Paper Summary for

Decentralized Access Control With Anonymous Authentication of Data Stored in Clouds.

5120519008 郭平雷

Security is becoming a very important issue in cloud computing. Just like normal web applications has user and authentication, user and authentication are also important concepts in cloud computing. But due to the distributed nature of cloud computing, normal authentication methods may not apply to it directly. So this paper addressed a method that can store user credentials in distribution system, and allow user to be authenticated anonymously.

Most traditional authentication methods store user credentials in a central server and the cloud storage is not encrypted, so the cloud storage provider would be able to know the real data the user is storing in their server. This is a big security issue. However, when data is encrypted, it is hard to share and transform the data. This paper provided its authentication based on ssh. Which is solve the transform problem, is not realistic for normal users., especially for windows users.

By using ssh, the part for encrypt and transport is already very mature. So the paper

mainly focus on key generation and keystore. And this comes up with another issue of

their theory, they need an or many authenticated departments to give the key to users as their identity, the users must provide their identity card or social health care number when they acquire keys. This is a very vulnerable step. First, the author assumed those departments can be trusted, however, fake identity card and the corruption in government departments make them hard to trust. Second, since all the user get keys from these trusted departments, they became the new centralized nodes in the distributed system, and if they got attacked, it will harm the whole system. Third one is that the user is not truly anonymous, since the government knows who they are when they give them the key. However, in many cases, people want to be anonymous just because of the governments, like they want to report corruption in security department, people in that department will notice and track them down in a second. The paper do said in distributed systems no one should be trusted without validation, however they think government can be trusted. The ideal distributed system should not rely on government. Since most governments are proven to be a big threat to personal privacy, like NSA.

Besides the issue with government, the part for search is also ignored in this paper, it does say it can match exact words when search, but it does not provide ways for showing people meta data or vague search. If user want to list a directory he stored, or search a keyword that got some typo. This method won’t help, since everything is encrypted and the cloud storage provider does not know anything. There are already many paper talking about the issue, how to search content when they are encrypted. Maybe authors in this paper does not take this as main concern.

In general, the theory in this paper put too many trust in government and neglect some important part in normal user’s usage. It might be very useful for some special situations, like reporting activities to government anonymously. But still have a long way to go for real world applications.