Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X
IMPACT FACTOR: 5.258

IJCSMC, Vol. 5, Issue. 7, July 2016, pg.436 – 440

Multi Notarized Identity Management in Cloud using Level based Cryptography

V.Prasath[1], R.Buvanesvari[2]

[1]Department of Computer Science, PKIET, Karaikal & Pondicherry University, India

[2]Department of Computer Science, PKIET, Karaikal & Pondicherry University, India

[1] prasathvijayan@gmail.com, [2] itsbuvana@yahoo.in

Abstract— Cloud computing is a recently developed with a new technology for complex systems with massive-scale services sharing among numerous users. Today most cloud computing system use asymmetric and traditional public key cryptography to provide data security and mutual authentication. Federated Identity Management is a secure single sign-on process between each other and it can enable the portability to share their identity across different networks. In this paper, a multi notarized federated identity system together with level-based cryptography for secure transaction management in cloud is implemented. An effective implementation of this notarized federated identity management together with level-based cryptography not only solves the complex problem of secure key sharing but also provide the access to the number of unknown cloud system can mutually authenticate in notary server.

Keywords—cloud computing, federated identity, notarized server, level-based cryptography, single sign on

I. INTRODUCTION

Level-based cryptography is a public key technology that allows the use of a public identifier of a user as the user's public key. It has also some attraction characteristics that seem to fit well the requirements of cloud computing. Currently the majority of cloud computing systems provide digital identity for users to access their services [1].

Unfortunately, the overuse of individual user information in online opens the door to identity theft, which poses a serious threat to personal finances and credit ratings of users and creates liabilities for corporations. Moreover, the increasing dangers of identity theft are negatively affecting people's collective confidence on the digital world for online financial transactions [2].

In web server communication, notary service owned by a trusted third-party to dynamically notarize assertions generated by identity providers has facilitates and provides support for secures transaction management. Additionally feature of this model is the avoidance of direct

communications between identity providers and service providers which improved privacy protection for users [3].

Most of cloud computing, it is important to intend an encryption and signature schemes for the entities to communicate mutually. In order to achieve the secure communication in cloud, one well-known identity management solution that deals with security issue is the single sign-on technique, which requires the user to authenticate only once to a cloud server, and then automatically authenticates the user to other cloud system.

II. SECURITY IN CLOUD COMPUTING

Cloud computing have many advantages in cost reduction, resource sharing, and timesaving for new service deployment. Cloud servers are potentially based at multiple locations and the services provided by the cloud may use different infrastructures across organizations which bring some new challenges for the system, especially security and privacy. All these characteristics of cloud make it complicated to provide security in cloud computing [4].

To ensure adequate security in cloud computing various security issues such as authentication, data confidentiality and integrity and non-repudiation, all need to be taken into account. WS-Security, WS-Trust, and WS-Security Policy provide a basic model for federation between Identity Providers and relying parties. Currently, WS-Security is wildly used in the cloud system to provide security at user level. WS-Federation enables the mechanisms for brokering of identity, attribute discovery and retrieval, authentication and authorization claims between federation partners, and protecting the privacy of these claims across organizational boundaries [5].

III. LEVEL BASED CRYPTOGRAPHY

The level-based hierarchy shows in Fig. 1 includes root setup, lower-level setup, extraction, encryption, and decryption. The root PKG will generate the root PKG system parameters and a root secret. At each lower-level PKG will get the root system parameters and generate its own lower-level secret. This lower-level secret will be used to generate private keys for the users in its domain. A user or PKG at level t with its identity requests his private key from its upper-level PKG, the upper-level PKG will use this identity, system parameters and its own private key to generate a private key for this user. User who wants to encrypt a message M can use the system parameters, receiver's identity and the message and receiver can use system parameters and his private key got from the PKG to decrypt the cipher text. Signing and verification can use parameters, its private key, and message M to generate a digital signature and sends to the receiver. Receiver verifies the signature at end [1].

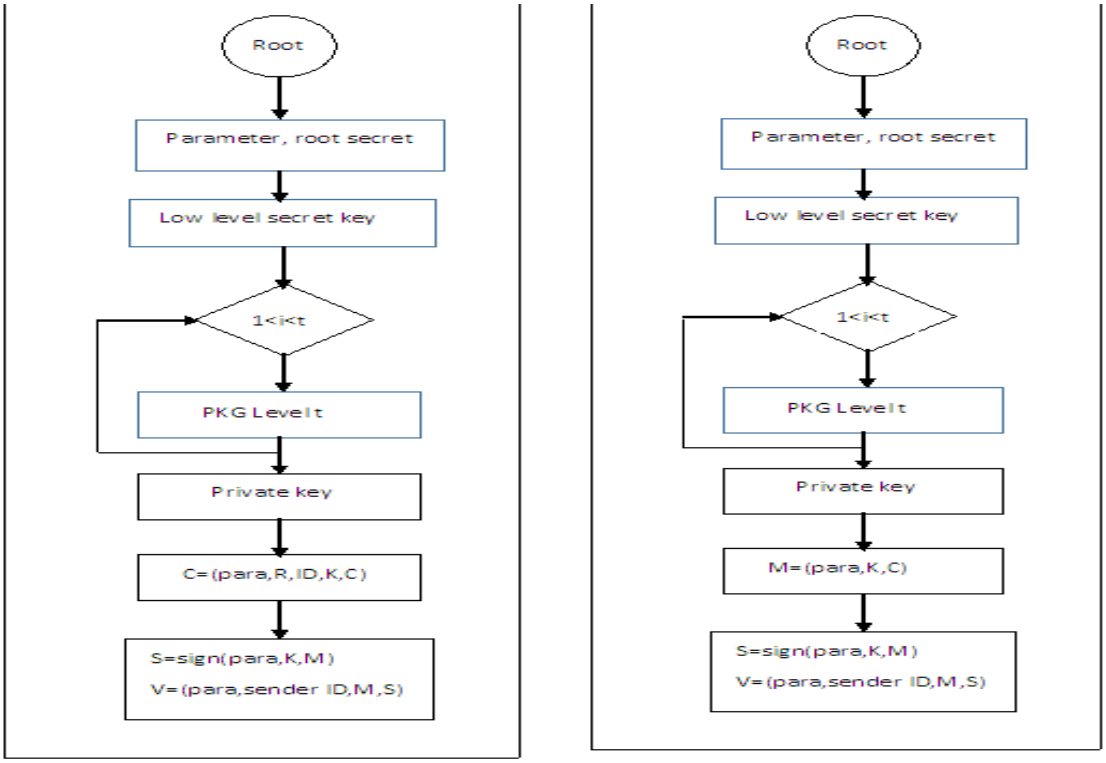

Fig. 1 Encryption and Decryption flow for level based security

IV. PROPOSED ARCHITECTURE

We present the model for multi notarized server management for cloud user. This model has entities such as: a user, a service provider, notarized identity provider and many notary servers. As is well-known, identity provider that supports automatic user authentications when the cloud providers are unknown to each other. In this model, we introduce a notarized identity provider which is owned by a trusted third-party to dynamically notarize assertions generated by identity providers and notarized server. As an extra feature provided by the notarized identity server in single sign on mechanism reduces possible collusions between identity providers and service providers and gives improved privacy protections for users on single sign on authentication by notarized server.

By adopting notarized identity provider together with level-based cryptography, not only solves the key distribution but also mutually authenticate the different cloud provider through notarized server. The notarized identity provider caches the assertions in the common notarized severs even when the users are located in insecure, untrusted locations. Cloud provider can easily identify a forged or tampered assertion so that the integrity of an assertion is maintained. Our system is a concrete solution for a trust broker model proposed by existing federated identity management together with level based cryptography for secure key sharing. Verification is achieved by authenticated dictionary technique. Service provider that provides particular service to user who are authenticated by trusted identity provider and notarized server to communicate the other service provider on single sign on process.

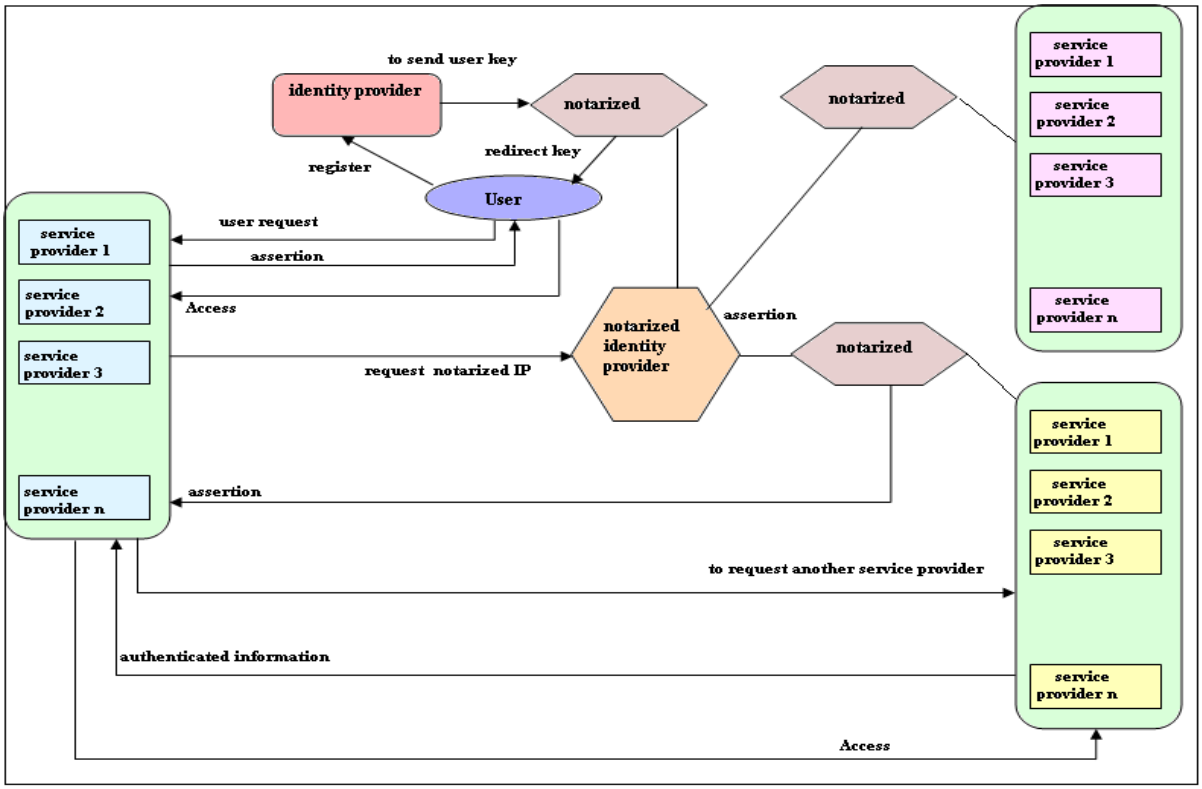

Fig. 2 Architecture for Multi Notarized Server in Cloud

Identity provider authenticates itself to the notary server, and submits the id, assertion, signature to the notarized identity provider. A service provider queries in the notarized identity provider for assertions associated with identity provider and the notary server returns to the notarized identity server. Identity provider focus on authentication through dictionary technique of cloud user as well as managing and sharing identity information with various notarized server to notarized identity server. An assertion that stored on the notary server implies the identity provider that generates the assertion is trustworthy.

The notary server acts as a bridge of trust between Identity providers and notarized Identity provider. Another advantage of storing assertions on the notary server is the prevention of direct contact between identity providers and notarized Identity providers. The operations rule submits and query that the roles of identity provider and service provider are interchangeable. Our multi notarized federated identity model that introduces a notary server and notarized Identity provider a trusted third-party that dynamically maintains assertions generated by identity providers. Assertions are generated by identity providers and stored by the notary server. When a service provider needs to verify an assertion, it queries the notary server for a notarized assertion that shows the trustworthiness of the notarized identity provider.

Once user can register to the Identity Management, then the identity provider, provide the identity to the user and user use this assertion to access the service from service provider. Further user also user can directly authenticated between mutually communicated cloud provider, if user want to access service from unknown cloud by accessing authentication from notarized identity server. User should request to the notarized server request to the assertion from identity provider to communicate from unknown service provider. Notarized server pass

on the assertion to unknown cloud with the help of WS security. User can easily access the service from unknown cloud using single sign-on process through notarized identity server that build by multi notarized server. That the multiple notarized server model not only more efficient but also mutually authenticate on unknown cloud service provider.

V. CONCLUSIONS

In this paper, we present a multi notarized server together with identity provider model for single sign-on process to effectively access the unknown cloud provider. An efficient implementation of multi notarized identity management model based on the level based cryptography provides more advanced way of key sharing in secure communication. The proposed multi notarized Identity server together with level-based cryptography, not only to access number of unknown cloud can provider mutually authenticate between notary servers but also for secret key distribution. That the multiple notarized server model not only be effective and efficient but also mutually authenticate number of unknown cloud provider be simplified in the clouds security.

REFERENCES

[1] Venugopal Gaddam et al, "Protection for Cloud Computing Using Level-Based Cryptograph", International Journal of Computer Science and Information Technologies, Vol. 5 (2), 2014.

[2] J. Breckling,"Cyber Security Industry Alliance". Internet security national survey, No. 2, December 2005. https://www.csialliance.org/StateofCyberSecurity2006/.

[3] Bhargav-Spantzel,A.C.Squicciarini, and E. Bertino. "Establishing and protecting digital identity in federation systems", In Proceedings of the 2005 ACMWorkshop on Digital Identity Management, pages 11–19, November 2005.

[4] Leavitt,N et al, "Is Cloud Computing Really Ready for Prime Time?", Computer 42(1), 15–20 (2009) 166 H.

[5] "Web Services Federation Language (WS-Federation)",December 2006, http://specs.xmlsoap.org/ws/2006 /12/federation/

[6] D. Yao, N. Fazio, Y. Dodis, and A. Lysyanskaya. "ID-based encryption for complex hierarchies with applications to forward security and broadcast encryption". In Proceedings of the ACM Conference on Computer and Communications Security (CCS), pages 354–363. ACM Press, 2004.

[7] M. T. Goodrich, R. Tamassia, and A. Schwerin. "Implementation of an authenticated dictionary with skip lists and commutative hashing". In Proc.2001 DARPA Information Survivability Conference and Exposition,Volume2, Pages68–82, 2001.

