International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Index Copernicus Value (2013): 6.14 | Impact Factor (2014): 5.611

# Survey on Distributed Mobile Cloud Computing Services: Signature Scheme for a Privacy-Aware Authentication

**Chaitali P. Kathar[1], Vidya Dhamdhere[2]**

[1]Pune University, G.H.R.C.E.M, Wagholi, Pune, Maharashtra, India

[2]Professor, Pune University, G.H.R.C.E.M, Wagholi, Pune, Maharashtra, India

**Abstract:** ***In recent societies, the number of mobile users has tremendously risen in recent years. The paper provides security and use for mobile users to access different mobile cloud computing services from multiple service providers using only a single private key. In this paper, we propose a new short signature scheme from the bilinear pairings. However, our scheme is represented from Inverse Computational Diffie-Hellman Problem (Inv-CDHP) based on bilinear pairing and does not require any hash function. We give the exact security proofs for the new signature scheme and the ring signature scheme in the model.***

**Keywords:** Cloud computing, Bilinear pairings, Authentication scheme, Mobile cloud computing services, Short signature

## 1. Introduction

The market of mobile phones has increased rapidly. According to the premier global market firm, the large worldwide Smartphone market increased by 42.5% year over year in the first quarter of 2013. The increse of mobility has changes our lives in an succeed way. Although there have been many papers discussing the complexity of every pairings and how to speed up the pairing computation [1,2], the computation of the pairing still remains time-consuming.

A user authentication scheme for mobile users in distributed cloud services environment should maintain the following benefits.

- The authentication scheme is on some efficient cryptosystems to show mutual authentication and user anonymity without using SSL.
- A trusted third party is required for user registration and service provider registration, but it is not required to participate in user authentication session later.
- A user can access mobile services from multiple service providers with only one private key.
- The authentication scheme does not require large computation operations on users' mobile devices.

In Asiacrypt 2001, Boneh, Lynn, and Shacham [3], proposed a short signature scheme using bilinear pairing on certain elliptic and hyperelliptic curves. They proposed a new short signature scheme of the bilinear pairings that unlike BLS scheme, uses general cryptographic hash functions such as SHA-1 or MD5, and does not require any special hash functions.
In 1984, Shamir asked for identity(ID)-based encryption and signature schemes to solve key management procedures of certificate-based public key infrastructures (PKIs). It is useful in situations where the validity of a signature must not be verifiable. For example, a software vendor might want to embed signatures into his products and allow only payed customers to check the authenticity of these products.

## 2. System View

- Cloud computing is an evolving paradigm with various momentums, but its unique aspects security and privacy challenges. It explores the roadblocks and its solutions to providing a trustworthy cloud computing environment.
- Despite increased usage of mobile computing, exploiting it is difficult due to its inherent problems such as resource scarcity, disconnections, frequent and mobility. Mobile cloud computing can solve these problems by executing mobile applications on resource providers to the mobile device. In this paper, they provide a survey of mobile cloud computing research, while the specific views in mobile cloud computing. They represent a taxonomy based on the key issues in this area, and discuss the different approaches taken to tackle these issues. They conclude the paper with a critical research of challenges that have not yet been met, and highlight directions for future work.
- Address the problem of QoS-guaranteed secured service provisioning in MCNs. They design maximization problem for quality-assured secured load sharing (QuaLShare) in MCN, and show its minimum solution using auction theory. In QuaLShare, the overloaded gateway finds the misbehaving gateways, prevents them from participated in the auction process. Theoretically, we characterize both the problem and the solution approaches in an MCN environment. Finally, they searched the existence of Nash Equilibrium of the scheme. They extend the solution for the case of multiple users, followed by theoretical analysis. Numerical analysis establishes the correctness of the proposed algorithms.
- There is various business view for the cloud computing application on mobile internet. But combined cloud computing technology into mobile internet gives birth to a series of security problems. One of the challenges is to construct the cloud computing secure architecture on mobile internet. After analyzing the cloud computing security risks and secure architectures, and taking into account the characteristics of mobile internet, this paper

designs a general secure cloud computing architecture on mobile internet with the advantages such as multi-hierarchy, multi-level, cross-platform and unified user interface.

- The rise of authenticating solutions based on RADIUS servers questions the complexity of their administration whose security and confidentiality are often an error especially with Cloud Computing architectures. More specifically, it raises the concern of server administration in a secure environment for both the granting access company and its users. This paper aims to resolve this issue by proposing an innovative paradigm based on of smart cards built on a context of SSL smart cards. They believe that EAP-TLS server smart cards offer the security and the simplicity required for an administration based on distributed servers. They represented the design of a RADIUS server in which EAP messages are fully processed by SSL smart cards. They present the scalability of this server links to smart card grids whose distributed computation manages the concurrence of numerous authenticating sessions. Lastly, they relate the details of the first experimental results obtained with the RADIUS server and an array composed of 32 Java cards, and demonstrate the feasibility and prospective scalability of this architecture.

## 3. Related Work

- Authentication is very significant mechanism in computer network systems for preventing unauthorized network access.
- The illustration presented in figure 3 conveys that the authentication for the cloud users can be done either by the cloud service provider or the service provider can outsource the identity management and authentication service Bilinear pairing

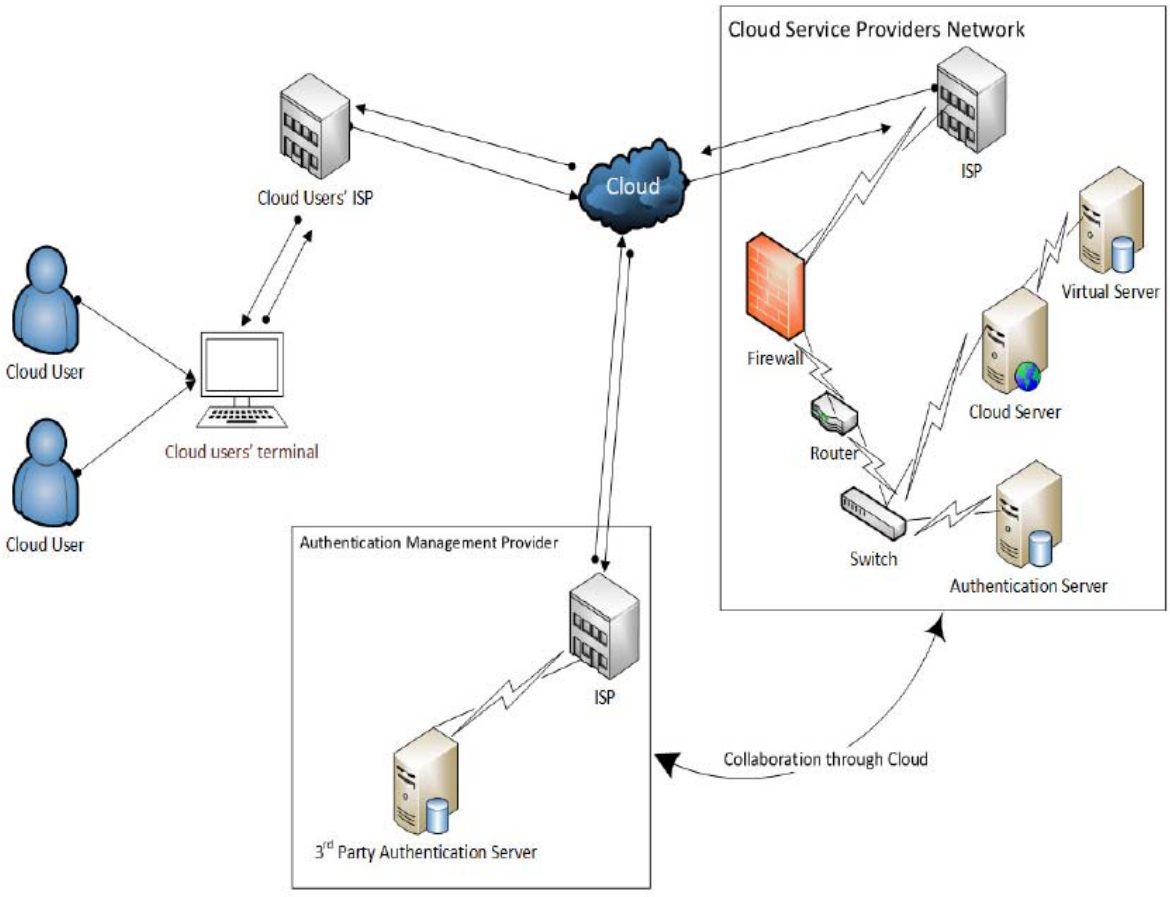


**Figure 3:** Authentication in the Cloud

The bilinear pairings namely the Weil pairings or Tate pairings may be used in main applications of cryptography and allowed us to construct identity (ID)-based cryptographic schemes. Suppose < G1; + > be an additive cyclic group of order q generated by P, where q is prime and < G1; _ >a multiplicative cyclic group of same order as of G1. We define a mapping e : G1 _ G1 ! G2, called a bilinear mapping if it satisfies the following properties:

In this paper, we propose a new short signature scheme from the bilinear pairings. A signature scheme consists of the following four algorithms : a parameter generation algorithm ParamGen, a key generation algorithm KeyGen, a signature generation algorithm Sign and a signature verication algorithm Ver.

Bilinear property $e(aP,bQ) = e(P,Q)^{ab}$, for all $P,Q \in G_1$ and $a,b \in Z_q^*$

Non-degeneracy property There exist $P,Q \in G_1$ such that $e(P,Q) \neq 1_{G_2}$

Computability property There exists an efficient algorithm to compute $e(P,Q)$, for all $P,Q \in G_1$.

**Advantages**

- **Short signature**-Short signatures are required in low-bandwidth communication environments. An relevant application of partially blind signature is in e-cash system. E-coins are stored in users' electronic wallets Which are typically implemented in smart cards with limited memory. The short length of the proposed signature makes the system much more practical.
- **Performance**-We can see that the verification is most important and the signing is least expensive assuming the pairing computation costs several times expensive than a point multiplication
- **Security**- Several security schemes for data sharing on untrusted servers have been proposed [12], [13], [14]. In these approaches, data owners store the encrypted data files in untrusted storage and distribute the corresponding decryption keys to authorized users.

## 4. Conclusion and Future Work

We demonstrated how to achieve digital signatures cryptosystem. In this paper, we focus on a signature scheme that is more important than BLS scheme. It has proposed a new anonymous authentication scheme for distributed cloud services environment. Our proposed scheme provides a possible way to fight against immoral interference with the right of privacy. We hope more schemes can be created to protect cloud user privacy.
In our future approach, the parties encrypt their arbitrarily partitioned data and upload the cipher texts to the cloud.

## 5. Acknowledgment

We would like to thank all the authors of different research papers referred during writing this paper. It was very knowledge gaining and helpful for the further research to be done in future.

## References

[1] P.S.L.M. Barreto, H.Y. Kim, B.Lynn, and M.Scott, E_cient algorithms for pairing-based cryptosystems, Advances in Cryptology-Crypto 2002, LNCS 2442, pp.354-368, Springer- Verlag, 2002.
[2] S. D. Galbraith, K. Harrison, and D. Soldera, Implementing the Tate pairing, ANTS 2002, LNCS 2369, pp.324-337, Springer-Verlag, 2002.
[3] D. Boneh, B. Lynn, and H. Shacham, Short signatures from the Weil pairing, InC. Boyd, editor, Advances in Cryptology-Asiacrypt 2001, LNCS 2248, pp.514-532, Springer-Verlag, 2001.
[4] An E_cient Signature Scheme from BilinearPairings and Its Applications Fangguo Zhang, Reihaneh Safavi-Naini and Willy Susilo
[5] A Privacy-Aware Authentication Scheme for Distributed Mobile Cloud Computing Services Jia-Lun Tsai and Nai-Wei Lo IEEE SYSTEMS JOURNAL, VOL. 9, NO. 3, SEPTEMBER 2015
[6] Mobile cloud computing: A survey Niroshinie Fernando∗ , Seng W. Loke ∗ , Wenny Rahayu Future Generation Computer Systems 29 (2013) 84–106
[7] An Improved Remote User Authentication Scheme with Smart Cards using Bilinear Pairings Debasis Giri and P. D. Srivastava
[8] Lamport, L., "Password authentication with insecure communication," Communications of the ACM, Vol. 24, (1981) 770-772.
[9] Wu, T. C., "Remote login authentication scheme based on a geometric approach," Computer Communications, Vol. 18, No. 12, (1995) 959-963.
[10] Hwang, M. S., "A remote password authentication scheme based on the digital signature method," International Journal of Computer Mathematics, Vol. 70, (1999) 657-666.
[11] Hwang, M. S. and Li, L. H., "A new remote user authentication scheme using smart cards," IEEE Transactions on Consumer Electronics, Vol. 46, No. 1, (2000) 28-30.
[12] M. Kallahalla, E. Riedel, R. Swaminathan, Q. Wang, and K. Fu, "Plutus: Scalable Secure File Sharing on Untrusted Storage," Proc. USENIX Conf. File and Storage Technologies, pp. 29-42, 2003.
[13] E. Goh, H. Shacham, N. Modadugu, and D. Boneh, "Sirius: Securing Remote Untrusted Storage," Proc. Network and Distributed Systems Security Symp. (NDSS), pp. 131-145, 2003.
[14] G. Ateniese, K. Fu, M. Green, and S. Hohenberger, "Improved Proxy Re-Encryption Schemes with Applications to Secure Distributed Storage," Proc. Network and Distributed Systems Security Symp. (NDSS), pp. 29-43, 2005.