Available online at www.sciencedirect.com

ScienceDirect

Procedia Computer Science 109C (2017) 710–717

Procedia Computer Science

www.elsevier.com/locate/procedia

The 8th International Conference on Ambient Systems, Networks and Technologies (ANT 2017)

Performance Evaluation of Virtual Identity Approaches for Anonymous Communication in Distributed Environments

Ibrahim Gomaa[a,b*], Adel M.Said [b], Emad Abd-Elrahman[b], Alaa Hamdy[a], Elsayed M.Saad[a]

[a] *Faculty of Engineering, Helwan University, Cairo, Egypt.*
[b] *National Telecommunication Institute, 5-Mahmoud El-miligy st., 6th district, Nasr City, Cairo, 11768, Egypt.*

Abstract

Today's enterprises core concept of security is the Identity (ID). When it comes to mapping identity in order to gain access to a specific service or digital account, cloud technology offers the most robust, cost-effective, easy-to-use solutions available. In this paper, the Virtual Identity (V_{ID}) concept is not only used to improve the user privacy and security on the network and service platforms but also, the V_{ID} performance is evaluated by implementing a mathematical model based on Baskett Chandy Muntz-Palacios (BCMP) model. Moreover, a simulation-based evaluation using OPNET Modeler is conducted to compare the simulation results against the analytical model based BCMP queuing analysis. Finally, the comparative study of our proposed models and the related work proves that our proposed models are suitable for anonymous communication in distributed virtual environments.

Peer-review under responsibility of the Conference Program Chairs.

Keywords: Virtual Identity ; Anonymous Communication; Virtual Environments; BCMP theory; IBE; PBE

1. Introduction

Today, keeping one identity for all services is not secure at all; different identities are also a headache for all users. Therefore, the easier way is to keep one main identity and let the trusted network managed or mapped this identity to virtual ones based on the requested service. Moreover, as cloud computing is transforming everything to be virtualized, the identity also will be virtualized in order to keep the user's privacy. In our previous works[1,2], two

* Ibrahim Gomaa. Tel.: +2-010-011-25368; fax: +2-022-263-6802.
E-mail address: igomaa@nti.sci.eg

Peer-review under responsibility of the Conference Program Chairs.
10.1016/j.procs.2017.05.382

novel approaches are proposed for generating virtual identities using Identity Based Cryptography (IBC); the Identity Based Encryption (IBE) and Pseudo Based Encryption (PBE).

Another consideration, particularly regarding securing the services introduced by the cloud providers, is the implementation of out of band and strong authentication mechanisms. Particularly, when sensitive data stored in the cloud, it needs out of band authentication such as a One-Time Password (OTP) to authenticate the user before getting access. Therefore, users should be challenged to authenticate themselves with more than a user ID and password [3-5]. One of the most suitable solutions used to authenticate SaaS applications is IAM (Identity and Access Management) which is used to create, terminate and manage user accounts.

In the previous works[1-2], the IBE and PBE are introduced as two approaches for generating virtual identities by collaboration with the Private Key Generator (PKG). The PKG is the security server entity that is used in generating the IDs that will be used in cloud service access based on the type of service required by the user. It is added as management point for users' login to the service providers. In this framework, each user has one main identity that mapped to virtual ones based on the requested service. Therefore, the user sends to the PKG his/her identity (e.g., user@homeoperator.com) and the requested service name. Then, the PKG creates and uses V_{ID} to generate the user's public and private keys as detailed in the previous work[1]. Accordingly, the shared secret key is generated by the service provider to encrypt the communication in the future.

In this paper, the performance is evaluated for V_{ID} framework by modeling the previously proposed two approaches based on IBE & PBE. Moreover, a simulation-based evaluation using OPNET Modeler is conducted to compare these results against the BCMP queuing analysis as analytical results. The rest of this paper is organized as follows. In section 2, the previous work related to this paper is reviewed. In section 3, the modeling concept for IBE and PBE is described. In section 4, an analytical model is implemented. In section 5, performance evaluation using OPNET Modeler is introduced. Therefore, simulation results and analysis are introduced and discussed. Finally, in section 6, the conclusion is given.

2. Related Work

Various techniques have been proposed to protect the data contents privacy via access control. To the best of our knowledge, the most of the anonymous communication protocols are largely depending on Identity-Based Encryption (IBE), Pseudonym Based Encryption (PBE)[1-2], mixnet protocols[6] and DC-net protocols[7]. Mixnet protocols[8-10] provide anonymous communication path that created by a "mix" of servers. It depends on background traffic statistical properties; therefore mixnet protocols can't provide provable anonymity. The DC-net protocols[11-12] solve the problem of provable anonymity and provide perfect sender anonymity. However, they work based on secure multiparty computation procedures, they suffer from the transmission collision problem[13].

Authors in[14] proposed source anonymous message authentication approach based on the Modified El-Gamal signature (MES) scheme, which is secure against no-message and adaptive chosen message attacks[15].

Work in[16] provided only sender anonymity for anonymous web browsing and multicast services. However, the author in[17] introduced the k-anonymous communication protocol that can provide anonymity for both sender and receiver. The new idea proposed in[18] is to hide senders and receivers messages. In addition, it tries to solve the difficulty of key distribution and communication overhead of k-anonymous communication protocol. Authors in[19] introduced a new approach based on ring signature.

The work in[20] proposed Fuzzy Identity-Based Encryption (FIBE), which considered Attribute-Based Encryption (ABE) scheme as a set of descriptive attributes. In the same work, ABE general schemes are presented such as Key Policy Attribute-Based Encryption (KP-ABE)[21] and Cipher-text-Policy Attribute-Based Encryption (CP-ABE)[22]. Authors in[23] proposed two approaches, AnonyControl and AnonyControl-F to prevent user's identity disclosure and allow cloud servers to control and secure users' access.

Work in[24] defines V_{ID} as a partial identity, in which, the identity is known as pseudonyms generated based on a subset of all user attributes. The EU project Daidalos[25] proposed virtual identity model, in which, the user identity is partitioned on the network layer as well as the application layer. There is specific IP address within a separated network stack assigned to each virtual identity[26]. Network anonymization techniques are proposed by authors in[27] to provide the network layer unlinkability. From the security and privacy perspectives, V_{ID} concept is considered in