Provably Secure Key-Aggregate Cryptosystemswith Broadcast Aggregate Keys for Online DataSharing on the Cloud

ABSTRACT:

Online data sharing for increased productivity and efficiency is one of the primary requirements today for any organization.The advent of cloud computing has pushed the limits of sharing across geographical boundaries, and has enabled a multitude of usersto contribute and collaborate on shared data. However, protecting online data is critical to the success of the cloud, which leads to therequirement of efficient and secure cryptographic schemes for the same. Data owners would ideally want to store their data/files onlinein an encrypted manner, and delegate decryption rights for some of these to users, while retaining the power to revoke access at anypoint of time. An efficient solution in this regard would be one that allows users to decrypt multiple classes of data using a single key ofconstant size that can be efficiently broadcast to multiple users. Chu et al. proposed a key aggregate cryptosystem (KAC) in 2014 toaddress this problem, albeit without formal proofs of security. In this paper, we propose CPA and CCA secure KAC constructions thatare efficiently implementable using elliptic curves and are suitable for implementation on cloud based data sharing environments. Welay special focus on how the standalone KAC scheme can be efficiently combined with broadcast encryption to cater to m data usersand m0 data owners while reducing the reducing the secure channel requirement from O(mm0) in the standalone case to O(m + m0).

EXISTING SYSTEM:

- Current technology for secure online data sharingcomes in two major flavors - trusting a third party auditor, or using the user's own key to encrypt her data whilepreserving anonymity.
- This system is popularly known as the key-aggregate cryptosystem (KAC), and derives its roots from the seminal work on broadcast encryption by Boneh et.al..
- KAC may essentially be considered as a dual notion of broadcast encryption. In broadcast encryption, a single ciphertext is broadcast among multiple users, each of whom may decrypt the same using their own individual private keys. In KAC, a single aggregate key is distributed among multiple users and may be used to decrypt ciphertexts encrypted with respect to different classes. For broadcast encryption, the focus is on having shorter ciphertexts and low overhead individual decryption keys, while in KAC, the focus is in having short ciphertexts and low overhead aggregate keys.

DISADVANTAGES OF EXISTING SYSTEM:

- The cloud is susceptible to privacy and security attacks, that are a major hindrance to its wholesome acceptance as the primary means of data sharing in todays world.
- This scheme is not practically deployable for two major reasons. Firstly, the number of secret keys would grow with the number of data classes. Secondly, any user revocation event would require Alice to entirely re-

encrypt the corresponding subset of data, and distribute the new set of keys to the other existing valid users.

- This makes the scheme inefficient and difficult to scale.
- Since the decryption key in public key cryptosystems is usually sent via a secure channel, smaller key sizes are desirable.
- Moreover, resource constrained devices such as wireless sensor nodes and smart phones cannot afford large expensive storage for the decryption keys either.
- Firstly, no concrete proofs of cryptographic security for KAC are provided by the authors.
- Secondly, the scheme does not explicitly address the issue of aggregate key distribution among multiple users. In a practical data sharing environment with millions of users, it is neither practical nor efficient to depend on the existence of dedicated one-to-one secure channels for key distribution. A public key based solution for broadcasting the aggregate key among an arbitrarily large number of users is hence desirable.

PROPOSED SYSTEM:

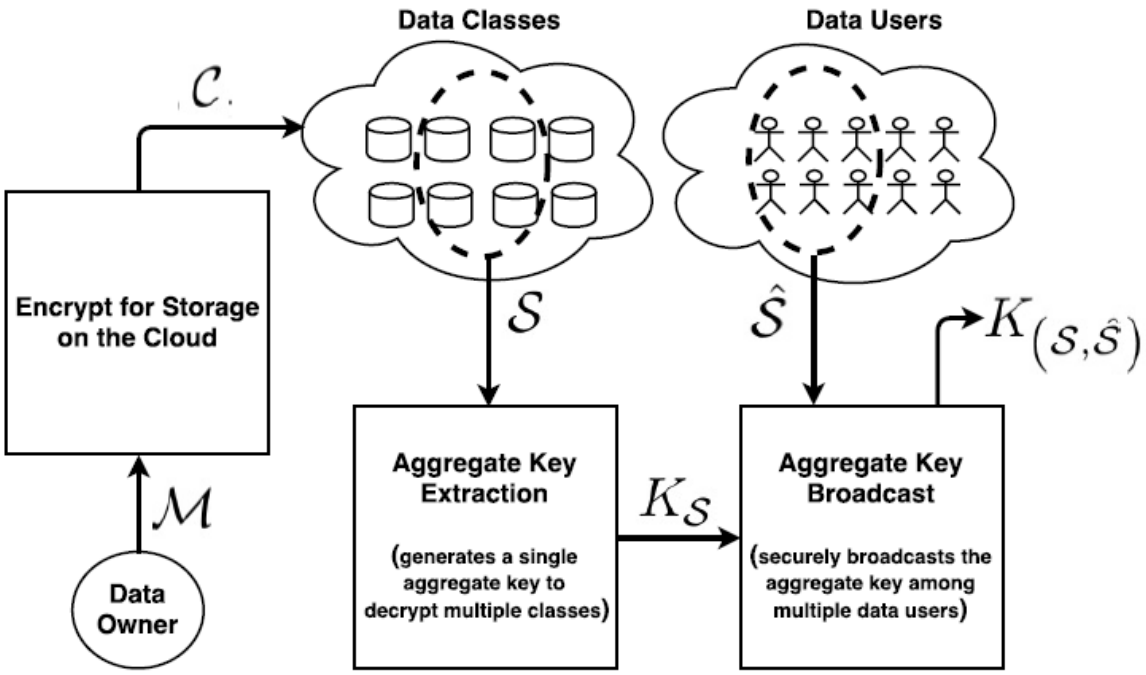
- In this paper, we attempt to build precisely such a data sharing framework that is provably secure and at the same time, efficiently implementable.
- In this paper we propose an efficiently implementableversion of the basic key-aggregate cryptosystem(KAC) using asymmetric bilinearpairings.
- We propose a CCA-secure fully collusion resistantconstruction for the basic KAC scheme with lowoverhead ciphertexts and aggregate keys.

- We demonstrate how the basic KAC frameworkmay be efficiently extended and combined withbroadcast encryption schemes for distributing theaggregate key among an arbitrary number of datausers in a real-life data sharing environment. Theextension has a secure channel requirement ofO(m + m0) for m data users and m0 data owners.
- In addition, the extendedconstruction continues to have the same overheadfor the public parameters, ciphertexts and aggregatekeys, and does not require any secure storage for theaggregate keys, which are publicly broadcast.

ADVANTAGES OF PROPOSED SYSTEM:

- We prove our construction to be semantically secure against a non-adaptive adversary in the standard model under appropriate security assumptions.
- We also demonstrate that the construction is collusion resistant against any number of colluding parties.
- To the best of our knowledge, this is the first KAC construction in the cryptographic literature proven to be CCA secure in the standard model.

SYSTEM ARCHITECTURE:



SYSTEM REQUIREMENTS:

HARDWARE REQUIREMENTS:

- System : Pentium Dual Core.
- Hard Disk : 120 GB.
- Monitor : 15'' LED
- Input Devices : Keyboard, Mouse
- Ram : 1 GB

SOFTWARE REQUIREMENTS:

- Operating system : Windows 7.
- Coding Language : JAVA/J2EE
- Tool : Netbeans 7.2.1
- Database : MYSQL

REFERENCE:

SikharPatranabis, YashShrivastava and DebdeepMukhopadhyaym, "Provably Secure Key-Aggregate Cryptosystemswith Broadcast Aggregate Keys for Online DataSharing on the Cloud", **IEEE Transactions on Computers, 2017.**