CMR
GROUP OF INSTITUTIONS
EXPLORE TO INVENT

CMR
INSTITUTE OF TECHNOLOGY
UGC AUTONOMOUS

Approved by AICTE, New Delhi & Permanently Affiliated to JNTUH, Hyderabad & Accredited by NBA, NAAC with 'A' Grade

Details Consultancy Project

Name of the faculty consultant or trainer	Organization to which consultancy or corporate training provided	Dates/duration of consultancy	Amount generated in INR
2022-2023			
Dr. L. Arokia Jesu Prabhu	Claro software Solutions Pvt Ltd	2022-2023	2,60,000
2021-2022			
Mr. N. Suresh	Claro software Solutions Pvt Ltd	2021-2022	2,50,000
2020-2021			
Dr. Alagumuthu Krishnan	Claro software Solutions Pvt Ltd	2020-2021	2,90,000
Dr. Praveen Kumar Kancherla	Amaravathi Research Academy	2020-2021	60,000
2019-2020			
Dr. K. Pradeep Reddy	Claro software Solutions Pvt Ltd	2019-2020	2,80,000

CMR
GROUP OF INSTITUTIONS
EXPLORE TO INVENT

Principal
CMR INSTITUTE OF TECHNOLOGY
Kandlakoya (V), Medchal,
Hyderabad- 501 401.

Kandlakoya, Medchal Road,
Hyderabad - 501 401.
Cell: 8008557612
Ph: 08418 - 200720
principal@cmritonline.ac.in

A Project Report

On

A CLOUD-BASED SAFE ANTI-COLLUSION DATA SHARING SYSTEM FOR ADAPTIVE GROUPS

Principal Investigator

Dr. L. Arokia Jesu Prabhu

Associate Investigators

Mr. N. Suresh **Dr. K. Ruben Raju**

CMR INSTITUTE OF TECHNOLOGY

(An Autonomous Institution)

KANDLAKOYA,MEDCHAL ROAD,HYDERABAD-501401

A.Y:2022-2023

Principal
CMR INSTITUTE OF TECHNOLOGY
Kandlakoya (V), Medchal Road,
Hyderabad-501 401.

ABSTRACT

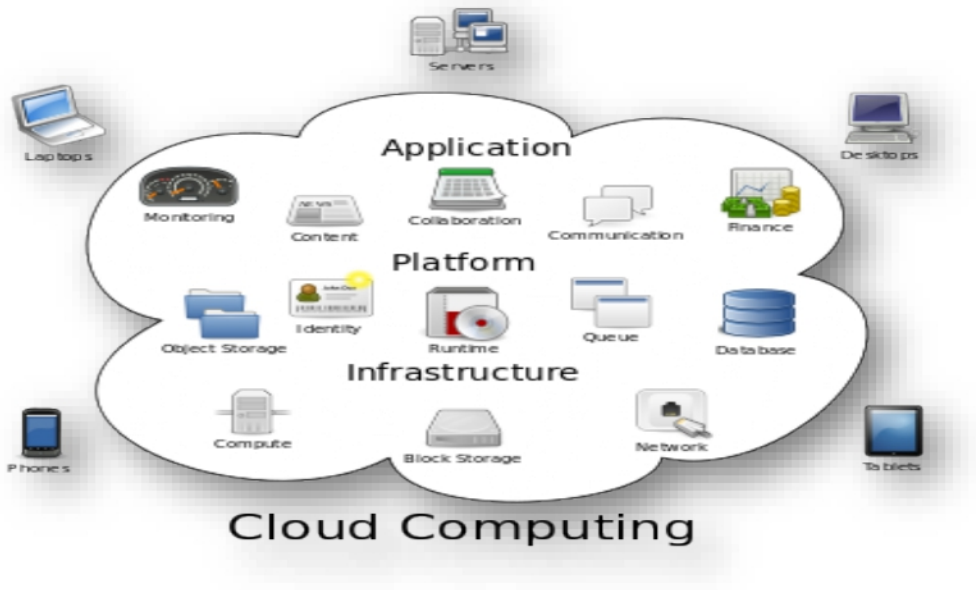
Benefited from cloud computing, users can achieve an effective and economical approach for data sharing among group members in the cloud with the characters of low maintenance and little management cost. Meanwhile, we must provide security guarantees for the sharing data files since they are outsourced. Unfortunately, because of the frequent change of the membership, sharing data while providing privacy-preserving is still a challenging issue, especially for an untrusted cloud due to the collusion attack. Moreover, for existing schemes, the security of key distribution is based on the secure communication channel, however, to have such channel is a strong assumption and is difficult for practice. In this paper, we propose a secure data sharing scheme for dynamic members. Firstly, we propose a secure way for key distribution without any secure communication channels, and the users can securely obtain their private keys from group manager. Secondly, our scheme can achieve fine-grained access control, any user in the group can use the source in the cloud and revoked users cannot access the cloud again after they are revoked. Thirdly, we can protect the scheme from collusion attack, which means that revoked users cannot get the original data file even if they conspire with the untrusted cloud. In our approach, by leveraging polynomial function, we can achieve a secure user revocation scheme. Finally, our scheme can achieve fine efficiency, which means previous users need not to update their private keys for the situation either a new user joins in the group or a user is revoked from the group.

Principal
CMR INSTITUTE OF TECHNOLOGY
Kandlakoya (V), Medchal Road,
Hyderabad-501 401.

INTRODUCTION

What is cloud computing?

Cloud computing is the use of computing resources (hardware and software) that are delivered as a service over a network (typically the Internet). The name comes from the common use of a cloud-shaped symbol as an abstraction for the complex infrastructure it contains in system diagrams. Cloud computing entrusts remote services with a user's data, software and computation. Cloud computing consists of hardware and software resources made available on the Internet as managed third-party services. These services typically provide access to advanced software applications and high-end networks of server computers.



Structure of cloud computing

How Cloud Computing Works?

The goal of cloud computing is to apply traditional supercomputing, or high-performance computing power, normally used by military and research facilities, to perform tens of trillions of computations per second, in consumer-oriented applications such as financial portfolios, to deliver personalized information, to provide data storage or to power large, immersive computer games.

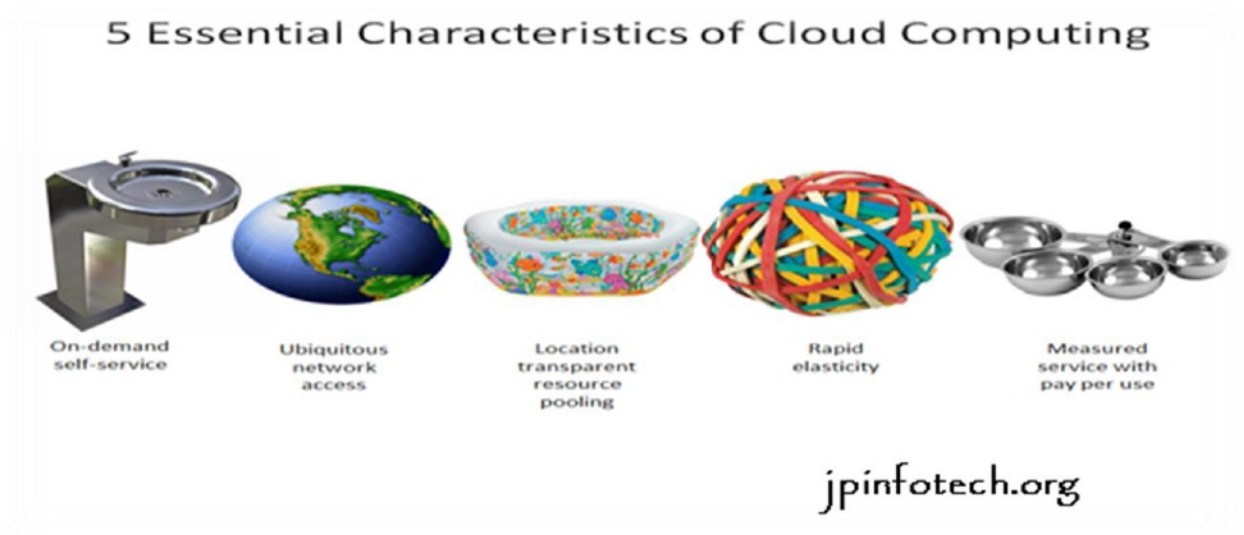
The cloud computing uses networks of large groups of servers typically running low-cost consumer PC technology with specialized connections to spread data-processing chores across them. This shared IT infrastructure contains large pools of systems that are linked together. Often, virtualization techniques are used to maximize the power of cloud computing.

Principal
CMR INSTITUTE OF TECHNOLOGY
Kandlakoya (V), Medchal Road,
Hyderabad-501 401.

Characteristics and Services Models:

The salient characteristics of cloud computing based on the definitions provided by the National Institute of Standards and Terminology (NIST) are outlined below:

- **On-demand self-service**: A consumer can unilaterally provision computing capabilities, such as server time and network storage, as needed automatically without requiring human interaction with each service's provider.
- **Broad network access**: Capabilities are available over the network and accessed through standard mechanisms that promote use by heterogeneous thin or thick client platforms (e.g., mobile phones, laptops, and PDAs).
- **Resource pooling**: The provider's computing resources are pooled to serve multiple consumers using a multi-tenant model, with different physical and virtual resources dynamically assigned and reassigned according to consumer demand. There is a sense of location-independence in that the customer generally has no control or knowledge over the exact location of the provided resources but may be able to specify location at a higher level of abstraction (e.g., country, state, or data center). Examples of resources include storage, processing, memory, network bandwidth, and virtual machines.
- **Rapid elasticity**: Capabilities can be rapidly and elastically provisioned, in some cases automatically, to quickly scale out and rapidly released to quickly scale in. To the consumer, the capabilities available for provisioning often appear to be unlimited and can be purchased in any quantity at any time.
- **Measured service**: Cloud systems automatically control and optimize resource use by leveraging a metering capability at some level of abstraction appropriate to the type of service (e.g., storage, processing, bandwidth, and active user accounts). Resource usage can be managed, controlled, and reported providing transparency for both the provider and consumer of the utilized service.

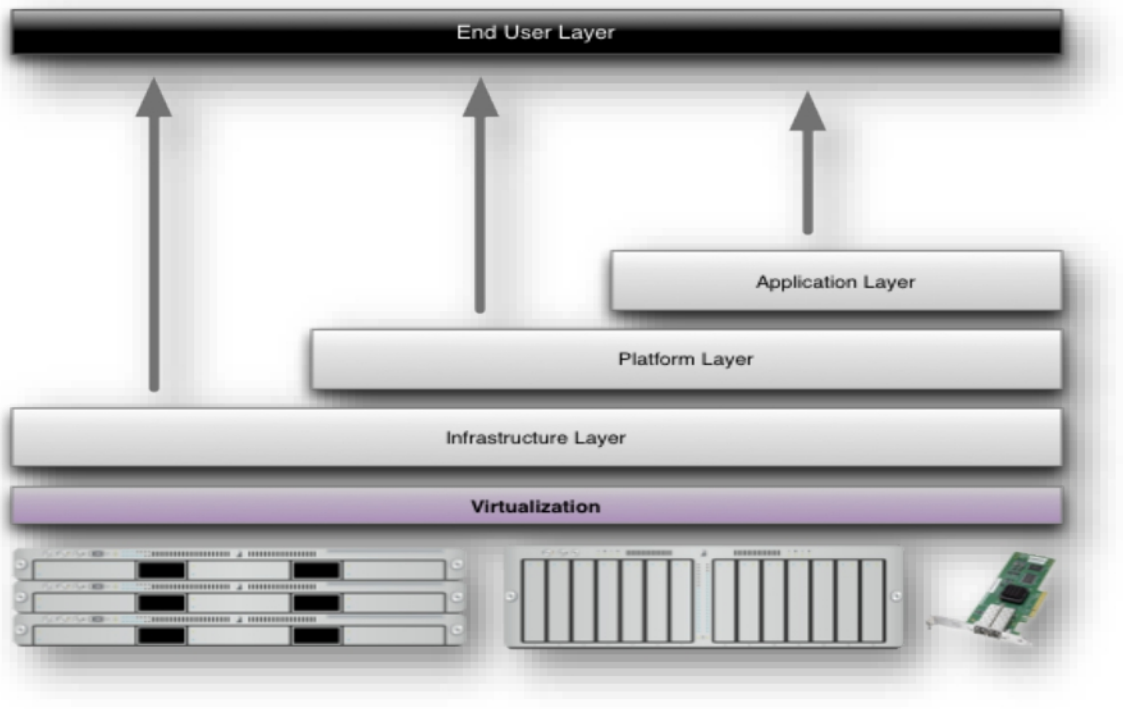


Characteristics of cloud computing

Principal
CMR INSTITUTE OF TECHNOLOGY
Kandlakoya (V), Medchal Road,
Hyderabad-501 401.

Services Models:

Cloud Computing comprises three different service models, namely Infrastructure-as-a-Service (IaaS), Platform-as-a-Service (PaaS), and Software-as-a-Service (SaaS). The three service models or layer are completed by an end user layer that encapsulates the end user perspective on cloud services. The model is shown in figure below. If a cloud user accesses services on the infrastructure layer, for instance, she can run her own applications on the resources of a cloud infrastructure and remain responsible for the support, maintenance, and security of these applications herself. If she accesses a service on the application layer, these tasks are normally taken care of by the cloud service provider.



Structure of service models

Benefits of cloud computing:

1. **Achieve economies of scale** – increase volume output or productivity with fewer people. Your cost per unit, project or product plummets.
2. **Reduce spending on technology infrastructure.** Maintain easy access to your information with minimal upfront spending. Pay as you go (weekly, quarterly or yearly), based on demand.
3. **Globalize your workforce on the cheap.** People worldwide can access the cloud, provided they have an Internet connection.
4. **Streamline processes.** Get more work done in less time with less people.
5. **Reduce capital costs.** There's no need to spend big money on hardware, software or licensing fees.
6. **Improve accessibility.** You have access anytime, anywhere, making your life so much easier!
7. **Monitor projects more effectively.** Stay within budget and ahead of completion cycle times.
8. **Less personnel training is needed.** It takes fewer people to do more work on a cloud, with a minimal learning curve on hardware and software issues.

9. **Minimize licensing new software.** Stretch and grow without the need to buy expensive software licenses or programs.
10. **Improve flexibility.** You can change direction without serious "people" or "financial" issues at stake.

Advantages:

1. **Price:** Pay for only the resources used.
2. **Security**: Cloud instances are isolated in the network from other instances for improved security.
3. **Performance:** Instances can be added instantly for improved performance. Clients have access to the total resources of the Cloud's core hardware.
4. **Scalability:** Auto-deploy cloud instances when needed.
5. **Uptime:** Uses multiple servers for maximum redundancies. In case of server failure, instances can be automatically created on another server.
6. **Control:** Able to login from any location. Server snapshot and a software library lets you deploy custom instances.

Traffic: Deals with spike in traffic with quick deployment of additional instances to handle the load.

Principal
CMR INSTITUTE OF TECHNOLOGY
Kandlakoya (V), Medchal Road,
Hyderabad-501 401.

SYSTEM STUDY

FEASIBILITY STUDY

The feasibility of the project is analyzed in this phase and business proposal is put forth with a very general plan for the project and some cost estimates. During system analysis the feasibility study of the proposed system is to be carried out. This is to ensure that the proposed system is not a burden to the company. For feasibility analysis, some understanding of the major requirements for the system is essential.

Three key considerations involved in the feasibility analysis are

- ECONOMICAL FEASIBILITY
- TECHNICAL FEASIBILITY
- SOCIAL FEASIBILITY

ECONOMICAL FEASIBILITY

This study is carried out to check the economic impact that the system will have on the organization. The amount of fund that the company can pour into the research and development of the system is limited. The expenditures must be justified. Thus the developed system as well within the budget and this was achieved because most of the technologies used are freely available. Only the customized products had to be purchased.

TECHNICAL FEASIBILITY

This study is carried out to check the technical feasibility, that is, the technical requirements of the system. Any system developed must not have a high demand on the available technical resources. This will lead to high demands on the available technical resources. This will lead to high demands being placed on the client. The developed system must have a modest requirement, as only minimal or null changes are required for implementing this system.

SOCIAL FEASIBILITY

The aspect of study is to check the level of acceptance of the system by the user. This includes the process of training the user to use the system efficiently. The user must not feel threatened by the system, instead must accept it as a necessity. The level of acceptance by the users solely depends on the methods that are employed to educate the user about the system and to make him familiar with it. His level of confidence must be raised so that he is also able to make some constructive criticism, which is welcomed, as he is the final user of the system.

Principal
CMR INSTITUTE OF TECHNOLOGY
Kandlakoya (V), Medchal Road,
Hyderabad-501 401.

SYSTEM REQUIREMENTS:

HARDWARE REQUIREMENTS:

- System : Pentium IV 2.4 GHz.
- Hard Disk : 40 GB.
- Floppy Drive : 1.44 Mb.
- Monitor : 15 VGA Colour.
- Mouse : Logitech.
- Ram : 512 Mb.

SOFTWARE REQUIREMENTS:

- Operating system : - Windows XP.
- Coding Language: J2EE

Data Base : MYSQL

Principal
CMR INSTITUTE OF TECHNOLOGY
Kandlakoya (V), Medchal Road,
Hyderabad-501 401.

SYSTEM ANALYSIS

EXISTING SYSTEM:

- Kallahalla et al presented a cryptographic storage system that enables secure data sharing on untrustworthy servers based on the techniques that dividing files into file groups and encrypting each file group with a file-block key.
- Yu et al exploited and combined techniques of key policy attribute-based encryption, proxy re-encryption and lazy re-encryption to achieve fine-grained data access control without disclosing data contents.

DISADVANTAGES OF EXISTING SYSTEM:

- The file-block keys need to be updated and distributed for a user revocation; therefore, the system had a heavy key distribution overhead.
- The complexities of user participation and revocation in these schemes are linearly increasing with the number of data owners and the revoked users.
- The single-owner manner may hinder the implementation of applications, where any member in the group can use the cloud service to store and share data files with others.

PROPOSED SYSTEM:

- In this paper, we propose a secure data sharing scheme, which can achieve secure key distribution and data sharing for dynamic group.
- We provide a secure way for key distribution without any secure communication channels. The users can securely obtain their private keys from group manager without any Certificate Authorities due to the verification for the public key of the user.
- Our scheme can achieve fine-grained access control, with the help of the group user list, any user in the group can use the source in the cloud and revoked users cannot access the cloud again after they are revoked.
- We propose a secure data sharing scheme which can be protected from collusion attack. The revoked users can not be able to get the original data files once they are revoked even if they conspire with the untrusted cloud. Our scheme can achieve secure user revocation with the help of polynomial function.
- Our scheme is able to support dynamic groups efficiently, when a new user joins in the group or a user is revoked from the group, the private keys of the other users do not need to be recomputed and updated.
- We provide security analysis to prove the security of our scheme.

Principal
CMR INSTITUTE OF TECHNOLOGY
Kandlakoya (V), Medchal Road,
Hyderabad-501 401.

ADVANTAGES OF PROPOSED SYSTEM:

- ✓ The computation cost is irrelevant to the number of revoked users in RBAC scheme. The reason is that no matter how many users are revoked, the operations for members to decrypt the data files almost remain the same.
- ✓ The cost is irrelevant to the number of the revoked users. The reason is that the computation cost of the cloud for file upload in our scheme consists of two verifications for signature, which is irrelevant to the number of the revoked users. The reason for the small computation cost of the cloud in the phase of file upload in RBAC scheme is that the verifications between communication entities are not concerned in this scheme.

In our scheme, the users can securely obtain their private keys from group manager Certificate Authorities and secure communication channels. Also, our scheme is able to support dynamic groups efficiently, when a new user joins in the group or a user is revoked from the group, the private keys of the other users do not need to be recomputed and updated.

Principal
CMR INSTITUTE OF TECHNOLOGY
Kandlakoya (V), Medchal Road,
Hyderabad-501 401.

LITERATURE SURVEY

1 "Oruta: Privacy-Preserving Public Auditing for Shared Data in the Cloud,"

AUTHORS: B. Wang, B. Li, and H. Li,

With cloud data services, it is commonplace for data to be not only stored in the cloud, but also shared across multiple users. Unfortunately, the integrity of cloud data is subject to skepticism due to the existence of hardware/software failures and human errors. Several mechanisms have been designed to allow both data owners and public verifiers to efficiently audit cloud data integrity without retrieving the entire data from the cloud server. However, public auditing on the integrity of shared data with these existing mechanisms will inevitably reveal confidential information-identity privacy-to public verifiers. In this paper, we propose a novel privacy-preserving mechanism that supports public auditing on shared data stored in the cloud. In particular, we exploit ring signatures to compute verification metadata needed to audit the correctness of shared data. With our mechanism, the identity of the signer on each block in shared data is kept private from public verifiers, who are able to efficiently verify shared data integrity without retrieving the entire file. In addition, our mechanism is able to perform multiple auditing tasks simultaneously instead of verifying them one by one. Our experimental results demonstrate the effectiveness and efficiency of our mechanism when auditing shared data integrity.

2. "Security Challenges for the Public Cloud,"

AUTHORS: K. Ren, C. Wang, and Q. Wang,

In this talk, I will first discuss a number of pressing security challenges in Cloud Computing, including data service outsourcing security and secure computation outsourcing. Then, I will focus on data storage security in Cloud Computing. As one of the primitive services, cloud storage allows data owners to outsource their data to cloud for its appealing benefits. However, the fact that owners no longer have physical possession of the outsourced data raises big security concerns on the storage correctness. Hence, enabling secure storage auditing in the cloud environment with new approaches becomes imperative and challenging. In this talk, I will present our recent research efforts towards storage outsourcing security in cloud computing and describe both our technical approaches and security & performance evaluations.

Principal
CMR INSTITUTE OF TECHNOLOGY
Kandlakoya (V), Medchal Road,
Hyderabad-501 401.

3. "Privacy-Preserving Public Auditing for Data Storage Security in Cloud Computing,"

AUTHORS: C. Wang, Q. Wang, K. Ren, and W. Lou

Cloud computing is the long dreamed vision of computing as a utility, where users can remotely store their data into the cloud so as to enjoy the on-demand high quality applications and services from a shared pool of configurable computing resources. By data outsourcing, users can be relieved from the burden of local data storage and maintenance. However, the fact that users no longer have physical possession of the possibly large size of outsourced data makes the data integrity protection in Cloud Computing a very challenging and potentially formidable task, especially for users with constrained computing resources and capabilities. Thus, enabling public audit ability for cloud data storage security is of critical importance so that users can resort to an external audit party to check the integrity of outsourced data when needed. To securely introduce an effective third party auditor (TPA), the following two fundamental requirements have to be met: 1) TPA should be able to efficiently audit the cloud data storage without demanding the local copy of data, and introduce no additional on-line burden to the cloud user; 2) The third party auditing process should bring in no new vulnerabilities towards user data privacy. In this paper, we utilize and uniquely combine the public key based homomorphic authenticator with random masking to achieve the privacy-preserving public cloud data auditing system, which meets all above requirements. To support efficient handling of multiple auditing tasks, we further explore the technique of bilinear aggregate signature to extend our main result into a multi-user setting, where TPA can perform multiple auditing tasks simultaneously. Extensive security and performance analysis shows the proposed schemes are provably secure and highly efficient.

4. "Computing Encrypted Cloud Data Efficiently under Multiple Keys,"

AUTHORS: B. Wang, M. Li, S.S. Chow, and H. Li,

The emergence of cloud computing brings users abundant opportunities to utilize the power of cloud to perform computation on data contributed by multiple users. These cloud data should be encrypted under multiple keys due to privacy concerns. However, existing secure computation techniques are either limited to single key or still far from practical. In this paper, we design two efficient schemes for secure outsourced computation over cloud data encrypted under multiple keys. Our schemes employ two non-colluding cloud servers to jointly compute polynomial functions over multiple users' encrypted cloud data without learning the inputs, intermediate or final results, and require only minimal interactions between the two cloud servers but not the users. We demonstrate our schemes' efficiency experimentally via applications in machine learning. Our schemes are also applicable to privacy-preserving data aggregation such as in smart metering.

Principal
CMR INSTITUTE OF TECHNOLOGY
Kandlakoya (V), Medchal Road,
Hyderabad-501 401.

5. **"Achieving Secure, Scalable, and Fine-Grained Data Access Control in Cloud Computing,"**

AUTHORS: S. Yu, C. Wang, K. Ren, and W. Lou,

Cloud computing is an emerging computing paradigm in which resources of the computing infrastructure are provided as services over the Internet. As promising as it is, this paradigm also brings forth many new challenges for data security and access control when users outsource sensitive data for sharing on cloud servers, which are not within the same trusted domain as data owners. To keep sensitive user data confidential against untrusted servers, existing solutions usually apply cryptographic methods by disclosing data decryption keys only to authorized users. However, in doing so, these solutions inevitably introduce a heavy computation overhead on the data owner for key distribution and data management when fine-grained data access control is desired, and thus do not scale well. The problem of simultaneously achieving fine-grainedness, scalability, and data confidentiality of access control actually still remains unresolved. This paper addresses this challenging open issue by, on one hand, defining and enforcing access policies based on data attributes, and, on the other hand, allowing the data owner to delegate most of the computation tasks involved in fine-grained data access control to untrusted cloud servers without disclosing the underlying data contents. We achieve this goal by exploiting and uniquely combining techniques of attribute-based encryption (ABE), proxy re-encryption, and lazy re-encryption. Our proposed scheme also has salient properties of user access privilege confidentiality and user secret key accountability. Extensive analysis shows that our proposed scheme is highly efficient and provably secure under existing security models.

Principal
CMR INSTITUTE OF TECHNOLOGY
Kandlakoya (V), Medchal Road,
Hyderabad-501 401.

CONCLUSION

In this paper, we design a secure anti-collusion data sharing scheme for dynamic groups in the cloud. In our scheme, the userscan securely obtain their private keys from group manager Certificate Authorities and secure communication channels. Also, our scheme is able to support dynamic groups efficiently, when a new user joins in the group or a user is revoked from the group, the private keys of the other users do not need to be recomputed and updated. Moreover, our scheme can achieve secure user revocation, the revoked users can not be able to get the original data files once they are revoked even if they conspire with the untrusted cloud.

Principal
CMR INSTITUTE OF TECHNOLOGY
Kandlakoya (V), Medchal Road,
Hyderabad-501 401.

A Project Report

On

BETTER P2P MULTIMEDIA DISTRIBUTION PRESERVING PRIVACY USING RECOMBINED FINGERPRINTS

Principal Investigator

Dr. AlagumuthuKrishnan

Associate Investigators

Dr. Vijender Kumar Solanki **Dr. K. Pradeep Reddy**

CMR INSTITUTE OF TECHNOLOGY

(An Autonomous Institution)

KANDLAKOYA,MEDCHAL ROAD,HYDERABAD-501401

A.Y:2020-2021

Principal
CMR INSTITUTE OF TECHNOLOGY
Kandlakoya (V), Medchal Road,
Hyderabad-501 401.

ABSTRACT

Anonymous fingerprint has been suggested as a convenient solution for the legal distribution of multimedia contents with copyright protection whilst preserving the privacy of buyers, whose identities are only revealed in case of illegal re-distribution. However, most of the existing anonymous fingerprinting protocols are impractical for two main reasons: 1) the use of complex time-consuming protocols and/or homomorphic encryption of the content, and 2) a unicast approach for distribution that does not scale for a large number of buyers. This paper stems from a previous proposal of recombined fingerprints which overcomes some of these drawbacks. However, the recombined fingerprint approach requires a complex graph search for traitor tracing, which needs the participation of other buyers, and honest proxies in its P2P distribution scenario. This paper focuses on removing these disadvantages resulting in an efficient, scalable, privacy-preserving and P2P-based fingerprinting system.

Principal
CMR INSTITUTE OF TECHNOLOGY
Kandlakoya (V), Medchal Road,
Hyderabad-501 401.

SYSTEM ANALYSIS

EXISTING SYSTEM:

- Most fingerprinting systems can be classified in three categories, namely symmetric, asymmetric and anonymous schemes.
- In symmetric schemes, the merchant is the one who embeds the fingerprint into the content and forwards the result to the buyer; hence, the buyer cannot be formally accused of illegal re-distribution, since the merchant also had access to the fingerprinted content and could be responsible for the re-distribution.
- In asymmetric fingerprinting, the merchant does not have access to the fingerprinted copy, but he can recover the fingerprint in case of illegal re-distribution and thereby identify the offending buyer.
- In anonymous fingerprinting, in addition to asymmetry, the buyer preserves her anonymity (privacy) and hence she cannot be linked to the purchase of a specific content, unless she participates in an illegal re-distribution.

DISADVANTAGES OF EXISTING SYSTEM:

- Developing a practical system using this idea appears difficult, because public-key encryption expands data and substantially increases the communication bandwidth required for transfers.
- Homomorphic encryption constrains the type of mathematical operations which can be performed on the content for embedding, making it difficult to use the more advanced and robust techniques in the data hiding literature.
- In addition, the application of this idea in a distributed scenario (such as P2P networks) is not simple, since embedding would have to be performed by peer buyers, requiring a complex and supervised protocol.

PROPOSED SYSTEM:

- The content is divided into several ordered fragments and each of them is embedded separately with a random binary sequence. The binary sequence for each fragment is called segment and the concatenation of all segments forms the whole fingerprint.
- The merchant distributes different copies to a reduced set of M seed buyers. The fingerprints of these buyers are such that their segments have low pair-wise correlations.
- The buyers other than the seed ones engage on P2P transfers of the content in such a way that each new buyer obtains fragments from at least two other buyers. The total number of buyers is N _ M.
- The communication between peer buyers is anonymous through an onion routing-like protocol using a proxy.
- The fingerprint of each new buyer is built as a recombination of the segments of its parents.
- Proxies know the pseudonyms of source and destination buyers and they have access to the symmetric keys used for encrypting the multimedia content.
- A transaction record is created by a transaction monitor to keep track of each transfer between peer buyers. These records do not contain the embedded fingerprints, but only an encrypted hash of them.
- The fingerprints' hashes are encrypted in such a way that the private key of at least one parent is required for obtaining their cleartext.

- The real identities of buyers are known only by the merchant. The transaction monitor records buyers' pseudonyms.
- In case of illegal re-distribution, a search is required through the distribution graph. The search starts from the seed buyers and is directed by a correlation function between the traced fingerprint and the fingerprints of the tested buyers. These tested buyers must co-operate with a tracing authority to compute the correlation between their fingerprint and the one extracted from the illegally re-distributed file. The fingerprints' hashes recorded in the transaction monitor are enough to prevent buyers from cheating in this step.
- At each step of the traitor tracing protocol, the buyer with maximum correlation is chosen as the most likely ancestor of the illegal re-distributor. This criterion is mostly right, but some incorrect choices may occur during the search process, requiring the exhaustion of a subgraph and backtracking.
- The search ends when perfect correlation is found between the fingerprint of the tested buyer and that of the illegally re-distributed file. If a buyer refuses to take a correlation test, the hash recorded in the transaction monitor can be used as evidence against her.

ADVANTAGES OF PROPOSED SYSTEM:

- This paper reviews the main features of the proposal suggested, highlights its main drawbacks, and suggests several significant improvements to achieve a more efficient and practical system, especially as traitor tracing is concerned, since it avoids the situations in which illegal redistributors cannot be traced with the proposal.
- Furthermore, better security properties against potentially malicious proxies are obtained.

Although the system proposed in this paper uses publickey encryption in the distribution and traitor tracing protocols, it must be taken into account that this encryption is only applied to short bit strings, such as the binary fingerprints and hashes, not to the content. The fragments of the content are encrypted using symmetric cryptography, which is much more efficient.

Principal
CMR INSTITUTE OF TECHNOLOGY
Kandlakoya (V), Medchal Road,
Hyderabad-501 401.

IMPLEMENTATION

MODULES:

1. Merchant
2. Buyers' Privacy
3. Transaction monitor
4. Database authentication attacks

MODULES DESCRIPTION:

Buyers' Privacy:

The identity of a buyer who has purchased a specific content could be revealed by a coalition of two parties: one of the proxies chosen by the buyer and the merchant (who can link her pseudonym to a real identity) or, similarly, the transaction monitor and the merchant. Better privacy could be achieved if, for example, the pseudonyms were encrypted by the proxies using the public key of the tracing authority.

Database authentication attacks:

An attacker may try to obtain the fingerprint of a buyer that is stored in the transaction monitor's database. An attacker may try to intercept the traffic between a buyer and one or more of her proxies and keep a copy of all the fragments of the content.

Transaction monitor:

It keeps a transaction register for each purchase carried out for each buyer. This transaction register includes an encrypted version of the embedded fingerprints. In case of illegal re-distribution, it participates in the tracing protocol that is used to Identify the illegal re-distributor(s).

Merchant:

He distributes copies of the content legally to the seed buyers. Each fragment of the content contains a different segment of the fingerprint embedded into it. The segments have low pair-wise correlations.

Principal
CMR INSTITUTE OF TECHNOLOGY
Kandlakoya (V), Medchal Road,
Hyderabad-501 401.

INPUT DESIGN

The input design is the link between the information system and the user. It comprises the developing specification and procedures for data preparation and those steps are necessary to put transaction data in to a usable form for processing can be achieved by inspecting the computer to read data from a written or printed document or it can occur by having people keying the data directly into the system. The design of input focuses on controlling the amount of input required, controlling the errors, avoiding delay, avoiding extra steps and keeping the process simple. The input is designed in such a way so that it provides security and ease of use with retaining the privacy. Input Design considered the following things:

- What data should be given as input?
- How the data should be arranged or coded?
- The dialog to guide the operating personnel in providing input.
- Methods for preparing input validations and steps to follow when error occur.

OBJECTIVES

1. Input Design is the process of converting a user-oriented description of the input into a computer-based system. This design is important to avoid errors in the data input process and show the correct direction to the management for getting correct information from the computerized system.

2. It is achieved by creating user-friendly screens for the data entry to handle large volume of data. The goal of designing input is to make data entry easier and to be free from errors. The data entry screen is designed in such a way that all the data manipulates can be performed. It also provides record viewing facilities.

3. When the data is entered it will check for its validity. Data can be entered with the help of screens. Appropriate messages are provided as when needed so that the user will not be in maize of instant. Thus the objective of input design is to create an input layout that is easy to follow

OUTPUT DESIGN

A quality output is one, which meets the requirements of the end user and presents the information clearly. In any system results of processing are communicated to the users and to other system through outputs. In output design it is determined how the information is to be displaced for immediate need and also the hard copy output. It is the most important and direct source information to the user. Efficient and intelligent output design improves the system's relationship to help user decision-making.

1. Designing computer output should proceed in an organized, well thought out manner; the right output must be developed while ensuring that each output element is designed so that people will find the system can use easily and effectively. When analysis design computer output, they should Identify the specific output that is needed to meet the requirements.

2.Select methods for presenting information.

3.Create document, report, or other formats that contain information produced by the system. The output form of an information system should accomplish one or more of the following objectives.

- Convey information about past activities, current status or projections of the
- Future.
- Signal important events, opportunities, problems, or warnings.
- Trigger an action.
- Confirm an action.

Principal
CMR INSTITUTE OF TECHNOLOGY
Kandlakoya (V), Medchal Road,
Hyderabad-501 401.

LITERATURE SURVEY

1) An efficient and fair buyer-seller fingerprinting scheme for large scale networks

AUTHORS: C.-C. Chang, H.-C. Tsai, and Y.-P. Hsieh

In digital watermarking, most existing schemes focus on the owners' copyright protection rather than protection of the customers' rights. Therefore, these schemes are unfair to legitimate customers who have no certificate to prove their right to use the watermarked digital content that they have purchased. In addition, these schemes are also unable to identify those who leak pirated copies of the watermarked digital content. To protect customers' rights and to identify the users of unauthorized copies, the fingerprinting technique is a feasible method for embedding a watermark so that content owners can identify users who have purchased the right to use the content and users who have not purchased this right. Although some fingerprinting schemes have been proposed in recent years, most of them are inefficient due to their homomorphic architecture that is based on public key cryptography. Therefore, in this paper, we propose a fair, traceable, and efficient watermarking scheme with a novel architecture. Due to the high computational complexity of the asymmetric cryptography, such as modular multiplications and exponentiations which lead much heavier burden than operations in symmetric cryptography, the proposed protocol transfers the demanding computational requirements from the buyer to a powerful server in protocol design. The proposed method can achieve these benefits: 1) the rights of legitimate buyers can be protected; 2) the proposed scheme is traceable; 3) the proposed scheme is more efficient than the previous schemes because public key cryptography is not frequently used; and 4) the buyer's anonymity can be well-protected until there is an infringement accusation.

2) Distributed multicast of fingerprinted content based on a rational peer-to-peer community

AUTHORS: J. Domingo-Ferrer and D. Megıas

In conventional multicast transmission, one sender sends the same content to a set of receivers. This precludes fingerprinting the copy obtained by each receiver (in view of redistribution control and other applications). A straightforward alternative is for the sender to separately fingerprint and send in unicast one copy of the content for each receiver. This approach is not scalable and may implode the sender. We present a scalable solution for distributed multicast of fingerprinted content, in which receivers rationally co-operate in fingerprinting and spreading the content. Furthermore, fingerprinting can be anonymous, in order for honest receivers to stay anonymous.

Principal
CMR INSTITUTE OF TECHNOLOGY
Kandlakoya (V), Medchal Road,
Hyderabad-501 401.

3) Secure logarithmic audio watermarking scheme based on the human auditory system

AUTHORS: M. Fallahpour and D. Megıas

This paper proposes a high capacity audio watermarking algorithm in the logarithm domain based on the absolute threshold of hearing of the human auditory system (HAS), which makes this scheme a novel technique. When considering the fact that the human ear requires more precise samples at low amplitudes (soft sounds), the use of the logarithm helps us design a logarithmic quantization algorithm. The key idea is to divide the selected frequency band into short frames and quantize the samples based on the HAS. Using frames and the HAS improves the robustness, since embedding a secret bit into a set of samples is more reliable than embedding it into a single sample. In addition, the quantization level is adjusted according to the HAS. Apart from remarkable capacity, transparency and robustness, this scheme provides three parameters (frequency band, scale factor and frame size) which facilitate the regulation of the watermarking properties. The experimental results show that the method has a high capacity (800–7,000 bits per second), without significant perceptual distortion (ODG >1) and provides robustness against common audio signal processing such as added noise, filtering and MPEG compression (MP3).

4) DNA-inspired anonymous fingerprinting for efficient peer-to-peer content distribution

AUTHORS: D. Megıas and J. Domingo-Ferrer

When selling electronic content, the merchant would like each buyer to receive a different copy of the content fingerprinted with a serial number, in order to be able to trace redistributors should illegal redistribution happen. On the other hand, the merchant would like content distribution to be as scalable as possible, in order for mass transactions to be possible. Multicast content distribution fails to satisfy the first requirement: all receivers get exactly the same copy of the content, which makes it difficult to trace illegal redistributors. Unicast distribution of fingerprinted content, on the other hand, fails to satisfy the second requirement: for each buyer, the merchant needs to compute a fingerprint and establish a connection. P2P content distribution is a third option combining the strengths of multicast and unicast: the merchant needs to establish unicast connections only with a few seed buyers; on the other hand, with a suitable fingerprinting mechanism, illegal redistributors can still be identified and honest buyers can stay anonymous. We present a P2P content distribution scheme with such an anonymous fingerprinting mechanism, which is inspired in the way DNA sequences combine and spread from ancestors to descendants.

Principal
CMR INSTITUTE OF TECHNOLOGY
Kandlakoya (V), Medchal Road,
Hyderabad-501 401.

5) Privacy-aware peer-to-peer content distribution using automatically recombined fingerprints

AUTHORS: D. Megıas and J. Domingo-Ferrer

Multicast distribution of content is not suited to content-based electronic commerce because all buyers obtain exactly the same copy of the content, in such a way that unlawful redistributors cannot be traced. Unicast distribution has the shortcoming of requiring one connection with each buyer, but it allows the merchant to embed a different serial number in the copy obtained by each buyer, which enables redistributor tracing. Peer-to-peer (P2P) distribution is a third option which may combine some of the advantages of multicast and unicast: on the one hand, the merchant only needs unicast connections with a few seed buyers, who take over the task of further spreading the content; on the other hand, if a proper fingerprinting mechanism is used, unlawful redistributors of the P2P-distributed content can still be traced. In this paper, we propose a novel fingerprinting mechanism for P2P content distribution which allows redistributor tracing, while preserving the privacy of most honest buyers and offering collusion resistance and buyer frame proofness.

Principal
CMR INSTITUTE OF TECHNOLOGY
Kandlakoya (V), Medchal Road,
Hyderabad-501 401.

CONCLUSION

The use of automatic recombined fingerprints has been recently suggested in the literature [12], [13], showing remarkable advantages: the fingerprints of buyers areunknown to the merchant (achieving anonymity) and fingerprint embedding is required only for a few seed buyers, whereas the other fingerprints are automatically obtained as a recombination of segments. However, the publishedsystem has some shortcomings: 1) it requires an expensive graph search in order to identify an illegal re-distributor, 2) some innocent buyers are requested to co-operate for tracing, and 3) the P2P distribution protocol requires honest proxies. This paper shows that the co-operation of honest buyers in traitor tracing entails several relevant drawbacks that can make the published system fail undersome circumstances. The improvements suggested in this paper overcome thedrawbacks of [12], [13] by recording the fingerprints using multiple encryption in such a way that the graph search is replaced by a standard database search, whilst buyers' frameproofness is retained. Also, misbehaving proxies are discouraged by means of random checks by the authority and using a four-party anonymous communication protocol to prevent proxies from accessing the cleartext of the fragments of the content. The final result is a fingerprinting system that features:

1) efficient and scalable distribution of multimedia contents in P2P networks.
2) efficient traitor tracing of illegal redistributors through a standard database search.
3) privacy preservation and buyer frameproofness.
4) mutual anonymity for merchant and buyers and between peer buyers.
5) collusion resistance.
6) avoidance of fingerprint embedding except for a few seed buyers.
7) avoidance of (complex) homomorphic (or any type of public-key) encryption of the multimedia content. Further research can be focused on developing a proof of concept of this proposal on a real distribution scenario.

Principal
CMR INSTITUTE OF TECHNOLOGY
Kandlakoya (V), Medchal Road,
Hyderabad-501 401.