JETIR.ORG ISSN: 2349-5162 | ESTD Year : 2014 | Monthly Issue
JOURNAL OF EMERGING TECHNOLOGIES AND INNOVATIVE RESEARCH (JETIR)
An International Scholarly Open Access, Peer-reviewed, Refereed Journal

IDENTITY-BASED SIGNATURES IN CLOUD COMPUTING

[1] K.Satyanarayana Asst.Professor(C)
Dept. of CSE,UCE,
Osmania University,Hyderabad.
Satya0401@yahoo.com

[2] Prof.S.Ramachandram,
Dept. of CSE,UCE,
Osmanaia University,Hyderabad.
schandram@gmail.com

Abstract

Identity-based cryptography (IBC) has gained popularity in recent years due to its lack of need for public-key certificate maintenance overhead. However, an unresolved but important problem regarding IBC is how to revoke a misbehaving user. Identity-based encryption (IBE) systems with revocable keys have recently been suggested, but little work has been done on the revocation issue of identity-based signatures so far. Revocation in identity-based settings may be accomplished by having the key generation centre refresh users' private keys regularly (KGC). Nevertheless, as the number of users grows, the strain on the KGC will grow much faster. We provide an efficient RIBS method that outsources the revocation operation to a cloud revocation server in this paper (CRS). Most of the calculations required during important updates are offloaded to the CRS in our suggested method. It is shown that the proposed method is existentially unforgeable in the random oracle model against adaptively selected messages and identity attacks, and we explain the new framework and security model for it. This system has reduced calculation and transmission costs than earlier IBS schemes, as well. To ensure that certificates are valid and up-to-date, certificate authorities (CAs) are in charge of all of these activities.

1. Introduction

1.1 Introduction

The public key in identity-based cryptosystems, on the other hand, is derived from the user's identification information. Revocation of an account is difficult to prove. For all non-revoked users, we recommended that the KGC regularly update secret keys. Many identity-based encryption systems include revocation capabilities by using this concept. There are two problems with their plan, though (Yi et al. 2021). In the first place, the KGC must remain operational, which poses certain security risks. Second, when the number of users grows, the KGC's overhead will soar. Many businesses are turning to cloud computing, which is rapidly evolving, to outsource computing jobs.

1.2 Research questions

One of the reasons for this is that smart grids enhance efficiency, reliability, affordability, and substantiality of energy services compared to conventional power networks. Enel's Telegestore initiative in Italy considered the first commercial use of smart grid technology, saves the country around 500 million Euros annually. Several additional smart grid initiatives have been suggested in the wake of Telegestore's success. Some of these initiatives are located across the globe, including Hydro One in Canada, EvoraInovGrid in Portugal, and the Modellstadt Mannheim (Moma) project in Germany (Zhu et al. 2021). Smart grids provide many advantages for electrical power networks, however, they are only deployed in a few places at a time. Smart grids are hampered by several issues, one of which is the handling of information gathered throughout the deployment process. A smart grid information management framework based on cloud computing technology has been developed as a result of earlier research and is described in this article as Smart-Frame.

1.3 Research objectives

There are three hierarchical levels in our framework: top, regional, and end-user. The first two levels are made up of cloud computing centres; the third level is made up of smart devices used by end-users. When it comes to controlling devices and accumulating data across regional cloud computing centres, the top cloud computing centre is responsible (Le et al. 2021). However, when it comes to particular areas (such as inside a city), the regional cloud computing centres are in charge of doing both.

1.4 Research significance

Regional clouds' information storage may re-encrypt sensitive data received from end-user devices using an identity-based re-encryption method, allowing the end-user services to decrypt and handle the data without compromising the cloud storages' private keys. Using identity-based encryption instead of digital certificates, which rely on conventional PKI (Public Key Infrastructure), we can save a substantial amount of computing and communication resources while also solving scalability problems. The money saved by not using digital certificates in the big data environment is huge (AlidadiShamsabadi et al. 2021). Electricity service efficiency, reliability, economics, and sustainability may all be improved with a smart grid. It's a critical part of today's energy system. Most difficult for smart grids to handle is the massive quantity of data generated by front-end intelligent equipment such as power assets and smart metres, as well as how to analyse it. There are many positive characteristics of cloud computing that make it an excellent option for dealing with these problems, including energy and cost savings, agility, scalability and flexibility.

2. Literature review

Shamir proposed the idea of identity-based encryption, which Boneh and Franklin quickly implemented. IBE does away with the need for a public key infrastructure to be provided (PKI). Any IBE or PKI setup should include a method for removing users from the system after their authorization has expired or the secret key to their account has been revealed. The issue of certificate revocation has been explored extensively in the conventional PKI context, and various solutions have gained widespread acceptance, such as the use of a certificate revocation list or the addition of validity periods to certificates (Sundaresan et al. 2021). Revocation in the context of IBE has been the subject of very little research. To offer various kinds of computing services for information management and big data analysis, our framework builds a hierarchical structure of cloud computing centres. Beyond the structural framework, we offer an identity-based cryptography solution that addresses the major security concerns of the proposed framework through signature and proxy re-encryption. Smart grids have several security flaws as a result of their widespread use. Because a security breach in a smart grid may result in significant financial loss, efforts are being made to solve the security issues that arise in these kinds of systems (Hamid et al. 2021). The focus here is on an identity-based key agreement mechanism that uses RSA primitives rather than our own. Identity-based key agreement protocol construction in a broad grid computing environment is the primary goal of our study, which is focused on providing a security framework for our Smart-Frame based on identity-based encryption/signature and proxy re-encryption methods.

3. Methodology

In reality, using a third party to do computationally intensive operations is not uncommon in the history of cryptography. Key-updating duties were delegated to a Key Update Cloud Server Provider (KU-CSP), and an identity-based encryption (IBE) method was suggested. Instead of following their lead, we've taken their method and applied it to IBS situations. It's a simple concept: put all of your key-update work on the cloud server. However, there are a few security concerns to keep in mind: the cloud server cannot rely upon 100% of the time. In other words, we divided a user's signing key into two parts: an initial identification key and time-update key Long-term keys are tied to the user's identity and are granted by the KGC, whereas short-term keys are tied to the identity of the user and are only valid for a limited period. A wide variety of digital signature schemes with various characteristics have been developed for various purposes and have been thoroughly researched in the literature. Using identity-based signature (IBS) methods, a user's digital public key may be effectively mapped to his or her actual identity (e.g., e-mail address). Current IBS methods, however, are not intended for white-box security (WBS), in particular for the protection of the private key when special attackers have complete access to the execution environment (Chia et al. 2021). The first white-box implementation of Shamir's classic IBS method is proposed in this article. For the most part, the plan calls for using a mathematical transformation to hide the original private key throughout the execution process while embedding it into a specific table. Using identity registration, any framework components that need to transmit or receive data may have their identities registered. Before sending data to the cloud storage, smart metres, intelligent sensors and other front-end devices, for example, must first register their identities with the service. But before they can receive or provide information to one other, cloud computing components and services must first register their identities. The signature calculation table of the encryption algorithm is given below. A private key is created for the registered component when an identity is registered. Encrypting data before it is transmitted over the network is done via data encryption. Before transmitting the data, the sender often encrypts it using the recipient's identity as the key. This method maintains the security of data since only the intended recipient has access to the private key that can be used to decode it. However, a receiver of ciphertext uses data decryption to recover the original data from the previously encrypted ciphertext.

Index	Value
1	X1 = h1(ID)^x1
2	X2 = h2(ID)^x2
...	...
i	Xi = hi(ID)^xi
...	...
λ-1	Xλ-1 = hλ-1(ID)^xλ-1
λ	Xλ = hλ(ID)^xλ

Table 1: The signature calculation table of the encryption algorithm is given above.

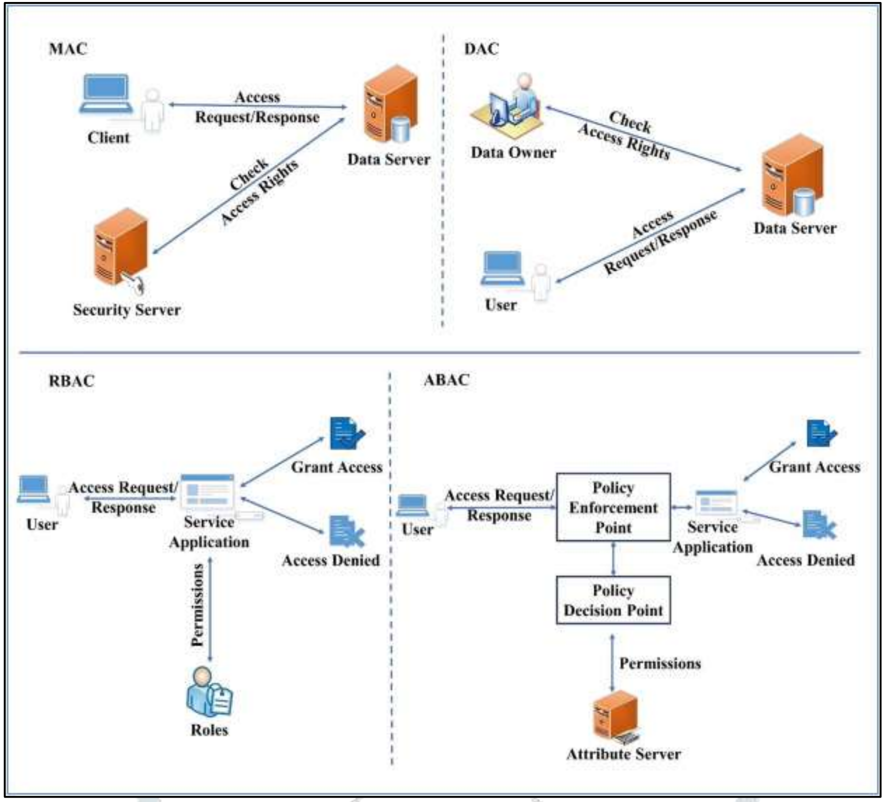

Fig 1: The Identity-based signatures in cloud computing architecture

(Source: Yi et al. 2021)

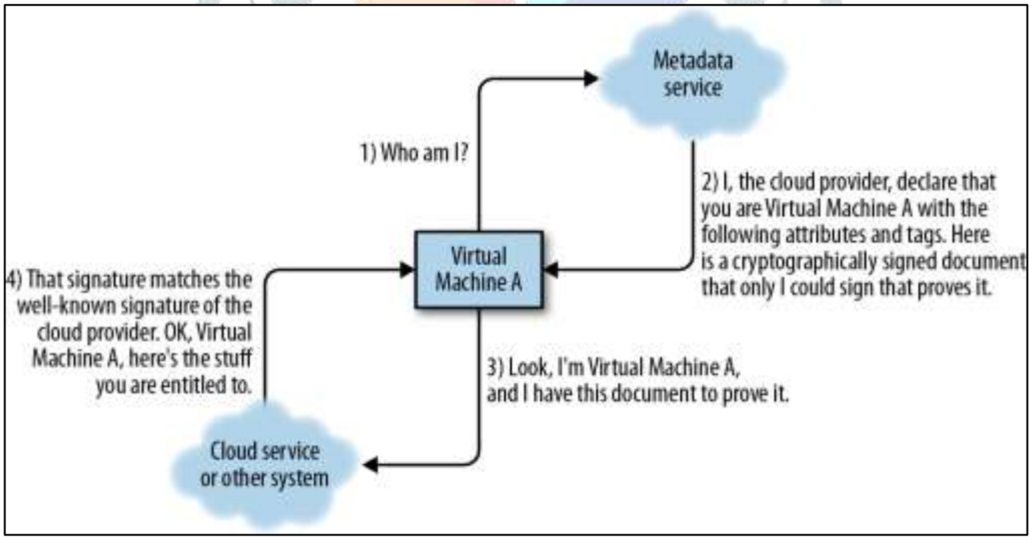
Metadata
service
1) Who am I?
2) I, the cloud provider, declare that
you are Virtual Machine A with the
following attributes and tags. Here
is a cryptographically signed document
that only I could sign that proves it.
Virtual
Machine A
4) That signature matches the
well-known signature of the
cloud provider. OK, Virtual
Machine A, here's the stuff
you are entitled to.
3) Look, I'm Virtual Machine A,
and I have this document to prove it.
Cloud service
or other system

Fig 2: The Service login System implementing Identity-based signatures in cloud computing

(Source: Le et al. 2021)

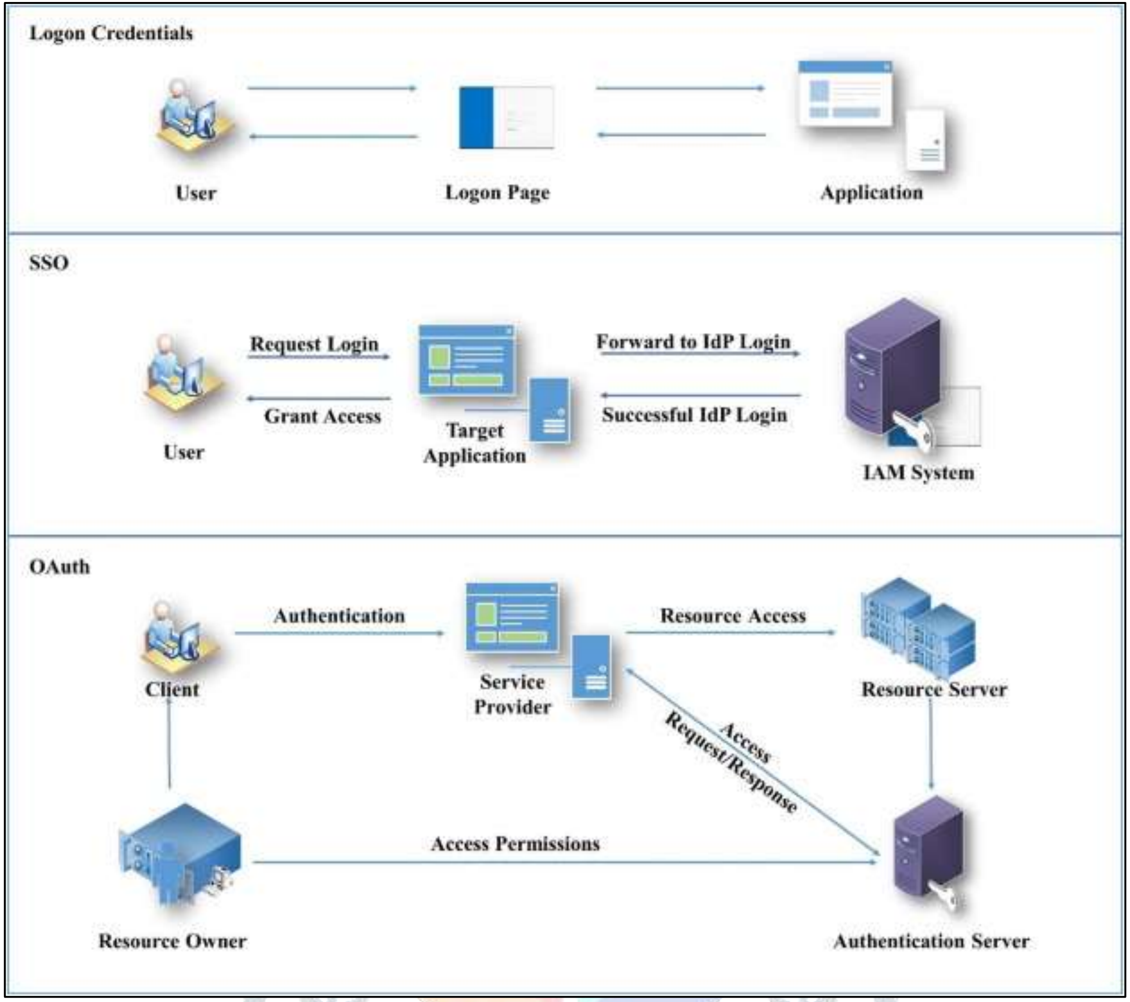

Fig 3: The Client to Customer Relation and the Authentication Procedure Implementing Identity-based signatures in cloud computing

(Source: Sundaresan et al. 2021)

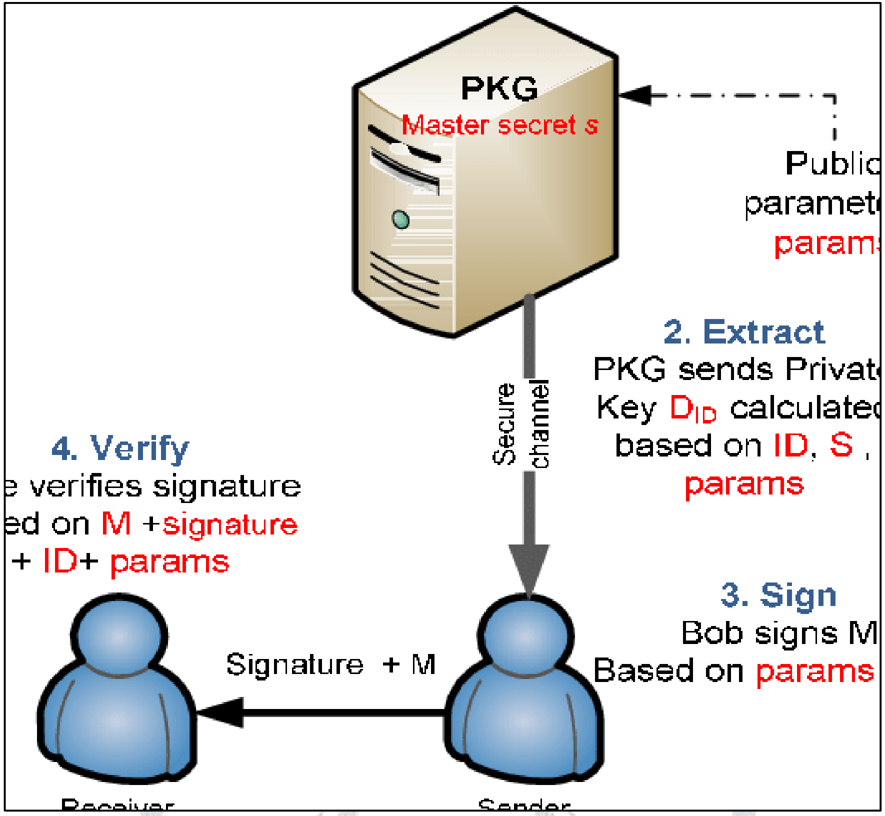

Fig 4: The Encryption Procedure Employed by the Identity-based signatures in cloud computing

(Source: Patel& Patel, 2021)

4. Discussion and analysis

A cloud revocation server (CRS) issues and updates the time update key regularly. Because it lacks the full signing key, the CRS is unable to forge a signature. KGC tells the cloud server to cease providing time update keys for revoked users when a request is made. Many current IBS systems may be made revocable using this approach. The use of smart grids to replace conventional power networks has lately gained traction in the electronic grid repair plans of several nations. Aside from that, we offer an identity-based encryption and signature solution as well as identity-based proxy re-encryption for the general framework (Patel& Patel, 2021). Because smart grid information is so sensitive, it's critical to provide it with information security to keep it safe. Because stolen information may be used to launch attacks on both people and the whole smart (power) grids at the national level, leaks in smart grids can lead to vulnerabilities that impact not just individuals but the entire country. Essentially, we want to make it possible for all parties involved, such as top and regional cloud computing centres and end-users, to utilise their identities as encryption keys or signature verification keys to represent themselves in the Smart-Frame. These identities may be used by the lower-level entities to encrypt their data and communicate securely with the higher-level entities.

5. Conclusion

5.1 Conclusion

One of our key concepts is the creation of three hierarchical tiers of cloud computing centres to better handle information: top, regional, and end-user. While each regional cloud centre is responsible for processing and maintaining regional data, the top cloud level offers a global perspective on the framework.

5.2 Recommendations

In addition, we have proposed a method based on identity-based cryptography and identity-based proxy re-encryption to enable framework security. Thus, our framework's scalability, adaptability, and security are all enhanced. Our system has a basic identity-based data confidentiality management built as a proof-of-concept.

References

AlidadiShamsabadi, F., &BakhtiariChehelcheshmeh, S. (2021). A cloud-based mobile payment system using identity-based signature providing key revocation. *The Journal of Supercomputing*, 1-25.

Chia, J., Chin, J. J., & Yip, S. C. (2021). A Pairing-Free Identity-Based Identification Scheme with Tight Security Using Modified-Schnorr Signatures. *Symmetry*, *13*(8), 1330.

Hamid, M. S., Babu, S., &Pitchai, R. (2021). Secure identity-based proxy re-encryption techniques for the healthcare system. *Materials Today: Proceedings*.

Le, H. Q., Vo, B., Duong, D. H., Susilo, W., Le, N. T., Fukushima, K., &Kiyomoto, S. (2021). Identity-based Linkable Ring Signatures from Lattices. *IEEE Access*.

Patel, M., & Patel, R. (2021). Improved identity-based encryption System (IIBES): A mechanism for eliminating the key-escrow problem. *Emerging Science Journal*, *5*(1), 77-84.

Sundaresan, A., Vinod, M., Nair, S. M., &Rajalakshmi, V. R. (2021). Enabling Identity-Based Data Security with Cloud. In *Computer Networks and Inventive Communication Technologies* (pp. 513-522). Springer, Singapore.

Yi, P., Li, J., Liu, C., Han, J., Wang, H., Zhang, Y., & Chen, Y. (2021). An efficient identity-based signature scheme with provable security. *Information Sciences*, *576*, 790-799.

Zhu, H., Wang, Y., Wang, C., & Cheng, X. (2021). An efficient identity-based proxy encryption using lattice. *Future Generation Computer Systems*, *117*, 321-327.