithms such as AES, DES, RSA, and others.

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

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 6, Issue 2, February 2018

The particular set of 64 characters chosen to represent the 64 place-values for the base varies between implementations. The general strategy is to choose 64 characters that are both members of a subset common to most encodings, and also printable. This combination leaves the data unlikely to be modified in transit through information systems, such as email, that were traditionally not 8-bit clean.[5] For example, MIME's Base64 implementation uses A–Z, a–z, and 0–9 for the first 62 values. Other variations share this property but differ in the symbols chosen for the last two values; an example is UTF-7.The earliest instances of this type of encoding were created for dialup communication between systems running the same OS — *e.g.*, uuencode for UNIX, BinHex for the TRS-80(later adapted for the Macintosh) — and could therefore make more assumptions about what characters were safe to use. For instance, uuencode uses uppercase letters, digits, and many punctuation characters, but no lowercase.[6][7][8][5]
Base64 is a group of similar binary-to-text encoding schemes that represent binary data in an ASCII string format by translating it into a radix-64 representation. The term Base64 originates from a specific MIME content transfer encoding.

Each base64 digit represents exactly 6 bits of data. Three 8-bit bytes (i.e., a total of 24 bits) can therefore be represented by four 6-bit base64 encodings.

Base64 table

The Base64 index table:

Value	Char	Value	Char	Value	Char	Value	Char
0	A	16	Q	32	g	48	w
1	B	17	R	33	h	49	x
2	C	18	S	34	i	50	y
3	D	19	T	35	j	51	z
4	E	20	U	36	k	52	0
5	F	21	V	37	l	53	1
6	G	22	W	38	m	54	2
7	H	23	X	39	n	55	3
8	I	24	Y	40	o	56	4
9	J	25	Z	41	p	57	5
10	K	26	a	42	q	58	6
11	L	27	b	43	r	59	7
12	M	28	c	44	s	60	8
13	N	29	d	45	t	61	9
14	O	30	e	46	u	62	+
15	P	31	f	47	v	G63	/

When the number of bytes to encode is not divisible by three (that is, if there are only one or two bytes of input for the last 24-bit block), add extra bytes with value zero so there are three bytes, and perform the conversion to base64. If there is only one significant input byte (e.g., 'M'), all 8 bits will be captured in the first two base64 digits (12 bits).

4.Key

Key is one service that helps to decrypt the encrypted message and key is generated bt using the RAND function.
Key is most important service which helps to member of group for reading the mesaage and by using key the message will be decrypted.

Key is the combination of random numbers which are generated by function .

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

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 6, Issue 2, February 2018

Random number generation is the generation of a sequence of numbers or symbols that cannot be reasonably predicted better than by a random chance, usually through a hardware random-number generator (RNG).
There are two principal methods used to generate random numbers. The first method measures some physical phenomenon that is expected to be random and then compensates for possible biases in the measurement process.
This describes in detail the [*now superseded*] deterministic random number generator (RNG) algorithm used in **CryptoSys API** and the **CryptoSys PKI** Toolkit. We assert that the following CryptoSys RNG functions are fully compliant with the requirements of FIPS PUB 140-2.

> Random Number Generators (RNGs) used for cryptographic applications typically produce a sequence of zero and one bits that may be combined into sub-sequences or blocks of random numbers. There are two basic classes: *deterministic* and *nondeterministic*. A deterministic RNG consists of an algorithm that produces a sequence of bits from an initial value called a seed. A nondeterministic RNG produces output that is dependent on some unpredictable physical source that is outside human control. There are no FIPS Approved nondeterministic random number generator.

5.History

History is the whole series of past events connected with a particular person or a group that contain the data like messages any attachment and file.

History helps to study the past events that are done before some years and days that all are comes under the history.

6.Advantages

- Providing Secure id for communication
- Access control on message
- User control
- Guarantees confidentiality

7.Applications

- Group message chatting
- Email services
- Security Based document

V. FUTURE SCOPE

For providing security over a communication and by saving time this technique is used. For sending various documents, files and other multimedia messages this scheme is used.

This paper is used when any security related communication between users are required then it gives the many more introduction and related information will be given here. For the sending any document over people and getting the knowledge of key sharing, key generation that all are present here which helps in many ways. The use of this paper is for. For Group message chatting, Email services, Security Based document.

VI. CONCLUSION

In this paper we have proposed various techniques and services that are provided in the project. The brief Idea about each services are shown here. The services that are provided in this project like encryption / decryption so on what techniques and on which function that all are working that all are explains here. Various function or inbuilt functions are used here. This paper presents a various techniques and algorithms that was proposed earlier by researchers for the better privacy-preserving data access.This key is anonymous in that the message received are known to the selected members of the group and then encryption and decryption technquies will be applied on the message.This is all that are present in useful for the various users.

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

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 6, Issue 2, February 2018

REFERENCES

[1] P. Zimmerman, "An Introduction to Cryptography", Doubleday & Company, Inc., United State of America, USA, 1999.
[2] C. Shannon, "Communication Theory of Secrecy Systems", Bell Systems Technical Journal, MD Computing, vol. 15, pp. 57-64, 1998.
[3] "Imperfect Forward Secrecy: How Diffie-Hellman Fails in Practice" *(PDF)*. Retrieved 30 October 2015.
[4] Trusted Computer System Evaluation Criteria. *United States Department of Defense. December 1985. DoD Standard 5200.28-STD. Archived from* the original *on 2006-05-27*
[5]The Base16,Base32,and Base64 Data Encodings. IETF. October 2006. doi:10.17487/RFC4648. RFC 4648.Retrieved March 18, 2010.
[6]Privacy Enhancement for Internet Electronic Mail: Part I: Message Encryption and Authentication Procedures. IETF. February 1993. doi:10.17487/RFC1421. RFC 1421.Retrieved March 18, 2010.
[7]^ Jump up to:[a] [b] Multipurpose Internet Mail Extensions: (MIME) Part One: Format of Internet Message Bodies. IETF. November 1996. doi:10.17487/RFC2045. RFC 2045.Retrieved March 18, 2010.
[8]^ Jump up to:[a] [b] The Base16, Base32, and Base64 Data Encodings. IETF. July 2003. doi:10.17487/RFC3548. RFC 3548.Retrieved March 18, 2010.