Secure Authentication in Cloud Big Data with Hierarchical Attribute Authorization Structure

ABSTRACT

The concept of the big data has been widely concerned among researchers. Nowadays, utilizing the big data to obtain valuable information has become an important trend. The primary goal of the big data research is to process large amounts of data to obtain significant information. Furthermore, in a long-term perspective, an appropriate approach for the big data processing is very critical [1][2]. However, it is unable to use a single computer or server to deal with the big data. Therefore, the distributed structure is particularly important in the construction of the big data.

EXISTING SYSTEM

In the cloud big data security assurance community, several access control schemes have been proposed, which mainly focus on the attribute-based encryption (ABE) to design the schemes. In the attribute-based access control system, only users with attributes that satisfy the access policy can access the cloud big data. In fact, users' attributes are distributed by the authority and the access policy is defined by the data owner. It is worth noting that only one authority in the system is not enough in real world circumstances. In order to improve the security and management efficiency, the method of multiple authorities is put forward to design big data access control schemes. At the same time, a number of hierarchical authorization structures are also presented, which can be used in organizations or companies to meet the requirement of authorization grant right decentralization. In the hierarchical access control system, the root authority distributes security parameters and attributes to domain authorities. After that, domain authorities will distribute the security parameters and attributes to users or sub-domain authorities.

DISADVANTAGES

- ➢ In the attribute-based access control system, only users with attributes that satisfy the access policy can access the cloud big data.
- ➢ In fact, users' attributes are distributed by the authority and the access policy is defined by the data owner.

PROPOSED SYSTEM

In this paper, we propose a secure authentication protocol for cloud big data with a hierarchical attribute authorization structure. Our proposed protocol resorts to the tree-based signature to significantly improve the security of attribute authorization. To satisfy the big data requirements, we extend the proposed authentication protocol to support multiple levels in the hierarchical attribute authorization structure. Security analysis shows that our protocol can resist the forgery attack and replay attack. In addition, our protocol can preserve the entities privacy. Comparing with the previous studies, we can show that our protocol has lower computational and communication overhead.

ADVANTAGES

- We present a secure authentication protocol for the two-level hierarchical attribute authorization structure in the cloud big data access control system to authenticate authorities or users.

- In order to meet big data application requirements, we extend the protocol to support multiple levels authentication in the hierarchical attribute authorization structure.

- With the tree-based secure signature, our protocol can provide security properties of forgery attack resistance, replay attack resistance and privacy preservation.

SYSTEM REQUIREMENTS

- **H/W System Configuration:-**

Processor	-	Pentium –IV
RAM	-	4 GB (min)
Hard Disk	-	20 GB
Key Board	-	Standard Windows Keyboard
Mouse	-	Two or Three Button Mouse
Monitor	-	SVGA

- **S/W System Configuration:-**

Operating System	:	Windows 7 or 8 32 bit
Application Server	:	Tomcat5.0/6.X

- Backend coding : Java
- Tool : Virtual Box
- Environment : Ubuntu
- Technology : Hadoop