April 17, 2018

Shared document access control using keystores

Emmanuel M. Arriaga

Shared document access control using keystores

ABSTRACT

User-generated content, e.g., documents, media, etc. is often created and shared over online document creation and file-hosting services. One technique to restrict access to shared documents is to specify a list of individuals with whom a document is to be shared. Current services do not address the scenario, frequent within enterprise settings, in which a document is made accessible to different groups of individuals based on their rank and clearance levels.

Techniques of this disclosure encrypt shared documents such that access is granted to individuals in possession of a certain key. Certain documents, e.g., sensitive documents intended for view only by top management, are associated one set of keys, while documents viewable by more employees have a different set of keys. Document access retains the single-step simplicity of create-and-share techniques. Access is selectively provided to users based on the key provided.

KEYWORDS

- Document encryption
- Keystore
- Cloud hosting
- Cloud storage
- Document management

BACKGROUND

Current online file-hosting and document creation services may not natively encrypt stored documents. Users share documents with each other via online file creation and hosting services that maintain lists of individuals with whom each document is shared. Some services

also enable sharing of documents via a link, e.g., URL, such that anyone in possession of the link can access the shared documents. Documents that are downloaded from a file-hosting service are unencrypted and does not include password protection. In the context of enterprise use, individual documents are encrypted and protected with passwords or other forms of authentication, in addition to sharing.

DESCRIPTION

This disclosure describes techniques that can be implemented by online file creation and hosting services to provide encryption of stored content. Per techniques of this disclosure, a public key is associated with each document or file, e.g., text files, spreadsheets, presentations, images, etc., stored on the file-hosting service. When a document is shared with a user, the public key is provided to the user. For example, a keystore is created for the receiving user where this type of information resides. When a document is shared publicly, the file-hosting service decrypts the document to enable broader access. The existence and use of encryption keys is implemented in a manner that does not require any user action, and is invisible to end users.

For enterprise users, shared keystores are set up for enterprise documents. These keystores can be managed and are accessible to approved employees. Differing levels of access restrict individual documents to select users.

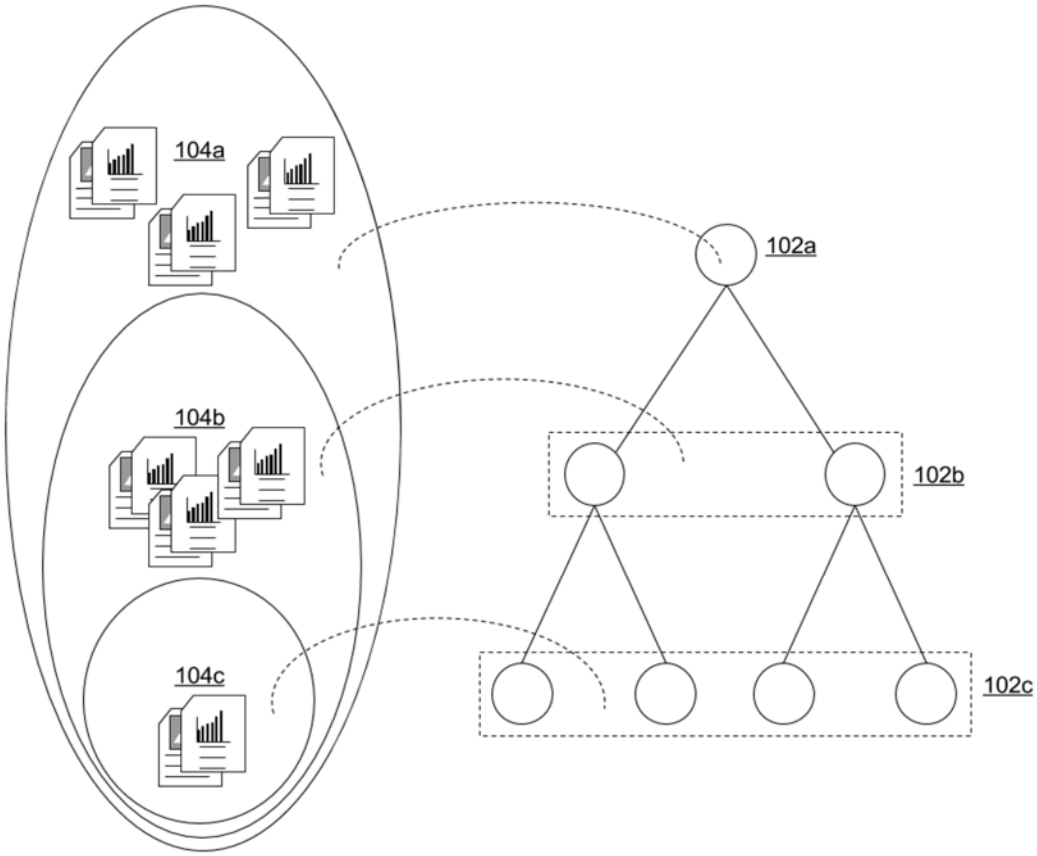

Fig. 1: Keystores that enable varying levels of access

Fig. 1 illustrates document encryption by an online file-hosting service for users that are members of an enterprise. Approved users, e.g., top management (102a) of an organization, are provided with keys that enable access to all documents/media of an organization, e.g., documents within set 104a that includes subsets 104b and 104c. Other users such as middle management (102b) and other employees (102c) are provided keys that enable access to a smaller set of documents (104b) and a restricted set of documents (104c) respectively.

The techniques described herein support arbitrary subsets of documents/media with corresponding key management for each subset, e.g., as illustrated in Fig. 2.

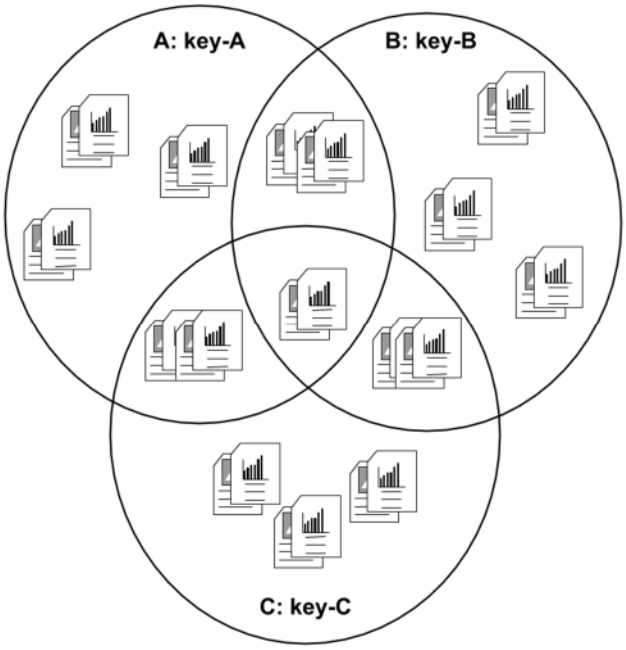

Fig. 2: Access to arbitrary subsets of documents using keystores

As illustrated in Fig. 2, the set of documents in each of sets A, B and C are accessed using respective keys- key-A, key-B and key-C. Further restrictions can be defined such that a document in the set A∩B is accessible only to users with both key-A and key-B, a document in A∩B∩C is accessible only to users with key-A, key-B, and key-C, etc. In a similar manner, a key can be defined for any subset of documents, e.g., a key can be defined to restrict access to the setA− A∩B (documents of set A that don't also belong to set B), etc.

In this manner, multiple keystores can be set up corresponding to groups, areas, or domains that users are granted access to. Even when users have general access to a shared storage space, e.g., for a team, the users are restricted from access to content of sensitivity level higher than permitted by their credentials. Management of these keystores is restricted to administrator users.

For a file-hosting service in a non-enterprise context, one implementation is to have two keystores: one that stores keys for public access, and one stores keys for private document

ownership. Transferring ownership of a document transfers ownership of the private key. Default keystores with limited encryption are provided by the file-hosting service, with increasing levels of encryption and/or keystore management being made available upon request by the user.

Implementations described herein provide access control without the need for a document-specific password. Access to a document is granted based on whether a user has the requisite keys in their keystore. In this manner, encryption is made transparent to the user even as data is secured against unauthorized access. A document that is exported or downloaded from the file-hosting service is encrypted automatically, e.g., using password protection.

CONCLUSION

Techniques of this disclosure automatically encrypt documents/media within a file-hosting service such that document access is enabled via cryptographic keys. Keystores are established for user accounts such that team members can access only documents to which they possess the key. For example, in an organizational hierarchy, upper management may be associated with keys to all documents, whereas lower management may possess keys to a smaller subset of documents. In this manner, encryption is made transparent to the user even as data is secured against unauthorized access. A document that is exported or downloaded from the file-hosting service is encrypted automatically, e.g., using password protection.