Recent Advances in Technology and Engineering (RATE-2017)
6th National Conference by TJIT, Bangalore

International Journal of Science, Engineering and Technology
An Open Access Journal

# Secure Storage of Data in Cloud Based Social Networks

[1]A. Praveena, [2]Dr. S. Smys

**Abstract**

Nowadays, Online Social Networks is one of the important terms we hear, which allows its users to connect by various link types. Everyday application developers come up with new social networking sites. Consequently, these websites gain huge profit just by providing a platform for the users to communicate. It has already become an important integral part of our daily lives, enabling us to contact our friends and families on time. Since the count of the users of social networks is increasing drastically, storage of such huge amount of data is difficult to accomplish. As a solution, Cloud provides a platform to store this tiny amount of data. More and more social network data has been made publicly available and analyzed in one way or another. However, the issues in securing the data and privacy of users in cloud-based social networks persist. Users are unaware of these issues. They share various pictures, videos and personal data on the networking site which prevail even after deletion. But some of the information revealed is meant to be private hence social network data has led to the risk of leakage of confidential information of individuals. This is because they collect huge personal data and users take risks of trusting them. Since more personalized information is shared with the public, violating the privacy of a target user become much easier. Hence, security of the social networking data stored in the cloud is one of the major issues in cloud-based social networks. In this paper, we propose a framework for secure storing of data on the cloud-based social networks. The framework encrypts the data before storing it in the cloud, and the data is decrypted only with the private key of the user, making the data secure in the cloud. The proxy re-encryption scheme is used to re-encrypt the data to make it more secure.

Keywords—Privacy attack, social network, Cloud computing

## Introduction

Social networks are online web based applications that allow their users to connect with their friends and share common interests, either professionally or personally with whom they share and these networks allow people to list details about themselves that are relevant to the nature of the network. Users post content to the application to update connections and share personal news, accomplishments, interests and more. This content can be in the form of simple text status updates, videos or photos. Common social networks such as Facebook and Twitter have hundreds of millions or even billions of users scattered all around the world sharing interconnected data. Geographically distributed users all around the world can share different types of data, some like videos and images very large, with each other. The size and number of such data items are growing dramatically every day. Users demand low latency access, data consistency and availability and privacy requirements from their social network service provider. However, social network service providers have a limited monetary capital to store every piece of data everywhere to minimize users' data access latency.

A possible solution would be to store the data related to every user in every available data centre. However, as different copies of user data may need updating regularly, and due to its very large size, such a huge investment becomes infeasible and

uneconomic. Hence, there is always a trade-off between the data storage cost and latency. Nowadays, many social network providers use their own private data centres to store users' data. However, building private data centres is extremely expensive and it is normally not an option for every social network provider. Even large providers are concerned about the rapidly increasing storage, data transmission and data centre energy usage and monetary costs. To reduce the cost related to data centre setup and maintenance, a better solution is to make use of Cloud Data Centres. Such geo-distributed cloud services with virtually unlimited capabilities are suitable for large scale social networks data storage in different geographical locations.

Cloud computing is a technology trend where users can rent software, hardware, and infrastructure on a per use (compute and/or data) basis. However, as many privacy issues exist in using cloud data centres and social network providers have to trust cloud providers to share their data with, combining private and public cloud data centres could be a smart solution. In addition, cloud rental is also very costly and energy expensive if naïve social media data replication and distribution were used. There are many cloud providers with different data centres around the world that facilitate the setting up, managing, and maintaining private storage infrastructure such as Amazon S3, Google Cloud storage, and Microsoft Azure. By using cloud data centres, social media service providers could store users' data in every geographical location to satisfy the latency requirement for users with much lower cost.

The establishment of social networks and the cloud computing technology has led to the enrollment of a large number of online users into the networks which enhanced the users to access and share their data in social networks. Cloud computing has therefore enhanced the freedom of interaction on social media that has made most users to freely share personal information via social media as well as storage of information into the cloud computing systems. Accumulation of diverse information raises problems related to data security that has prompted the need for maintaining personal data private and improvement of the trust towards the service provider. This study investigates the security concerns that arise from the use of cloud technology in social networks.

Now the problem is will the shared data be safely secured and retrieved by the same users in the cloud? This made the platform to ensure the data using various technologies in cloud computing. The immediate climb of cloud technology has challenged the service in the issue of security. Sharing the data in the cloud has some benefits like availability, reliability, fault-tolerance, better performance. The significant solution for cloud service [4-7] in preserving privacy for shared data is encrypting and decrypting the data. The data are encrypted before it gets stored in the cloud [8-10]. If another user wants to retrieve the same data the user needs to have the decryption key. For instance, in an organization, the data are stored in the cloud, and the employees are given their public key to encrypt the data and store it the cloud when the data are needed they can retrieve the data by using their private key. However, there is a chance of leaking of data for competitors. The encrypted data are not secured.

Hence, the data must re-encrypted. To resolve this challenge, in this paper, we introduce a framework for secure sharing of data in cloud among different users in the cloud. In our proposed framework, the sender encrypts the data and sends to the proxy server. However, the encrypted data again is re-encrypted before sending into the cloud. If the receiver wants to decrypt the data, the receiver needs to have the valid ID. When key manager authenticates the user ID, the group key manager will send the decryption key to the receiver and get the data from the cloud using his private key which is distributed by the group key manager. Without the key distribution from key manager, no user's can decrypt the data.

The rest of the paper is organized as follows. In Section II, we discuss background on related topics. Section III analyzes the related work. We describe our proposed system in Section IV. In Section IV, Cloud security and its issues are discussed. We present an efficient algorithm to encrypt the social network data while storing it in cloud data centres. Finally, we

conclude the paper with concluding remarks in Section VI.

**Background for the study**

**CLOUD COMPUTING**

The most extensive and attracted standard is cloud computing which is spread all over via the internet. Especially cloud is a promising one in both academics as well as in industry. The large storage of data is transformed into the cloud by the third party or proxy, but there is a chance of data confidentiality lost in the cloud environment. In spite, all this cloud computing is scalable, easy computational and maintenance at lower cost. Data stored in the cloud are retrieved by ease through access to online resources at anytime from any place [3][4]. Since the service for cloud environment is provided by the service providers, it is called as the next evolutionary technology. The recent trend in cloud computing has attracted big search engines such as Google Apps, which accredit service of date access through online [7][8]. In Cloud computing the data is stored and retrieved data via a browser, the user does not come to know where their data are stored in the cloud or will it be securely stored? Alternatively, whether data can be accessed by the competitors? These are the questions which remind user before uploading their data into the cloud environment. The main aim enumerates that personal data of every individual should be securely healed in a profitable manner taken into consideration of data confidentiality.

*B. Social Network*

Rapid growth in social networks made users to share their large data like photos and videos. The easiest way of interaction and communication between the people worldwide is connected through the social network. Enormous The common data in the social networks like Facebook, twitter, MySpace, blog, YouTube and Flickr are increasing for decades, enormous and huge data are stored on the social network so handling such data are very challenging and arduous task too. Furthermore, technology has to be developed. Facebook applications which are maintained by the service providers in the cloud and it must be a trusted party. The users sharing their data in the social network among their group mostly bet bottom dollar on the Facebook administrator to set pertinent settings.

Cloud computing is mostly hosted on social networks for storage of massive data. Utilization of crypto-based encryption in social networks can afford secure storage of data storage in the cloud environment, usually social network compromise with privacy issues to provide the feel of a secure way of shared data in the cloud. In the past and upcoming years, an online user in the social networking has been increasing, so the responsibility of service provider enlarges cloud platform.

Currently, social networking and cloud computing are being used together in a number of ways [6]. The two options that exist are that the social media networks can either be incorporated into a social network or it can have scalable applications in the social networks. In social cloud systems, the cloud-based application offers authentication and user management services by the aid of social networks. Most organizations through social media use cloud computing to carry out most of their functions [2]. These companies, however, are faced with a number of challenges and the pressures to provide protection to information assets that belong to customers as well as other sensitive information.

Security, availability, and privacy are the topmost concerns in any cloud environment [1]. From the security standpoint, the cloud is perceived to be a double-edged sword. Social media users are vulnerable to different but related risks. Criticisms have been made about the privacy and security related to unauthorized access and utilization of information found on the cloud for ill motives and other malicious purposes. While the effectiveness of cloud computing in the social network is highly commendable, there is still a weakness in terms of its performance since the policies and practices that are associated with privacy and security remains weak. In this particular research, we seek to gain insight into the privacy concerns associated with cloud computing in social networks, assessment of the best practices to curb data leaks and other security concerns [17]. This paper has investigate the data security concerns those arises from use of cloud computing in social networks and propose the possible solutions to the challenges

***How social media uses cloud***

The present generation has embraced the use of social networks in many roles both personal and commercial [23]. In order to manage such a high

traffic, cloud technology has been adapted. Social networks have helped to a larger extent in enhancing the internet usability. Large multimedia content is stored in the cloud storage systems [14]. A lot of space is usually occupied by photographs and videos which are part of the most popular content found on social networks. Cloud computing providers like Amazon and Sales force have diversified in the services offered that are inclusive of enterprise resource planning and customer relationship management [12]. Customers can, therefore, utilize these services without necessarily purchasing them since they are located in the cloud services.

Besides data storage, social sites utilize clouds in other tasks such as big data analytics. Facebook, for instance, has a more improved analytics that are used mainly the business users. Social networks use clouds to reduce the costs related to data backup and also data recovery when a disaster occurs [5]. Data stored at a particular location is riskier than one found in the cloud. This is due to the hardships encountered during recovery. Through cloud computing, social network users can now access shared resources from anywhere on the globe. This is beneficial to most social networks as they maintain personal information of its clients and therefore should not lose any part of the information, however, trivial it is. Every user of the social network, therefore, utilizes cloud computing technology [11].

**Related Work**

The fundamental factor defining the success of any new computing technology is the level of security it provides. Whether the data residing in the cloud is secure to a level so as to avoid any sort of security breach or is it more secure to store the data away from cloud in our own personal computers or hard drives? The cloud service providers insist that their servers and the data stored in them is sufficiently protected from any sort of invasion and theft. Such companies argue that the data on their servers is inherently more secure than data residing on a myriad of personal computers and laptops. However, it is also a part of cloud architecture, that the client data will be distributed over these individual computers regardless of where the base repository of data is ultimately located. There have been instances when their security has been invaded and the whole system has been down for hours. At-least half a dozen of security breaches occurred last year bringing out the fundamental limitations of the security model of major Cloud Service Providers (CSP).

In case of a public-cloud computing scenario, we have multiple security issues that need to be addressed in comparison to a private cloud computing scenario. A public cloud acts as a host of a number of virtual machines, virtual machine monitors, and supporting middleware [18] etc. The security of the cloud depends on the activities of these objects as well as on the interactions between them. Moreover, in a public cloud enabling a shared multi-tenant environment, as the number of users increase, security risks get more intensified and diverse. It is necessary to identify the attack surfaces which are prone to security attacks and mechanisms ensuring successful client-side and server-side protection [19].

Cloud computing security challenges and issues were discussed by various researchers. This section aims to present a summary of existing review articles related to securing data in the Cloud. Xiao and Xiao [14] identifies the five concerns of Cloud computing; confidentiality, integrity, availability, accountability, and privacy and thoroughly reviews the threats

to each of the concerns as well as defense strategies. Chen and Zhao [15] outline the requirements for achieving privacy and security in the Cloud and also briefly outline the requirements for secure data sharing in the Cloud. Zhou [16] provided a survey on privacy and security in the Cloud focusing on how privacy laws should also take into consideration Cloud computing and what work can be done to prevent privacy and security breaches of one's personal data in the Cloud. Wang et al. [17] explored factors that affect managing information security in Cloud computing. It explains the necessary security needs for enterprises to understand the dynamics of information security in the Cloud. Wang [18] carried out a study on the privacy and security compliance of Software-As-A-Service (SaaS) among enterprises through pilot testing privacy/security compliance. "Although researchers have identified numerous security threats to the Cloud, malicious insiders still represent a significant concern." There are many examples [13] of insider attacks such as Google Docs.

Meiko et al [24] discuss the technical security issues arising from adopting the cloud computing model such as XML-attacks, Browsers related attacks, and flooding attacks. Bernd et al [25] discuss the security vulnerabilities existing in the cloud platform. The authors grouped the possible vulnerabilities into technology related, cloud characteristics -related, security controls-related Subashini et al [26] discuss the security challenges of the cloud service delivery model, focusing on the SaaS model. CSA [27] discusses critical areas of cloud computing. They deliver a set of best practices for the cloud provider, consumers and security vendors to follow in each domain [28].

It's clear from many of the reviews, that the Cloud is very susceptible to privacy and security attacks and currently there is on-going research that aims to prevent and/or reduce the likelihood of such attacks. In order to eliminate the need of certificates that make publicly available the mapping between identities and public keys in traditional public key systems, Shamir (1984) presented a good idea for public key systems, called identity (ID)-based public key system. In an ID-based public key system, a user's identity (e.g. name, e-mail address or social security number) is viewed as the user's public key. However, Shamir's systemis not easy to be realized in practice. In 2001, Boneh and Franklin (2001) used Shamir's idea to propose the first practical ID-based encryption (IBE) scheme. In 1998, Blaze et. al. introduced a concept called Proxy re-encryption (PRE). It is maintained by a third party and hence also known as a semi-trusted proxy. However, the scheme proposed had drawbacks. The proxy server designed was bidirectional and had collusion issues. Since then some PRE schemes have been developed which address various security issues.

## CLOUD SECURITY AND ITS ISSUES:

### *A. Cloud Security*

Security remains the biggest barrier preventing companies from entering into the cloud. Security is a continuous consideration in IT-related projects. Unlike many other traits in technological contexts, security is notoriously hard to quantify or even compare qualitatively. For this reason, security evaluation of cloud offerings will mostly hinge on company reputation and, eventually, real-world track records – but even real world track records are difficult to compare between companies, because security breaches may not be publicly disclosed unless compelled by regulation.

Businesses using cloud services want to ensure that their data is secure from both external attackers as well as internal snoopers (employees of the cloud provider). Although data theft and snooping is mitigated by properly encrypting data to be stored within the cloud [29], encryption cannot prevent denial-of-service attacks such as data deletion or corruption. Some early research users of Amazon S3 suggest, "users should employ some kind of data authentication technology to assure themselves that data returned by S3 is the same as the data that was stored there. Technology such as an HMAC or a digital signature would protect users from both accidental data modification by Amazon and from malicious modification by third parties who managed to crack a password or intercept a password reset email message". Service integrity is another security issue: businesses want to ensure their running services are not subject to denial-of-service attacks or hijacked. The latter can be very insidious, as a third party might (for example) gain control of a business's e-commerce site and besmirch its reputation. This situation is the digital equivalent of identity theft. Isolation is a related concern – cloud providers serve many customers and they all share common hardware and infrastructure. Although resource virtualization prevents customers from having to explicitly coordinate resource sharing, the cloud provider must ensure that multiple customers do not interfere with each other, maliciously or otherwise [45].

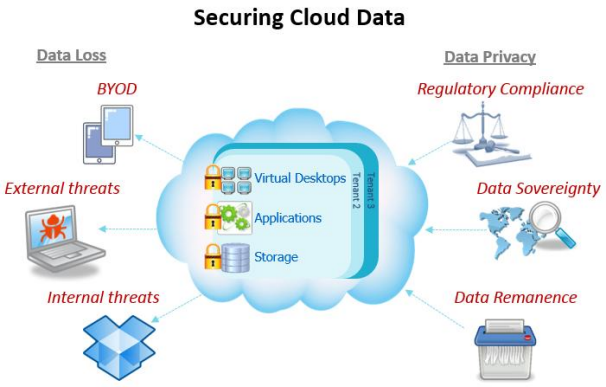
### *B. Parameters affecting cloud security*

There are numerous security issues for cloud computing as it encompasses many technologies including networks, databases, operating systems, virtualization, resource scheduling, transaction management, load balancing, concurrency control and memory management [24]. Security issues for many of these systems and technologies are applicable to cloud computing. For example, the network that interconnects the systems in a cloud has to be secure. Furthermore, virtualization paradigm in cloud computing results in several security concerns. For example, mapping the virtual

machines to the physical machines has to be carried out securely. Data security involves encrypting the data as well as ensuring that appropriate policies are enforced for data sharing. In addition, resource allocation and memory management algorithms have to be secure. Finally, data mining techniques may be applicable to malware detection in clouds [30].

*C. Security Issues faced by Cloud computing*

Whenever a discussion about cloud security is taken place there will be very much to do for it. The cloud service provider for cloud makes sure that the customer does not face any problem such as loss of data or data theft. There is also a possibility where a malicious user can penetrate the cloud by impersonating a legitimate user, there by infecting the entire cloud. This leads to affects many customers who are sharing the infected cloud [31].




The issues that rise while discussing security of a cloud are 1. Data Issues 2. Privacy issues 3. Infected Application 4. Security issues

## Proposed Work

In this paper, we propose a framework for secure storing of data on the cloud-based social networks. The framework encrypts the data before storing it in the cloud, and the data is decrypted only with the private key of the user, making the data secure in the cloud. The proxy re-encryption scheme is used to re-encrypt the data to make it more secure.

*A. Revocable Hierarchical Identity-Based Encryption*

The groundwork of public key cryptography which is shared among every user before clarification between the sender and receiver is, both must have their encrypted and signature authenticated certificate from the certificate authority (CA) [13].This will help to identify the valid user, receiver and setting up of their data encryption.

A RHIBE scheme consists of seven algorithms: System setup, Encryption, Initial key extract, Initial key delegate, Time key update, Time key delegate and Decryption algorithms:

**System setup:** This algorithm is a probabilistic algorithm which takes as input a security parameter l and the total number T of all periods, it returns a system secret key α, a time secret key β and the public parameters Parms. The public parameters Parms are made public and implicitly inputted to all the following algorithms.

**Encryption:** Take an identity vector id and a message M as input, the algorithm generates a ciphertext C.

Initial key extract: Take the system secret key α and a user's identity vector id as input, the algorithm returns the user's initial secret key Did .

**Initial key delegate:** Take the initial secret key Did for the identity vector id = (id1, . , idj ) and a user's identity id′ = (id1, . . , idj , idj+1) as input, the algorithm returns the user's initial secret key D′ id for the identity vector id′. Here, the vector id = (id1, ., idj ) is the user's identity at level j and the vector id′ = (id1, . , idj , idj+1) is the user's identity at level j + 1.

**Time key update:** For a period t , take the time secret key β and a user's identity vector *id* as input, the algorithm returns the user's time update key T*id*,t . Note that the non-revoked user can use the initial secret key D*id* and the time update key T*id*,t to obtain the decryption key D*id*,t .

**Time key delegate:** For a period t , take the time update key T*id*,t for identity vector *id* = (*id*1, . . . , *id*j ) and a user's identity *id*′ = (*id*1, . . . . , *id*j , *id*j+1) as input, the algorithm returns the user's time update key T*id*′,t for identity vector *id*′.

**Decryption:** The algorithm takes a ciphertext C and the user's decryption key D*id*,t as input. If the identity vector of the secret key *id* is a prefix of the identity vector used to encrypt the ciphertext, and the key and ciphertext are not both semi-functional, the algorithm returns a plaintext M.

*B. AES*

AES is a variant of Rijndael which has a fixed block size of 128 bits, 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 (see fig 2):

• 10 cycles of repetition for 128-bit keys.
• 12 cycles of repetition for 192-bit keys.
• 14 cycles of repetition for 256-bit keys.

The advantages of AES are many. AES is not susceptible to any attack but Brute Force attack. However, Brute Force attack is not an easy job even for a super computer. This is because the encryption key size used by AES algorithm is of the order 128, 192 or 256 bits which results in billions of permutations and combinations. High speed [12] and low RAM requirements were criteria of the AES selection process. Thus AES performs well on a wide variety of hardware; from 8-bit smart cards to high-performance computers. AES is also much faster than the traditional algorithms; therefore in our work AES is adopted [15]. Recently Compact AES S-box is developed to be more efficient [16].

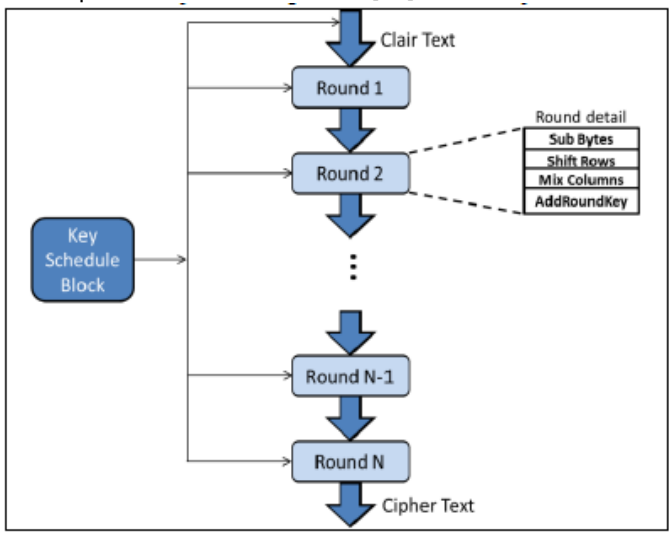



Fig: AES Encryption Steps

C. Proxy re-encryption

Proxy re-encryption plays a major role in the social networking issues since it deals with the privacy concerns. Proxy re-encryption allows a proxy to transform a ciphertext computed under Alice's public key into one that can be opened by Bob's secret key. The users of the social network who update their data like his/her contacts, photos, and videos and wants to share data among themselves. So the user encrypts the data and puts into the cloud.And the user can retrieve the data using ease access via the internet [17]. The Group Key Manager(GKM) will authenticate the user ID, and the user has to encrypt the data before sending it into the cloud using the public key. A new technique called proxy re-encryption without depending on the cloud services, the ciphertext is re-encrypted by using the symmetric key generated by a traditional method called the Advanced Encryption Standard (AES) Algorithm. It performs the operation of the delegation which allows the key to decrypt the data from the cloud. Unidirectional: In this (RKA B)-1 =RKB A this happens in a unidirectional way as a proxy can re-encrypt and predecrypt the data using an independently generated symmetric key.

*D. Framework*

In the framework, every user has a public key to encrypt the data. The users can decrypt the data with the private key, after the confirmation of their user ID with the Key Manager. In case the user leaves the group, the user cannot decrypt the data as the group key manager will mark that user as invalid and does not distribute the private key to that particular user. Figure 2 explain the flow of the framework. The framework consists of four components as shown in figure.1 and the components are discussed below.

*D. The Framework construction*

1) Cloud Service: The cloud service provider provides the service to the user based on the Service-Level Agreements (SLA). In this framework, we address the security of the underlying platform Infrastructure as a Service(IaaS) as data storage is provided as a part of IaaS. This framework enables safely secured data storage. Cloud computing mainly aims to provide self-resource provisioning, scalability, reliability, and elasticity. It resolves the client problem due to zero cost maintenance. On the whole, it provides a package for storing the extensive data and management.

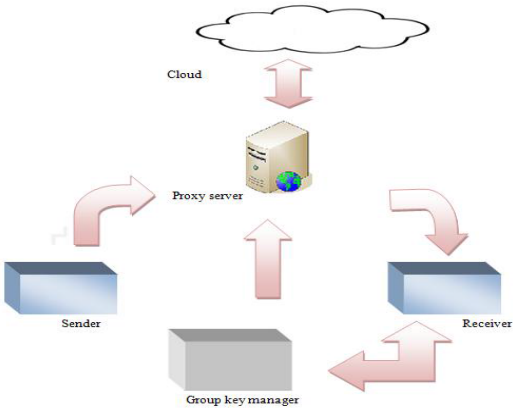
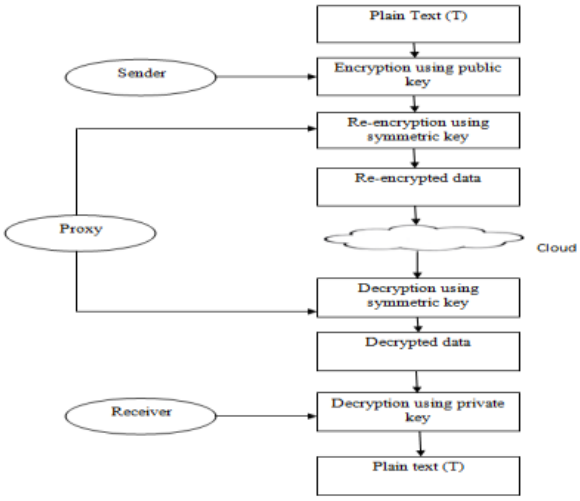
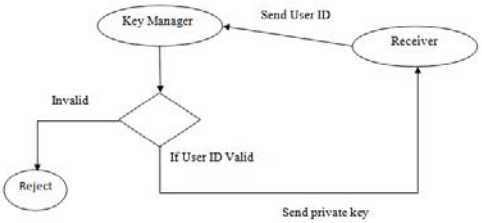



Fig : Framework Outline




2) Group Key Manager: The Group key manager's task is to compute the keys and distribute them among the users and the proxy. The schemes generated are as follows:

Generate a public key (sek) for public key and a private key (rdk) for encryption and decryption after authenticating the users with their User ids. It uses an Identity-based algorithm to generate the keys.

▪Generate a symmetric key (sk) for the proxy to re-encrypt the data and pre-decrypt the data. The symmetric key is generated using the DES algorithm.

3) The Proxy: The proxy server stands between the user and the cloud. The Group Key Manager (GKM) will authenticate the user ID, and user encrypts the data T with the public key (see) and sends the ciphertext C(T)=ENC(T) to the proxy. The proxy re-encrypts the ciphertext C(T) with its symmetric key (sk), generated through a traditional AES Algorithm producing Cp(T)=ENC(C(T)) and puts it in the cloud. When the user on the other side wants to access the data, the user undergoes the authentication process with the Group key manager. The GKM will provide the private key (rdk ) to the user when the User's ID is verified. The proxy retrieve is the data from the cloud using keyword search technique and pre-decrypts the data C(T)=DEC(Cp(T)) using the symmetric key (sk).The user who wants to read the data will decrypt the data T=DEC(C(T)) using his private key (rdk).

Algorithm:

1. Alice encrypts the plaintext T using Public key (see), i.e., C(T)=ENC(T).

2. The proxy re-encrypts C(T) with the symmetric key(sk) i.e,Cp(T)=REENC(C(T)).

3. Send the data to the cloud after re-encryption.

4. Pre-decryption of the stored data by the proxy using symmetric key (sk), i.e., C(T)=PREDEC(Cp(T)).

5. Authentication of the receiver User ID by GKM.

6. Decryption by the user through his private key(rdk) i.e,T=DEC(C(T))

4) Users: Users use numerous devices such as mobiles, laptops, and other hand devices through which they upload and share their data. The users in the framework use the keys to encrypt their personal data and decrypt it from the cloud.

*E. User Management*

The users can register themselves in the group at any point of time, and also they can leave the group at any time. Consequently, a prior authentication has to occur before any member joins the group to

secure the data and the key has to be revoked for that particular member.

1) Registration: During the process, the new user provides his/her user ID to the GKM and gets authenticated. The GKM provides a public key to the user. Using this public key the user can share the data in the group in a secure manner.

2) Revocation: Sometimes the user can detach from the group, or the administrator may remove he/she. In such cases, the GKM holds the information about the detached user's ID. Based on the information the GKM does not authenticate that particular user and does not share the private key. This prevents the user from accessing the data and keeping the data secure in the cloud.

*F. Security*

The framework is mainly designed to secure the data in the cloud. The proposed framework secures data in two ways:

1) Unidirectional Scheme: The proxy remains oblivious to the encrypted data as the private key is shared only with the receiver. The proxy has symmetric key through which it re-encrypts and pre-decrypts the data. As a result, the proxy cannot read the data and the hence the framework follows the unidirectional scheme. A scheme in which the proxy can convert in one direction is called unidirectional scheme.

2) Collusion: Collusion occurs when proxy and Alice collude to know Bob's private key. In this framework, collusion is completely avoided as private key is maintained by the GKM and is shared only with user who wants to access the data.

## Conclusion

Cloud Computing is still a new and evolving paradigm where computing is regarded as on demand service. Once the organization takes the decision to move to the cloud, it loses control over the data. Security of the Cloud relies on trusted computing and cryptography. Thus, in our proposed work, only the authorized user can access the data. In this paper, we have introduced a secure framework for sharing the data in the social network. Our framework focuses on the Revocable Hierarchical Identity-Based Encryption and proxy re-encryption scheme of unidirectional variety. Using the RHIBE method, without depending the cloud services the data are encrypted from the proxy server. Key manager distributes public/private keys for each user using authentication. Receivers ID is validated and the data are securely encrypted. The framework also eliminates the problem of collusion by not sharing the private key with the user. The framework also supports user management which consists of user registration and user revocation.

## References

[1] R. Gross, A. Acquisti, and H. J. H. III, "Information revelation and privacy in online social networks," in WPES, 2005, pp. 71–80.

[2] K. P. N. Puttaswamy, A. Sala, and B. Y. Zhao, "Starclique: guaranteeing user privacy in social networks against intersection attacks," in CoNEXT, 2009, pp. 157–168.

[3] J. He, W. Chu, and V. Liu, "Inferring Privacy Information from Social Networks," Proc. Intelligence and Security Informatics, 2006.

[4] L. Sweeney, "k-anonymity: A model for protecting privacy," International Journal of Uncertainty, Fuzziness and Knowledge-Based Systems, vol. 10, no. 5, pp. 557–570, 2002.

[8] A.Annapoorani, Ms.P.Indira Priya, Inferring Private Information from Social Network Using Collective Classification, International Journal of Innovative Research in Computer and Communication Engineering, Volume 4, Special Issue 1, March 2014

[9] Jayasree Dasari, K.R.Koteswara Rao, "Sanitization Techniques for Protecting Social Networks from Inference Attacks," International Journal of Computer Science and Mobile Computing, IJCSMC, Vol. 3, Issue. 12, December 2014, pg.236 –244.

[10] Chethana Nair, Neethu Krishna, Siby Abraham, "Generalization Algorithm For Prevent Inference Attacks in Social Network Data", International Journal of Research in Computer and Communication Technology", IJRCCT, December 2014.

[11] Divya.R, B.Mahesh and R.Ushasree, "Data Implication Attacks on Social Networks with Data Sanitization", International Journal of Current Engineering and Technology, Vol.4, No.3 (June 2014).

[12] Brinal Colaco, Shamsuddin Khan, "Privacy Preserving Data Mining for Social Networks", International Journal of Engineering Research & Technology, Vol. 3 - Issue 8, August – 2014.

[13] Pooja Shelke, Ashish Badiye, "Social Networking: Its Uses and Abuses", Research Journal of Forensic Sciences, Maharashtra, (2013): 2-7.

[14] Ahmadinejad, Seyed Hossein, and Philip WL Fong. "On the feasibility of inference attacks by third-party extensions to social network systems." Proceedings of the 8th ACM SIGSAC symposium on Information, computer and communications security.ACM, 2013.

[17] R.Pranay, P. Pavan Kumar, "A Survey on Obstruction of Confidential Information Attacks in Social Networks",

International Journal of Research in Information Technology, Volume 2, Issue 6, June 2014.
[20] B. Zhou, Jian Pei, Wo-Shun Luk, "A brief survey on anonymization techniques for privacy preserving publishing of social network data," ACM SIGKDD Explorations Newsletter, Vol. 10, pp. 12-22, 2008.
[21] Saikat Guha, Kevin Tang, Paul Francis, "NOYB: Privacy in Online Social Networks", in Proc. of first workshop on Online social networks WOSN'08, ACM New York, NY, USA, pp 49-54, 2008.
[22] Gary Blosser, Justin Zhan, "Privacy Preserving Collaborative Social Network", In Proc. of International Conference on Information Security and Assurance ISA 2008, Busan, pp, 543 - 548, 2008.
[23] Alina Campan, Traian Marius Truta, Nicholas Cooper, "P-Sensitive K-Anonymity with Generalization Constraints", In: Transactions on Data Privacy archive, Vol. 3 Issue 2, pp 65-89, 2010.
[24] Elena Zheleva, Lise Getoor, "Privacy in Social Networks: A Survey", In: Social Network Data Analytics, Springer US, pp 277-306, 2011.
[25] Roy Ford, Traian Marius Truta, and Alina Campan, "P-Sensitive K-Anonymity for Social Networks".
[26] A. Narayanan, V. Shmatikov, "De-anonymizing social networks", In Proc of 30th IEEE Symposium on Security and Privacy, Berkeley, CA, pp 173-187, 2009.
[27] Z. Lijie and Z. Weining, "Edge Anonymity in Social Network Graphs," in Proc. of International Conference on Computational Science and Engineering CSE '09, pp 1-8, 2009.
[28] X. Ying and X. Wu, "On link privacy in randomizing social networks," In: Advances in Knowledge Discovery and Data Mining, pp.28-39, 2009
[29] Amin Tootoonchian, Stefan Saroiu, Yashar Ganjali, Alec Wolman, "Lockr: Better Privacy for Social Networks", in Proc. of the 5th ACM International Conference on Emerging Networking Experiments and Technologies (CoNEXT), 2009.
[30] Philip W. L. Fong, Mohd Anwar, and Zhen Zhao, "A Privacy Preservation Model for Facebook-Style Social Network Systems", In: Computer Security - ESORICS 2009, Lecture Notes in Computer Science, Vol. 5789, 2009, pp 303-320, 2009.
[31] X. Tang and C.C. Yang, "Generalizing Terrorist Social Networks with K-Nearest Neighbor and Edge Betweenness for Social Network Integration and Privacy Preservation," In Proc. of IEEE International Conference on Intelligence and Security Informatics, 2010.
[32] Lihui Lan, Shiguang Ju Hua Jin, "Anonymizing Social Network using Bipartite Graph", In Proc. of International Conference on Computational and Information Sciences (ICCIS), Chengdu, pp 993 - 996, 2010.
[33] Xuan Ding, Lan Zhang, Zhiguo Wan, and Ming Gu, "A Brief Survey on De-anonymization Attacks in Online Social Networks", In Proc. of International Conference on Computational Aspects of Social Networks, Taiyuan, pp 611 - 615, 2010.
[34] Jinyuan Sun, Xiaoyan Zhu, and Yuguang Fang, "A Privacy-Preserving Scheme for Online Social Networks with Efficient Revocation", In Proc. of INFOCOM, IEEE, San Diego, CA, pp 1-9, 2010.
[35] Aaron Beach, Mike Gartrell, Richard Han, "q-Anon: Rethinking Anonymity for Social Networks", In Proc. of IEEE Second International Conference on Social Computing (SocialCom), Minneapolis, MN, pp 185 – 192, 2010.

**Author's Details**

[1]Assistant Professor, Department of Computer Science and Engineering, Jansons Institute of Technology, Coimbatore, Tamilnadu, India, Email: praveenasngp@gmail.com

[2]Professor, Department of Electronics and Communication Engineering, R.V.S.Technical Campus, Coimbatore, Tamilnadu, India, smys375@gmail.com