**LITERATURE SURVEY**

**ABSTRACT:** "Mona: Secure Multi-Owner Data Sharing for Dynamic Groups in the Cloud,"

**TITLE:** Cloud imposes low maintenance and allows distribution data to be shared with multiple users. Distribution of data among multiple users imposes ownership constraint on data usage. Unfortunately, sharing data in a multi-owner manner while preserving data and identity privacy from an untrusted cloud is still a challenging issue, due to the frequent change of the membership. In this project, we propose a secure sharing of data among multiple-owners for dynamic groups in the cloud. By leveraging group signature and dynamic broadcast encryption techniques, any cloud user can anonymously share data with others. Meanwhile, the storage overhead and encryption computation cost of our scheme are independent with the number of revoked users.

**ABSTRACT:** "Cryptographic Cloud Storage"

**TITLE:** We consider the problem of building a secure cloud storage service on top of a public cloud infrastructure where the service provider is not completely trusted by the customer. We describe, at a high level, several architectures that combine recent and non-standard cryptographic primitives in order to achieve our goal. We survey the benefits such an architecture would provide to both customers and service providers and give an overview of recent advances in cryptography motivated specifically by cloud storage.

**ABSTRACT:** "P2B: Privacy Preserving Identity-Based Broadcast Proxy Re-Encryption,"

**TITLE:** This paper proposes Privacy Preserving Identity-Based Broadcast Proxy Re-encryption (P2B) - a scheme to provide privacy preserving in identity-based broadcast proxy re-encryption. P2B uses Lagrange interpolation polynomial theorem to provide privacy to identities of the receiver group of broadcasted re-encrypted ciphertext. Proxy re-encryption is an efficient solution to securely share cloud data with receivers. For sharing data with a group of receivers, the sender needs to regenerate the re-encryption key for every receiver, which leads to an overhead on the sender side. To solve the issue, identity-based proxy re-encryption is extensible to identity-based broadcast proxy re-encryption. However, the later poses a privacy issue on the receiver side, as each receiver of the receiver group needs to know the other receiver's identity. We solve the problem using the Lagrange interpolation method. We prove that our scheme is secure against chosen plaintext attack using random oracle model and it successfully hides the identities of the receivers. Finally, we implement P2B and compare it with other existing systems. It is seen that P2B reduces the decryption time by 68% than recent existing Broadcast proxy re-encryption schemes and 98% than the existing privacy preserving schemes.

**ABSTRACT:** "Identity-Based Encryption Transformation for Flexible Sharing of Encrypted Data in Public Cloud,"

**TITLE:** With the rapid development of cloud computing, an increasing number of individuals and organizations are sharing data in the public cloud. To protect the privacy of data stored in the cloud, a data owner usually encrypts his data in such a way that certain designated data users can decrypt the data. This raises a serious problem when the encrypted data needs to be shared to more people beyond those initially designated by the data owner. To address this problem, we introduce and formalize an identity-based encryption transformation (IBET) model by seamlessly integrating two well-established encryption mechanisms, namely identity-based encryption (IBE) and identity-based broadcast encryption (IBBE). In IBET, data users are identified and authorized for data access based on their recognizable identities, which avoids complicated certificate management in usual secure distributed systems. More importantly, IBET provides a transformation mechanism that converts an IBE ciphertext into an IBBE ciphertext so that a new group of users not specified during the IBE encryption can access the underlying data. We design a concrete IBET scheme based on bilinear groups and prove its security against powerful attacks. Thorough theoretical and experimental analyses demonstrate the high efficiency and practicability of the proposed scheme.

**ABSTRACT:** “Achieving Secure, Scalable,and Fine-Grained Data Access Control in Cloud Computing,”

**TITLE:** 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.

**ABSTRACT:** "Cloud-Assisted Attribute-Based Data Sharing with Efficient User Revocation in the Internet of Things

**TITLE:** Nowadays, the development of the Internet of Things (IoT) has received much attention from both industry and academia. Sensors and devices connected to the IoT network can conveniently gather and collect information for further usage and analysis by IoT users. However, a large quantity of data produced by IoT devices contain sensitive information, which leads to many challenging security issues in IoT systems. The most important one is how to efficiently and securely share IoT data with valid IoT users while forbidding others from obtaining the data. In this article, we propose a cryptographic method to protect the privacy of IoT data while maintaining the functionality of efficient data sharing and user revocation. Our solution relies on a revocable attribute-based encryption (ABE) scheme to encrypt IoT data. The ABE technique makes fine-grained access control available on the encrypted IoT data, while the revocation technique makes invalid users unable to access future encrypted IoT data. To alleviate the issue of resource limitation of IoT devices, we involve a cloud-assisted data sharing and user revocation technique. Finally, we experimentally tested our scheme, and the performance evaluation results demonstrate the practice of our solution scheme.

**ABSTRACT:** "Efficient and privacy-aware attribute based data sharing in mobile cloud computing

**TITLE:** In the era of cloud computing, it is convenient to share large-scale data among various kinds of users. As a kind of attribute-based encryption, ciphertext-policy attribute-based encryption (CP-ABE) is a potential technique for realizing fine-grained access control on shared data. However, traditional CP-ABE is not suitable for mobile cloud computing, where mobile users are resource-limited and privacy is fragile. In this paper, we propose an efficient and privacy-aware attribute-based data sharing system supporting offline key generation and offline encryption. In the proposed system, sensitive attribute values specified in an access structure are not explicitly sent along with a ciphertext. The online/offline encryption mechanism alleviates the computational burden of mobile users by performing most of encryption tasks without draining the battery. In addition, the online/offline key generation mechanism allows the attribute authority to finish most of operations in the key generation process in advance, which enables efficient mobile user registration. Finally, the proposed system is proven fully secure in the standard model and performance analysis shows its effectiveness in mobile cloud computing.

**ABSTRACT:** "Anonymous and Traceable Group Data Sharing in Cloud Computing,"

**TITLE:** Group data sharing in cloud environments has become a hot topic in recent decades. With the popularity of cloud computing, how to achieve secure and efficient data sharing in cloud environments is an urgent problem to be solved. In addition, how to achieve both anonymity and traceability is also a challenge in the cloud for data sharing. This paper focuses on enabling data sharing and storage for the same group in the cloud with high security and efficiency in an anonymous manner. By leveraging the key agreement and the group signature, a novel traceable group data sharing scheme is proposed to support anonymous multiple users in public clouds. On the one hand, group members can communicate anonymously with respect to the group signature, and the real identities of members can be traced if necessary. On the other hand, a common conference key is derived based on the key agreement to enable group members to share and store their data securely. Note that a symmetric balanced incomplete block design is utilized for key generation, which substantially reduces the burden on members to derive a common conference key. Both theoretical and experimental analyses demonstrate that the proposed scheme is secure and efficient for group data sharing in cloud computing.

**ABSTRACT:** "Group Signatures,"

**TITLE:** A **group signature scheme** is a method for allowing a member of a group to anonymously [sign](https://en.wikipedia.org/wiki/Digital_signature) a message on behalf of the group. The concept was first introduced by [David Chaum](https://en.wikipedia.org/wiki/David_Chaum) and Eugene van Heyst in 1991. For example, a group signature scheme could be used by an employee of a large company where it is sufficient for a verifier to know a message was signed by an employee, but not which particular employee signed it. Another application is for [keycard](https://en.wikipedia.org/wiki/Keycard) access to restricted areas where it is inappropriate to track individual employee's movements, but necessary to secure areas to only employees in the group.

**ABSTRACT:** "Short Signature from the Weil Pairing"

**TITLE:** This paper proposes a short signature scheme, the security of which is based on the hardness of discrete logarithms. The main advantage of this signature scheme over DSA signature schemes is a one fourth reduction in the signature length, as well as in the verification computation. Moreover, we provide a close reductionist security proof for existential unforgeability under adaptive chosen-message attacks in random oracle model, offering better security guarantees than existing discrete-log based signatures. The new scheme is needed in low-bandwidth communication, low-storage and less computation environments, and is particularly suited for smart card, PDA and mobile phone.