IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

SECURE AUTHENTICATED KEY MANAGEMENT PROTOCOL FOR CLOUD COMPUTING ENVIRONMENTS

SOMA SANKARI @ SOWMYA S

STUDENT

SRI SARADA COLLEGE FOR WOMEN

ABSTRACT

Many services have moved to the cloud platform as a result of the dependability and efficiency of cloud computing technologies maturing. Three-factor Mutual Authentication and Key Agreement (MAKA) protocols for multi-server architectures are receiving a lot of interest since they provide easy access to the services and safeguard the privacy of communication on the public network. However, many of the three-factor MAKA protocols now in use either lack a formal security proof, which makes them vulnerable to numerous attacks, or they have large computation and transmission costs. Additionally, the majority of three-factor MAKA protocols lack a dynamic revocation mechanism, making it difficult for unscrupulous users to have their access quickly revoked. We provide a provable dynamic revocable three-factor MAKA protocol to overcome these disadvantages. This protocol uses Schnorr signatures to manage users dynamically and offers a formal security proof in the random oracle. Our protocol can accommodate a range of requirements in multi-server situations, according to security study. Performance research shows that the suggested scheme is ideal for smart devices with limited processing resources. The whole simulation implementation demonstrates the protocol's viability.

Keywords: Cloud computing, Protocol, Security, Authentication

INTRODUCTION

The beginning of 90s marked the Internet era, wherein severalcomputers access a single server. The global use of internet demands web servers with high power and capacity to handle the requests from multiple users at the same time through Internet. Owing to meet the demands of the internet users, many services are being provided which in turn increases the storage requirements. Further, more and more application logics are being shifted from personal computers to the Internet servers, thanks to the increased speed of access to the internet and the facilities to access the variousservices. Nowadays, massive computations are handled by the providers dedicated for this purpose. In this way, multiple users can share the same infrastructure thereby maximizing the efficiency of the infrastructure and minimizing the cost. The rapid growth in software development necessitates improved and increased hardware potential such as central processing unit (CPU) with higher speed, hard disk with greater storage capacity and operating system (OS) characterizing higher performance.

CLOUD COMPUTING

Over the past few years, advances in the field of network-based computing and applications on demand have led to an explosive growth of application models such as cloud computing, software as a service, community network, web store, and so on. As a major application model in the era of the Internet, cloud computing has become a significant research topic among the scientific and industrial communities since 2007. Commonly,cloud computing is described as a range of services which are provided by an Internet-based cluster system. Such cluster systems consist of a group of low- cost servers or personal computers (PCs), organizing the various resources of the computers according to a certain management strategy, and offering safe, reliable, fast, convenient and transparent services such as data storage, accessing and computing to clients. According to the top ten strategic technology trends for 2012 provided by Gartner (a famous global analytical and consulting company), cloud computing spearheads the list indicating that cloud computing will havean increased impact on majority of the enterprises and organizations in 2012. Meanwhile, smart phones are considered to be the representative of various mobile devices that are connected to the Internet with the rapidly growing wireless network technology. Ubiquity and mobility will be the two major characteristics of the next generation network. These features provide a range of personalized network services through numerous network terminals and modes of access. The technology of cloud computing aims to provide centralized computing, services and specific applications as utilities for a pricesimilar to that of water, gas or electricity being offered to users.

National Institute of Standards and Technology (NIST) defines cloud computing as a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications and services) that can be rapidly provisioned and released with minimal management effort or service providerinteraction. In other words, it is the capacity to procure parts of mass assets rapidly and effectively as indicated by necessity of the customers and the customer is charged for those assets on utilization premise. It is an online handling, whereby shared assets, programming, and data are given on interest to PCs, mobile phones, and other comparative gadgets permitting clients to alter their processing limit contingent upon what amount is required at a giventime or for a given undertaking. Five vital qualities of distributed computingas recorded by NIST include (I) on-request self-administration, (ii) broad

system access (iii)resource pooling, (iv) rapid versatility and (v) measured administration. In general cloud computing revolves around two concepts namely Cloud Platforms (CP) and Cloud Services (CS).

THE NEED OF SECURITY IN CLOUD COMPUTING

Security is the highest concern in the cloud environment. Confidentiality of data is to be ensured by cryptography algorithms. Cloud storage is a service model in which data is maintained, managed and backed up remotely and made available to users over a network. Once the data is outsourced to the cloud, CSP is only responsible for maintaining, monitoring and controlling the data. Cloud services allow individuals and businesses to use softwareand hardware that are managed by third parties at remote locations. Examples of cloud services include online file storage, social networking sites, webmail,and online business applications. The cloud computing model allows accessto information and computer resources from anywhere a network connection is available. Cloud computing provides a shared pool of resources, including data storage space, networks, computer processing power, and specialized corporate and user applications. One of the most fundamental services offered by cloud providers is data storage, wherein the data owners can access the information through any mobile devices. However, it also poses a significant risk to the confidentiality of those stored files owing to access through any kind of devices. Specifically,when the data files (such as business plans) stored in the cloud are sensitive and confidential and needs to be shared only with authorized people and not everyone, the cloud servers managed by cloud providers are not fully trusted. To preserve data privacy, the basic solution is to encrypt data files, and then upload the encrypted data into the cloud.

PROBLEM ENCOUNTERED IN SECURITY FOR CLOUD STORAGE

The aim of this thesis is to propose methodologies towards efficientkey management and encryption technique for secure storage and sharing the information over the cloud service provider based on their trust value.

DATA OBFUSCATION TECHNIQUE FOR SECURE STORAGE

As per services offered by the cloud, IaaS, PaaS and SaaS are the well-known services, in which the additional service is SecaaS (Security as a Service). On considering cloud services, security poses the main concern. As per standards, cloud services are mostly offered by third parties. When storingthe information in third party storage or sharing the information through the third-party medium, secure sharing of information may be questionable and is of great concern. For ensuring secure sharing, cloud service providers maintain service level agreement to prove their integrity on present level of security. But again, most of CSPs need a third-party auditor to prove the integrity level of their organization security. Mostly, research works concentrate on cryptographic techniques forsecure sharing of data but there is no such mentioned work to words data integrity. In this work, a data masking technique called obfuscation is implemented. It is used to protect the data from unwanted modification through data breaching attacks. In this work, enhanced Vigenere encryption isused to perform obfuscation so that the privacy of users' data is maintained. Enhanced Vigenere encryption algorithm is combined with intelligent rules tomaintain the dissimilarity between the data masking for performing encryption with different set of rules. This work mainly concentrates on data privacy with reduced time complexity for

encryption and decryption. Mostly, available security processes maintain the privacy of data byensuring the usage of advanced cryptographic techniques. But what kind of privacy is provided for the data stored in public cloud? Even though, it can be said that the data is available in public cloud, it still belongs to some private concerns. So, the concern is on data integrity in public cloud for private data. It is assumed that the data stored in the cloud in allotted specific storage spacedoes not require any cryptographic algorithm for encryption and decryption. Even, if the CSPs provide algorithms for encryption, it incurs unwanted time resource for encrypting and decrypting the user's own private data. With that, another point of discussion is that the attacker can easily get the data from cloud if they know the algorithm and key what the user contains. This proposed work projects mainly on providing security for users' information in public cloud with less computational cost. In previous work, Mowbray et al (2012) specifies about the privacy manager for defining the policy specification. In this research work, the policy specification ismaintained by the clients themselves so that they can choose their encryption algorithm and where to apply that algorithm.

PROPOSED SECURE DATA SHARING SYSTEM

Secure data sharing in dynamic group environments requires group signature and implementation of broadcasting techniques to share the information and keys among them. This may lend to unwanted signature generation for all users *'Ln* the group even to the users who are not interested in the current data from the specific data owner. This leads to heavy overhead as the group signature is provided for all the user when an individual user requires the data from a particular data owner. The proposed approach aims to provide decentralized access control that supports anonymous authentication, that is the identity of the users is not known before storing the data. Only valid users who match in terms of signature and keys will be able to decrypt the stored data. It also supports creation, modification and reading data that is stored in cloud. An Individual User Policy Attribute Based Excerption (IUP-ABE) technique, wherein data is encrypted and decrypted on the basis of user requested attributes, is used. To achieve secure trusted data sharing for dynamic groups in the cloud, it is expected to combine the group signature and dynamic broadcast encryption techniques. Specifically, the group signature scheme enables users to anonymously use the cloud resources and the dynamic broadcast encryption technique allows the data owners to securely share their data files with others including the users who have joined recently. The drawback in the dynamic broadcast encryption scheme is that each user has to compute revocation parameters in order to protect the confidentiality of data from the revoked users. The result is that both the computational overhead of the encryption and the size of the cipher text increase with the number of revoked users. Thus, the heavy overhead and large cipher text size may restrain the adoption of the broadcast encryption scheme to groups involving large number of users. To tackle this challenge, the group manager computes the revocation parameters a d facilitates the availability of data by migrating them into the cloud. Such a design can significantly reduce the computational overhead of users in encrypting the files and size of the cipher text. Specifically, the computational overhead owing to the encryption operations at the user's side and the size of the cipher text is a constant and is independent of the number of revoked users. A secure multi-owner data sharing scheme is proposed. It implies that any user in the group can securely share data with others in the distrusted cloud environment. The distrusted environment represents not only the cloud database, but also the access device which gets information through proper credentials. The data owner can access the data from any device such as laptop, mobiles and so on by using their credentials. If this is the case, then there is a need for energy efficient mobile environment for performing all computational processes. In this context, a secure and privacy-preserving access

control, which guarantees any member in a group to anonymously utilize the cloud resource, is provided to the users.

System initialization is done by creating a cloud architecture in which data owner creates an account with cloud server. Further, more users can join the group of data owner with the view to access the data and to share files. This is possible through making a request to the data owner. During registration process, users need to provide an approval for data access in cloud. Once, user gets registered with the cloud system, he is free to access any file until lifetime expiry or revocation on the basis or request. Initially, data owner collects attributes relevant to the data file units and encrypt it. Then, the encrypted data is uploaded to the cloud server. Policy engine used in the system automatically runs and generates access structure of the data file. It also generates the user's public key. Once the access structure satisfies the attributes given by the user, the decrypted file can be downloaded by the user. After successful creation of cloud setup, users need to get registered with the system through user registration process. While registering, users need to submit their personal details for completion of registration process. It is to be noted that the system guarantees identity privacy. During registration process, user is provided with a unique identity privacy. During registration process, user is provided with a unique identify I and access structure T. This generates a secret key ski for me. Data file F can be then encrypted by using I's public Key Pk and thereby cipher text C is generated. User revocation is the process of removal of user from system's user list. This process is performed by the data owner. The system keeps Revocation List (RL) for each attribute. If a user has to be revoked, his access structure is removed from RL, so that the user can no longer access the data in the cloud. The process of file upload is as follows. During file upload, the data owner initially assigns file identity ID to the considered data files. Then, the data files are encrypted using his public key pk. Along with encryption, attributes for encryption are also added. Then, the file is uploaded to the cloud.

The procedure involved in file access is explained subsequently. Users can access the stored data files if they have a valid secret key. While accessing files, user's secret key is validated against access structure of the user. If it satisfies user's access structure, decrypted data file can be downloaded by the data consumer. File deletion can be performed by the data owners, if they on longer need a particular file. For file deletion, data owner has to provide File Identifier along with the secret key. If owner's signature is verified successfully, then cloud server positively deletes the file with the specified identity.

CONCLUSIONS

In this research work, a framework for secure and efficient storing and sharing of information over the public cloud storage is proposed. For this purpose, two different strategies are followed for storing and sharing the data. For storing the data in a public cloud, the user does not require any approval from a third-party auditor. But, for encryption and key management, the user needs the help of a third-party auditor. So, to avoid this additional overhead, the proposed system employs a data masking technique called obfuscation method by using Vigenere encryption algorithm in an extended format. In case of sharing the information, the system definitely needs a third-party auditor for framing key management policies and sharing the information between the users in a secure way. For this process, the proposed work uses the IUP-ABE technique, which provides individual key for each user to access data from each data owner. By this way, an individual user can access only the particular file from the specific data owner. If the user needs some other information from the data owner, then again for that the user has to get the access permission individually. Finally, the proposed system evaluates the trust value of the service provider using a technique that integrates Genetic Algorithm with Intelligent rules for showing the efficiency of service provider.