Privacy-Preserving Data Encryption Strategy for Big Data in Mobile Cloud Computing

ABSTRACT

Privacy has become a considerable issue when the applications of big data are dramatically growing in cloud computing. The benefits of the implementation for these emerging technologies have improved or changed service models and improve application performances in various perspectives. However, the remarkably growing volume of data sizes has also resulted in many challenges in practice.

EXISTING SYSTEM

Despite many benefits of using mobile cloud computing, there are great concerns in protecting data owners' privacy during the communications on social networks or mobile apps[11]. One of the privacy concerns is caused by unencrypted data transmissions due to the large volume of data[12][13]. Considering an acceptable performance level, many applications abandon using cipher texts in mobile cloud data transmissions[14]. This phenomenon can result in privacy leakage issues since plain texts are unchallenging for adversaries to capture information in a variety of ways, such as jamming, monitoring, and spoofing [15]. This privacy issue is exigent because it faces to a contradiction between the security levels and performance that is usually attached to timing constraints.

DRAWBACKS

- The privacy concerns is caused by unencrypted data transmissions due to the large volume of data.
- This privacy issue is exigent because it faces to a contradiction between the security levels and performance that is usually attached to timing constraints.

PROPOSED SYSTEM

In this paper, we concentrate on privacy and propose a novel data encryption approach, which is called Dynamic Data Encryption Strategy (D2ES). Our proposed approach aims to selectively encrypt data and use privacy classification methods under timing constraints. This approach is designed to maximize the privacy protection scope by using a selective encryption strategy within the required execution time requirements. The performance of D2ES has been evaluated in our experiments, which provides the proof of the privacy enhancement.

ADVANTAGES

- Concentrate on privacy.
- selectively encrypt data and use privacy classification methods under timing constraints.

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