**Cost-Effective Authentic and Anonymous Data**

**Sharing with Forward Security**

**ABSTRACT**

Data sharing has never been easier with the advances of cloud computing, and an accurate analysis on the shared data provides an array of benefits to both the society and individuals. Data sharing with a large number of participants must take into account several issues, including efficiency, data integrity and privacy of data owner. Ring signature is a promising candidate to construct an anonymous and authentic data sharing system. It allows a data owner to anonymously authenticate his data which can be put into the cloud for storage or analysis purpose. Yet the costly certificate verification in the traditional public key infrastructure (PKI) setting becomes a bottleneck for this solution to be scalable. Identity-based (ID-based) ring signature, which eliminates the process of certificate verification, can be used instead. In this paper, we further enhance the security of ID-based ring signature by providing forward security: If a secret key of any user has been compromised, all previous generated signatures that include this user still remain valid. This property is especially important to any large scale data sharing system, as it is impossible to ask all data owners to reauthenticate their data even if a secret key of one single user has been compromised. We provide a concrete and efficient instantiation of our scheme, prove its security and provide an implementation to show its practicality..

**EXISTING SYSTEM**

User uploading the data to a third party platform such as Microsoft Hohm. From the collected data a statistical report is created, and one can compare their energy consumption with others (e.g., from the same block). This ability to access, analyze, and respond to much more precise and detailed data from all levels of the electric grid is critical to efficient energy usage.

at this point Datacenter ’s signature is ambiguous and so C will not be convinced of anything at all by seeing it. We see that the tendering process is immune to abuse by A. Adding forward security to it can further improve the security protection level. With forward security, the key exposure of either party does not affect the e-contracts previously signed

**PROPOSED SYSTEM:**

Data sharing with a large number of participants must take into account several issues, including efficiency, data integrity and privacy of data owner. Ring signature is a promising candidate to construct an anonymous and authentic data sharing system. It allows a data owner to anonymously authenticate his data which can be put into the cloud for storage or analysis purpose. Yet the costly certificate verification in the traditional public key infrastructure (PKI) setting becomes a bottleneck for this solution to be scalable. Identity-based (ID-based) ring signature, which eliminates the process of certificate verification, can be used instead. In this paper, we further enhance the security of ID-based ring signature by providing forward security: If a secret key of any user has been compromised, all previous generated signatures that include this user still remain valid. This property is especially important to any large scale data sharing system, as it is impossible to ask all data owners to reauthenticate their data even if a secret key of one single user has been compromised. We provide a concrete and efficient instantiation of our scheme, prove its security and provide an implementation to show its practicality.

**MODULE DESCRIPTION:**

# Number of Modules:

After careful analysis the system has been identified to have the following modules:

1. Authentication.
2. Data sharing.
3. Cloud computing.
4. Identity-based Ring Signature
5. Forward security,.
6. Smart grid.

# Authentication,

Authentication is the act of confirming the truth of an attribute of a single piece of data (datum) or entity. In contrast with [identification](http://en.wikipedia.org/wiki/Identity_document) which refers to the act of stating or otherwise indicating a claim purportedly attesting to a person or thing's identity, authentication is the process of actually confirming that identity. It might involve confirming the identity of a person by validating their [identity documents](http://en.wikipedia.org/wiki/Identity_document), verifying the validity of a Website with a [digital certificate](http://en.wikipedia.org/wiki/Public_key_certificate), tracing the age of an artifact by [carbon dating](http://en.wikipedia.org/wiki/Carbon_dating), or ensuring that a product is what its packaging and labeling claim to be. In other words, authentication often involves verifying the validity of at least one form of identification.

# data sharing:

Data sharing is the practice of making data used for scholarly research available to other investigators. Replication has a long history in science. The motto of The Royal Society is 'Nullius in verba', translated "Take no man's word for it."[[1]](http://en.wikipedia.org/wiki/Data_sharing#cite_note-1) Many funding agencies, institutions, and publication venues have policies regarding data sharing because transparency and openness are considered by many to be part of the [scientific method](http://en.wikipedia.org/wiki/Scientific_method).

A number of funding agencies and science journals require authors of [peer-reviewed](http://en.wikipedia.org/wiki/Peer_review) papers to share any supplemental information (raw data, statistical methods or source code) necessary to understand, develop or [reproduce](http://en.wikipedia.org/wiki/Reproducibility) published research. A great deal of scientific research is not subject to data sharing requirements, and many of these policies have liberal exceptions. In the absence of any binding requirement, data sharing is at the discretion of the scientists themselves. In addition, in certain situations agencies and institutions prohibit or severely limit data sharing to protect proprietary interests, national security, and subject/patient/victim confidentiality. Data sharing may also be restricted to protect institutions and scientists from use of data for political purposes.

Data and methods may be requested from an author years after publication. In order to encourage data sharing and prevent the loss or corruption of data, a number of funding agencies and journals established policies on [data archiving](http://en.wikipedia.org/wiki/Scientific_data_archiving).

# Cloud computing.

cloud computing is a computing term or metaphor that evolved in the late 2000s, based on utility and consumption of computer resources. Cloud computing involves deploying groups of remote servers and software networks that allow different kinds of data sources be uploaded for real time processing to generate computing results without the need to store processed data on the cloud.

**Identity-based Ring Signature**

private or hybridIdentity-based (ID-based) cryptosystem, introduced by Shamir , eliminated the need for verifying the validity of public key certificates, the management of which is both time and cost consuming. In an IDbased cryptosystem, the public key of each user is easily computable from a string corresponding to this user’s publicly known identity (e.g., an email address, a residential address, etc.). A private key generator (PKG) then computes private keys from its master secret for users. This property avoids the need of certificates (which are necessary in traditional public-key infrastructure) and associates an implicit public key (user identity) to each user within the system. In order to verify an ID-based signature, different from the traditional public key based signature, one does not need to verify the certificate first. The elimination of the certificate validation makes the whole verification process more efficient, which will lead to a significant save in communication and computation when a large number of users are involved (say, energy usage data sharing in smart-grid).

# Forward security,

In cryptography, forward secrecy (FS; also known as perfect forward secrecy, or PFS) is a property of key-agreement protocols ensuring that a session key derived from a set of long-term keys cannot be compromised if one of the long-term keys is compromised in the future.

Even worse, the “group" can be defined by the adversary at will due to the spontaneity property of ring signature: The adversary only needs to include the compromised user in the “group" of his choice. As a result, the exposure of one user’s secret key renders all previously obtained ring signatures invalid (if that user is one of the ring members), since one cannot distinguish whether a ring signature is generated prior to the key exposure or by which user. Therefore, forward security is a necessary requirement that a big data sharing system must meet. Otherwise, it will lead to a huge waste of time and resource. While there are various designs of forward-secure digital signatures adding forward security on ring signatures turns out to be difficult. As far as the authors know, there are only two forward secure ring signature schemes . However, they are both in the traditional public key setting where signature verification involves expensive certificate check for every ring member. This is far below satisfactory if the size of the ring is huge, such as the users of a Smart Grid.

# Smart grid

A **smart grid** is a modernized electrical **grid** that uses analog or digital information and communications technology to gather and act on information - such as information about the behaviours of suppliers and consumers - in an automated fashion to improve the efficiency, reliability, economics, and sustainability of the We implement the Smart Grid example introduced in Section 1, and evaluate the performance of our IDFSRS scheme with respect to three entities: the private key generator (PKG), the energy data owner (user), and the service provider (data center). In the experiments, the programs for three entities are implemented using the public cryptographic library MIRACL , programmed in C++. All experiments were repeated 100 times to obtain average results shown in this paper, and all experiments were conducted for the cases of jNj = 1024 bits and jNj = 2048 bits respectively. The average time for the PKG to setup the system is shown in Table 4, where the testbed for the PKG is a DELL T5500 workstation equipped with 2.13 GHz Intel Xeon dual-core dual-processor with 12GB RAM and running Windows 7 Professional 64-bit operating system. It took 151 ms and 2198 ms for the PKG to setup the whole system for jNj = 1024 bits and jNj = 2048 bits respectively. The average time for the data owner (user) to sign energy usage data with different choices of n and T are shown in Fig. 3 and 4, for jNj = 1024 bits and jNj = 2048 bits respectively. The testbed for the user is a laptop personal computer equipped with 2.10 GHz Intel CPU with 4GB RAM and running Windows 7 operating system. The average time for the the service provider (data center) to verify the ring signature with different choices.

**System Configuration:**

HARDWARE REQUIREMENTS:

Hardware - Pentium

Speed - 1.1 GHz

RAM - 1GB

Hard Disk - 20 GB

Floppy Drive - 1.44 MB

Key Board - Standard Windows Keyboard

Mouse - Two or Three Button Mouse

Monitor - SVGA

SOFTWARE REQUIREMENTS:

Operating System : Windows

Technology : Java and J2EE

Web Technologies : Html, JavaScript, CSS

IDE : My Eclipse

Web Server : Tomcat

Tool kit : Android Phone

Database : My SQL

Java Version : J2SDK1.5

**CONCLUSION**

Motivated by the practical needs in data sharing, we proposed a new notion called Forward Secure ID-Based Ring Signature. It allows an ID-based ring signature scheme to have forward security. It is the first in the literature to have this feature for ring signature in ID-based setting. Our scheme provides unconditional anonymity and can be proven forward-secure unforgeable in the random oracle model, assuming RSA problem is hard. Our scheme is very efficient and does not require any pairing operations. The size of user secret key is just one integer, while the key update process only requires an exponentiation. We believe our scheme will be very useful in many other practical applications, especially to those require user privacy and authentication, such as ad-hoc network, e-commerce activities and smart grid. Our current scheme relies on the random oracle assumption to prove its security. We consider a provably secure scheme with the same features in the standard model as an open problem and our future research work