Optimizing Share Size in Efficient and Robust Secret Sharing Scheme for Big Data

ABSTRACT

Big Data is becoming a new era in data exploration. The amount of data is increasing exponentially and thus, a numerous applications such as cloud or distributed storage system, are introduced to reduce the burden of data management for data owners. However, along with the data utilization of such systems, there are a lot of security challenges in which the most common threats are the data leakage and destruction. To protect against the threats, secret sharing scheme is an ideal method which has been used more popularly in distributed systems.

EXISTING SYSTEM

Secret sharing scheme has been applied commonly in distributed storage for Big Data. It is a method for protecting outsourced data against data leakage and for securing key management systems. The secret is distributed among a group of participants where each participant holds a share of the secret. The secret can be only reconstructed when a sufficient number of shares are reconstituted. Although many secret sharing schemes have been proposed, they are still inefficient in terms of share size, communication cost and storage cost; and also lack robustness in terms of exact-share repair.

DRAWBACKS

- The secret can only be reconstructed when there are enough number of shares combining together.
- Each share cannot be used alone to extract meaningful information.

PROPOSED SYSTEM

we propose a new secret sharing scheme based on Slepian-Wolf coding. Our scheme can achieve an optimal share size utilizing the simple binning idea of the coding. It also enhances the exact-share repair feature whereby the shares remain consistent even if they are corrupted. We show, through experiments, how our scheme can significantly reduce the communication and storage cost while still being able to support direct share repair leveraging lightweight exclusive-OR (XOR) operation for fast computation.

ADVANTAGES

- Proposed Scheme can achieve an optimal share size utilizing the simple binning idea of the coding.
- Enhances the exact-share repair feature whereby the shares remain consistent even if they are corrupted.

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