# Revocable Identity-Based Access Control for Big Data with Verifiable Outsourced Computing

## ABSTRACT

Big data and big data analytics have a wide range of applications, such as biology [1], social sciences [2], smart grid [3], digital forensics [4], [5], and Internet of Things (IoT) [6]. For example, in a smart grid, 22 gigabytes of data could be generated by the smart grid each day from its two million customers at one utility according to the estimation reported [7]. The knowledge mined from this big dataset can not only enhance the efficiency and reliability of the legacy grid, but also inform the strategies undertaken by the utility company to enhance consumer interaction [3].

## EXISTING SYSTEM

In general, data authenticity and confidentiality can be achieved using secure signature and encryption schemes, respectively. To collectively provide confidentiality, integrity, non-repudiation and authentication, one can use the conventional "signature-then-encryption" strategy, which allows the sender to sign a message prior to encrypting the signed message. However, this approach is not fit-for-purpose in a big data environment which requires real-time and large-scale data processing. Signcryption is one of several promising techniques to simultaneously achieve big data confidentiality and authenticity. However, signcryption suffers from the limitation of not being able to revoke users from a large-scale system efficiently.

## DRAWBACKS

- Signature-then-encryption approach is not fit-for-purpose in a big data environment which requires real-time and large-scale data processing.
- Signcryption suffers from the limitation of not being able to revoke users from a large-scale system efficiently.

## PROPOSED SYSTEM

In our Proposed system the first identity-based (ID-based) signcryption scheme with efficient revocation as well as the feature to outsource unsigncryption to enable secure big data communications between data collectors and data analytical system(s). Our scheme is designed to achieve end-to-end confidentiality, authentication, non-repudiation, and integrity simultaneously, while providing scalable revocation functionality such that the overhead demanded by the private key generator (PKG) in the key-update phase only increases logarithmically based on the cardiality of users. Although in our scheme the majority of the unsigncryption tasks are outsourced to an untrusted cloud server, this approach does not affect

the security of the proposed scheme. We then prove the security of our scheme, as well as demonstrating its utility using simulations.

## ADVANTAGES

- identity-based (ID-based) signcryption scheme with efficient revocation.
- Our scheme is designed to achieve end-to-end confidentiality, authentication, non-repudiation, and integrity

## 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