IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received February 7, 2019, accepted March 5, 2019, date of publication March 18, 2019, date of current version April 1, 2019.

Digital Object Identifier 10.1109/ACCESS.2019.2904854

Virtual Identity Performance Evaluations of Anonymous Authentication in IDaaS Framework

IBRAHIM GOMAA[1], EMAD ABD-ELRAHMAN[2], ELSAYED SAAD[1], AND ADLEN KSENTINI[3], (Member, IEEE)

[1]Electronics, Communications and Computer Engineering Department, Faculty of Engineering, Helwan University, Cairo 11795, Egypt
[2]Computers and Systems Department, National Telecommunication Institute, Cairo 11768, Egypt
[3]Communication Systems Department, EURECOM, Campus SophiaTech, CS 50193 - 06904 Biot Sophia Antipolis cedex, France

Corresponding author: Ibrahim Gomaa (igomaa@mcit.gov.eg)

This work was supported in part by the Egyptian National Telecommunication Institute (NTI), Cairo, Egypt.

ABSTRACT Identity-as-a-Service (IDaaS) is one of the most famous fruitful authentication services for cloud deployment to the Software-as-a-Service (SaaS) model. It is a third party approach for identity management, including creation, authentication, and privacy assurance. In this paper, the Virtual Identity (V_{ID}), as a new realization for IDaaS terminology which can be used in virtual environments, is proposed to improve the user privacy and to provide the anonymous Single sign-on (SSO) in such types of distributed environments. Actually, two V_{ID} frameworks based on the Identity-Based Encryption (IBE) and Pseudonym-Based Encryption (PBE) approaches are proposed and then implemented using *MIRACL* library. The V_{ID} approaches performance is evaluated analytically by implementing a mathematical model based on *BCMP* (Baskett Chandy Muntz Palacios) queuing model. In addition, a simulation-based evaluation using *OPNET* Modeler is introduced to compare the analytical-based *BCMP* queuing model against the *OPNET* simulation results. Moreover, the proposed approaches are compared against state-of-the-art work.

INDEX TERMS Distributed computing, identity management systems, platform virtualization, analytical models, performance evaluation.

I. INTRODUCTION

Since the era's of cloud computing service models (i.e. IaaS, PaaS, and SaaS) has begun, the Identity management is considered as a dominant challenge. Therefore, the privacy and authentication mechanisms that secure these identities are the key stone for successful real platforms for multi-tenant applications.

The concept of V_{ID} under the global umbrella of IDaaS framework means that the on-demand identity creation is based on the user main identity. So, instead of accessing the services with one identity for all services or many identities for each service, the virtual one that is created based on the requested service is used. This virtual identity is mapped based on the user context in terms of the main identity credential and the requested service by the user for each login. The proposed schemes to access multi-service depend on a third party component as trusted system which is called Private Key Generator (PKG). Users have to declare their main identities to the PKG system and the PKG is responsible for generating the corresponding virtual identity based on the requested service. The first response by the users to the PKG query will include the users credential for accessing specific service. Some familiar contexts that are used in users virtual identities generation are: user main IDs, digital certificates (which contain public keys) and credit cards. An important characteristic of the main identity is that it is public. It is defined by main identity provider for confirming the legitimate owner of this identity that can be used for authentication process in cloud applications.

Different authentication patterns have been analyzed [1] for accessing cloud applications. They mainly include direct authentication pattern, Brokered, Single sign-on (SSO), and federated authentication patterns.

The framework of IDaaS has been addressed by different ways. It depends on the IT challenge and the cloud based applications nature like SaaS. The Identity and Access Management (IAM) [2] is implemented as an on-premises solution for social SSO services and SaaS applications. An identity management system for cloud web services has

The associate editor coordinating the review of this manuscript and approving it for publication was Yilun Shang.

been proposed in [3] as IDaaS model. This proposed system combined the authentication and authorization based access control using some attributes. It used an Attribute Based Access Control (ABAC) mechanism in their cloud web services accessing. That approach is considered as hybrid between two common known SSO models; the Security Assertion Markup Language (SAML) and OAuth protocols. A service-oriented identity management model for web service environments has been considered either for authentication or authorization [4]. The identity management in cloud based services has different perspectives in the digital transformation forecasting challenges [5]. IAM can manage the flexibility and scalability challenges for cloud services deployments including authentication and authorization.

A. WORK CONTRIBUTIONS

The new proposed approaches for V_{ID} are evaluated in distributed virtual environments. The goal of this work is to implement an identity, which could help in preventing the reverse of access chain in the virtualized environment through hiding the main user identity. This means that, instead of executing a service using the user main or common identity, we hope to execute a service with a new generated identity, which is the virtual one (i.e. V_{ID}) as initiated in [6]. For achieving high degree of security and efficiency, the IBE and PBE are designed and implemented based on Elliptic Curve Cryptography (ECC) [7]. Those proposed approaches are implemented, validated and verified using Multi-precision Integer and Rational Arithmetic C/C++ (MIRACL library) [8].

In addition, the performance of both approaches is evaluated under different infrastructure configurations and network conditions through OPNET Modeler [9] as a very dedicated simulation tool. The obtained results show the impact of cloud users and their locations (either remote or local) on the application response time. Moreover, Application Characterization Environment (ACE) whiteboard is used to simulate the overall flow of data across different tiers from start to end of the application task for V_{ID} creation process either based on IBE or PBE [10].

We believe that, the simulation based performance evaluation is not enough to measure the system performance. Moreover, modelling security communication is well known in this domain [11]. Therefore, we support our previous OPNET Modeler simulation by an analytical model, which is investigated based on queuing network principles to evaluate the impacts of the proposed solutions on the virtual infrastructure. The mathematical models are built based on BCMP theory [12] for both IBE & PBE workflows [13] and the validation for different network access conditions is done using MATLAB tool [14]. IBE and PBE can also be used for big data secure access mechanisms when integrated with cloud computing as scalable solution [15]. Finally, this paper is concluded with a detailed comparison between our models and the relevant work.

We can summarize the major contributions of this work as follows:

- Modeling the concept of virtual identity creation either based on IBE or PBE. In particular, we introduce the two mechanisms using ECC.
- Implementing the proposed virtual identity approaches in MIRACL security library.
- Using BCMP queuing network as an analytical model, we conduct the performance evaluation for our two proposals (IBE and PBE).
- Performing a simulation based performance evaluation for the same approaches using OPNET Modeler and comparing our results under different scenarios of cloud computing services access. Then, we compare our solutions against the literature work.

B. PAPER ORGANIZATION

The rest of this work is structured as follows; Section II highlights some relevant works. The problem statement is considered in Section III with modeling concept details for IBE & PBE besides the implementation environment based MIRACL. Section IV introduces the proposed framework for IBE & PBE workflows. Section V presents the performance evaluation results and analysis. Section VI concludes this work with some perspectives.

II. RELATED WORKS

The access control privacy for data contents can be assured using different methodologies. The state of the art algorithms for anonymous communication can be categorized into four types as follows:

- Identity-Based Encryption (IBE) [16],
- Pseudonym Based Encryption (PBE) [17],
- DC-net protocols [18] and
- Mixnet protocols [19], [20], [21], and [22].

The anonymous communication path created by the (*Mix*) servers for Mixnet protocols proposed in [20], [21], and [22] relies upon the statistical properties of background traffic. Hence, the Mixnet protocols cannot assure the provable anonymity. For the DC-net protocols proposed in [23], they can tackle the provable anonymity problem and assure perfect anonymity for the sender anonymity. Although, those protocols depend upon secure multiparty computation procedures, they still suffer from the problem of transmission collision [24].

The sender anonymous message authentication approach based on MES (Modified El-Gamal Signature) scheme proposed in [25] targeted the source security against either adaptive chosen message or no-message attacks [26].

The work in [27] considered another way of anonymous communication for WEB browsing and original source for multicast services. However, the work in [28] considered both sender and receiver anonymity by providing the k-anonymous communication protocol. The authors in [29] proposed new concept for hiding both senders' and receivers' messages.

They solved the faced difficulty for the k-anonymous communication protocol either for the key distribution process or the protocol communication overhead. In the same directions, a ring signature approach is proposed in [30].

A new concept of IBE called Fuzzy Identity-Based Encryption (FIBE) was proposed in [31]. This approach looks at the identity as a group of descriptive attributes in the direction of Attribute-Based Encryption (ABE) schemes. Those schemes can be categorized either as a Key Policy Attribute-Based Encryption (KP-ABE) or a Cipher-text-Policy Attribute-Based Encryption (CP-ABE) [32] and [33]. The semianonymity for access control is introduced by AnonyControl and AnonyControl-F approaches proposed in [34]. Those approaches can prevent the user's identity disclosure. Moreover, they can permit cloud servers to control the security of users access.

Li *et al.* [35] defined V_{ID} as a partial identity, in which, the identity is known as pseudonyms produced based on a subset of user attributes. Sarma *et al.* [36] proposed V_{ID} model, in which, the user identity is divided between both network and application layers. They assigned for each virtual identity a specific IP address associated with a separated network stack [37]. Moreover, the network layer unlinkability concept can be achieved using anonymization techniques proposed in [38]. Another access domain which is the Mobil-IP (MIP) considered the concept of V_{ID} framework [39] to cope with the mobility either security or privacy issues.

Shen *et al.* [40] proposed an identity-based shared data integrity auditing scheme based on identity-based cryptography to hide sensitive information that are needed to be shared in the cloud. In this approach, the file contains the sensitive information sanitized to data blocks. Therefore, the data blocks transformed to signature which is used to audit data integrity that realized the cloud shared data.

Mehmood *et al.* [41] proposed an anonymous authentication approach to provide anonymity and privacy for health care application users. In this scheme, anonymous authentication is satisfied by utilizing a rotating group signature scheme based on ECC. However, privacy at the network layer is satisfied by using The Onion Router (TOR).

Feng *et al.* [42] proposed an anonymous authentication based on trust scheme to provide anonymity and privacy preserving for Pervasive Social Networking (PSN). In this scheme, anonymous authentication is based on group signature to authenticate trust levels. However, to secure the communications in PSN and avoid privacy leakage, identities of nodes should be authenticated.

The work introduced by Barisch [43] is one of the known workload models in V_{ID} modelling. It is the nearest analytical work to our proposals. Barisch introduced an analytical model to evaluate the overhead caused by V_{ID} concept on the network infrastructure using BCMP theorem [12]. Therefore, in the current work, the proposed algorithms for V_{ID} will be evaluated and compared against that model [43] for the same impact.

Moreover, a series of related works have been proposed in the context of identity authentication mechanisms that can be used for remote servers accessing [44]–[47]. Throughout the work proposed in [44], a dynamic ID based authentication scheme is introduced. This work is not only based on simple hash functions and some XORing operations but also uses password randomization for each session to improve the dynamic property of identity.

A multi-server authentication scheme has been proposed in [45]. This work also mapped one identity to different server access identities. Through the work of [46], the authors tried to analyze the work published in [45]. They have extracted some common vulnerabilities in the previous work [45], such as attacks like forgery attack, replay attack, user impersonation attack in addition to some weaknesses in their mutual authentication technique. However, the work in [47] introduced lightweight mutual authentication scheme to protect identity in unsecure environments. Despite, the crypt-analysis of [47] scheme which can achieve user anonymity and resist common attacks, the login and authentication phase of this scheme needs much more operation than others.

III. PROBLEM STATEMENT

Nowadays, we are encountering an explosion in the volume of data that is created by social network users (i.e. Facebook, YouTube, Twitter ...). Those users share opinions, personal details, videos, pictures and very often their identities for each service with public or even their friends. Therefore, it is a huge problem to secure users identities and personal data during all activities that they do on the cloud networking or the Internet [48].

Moreover, it is crucial to trust the use of e-Services, e-Government, e-Health, e-Commerce and ensuring the free movement of data and knowledge especially in virtual interactions, e.g., through cloud networking or over the Internet.

IDaaS concept is one of core stone in new digital transformation world. Nowadays, each user can have different identities that can be used for accessing different services. This is especially clear with cloud computing access and multi-tenant services like cloud Software-as-a-Service (SaaS) model. But, keeping many identities for each customer services is so difficult. For this, there are many directions towards treat this problem. One direction went to using identity provider who is capable of managing users identities under the form of third party providers (i.e. Identity Provider). While others like Google went to Google Apps identity services (IDaaS) for managing all Google services using one identity which is the user Gmail address for example. Moreover, Google direction attacked the first direction as it avoids users dependency on third party solutions. But, at the same time this third party solution is considered in some vital accessing domains over Internet like banking systems.

Therefore, the feasibility of any proposed solution is depending on the security, privacy, reliability and cost effectiveness of it. That's why; we search for proposing new identity concept called Virtual Identity. The proposed V_{ID}

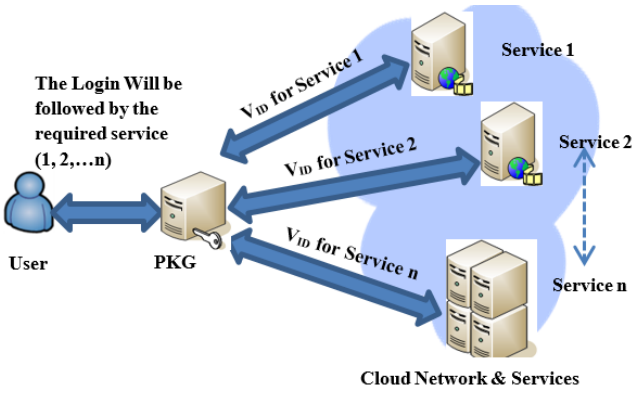


FIGURE 1. IBE and PBE main framework.

can assure all the previous security dependencies towards a feasible cloud based IDaaS solution.

In this respect, we have to propose new models, algorithms and frameworks to provide authentication and privacy mechanisms that protect users identities and ensure protection against illegitimate and malicious behaviors. Therefore, we are searching for more than traditional authentications based on username or passwords. For virtual environments and SaaS applications, we are looking for an authentication path vector based on context aware information relevant to each user demanded service in order to create its relevant access identity. So, each user will have one main identity and different virtual ones mapping based on each service access as shown in Fig. 1 framework.

IV. PROPOSED V_{ID} APPROACHES

The concept of anonymous communications and anonymity on Internet, which has been raised in recent years to protect user's privacy from being disclosed, is extremely significant. Therefore, we have proposed and designed new framework to create user virtual identity-based IBE and PBE to establish anonymous communication with cloud service provider different applications.

Our proposed framework contains three entities:

1) The user (U) who needs the service.
2) The service provider (SP) that delivers the service.
3) The Private Key Generator (PKG), which is the security server that is used in generating the IDs which will be used in cloud service access based on the type of service required by user as shown in Fig. 1.

Fig. 1, highlights the main concept in V_{ID} design for different services required by a single user (main identity). Table 1 summarizes the main notations definition used in IBE and PBE frameworks.

A. MODELLING CONCEPTS FOR IBE AND PBE

The basis of two secure mechanisms for creating a V_{ID} is given in [6], the first one is based on IBE and the second is based on PBE using Elliptic Curve Cryptography (ECC). However, the ECC introduces equal or more security strength

TABLE 1. IBE & PBE main notations and definitions.

Symbol	Definition
V_{ID}	User Virtual Identity
U	User
SP	Service Provider
PKG	Private Key Generation
Ser	User Requested Service
UP	User Public Key
UD	User Private Key
U_{ID}	User Identity
SV_{ID}	Signature of User Virtual Identity
P_{pub}	PKG public Key

TABLE 2. Mathematical notations.

Notation	Description
a, b	Coefficients in E(GF(n))
n	Large prime number
N	The proper parameter if it is a prime number
P	An arbitary generator point (a base point)
q	Order of P in E(GF(n))
S	Master Secret Key
H	Secure hash function
k	Unpredictable integer in the interval [1, n-1]
(r, s)	Integers in the interval [1, n-1]
m	Message in plain text
c	Message in cipher text
K_s	Pre-shared secret key
$multi_a$	IBC function to calculate a by UP
$multi_b$	IBC function to calculate b by P

TABLE 3. Processing times for IBE.

Message ID	Source	Destination	Depends On	Processing Time (sec)
1	U	PKG	Beginning	N/A
2	PKG	U	ID:1	0.034
3	U	SP	ID:2	0.004
4	SP	PKG	ID:3	0.0015
5	PKG	SP	ID:4	0.0015
6	SP	U	ID:5	0.009
Six messages total				0.05

TABLE 4. Processing times for PBE.

Message ID	Source	Destination	Depends On	Processing Time (sec)
1	U	PKG	ID:1	0.0265
2	U	SP	ID:2	0.0065
3	SP	PKG	ID:3	0.0015
4	PKG	SP	ID:4	0.0015
5	SP	U	ID:5	0.009
Five messages total				0.045

compared to other cryptography approaches [49]. Therefore, ECC is chosen in the design of the previously proposed solutions. Multi-precision Integer and Rational Arithmetic C/C++ (MIRACL) library was used during the evaluation of our solutions to observe the processing time for all the implemented functions and executed security entities. The processing times for IBE and PBE as captured during validation will appear later on, Table 3 and Table 4.

The two proposed V_{ID} solutions IBE and PBE use PKG to calculate the V_{ID}. However, these approaches assume that a centralized TA (Trust Authority) is in charge of the PKG.

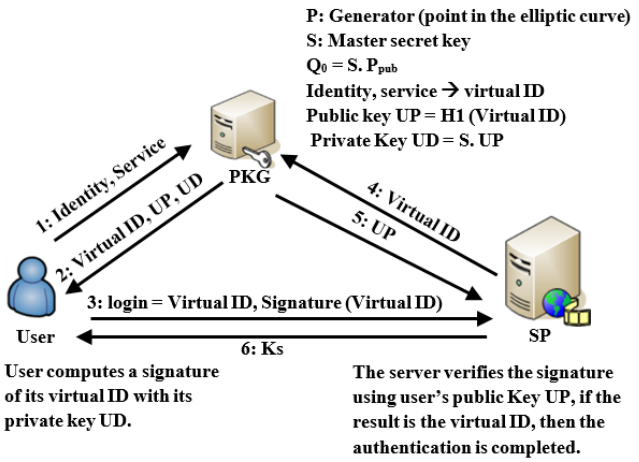


FIGURE 2. IBE model.

Thus, the anonymous communications are not anonymous to the TA. They are different in the encryption technique. Nevertheless, security requirements for both approaches are the same.

B. MIRACL VALIDATION TOOL

In MIRACL (Multi-precision Integer and Rational Arithmetic C/C++ Library) [8] most programs are provided in both C and C++ versions which simplify any program development. It is considered the primary tool for cryptographic system implementers. MIRACL supports RSA, Diffie-Hellman Key exchange and the latest version offers full support for Elliptic Curve Cryptography over GF (p) and GF (2m).

MIRACL also supports Elliptic Curve Diffie-Hellman (ECDH) key agreement protocol, Menezes-Vanstone Protocol and Elliptic Curve Digital Signature Algorithm (ECDSA), which we will utilize to implement and design our proposed protocols.

To evaluate the speed of the cryptography operations in the proposed framework, the IBE and PBE are provided with ''MIRACL library'', the communications between entities are modified and implemented. The following elliptic curve equation: $(y^2 = x^3 - 3x + b \mod p)$ is used where (p) is a 256-bits prime number to accelerate perfect forward Transport Layer Security (TLS) handshakes that use ECDSA and/or ECDHE [50], and (b) is determined through a function in MIRACL. The function can calculate the number of points in a finite field which should be a prime number. The details will be highlighted in the next section.

C. THE FIRST APPROACH: IDENTITY BASED ENCRYPTION (IBE)

IBE is based on the Identity-based Cryptography (IBC) that can be traced back to the IBE firstly proposed by Shamir *et al.* [30]. The security requirements in the context of anonymous communication in cloud networking are presented. Moreover, a platform to provide secure messages in a cloud network based on IBC and ECC is built. Simulation model, an analytical model and performance evaluation are achieved to validate the IBE scenario shown in Fig. 2.

1) PRELIMINARY STEPS FOR IBE

First of all, ECC main parameters are initialized. Therefore, a particular curve E is selected over the finite field of order (n), where (n) is a big prime number $(GF(n))$. Then, an arbitrary generator point (P) is picked on the curve as the base point of E and q (as an order of P). Moreover, Elliptic Curve Digital Signature Algorithm (*ECDSA*) is used for key generation, signature generation and signature verification through V_{ID} creation and verification based IBE. The American National Standards Institute (ANSI) developed *ECDSA* that uses the Elliptic Curve Discrete Logarithm Problem (*ECDLP*) which described as: Given $P \in E(GF(n))$ where (n) is a prime number and $q = a*p$, find $a(1 \leqslant a \leqslant n)$. Table 2 describes the mathematical notations used during the design and implementation phases for both approaches. The main steps for IBE scheme are summarized in Algorithm 1.

Algorithm 1 IBE Scheme

1: **Input:** U_{ID},Ser
2: **Output:** V_{ID},K_s
3: User sends (U_{ID}, Ser) to PKG
4: PKG computes (V_{ID}, UP, and UD)
5: User login to SP with (V_{ID}, SV_{ID})
6: SP sends V_{ID} to PKG
7: SP receives UP from PKG
8: **if** UP.SV_{ID}= V_{ID} **then**
    authentication completed
9: **else**
    authentication failed
10: **end if**
11: SP generates K_s

The proposed platform, shown in Fig. 2, is built to calculate the speed of IBE functions. A *MIRACL* code is developed to facilitate the platform implementation. We have to choose the appropriate parameters of the elliptic curve. The equation of the elliptic curve is: $(y^2 = x^3 + ax + b \mod n)$ where $a, b \in GF(n)$ should satisfy $4a^3+27b^3 \neq 0 \pmod n$ where n is a big prime number. Accordingly, assume $GF(n) > 3$. The points of this curve will define a finite field; their number must be a prime number. In order to satisfy this condition, the parameter (a) and a prime number (n) are fixed in elliptic curve equation. Therefore, the parameter (b) in elliptic curve is chosen to satisfy this condition. The function in *MIRACL* is used to calculate the number of the points in a finite field. Therefore, Elliptic Curve Point Generation (Ecpg()) algorithm is developed to generate ECC point. The principle of the algorithm is as shown in Algorithm 2.

2) IMPLEMENTATION STEPS OF IBE PROTOCOL

(a) System Setup:

a- Each user (U) sends (U_{ID}): User ID and Ser: Requested Service to PKG: Private Key Generator. The PKG is in

Algorithm 2 ECPG()

1: **Input:** a, n
2: **Output:** N is a prime number
3: Initialize b
4: Compute N
5: **while** $N \neq prime$ **do**
6: $b = b + 1$
7: compute N
8: **end while**

charge of the anonymous communication system. Therefore, the anonymous communications are not anonymous to the TA or PKG.

a- PKG generates its parameters, including a master secret key S, which is involved in users private keys generation, and the system parameters which are the prime number n, the order q, the generator point P, PKG's public key are applied

(b) Key Extraction:

When PKG receives (U_{ID}) and Ser, it generates its parameters and keys, then executes Elliptic Curve Digital Signature Algorithm Key Generation ($EcdsaKgen1()$) to generate the user's V_{ID}, UP and UD as detailed in Algorithm 3.

Algorithm 3 EcdsaKgen1()

1: **Input:** $P \in E(GF(n))$ where (n) is a prime number and $q = a * p$
2: **Output:** V_{ID}, UP, UD
3: Calculate S (master secret key)
4: P_{pub} = S.P
5: V_{ID} = original identity.P
6: UP = H. V_{ID}
7: $UD = S.UP$

(c) Signature Generation:

The user receives UD, UP and V_{ID} from PKG. In order to determine V_{ID} signature SV_{ID}, the user receives V_{ID}, UP and UD from PKG then executes Elliptic Curve Digital Signature Algorithm Signature Generation (EcdsaSign (V_{ID}, UD)) as in Algorithm 4 to compute the signature of the virtual identity (SV_{ID}).

Algorithm 4 EcdaSign (V_{ID}, UD)

1: **Input:** V_{ID}, UP , UD
2: **Output:** SV_{ID}
3: initialize r = 0
4: generate n
5: $d = UDmod(n-2)$
6: $Q = d.UP$
7: **while** $r = 0 \| s = 0$ **do**
8: $k \in [1, n-1]$
9: $k.UP = (x1, y1)$
10: $r = x1\ mod$ n
11: $s = k - 1.(H(\ V_{ID}) + $ d.r) mod n
12: **end while**
13: $SV_{ID} = (r, s)$

(d) Signature Verification:

Once the Service Provider (SP) receives the signature of the virtual identity (SV_{ID}), it asks PKG for the public key in order to check the signed virtual identity. Then, execute (the Elliptic Curve Digital Signature Algorithm Signature verification) to verify virtual identity signature (r, s) by performing the algorithm EcdsaVer (V_{ID}, UP) shown in Algorithm 5.

Algorithm 5 ECDSAVER (V_{ID}, UD)

1: **Input:** V_{ID},$SV_{ID} = (r, s)$
2: **Output:** Verify SV_{ID}
3: **if** $1 \leqslant (r, s) \leqslant n - 1$
4: $w = s - 1\ mod$ n
5: $u1 = H(V_{ID}).w$ mod n
6: $u2 = r.w$mod n
7: $u1.UP + u2.Q = (x0, y0)$
8: **if** $r = x0\ mod$ n
Valid SV_{ID}
9: **else**
Invalid SV_{ID}
10: **end if**
11: **else**
Invalid SV_{ID}
12: **end if**

(e) Encrypt Future Communication:

In case, the signature verification succeeded, the service provider generates Shared Secret Key (K_s) and sends it to the user. Otherwise, it is discarded. EcdhEncrypt (m) generates the pre-shared key K_s to encrypt future communication as shown in Algorithm 6. The resulting cipher text is denoted by c. The decryption of cipher text c using the same pre-shared key K_s is given as EcdhDecrypt(c) as shown in Algorithm 7.

Algorithm 6 EcdhEncrypt (m)

1: **Input:** m, UP, $multi_b$
2: **Output:** C
3: Generate $a \in GF(n)$
4: $multi_a = a.UP$
5: $K_s = a.multi_b$
6: $C = \{m\}.K_s$

Algorithm 7 EcdhDecrypt (C)

1: **Input:** C, UP, $multi_a$
2: **Output:** m
3: Generate $b \in GF(n)$
4: $multi_b = b.UP$
5: $K_s = b.multi_a$
6: $m = \{C\}.K_s$

D. THE SECOND APPROACH: PSEUDONYM BASED ENCRYPTION (PBE)

The second approach, PBE, (shown in Fig. 3) is based on Pseudonym-Based Encryption that was proposed earlier for Key management for anonymous communication in mobile ad-hoc networks [17]. In this approach, the user uses Pseudonym Based Encryption (PBE) to calculate its own V_{ID}. The PKG will compute the user's private key that depends on its secret master key. In PBE, the PKG will act as an authority which certifies that the user has the private key corresponding to public key. Algorithm 8 summarizes the main steps for generating V_{ID} through PBE scheme.

1) PRELIMINARY STEPS FOR PBE

The same preliminary steps as detailed before in IBE are used.

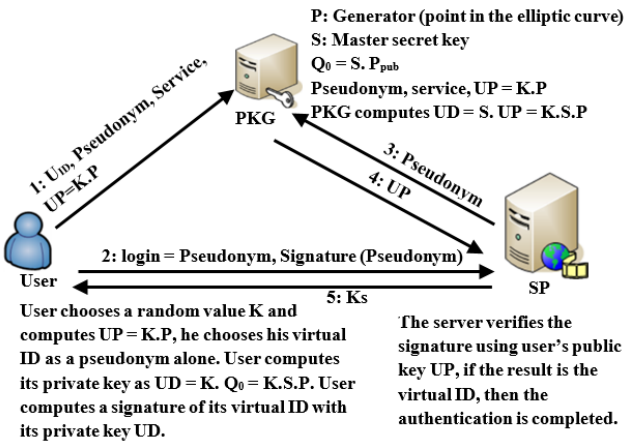


FIGURE 3. PBE model.

Algorithm 8 PBE Scheme

1: **Input:** U_{ID},*Ser*
2: **Output:** V_{ID},K_s
3: User sends U_{ID},*Ser*,UP, Pseudonym to PKG
4: PKG computes V_{ID}, UP, UD
5: User computes UD
6: User login to Sp with Pseudonym, Signature (Pseudonym)
7: SP sends Pseudonym to PKG
8: SP receives UP from PKG
9: **if** UP.Signature (Pseudonym) = Pseudonym **then**
authentication completed
10: **else**
authentication failed
11: **end if**
12: SP generates K_s

2) IMPLEMENTATION STEPS OF PBE PROTOCOL

In this sub-section, we briefly extract the implementation sequence of PBE scheme design as follows:

(a) System Setup:

As shown in Fig. 3, the user sends U_{ID}: User ID, Ser: Requested Service, V_{ID}: Pseudonym and UP: User Public Key to PKG.

The PKG or TA (the Trust Authority) will compute the user's UD that depends on its secret master key. The TA computes the user's UD and will not send the key pair (public/private) to the user because the UP and UD are already calculated by the user.

(b) Key Extraction:

Given U_{ID}: User ID and Ser: Requested Service V_{ID}: Virtual ID (Pseudonym), UP: User Public Key, user chooses random value k to calculate:

1) The User public key $UP = K * P$ (K is a random value and P is a point on elliptic curve).
2) The User private key $UD = S * UP$ (S is the master secret key of U).
3) The Virtual Identity V_{ID} (V_{ID} = pseudonym).

User generates the parameters and keys, then executes Elliptic Curve Digital Signature Algorithm Key Generation 2 (EcdsaKgen2()) to generate the user's UP and UD as detailed in Algorithm 9.

(c) Signature Generation:

Algorithm 9 EcdsaKgen2 ()

1: **Input:** $P \in E(GF(n))$ where (n) is a prime number and $q = a * p$
2: **Output:** V_{ID}, UP, UD
3: Generate random integer $K \in [2, n-2]$
4: Calculate S (master secret key)
5: $UP = K.P$
6: V_{ID} = Pseudonym
7: UD = S.UP

In order to sign the user V_{ID} using a UD derived from the user to determine V_{ID} signature (SV_{ID}), the user generates V_{ID}, UP and UD as mentioned before then executes EcdsaSign (V_{ID}, UD) as shown in Algorithm 4 to determine SV_{ID}.

(d) Signature Verification:

Once the service provider receives the signed V_{ID}, he asks PKG for the UP to check the SV_{ID}. Then executes EcdsaVer (V_{ID}, UP) shown in Algorithm 5, EcdsaVer to verify the virtual identity.

(e) Encrypt Future Communication:

In case the verification of the signature is successful, the service provider SP generates shared secret key (Ks) and sends it to the user (U). Otherwise, it is discarded. After generating the pre-shared key (*Ks*), we denote encrypting future communication (i.e., a message *m*) using *Ks* as EcdhEncrypt (*m*), shown in Algorithm 6. The resulting cipher-text is denoted by (*c*). The decryption of cipher-text (*c*) using the same pre-shared key is given as EcdhDecrypt(c) shown in Algorithm 7.

E. IBE AND PBE APPROACHES IMPLEMENTATIONS COMPARISON

Public-key based solution such as Identity-Based Cryptographic (IBC) is an asymmetric key cryptographic technique, in which a user's UP can be an identifier of the user and the corresponding UD is created by binding the identifier with a system master secret [49]. Therefore, they are used as a solution for anonymous communications. However, IBE and PBE increase the level of security in order to prevent any form of attack and guarantees Non-Repudiation, Integrity, Privacy and Protection. The proposed solutions have two new contributions; dynamicity and anonymity. The dynamicity is achieved based on using time-stamp calculation for each login to the same service that will generate each time new identity. Moreover, anonymity is achieved through hiding the main identity and depends on using the virtual one for each service.

According to Table 3 and Table 4, the processing times for all messages are around 0.05 Sec and 0.045 Sec for IBE and PBE respectively. The results obtained by computing machine specs; Intel Core 2 Duo CPU E8400 @ 3.00GHz x 2, memory 4GB in Linux Ubuntu 12.10. The processing times shown in those tables are captured during the two scenarios validation in *MIRACL*.

For the scalability issue, we can clearly see from the execution time mentioned before that, the proposed cryptosystem is feasible in anonymous communication in cloud and distributed environments. Table 5, evaluates the time needed to

TABLE 5. IBE and PBE scalability.

No of Users	V_{ID} creation time IBE	V_{ID} creation time PBE
1000	40 S	32 S
5000	200 S	160 S
10000	400 S	320 S
50000	2000 S	1600 S

create the V_{ID} for different number of users as a simulation scheme for large number of cloud access users. The PBE provides a short time for V_{ID} creation because of the low number of messages used to create it.

V. PERFORMANCE EVALUATION FOR IBE AND PBE

The performance evaluation of the new approaches for V_{ID} creation will be carried out in this section. The performance of IBE and PBE are evaluated under different configurations and network conditions.

A. ANALYTICAL MODEL BASED BCMP QUEUING NETWORK

In this part, the modelling of the security functions either for the IBE or PBE models is introduced. The entities are represented by different servers (i.e. U, PKG and SP) to compute the consumed time in the communication process proposed according to the messaging workflow in Fig. 2 (for IBE) and Fig. 3 (for PBE). To achieve that, the queuing network technique based BCMP is used. The BCMP queuing network model is helpful for simulating analytically the servers behavior and protocols interactions. Moreover, the BCMP network may be used as open, closed, or mixed for each type of the selected scheduling disciplines. A mixed queuing network, that consists of a number ($N >= 1$) stations / service centers is used. This network model can produce a good approximation of the interactions for the complex protocols. The approximation can give a compromise solution between precision and complicated ones.

1) IBE COMMUNICATION PROCESS

Fig. 4, shows a queuing representation model for the security servers. This model is built according to the processing time for IBE protocol messages listed before in Table 3. As cleared, there are three stations/servers (U, PKG, and SP).

The system state can be defined as the number for each class of customers in each service center. So, the state S of the system is represented by $(S_1, S_2, ..., S_N)$ where $S_i = (n_{i1}, n_{i2}, ..., n_{in})$ denotes the state of each service center (i) and (n_{iq}) is the number of users of class (q) in service center (i). According to the BCMP [12], the probability of distribution state in the BCMP network has the following form:

$$p(s) = cd(S)g_1(y_1)g_2(y_2)...g_i(y_i) \quad (1)$$

Such that (c) is a normalizing constant that is selected to make the equilibrium state probabilities sum to 1, $d(S)$ is a function of customers in the system, and each g_i is a function that depends on the type of service center i. The number of

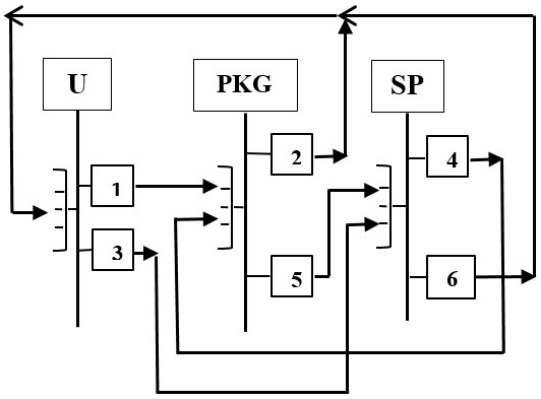


FIGURE 4. IBE queuing model.

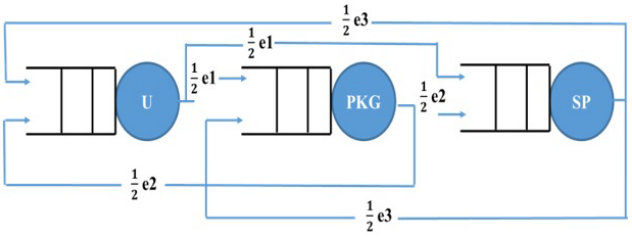


FIGURE 5. Arrival rate for each server for the IBE scenario.

messages at server i is represented by n_i while, $\mu_{i,q}$ is the service rate at server i of the message class q, and $\lambda_{i,q}$ is the arrival rate at server i of the message class q.

$$g(y_i) = \begin{cases} \dfrac{n_i}{{\mu_i}^{n_i}} \cdot \prod_{q=1}^{Q} \dfrac{\lambda_{i,q}^{n,q}}{n_{i,q}!} & \text{Service Centers of Type 1} \\ n_i! \prod_{q=1}^{Q} \dfrac{\lambda_{i,q}^{n,q}}{\mu_{i,q}^{n,q}.n_{i,q}!} & \text{Service Centers of Types 2, 4} \\ \prod_{q=1}^{Q} \dfrac{\lambda_{i,q}^{n,q}}{\mu_{i,q}^{n,q}.n_{i,q}!} & \text{Service Centers of Type 3} \end{cases} \quad (2)$$

We assumed that the IBE servers model are processor shared and Poisson distribution represents the distribution of the arrival rate of messages. As stated before, IBE model has six messages in the signaling flow, and they are supposed to be of the same class for simplicity $(i.e. \lambda_i - \lambda_{i,q})$. According to that, equation (1) can be simplified to be [12],

$$p_i(n_i) = (1 - \rho_i)\rho_i^{n_i} \quad (3)$$

where:

$$\rho_i = \sum \frac{\lambda_i}{\mu_i} \quad (4)$$

For the system stability, the condition $(\lambda_i < \mu_i)$ must be achieved for each server i. Moreover, for each message, the packet loss probability is small. Therefore, it can be

ignored. According to Fig. 4, each server utilization can be calculated as follows:

$$\rho_u = \lambda_u(\frac{1}{\mu_1} + \frac{k}{\mu_3}) \tag{5}$$

$$\rho_{PKG} = \lambda_{PKG}(\frac{1}{\mu_2} + \frac{k}{\mu_5}) \tag{6}$$

$$\rho_{SP} = k.\lambda_{SP}(\frac{1}{\mu_4} + \frac{k}{\mu_6}) \tag{7}$$

where k is the number of requested services.

Assuming that the system is stable, the arrival rate of messages (λ_i) in average for each server (i) is different and can be estimated according to the messages flow in each server queue. The message flow is divided into two parts:

1) Messages received from outside with the arrival rate (λp_{0i}), where (p_{0i}) is the probability that a client message arrives the system at server i.
2) Messages coming from server j with the arrival rate ($\lambda_j p_{ji}$) for all servers ($j = 1, 2, ..., M$), where p_i is the probability that a customer finishes his service at server i and goes to server j.

Therefore, the average of arrival rate for each server i can be calculated. However $\lambda_i = e_i\lambda$, and e_i is the rate of visiting server i to the average number of messages for that server. Therefore, λ_i can be structured as follows:

$$\lambda_i = \lambda p_{0i} + \sum_{j=1}^{M} \lambda_j p_{ji} \tag{8}$$

$$e_i = p_{0i} + \sum_{j=1}^{M} e_j p_{ji} \tag{9}$$

Based on (9), all system equations can be deduced to satisfy the visit rate for each server i. As shown in Fig. 4 and Fig. 5, the IBE model considers at different servers the average messages type and does not consider the time sequence of each procedure. This is sufficient enough and does not affect on the overall system performance evaluation.

Regarding Fig. 5, the distributions of messages for the three servers (U, PKG, and SP) can be introduced by the following equations considering that one service for each user is requested at the SP.

$$e_1 = \frac{1}{2}e_2 + \frac{1}{2}e_3 \tag{10}$$

$$e_2 = \frac{1}{2}e_1 + \frac{1}{2}e_3 \tag{11}$$

$$e_3 = \frac{1}{2}e_1 + \frac{1}{2}e_2 \tag{12}$$

The arrival rate for each server can be calculated by solving the equations (8-12), that gives:

$$\lambda_u = \lambda_{PKG} = \lambda_{SP} \tag{13}$$

and

$$E(n_i) = \sum_{n_i=1}^{\infty} n_i p_i(n_i) = \frac{\rho_i}{1-\rho_i} \tag{14}$$

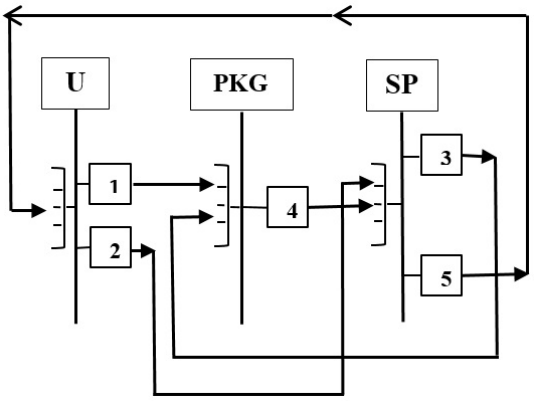


FIGURE 6. PBE queuing model.

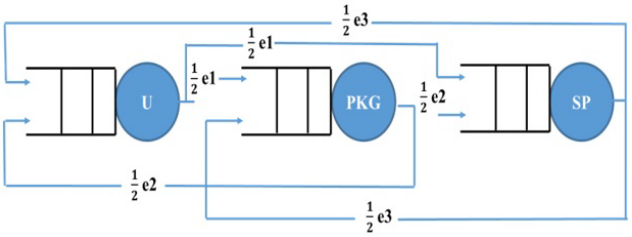


FIGURE 7. Arrival rate for each server for the PBE scenario.

where i stands for the servers/stations (U, PKG, and SP). From (3), the mean queue size corresponding to the average number of clients waiting on servers is calculated as in (14). Using the LittleLaw [12], the service processing time at each server i is as follows:

$$T_i = \frac{E(n_i)}{\lambda_i} = \frac{1}{(1-\rho_i)\mu_i} = \frac{1}{\mu_i - \lambda_i} \tag{15}$$

To estimate the total processing time (D) of the service implementation in the IBE workflow, the following values are assumed which are: service processing time at the three servers and waiting time at each server's queue. Assuming that, there is no queuing introduced in the U and the transmission time is ignored, its waiting time is approximated to zero, and then D becomes:

$$D = T_u + T_{PKG} + T_{SP} \tag{16}$$

2) PBE COMMUNICATION PROCESS

As shown in Fig. 6 and Fig. 7, the PBE queuing model and arrival rate for each server are designed.

Therefore, the utilization of each server can be calculated as follows:

$$\rho_u = \lambda_u(\frac{1}{\mu_1} + \frac{nk}{\mu_2}) \tag{17}$$

$$\rho_{PKG} = k(\frac{\lambda_{PKG}}{\mu_4}) \tag{18}$$

$$\rho_{SP} = k.\lambda_{SP}(\frac{1}{\mu_3} + \frac{1}{\mu_5}) \tag{19}$$

where k is the number of requested services. Assuming the system is stable, the average arrival rate of messages λ_i for each server i is different and is calculated according to the messages flow in each server queue. Therefore, the arrival rate average for each server i can be computed and the rate of visiting server i to the average number of passages of that server as in equations (8) and (9).

Based on (9) and according to the arrival rate model for each server for the PBE scenario (Fig. 6 and Fig. 7), the distribution of messages for the three servers (U, PKG, and SP) can be introduced by the following equations assuming that one service for each user is requested at the SP:

$$e_1 = \frac{1}{2}e_3 \tag{20}$$

$$e_2 = \frac{1}{2}e_1 + \frac{1}{2}e_3 \tag{21}$$

$$e_3 = \frac{1}{2}e_1 + e_2 \tag{22}$$

Solving the previous equations(18-22),that gives:

$$\lambda_u = \frac{2}{3}\lambda_{PKG} = \frac{1}{2}\lambda_{SP} \tag{23}$$

and

$$D = T_u + T_{PKG} + T_{SP} \tag{24}$$

B. PERFORMANCE EVALUATION USING OPNET MODELER

Optimized Network Performance (OPNET) Modeler [9] is a discrete event simulation tool. OPNET introduces a development environment supporting the simulation and modeling of communication networks.

Two different scenarios for IBE and PBE are implemented using OPNET Modeler (multiple and single service for each user). For each protocol, the application response time is measured in the two cases; multiple and single service. Finally, the results obtained are compared against the analytical model and the performance evaluation is concluded.

1) NETWORK MODEL SCENARIOS

IBE and PBE are implemented using OPNET Modeler for single and multiple services. For each protocol, the application response time is measured in the two cases; single service for each user and multiple services model.

ACE is used to evaluate the proposed solutions. First, ACE whiteboard is used to draw exchanging messages among the three entities U, PKG and SP. Therefore, the processing times are provided for each message as obtained from MIRACL library.

After that, from the ACE whiteboard, the network topology is drawn as illustrated in Fig. 8. For each proposed solution, the performance is evaluated in two cases, the first one is when clients (users) need single service and the second one is when users need more than one service access (ten services). Finally, the obtained results are compared for both approaches.

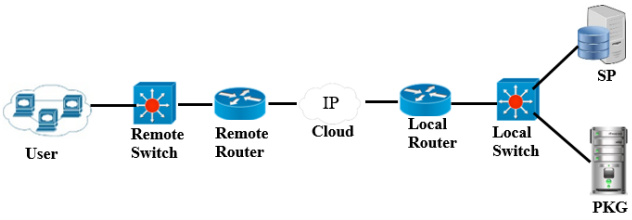


FIGURE 8. IBE single service topology.

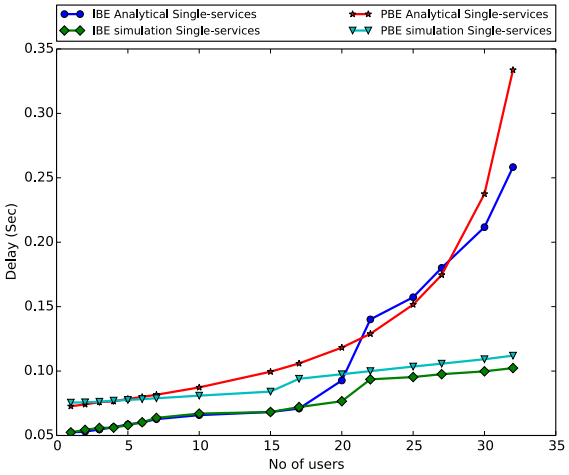


FIGURE 9. IBE versus PBE single service model.

2) SIMULATION VERSUS ANALYTICAL RESULTS

The results show that the number of users and their locations (either remote or local) affect the response time. ACE whiteboard is used to simulate the overall flow of data across different tiers from start to end of the application task for V_{ID} creation. The mathematical models are built based on BCMP theory and the validation for different network access conditions is done using MATLAB tool [14].

Four different scenarios are implemented. In all scenarios, the application response time is measured, which is described as the time taken for all the tasks in the custom application to complete. Moreover, the overall delay is evaluated. Therefore, Cloud-based evaluation can be measured by increasing the number of users as it is logic for cloud service providers.

1) SINGLE SERVICE MODEL
   From Fig. 9, it should be noted that the delay has closed values for analytical and simulation models either for IBE or PBE which proves that the model concept makes sense. Moreover, the system is stable for different number of users in the two proposed algorithms according to the number of services the users have. Despite, the user in PBE model is in charge of the identity creation process not only the PKG, the system is stable for more number of users using PBE single service model than the users who are using IBE single service model.
2) MULTIPLE SERVICE MODEL
   The scenario of multiple services, Fig. 10 is more realistic than the previous single service; however, the number of users is different in the two scenarios according to the

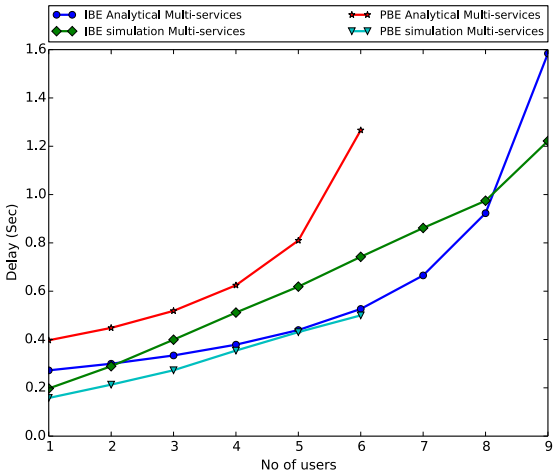


FIGURE 10. IBE versus PBE multiple service model.

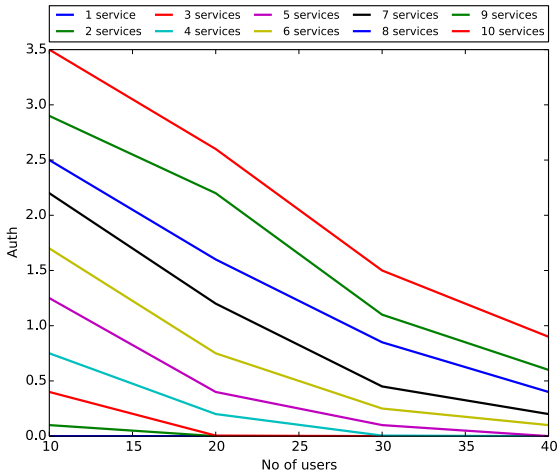


FIGURE 11. Barisch's model.

test environments. Moreover, the number of users with PBE multiple services is less than the same cases for IBE because of the user in PBE model is in charge of the process not only the PKG as detailed before in PBE workflow Fig. 3.

C. IBE AND PBE VERSUS BARISCH'S MODEL

A comparison between the overhead introduced by the V_{ID} concept of the proposed models and the state of the art Barisch's model [43] is done. The used key metrics for performance evaluation is similar in both Barisch's model and the proposed models. However, Barisch's model workflow depends on the selection and activation of V_{ID} in the service preparation phase and then start the service consumption phase. In IBE and PBE models, the V_{ID} is created each time the user needs the service. Therefore, the authentication load for selection and activation of V_{ID} at Barisch's model compared with the creation process of V_{ID} at IBE and PBE models is calculated for each V_{ID} which has a separate authentication process. In addition, the average number of available V_{ID} is depending on the mean number of simultaneously service session that a user has. Therefore, the total overhead introduced by V_{ID} concept is the same as if the number of simultaneously service session is multiplied by the number of users.

The load is defined as in [43] as the number of simultaneous service sessions that a user has. Therefore, for Barisch's model, the authentication load is involved during the activation process of V_{ID} and calculated as the activation rate multiplied by the mean termination rate of the service. Therefore, the authentication load for Barisch's model (Aauth) is high for a low number of services that user has and low for a high number of services that user has (which mean that no more V_{ID} activation occurs) as shown in Fig. 11.

The authentication load for IBE and PBE depends on the ability of PKG to handle all user requests. Therefore, the authentication load is low for low number of services that a user has and high for a high number of services

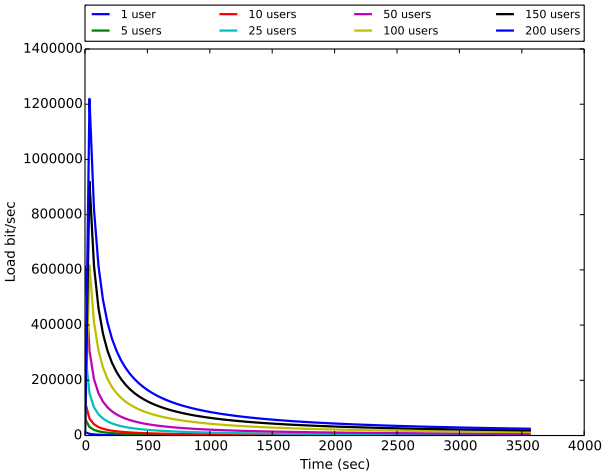


FIGURE 12. PKG Authentication load for PBE model.

that a user has. Moreover, for IBE and PBE models the user can create his own V_{ID} at any time independent of the number of users, number of services and activation process as in Barisch's model.

Fig. 12 and Fig. 13, show that PKG authentication load increases with increasing the number of users. Moreover, the two figures show how the load is changed with the number of users of the two models. Many users will increase the load on the PKG server but all users can create their own V_{ID}(s). However, unlike [43], the value of load on PKG at IBE is greater than the value of PKG load at PBE because the users at PBE model are in charge of the process. Hence, the load created by 50 users when using IBE model is the same for 200 users when using PBE model.

Fig. 14 and Fig. 15 show the authentication load of PKG and the changes of the number of users for IBE and PBE respectively. More users will increase the load on the PKG server but all users can create their own V_{ID}(s). Moreover, unlike [43], the load on PKG at IBE is more than the load at PBE because the users at PBE are in charge of the process. Hence, 50 users at IBE made the same load as 200 users at PBE.

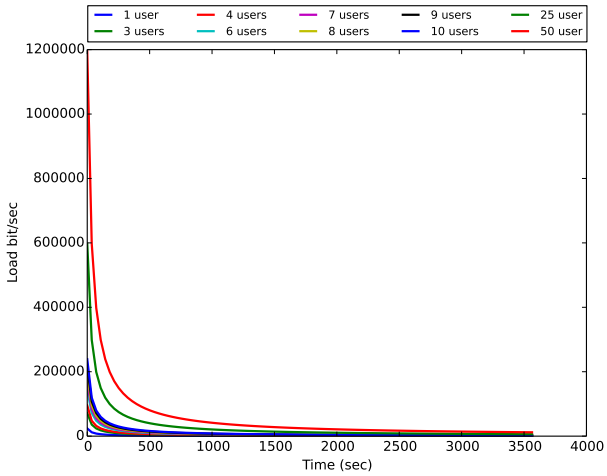


FIGURE 13. PKG Authentication load for IBE model.

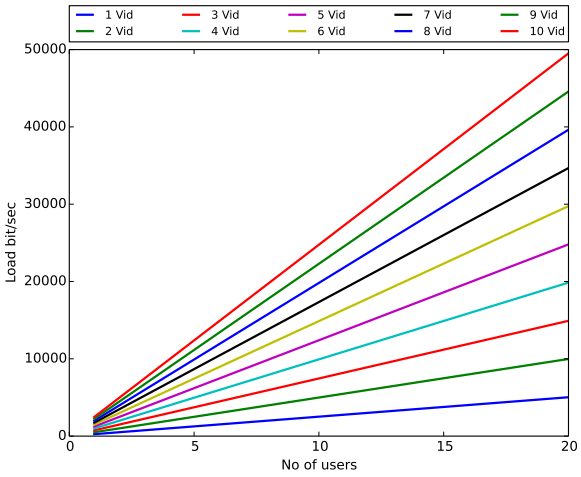


FIGURE 14. Increasing number of V_{ID} with load for IBE.

TABLE 6. Computational total cost comparison.

Scheme	Total cost of registration, login and authentication phase
[44], 2015	$17\ T_H + 10\ T_X$
[45], 2017	$22\ T_H + 12\ T_X$
[46], 2018	$20\ T_H + 10\ T_X$
[47], 2018	$8\ T_X + 22\ T_H + 6\ T_G$
IBE (our proposal)	$2\ T_H + 1\ T_X + 10\ T_M$
PBE (our proposal)	$1\ T_H + 1\ T_X + 9\ T_M$

As mentioned previously, the authentication load is involved during V_{ID} activation. Therefore, the authentication load is high for low load situation. Moreover, the authentication load is low for high load situation which means that the V_{ID} activation did not take place. The rest of performance evaluation metrics are not comparable with the state of the art model because the user at our models creates his own V_{ID}. So, there is no selection and activation process.

D. COMPUTATION & SECURITY COMPARISONS

In this part, we introduce both computation and communication costs comparison between the proposed approaches (IBE & PBE) and relevant works [44]–[47]. In addition,

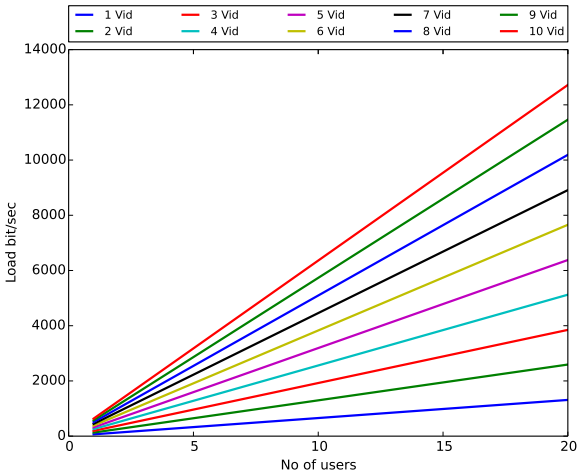


FIGURE 15. Increasing number of V_{ID} with load for PBE.

TABLE 7. Computational cost comparison.

Scheme	Total number of messages
Saraswathi et al. [44], 2015	3
Jingarala et al. [45], 2017	3
Sahoo et al. [46], 2018	3
Wu et al. [47], 2018	4
IBE (our proposal)	5
PBE (our proposal)	4

TABLE 8. Security comparison.

Scheme	AVISPA back-ends			
	OFMC	CL-AtSe	SATMC	TA4SP
[44], 2015	Vulnerable to replay attack, know-key security attack, card loss attack, user impersonation forgery attack, denial of service attack.			
[45], 2017	Vulnerable to replay attack, user impersonation attack, forgery attack.			
[46], 2018	Pass	Pass	-	-
[47], 2018	Pass	Pass	-	-
IBE	Pass	Pass	Pass	Not Supported
PBE	Pass	Pass	Pass	Not Supported

we present the security comparative study between the proposed approaches and the same related works.

The computational cost comparison of IBE and PBE against other existing approaches is given in Table 6. In this comparison, we defined the notations T_M; T_X; T_H; T_G to denote multiplication function, XOR operation, one-way hash function and modular exponentiation respectively. As shown in Table 6, the proposed approaches have a total cost less than the existing similar approaches in the literature.

In Table 7, the communication cost of IBE and PBE has been compared with the same related work schemes. Despite of the overall number of exchanged messages in some related works are less bit-wise than the proposed schemes the computational and communication total cost of the proposed algorithms is better than the related work schemes, due to the big differences in total computational cost between the proposed schemes and other schemes.

Table 8, shows the security comparison for the automated validation of the proposed schemes with other related schemes. The proposed approaches passed three

out of four AVISPA back-ends (OFMC (On-the-fly Model-Checker), CLAtSe (CL-based Attack Searcher), SATMC (SAT-based Model-checker), and TA4SP (Tree-Automata-based Protocol-Analyser)) [44]–[47]. However, the two schemes, Saraswathi *et al.* scheme and Jingarala *et al.* scheme are vulnerable to some attacks [46]. In addition, Sahoo *et al.* [46] scheme and Xu *et al.* [47] scheme passed two out of four AVISPA [51] back-ends. Hence, the proposed schemes are considerably more secure as compared to the competent state of the art schemes.

VI. CONCLUSION

In this paper, a new terminology for virtual environments and SaaS applications accessing is introduced. It is based on IBE and PBE frameworks to handle the anonymous communication in such types of cloud environments. First, the design of V_{ID} including the process of V_{ID} creation and implementations of both approaches through MIRACL are introduced. Then, performance evaluation of V_{ID} concept is carried out analytically and through simulation. BCMP mathematical model is implemented to realize analytically IBE and PBE based workflows while the OPNET Modeler is used as a simulation tool to calculate the processing delay using either single or multiple services accessed by each login user. The results of the two scenarios (analytical and simulation) are close to each other proving that our proposed model concepts cope with the real scenarios. Finally, we conducted a comparative study between our alternative solutions (IBE and PBE) against Barisch's model. The comparison indicated that the proposed V_{ID} approaches are suitable for cloud-based SaaS applications.

Future work will focus on integrating the proposed solutions in real cloud computing platform like OpenStack [52]. It will be in correlation with the keystone security server for best integration with cloud scalability. Moreover, one of the promising future work is to extend our solutions to include group communication and design security model to compare quantitatively the IBE and PBE with the approaches of related work. Another direction, is the feasibility study of the proposed solutions as a business model for cloud identity providers over Internet.

REFERENCES

[1] K. K. Liyanaarachchi, "Analyzing authentication patterns for cloud services," *IEEE Potentials*, vol. 37, no. 5, pp. 8–15, Sep./Oct. 2018. doi: 10.1109/MPOT.2015.2451677.

[2] C. A. Christiansen and L. Stuart, "Identity as a service on the journey to the cloud," Framingham, MA, USA, White Paper IDC#US41243816, May 2016. [Online]. Available: https://www.oracle.com/assets/iaas-journey-to-the-cloud-3097328.pdf

[3] I. Indu and P. M. R. Anand, "Identity and access management for cloud web services," in *Proc. IEEE Recent Adv. Intell. Comput. Syst. (RAICS)* Trivandrum, India, Dec. 2015, pp. 406–410. doi: 10.1109/RAICS.2015.7488450.

[4] C. Emig, F. Brandt, S. Kreuzer, and S. Abeck, "Identity as a service—Towards a service-oriented identity management architecture," in *Dependable and Adaptable Networks and Services* (Lecture Notes in Computer Science), vol. 4606. Berlin, Germany: Springer, 2007, pp. 1–8.

[5] G. Rowe, N. Nikols, and D. Simmons. The Future of Identity Management. TechVision Research (2018–2023). Accessed: Mar. 2019. [Online]. Available: https://techvisionresearch.com/wp-content/uploads/2018/01/The-Future-of-Identity-Management-2018-final.pdf

[6] I. A. Gomaa and E. Abd-Elrahman, "A novel virtual identity implementation for anonymous communication in cloud environments," *Procedia Comput. Sci.*, vol. 63, pp. 32–39, Jan. 2015. doi: 10.1016/j.procs.2015.08.309.

[7] D. F. Aranha, P. S. L. M. Barreto, R. C. C. F. Pereira, and J. E. Ricardini. (Feb. 2019). *A Note on High-Security General-Purpose Elliptic Curves*. [Online]. Available: https://eprint.iacr.org/2013/647.pdf

[8] (Feb. 2019). *MIRACL Library*. [Online]. Available: https://libraries.docs.miracl.com/

[9] (Feb. 2019). *OPNET Modeler*. [Online]. Available: https://www.riverbed.com/gb/products/steelcentral/opnet.html

[10] I. A. Gomaa, E. Abd-Elrahman, and M. Abid, "Virtual identity approaches evaluation for anonymous communication in cloud environments," *Int. J. Adv. Comput. Sci. Appl.*, vol. 7, pp. 367–376, Feb. 2016.

[11] A. D. Tesfamicael, V. Liu, E. Foo, and W. Caelli, "Modeling for performance and security balanced trading communication systems in the cloud," in *Proc. IEEE 36th Int. Perform. Comput. Commun. Conf. (IPCCC)*, Dec. 2017, pp. 1–7. doi: 10.1109/PCCC.2017.8280506.

[12] F. Baskett, K. M. Chandy, R. R. Muntz, and F. G. Palacios, "Open, closed, and mixed networks of queues with different classes of customers," *J. ACM*, vol. 22, no. 2, pp. 248–260, Apr. 1975. doi: 10.1145/321879.321887.

[13] I. Gomaa, A. M. Said, E. Abd-Elrahman, A. Hamdy, and E. M. Saad, "Performance evaluation of virtual identity approaches for anonymous communication in distributed environments," *Procedia Comput. Sci.*, vol. 109, pp. 710–717, Jan. 2017. doi: 10.1016/j.procs.2017.05.382.

[14] (Dec. 2018). *MATLAB Online*. [Online]. Available: https://www.mathworks.com/products/matlab-online.html

[15] I. A. Gomaa and E. Abd-Elrahman, "Integration with cloud computing security," in *Big Data: Storage, Sharing, and Security*, vol. 8. Boca Raton, FL, USA: CRC Press, 2016, pp. 203–228.

[16] D. Boneh and M. Franklin, "Identity-based encryption from the weil pairing," *SIAM J. Comput.*, vol. 32, no. 3, pp. 586–615, Jan. 2003. doi: 10.1137/S0097539701398521.

[17] D. Huang, "Pseudonym-based cryptography for anonymous communications in mobile ad hoc networks," *Int. J. Secur. Netw.*, vol. 2, nos. 3–4, pp. 272–283, Apr. 2007. doi: 10.1504/IJSN.2007.013180.

[18] D. Chaum, "The dining cryptographers problem: Unconditional sender and recipient untraceability," *J. Cryptol.*, vol. 1, no. 1, pp. 65–75, Jan. 1988. doi: 10.1007/BF00206326.

[19] D. L. Chaum, "Untraceable electronic mail, return addresses, and digital pseudonyms," *Commun. ACM*, vol. 24, no. 2, pp. 84–90, Feb. 1981. doi: 10.1145/358549.358563.

[20] G. Danezis, R. Dingledine, and N. Mathewson, "Mixminion: Design of a type III anonymous remailer protocol," in *Proc. Symp. Secur. Privacy*, Washington, DC, USA, May 2003, pp. 2–15.

[21] P. F. Syverson, D. M. Goldschlag, and M. G. Reed, "Anonymous connections and onion routing," in *Proc. IEEE Symp. Secur. Privacy*, Washington, DC, USA, May 1997, pp. 482–494.

[22] M. K. Reiter and A. D. Rubin, "Crowds: Anonymity for Web transactions," *ACM Trans. Inf. Syst. Secur.*, vol. 1, no. 1, pp. 66–92, Nov. 1998.

[23] J. Ren, L. Harn, and T. Li, "A novel provably secure anonymous communication (PSAC) Scheme," in *Proc. Int. Conf. Wireless Algorithms, Syst. Appl. (WASA)*, Aug. 2007, pp. 275–280. doi: 10.1109/WASA.2007.39.

[24] P. Golle and A. Juels, "Dining cryptographers revisited," in *Advances in Cryptology—EUROCRYPT*. Berlin, Germany: Springer, 2004, pp. 456–473.

[25] J. Ren, T. Li, and Y. Li, "Anonymous communications in overlay networks," in *Proc. IEEE Mil. Commun. Conf. (MILCOM)*, Nov. 2008, pp. 1–6. doi: 10.1109/MILCOM.2008.4753343.

[26] D. Pointcheval and J. Stern, "Security proofs for signature schemes," in *Advances in Cryptology—EUROCRYPT*, vol. 96. Berlin, Germany: Springer, 1996, pp. 387–398. doi: 10.1007/3-540-68339-9_33.

[27] C. Shields and B. N. Levine, "A protocol for anonymous communication over the Internet," in *Proc. 7th ACM Conf. Comput. Commun. Secur.*, New York, NY, USA, Nov. 2000, pp. 33–42. doi: 10.1145/352600.352607.

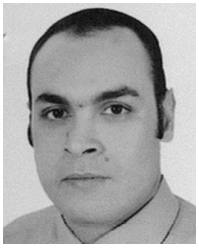
[28] P. Wang, P. Ning, and D. S. Reeves, "A K-anonymous communication protocol for overlay networks," in *Proc. 2nd ACM Symp. Inf., Comput. Commun. Secur.*, New York, NY, USA, Mar. 2007, pp. 45–56. doi: 10.1145/1229285.1229296.

[29] Beimel and Dolev, "Buses for anonymous message delivery," *J. Cryptol.*, vol. 16, no. 1, pp. 25–39, Jan. 2003. doi: 10.1007/s00145-002-0128-6.

[30] R. L. Rivest, A. Shamir, and Y. Tauman, "How to leak a secret," in *Advances in Cryptology—ASIACRYPT*. Berlin, Germany: Springer, 2001, pp. 552–565.

[31] A. Sahai and B. Waters, "Fuzzy identity-based encryption," in *Advances in Cryptology—EUROCRYPT*. Berlin, Germany: Springer, 2005, pp. 457–473. doi: 10.1007/11426639_27.
[32] V. Goyal, O. Pandey, A. Sahai, and B. Waters, "Attribute-based encryption for fine-grained access control of encrypted data," in *Proc. 13th ACM Conf. Comput. Commun. Secur.*, Alexandria, VA, USA, Oct./Nov. 2006, pp. 89–98. doi: 10.1145/1180405.1180418.
[33] J. Bethencourt, A. Sahai, and B. Waters, "Ciphertext-policy attribute-based encryption," in *Proc. IEEE Symp. Secur. Privacy (SP)*, May 2007, pp. 321–334. doi: 10.1109/SP.2007.11.
[34] T. Jung, X.-Y. Li, Z. Wan, and M. Wan, "Control cloud data access privilege and anonymity with fully anonymous attribute-based encryption," *IEEE Trans. Inf. Forensics Security*, vol. 10, no. 1, pp. 190–199, Jan. 2015. doi: 10.1109/TIFS.2014.2368352.
[35] Z.-R. Li, E.-C. Chang, K.-H. Huang, and F. Lai, "A secure electronic medical record sharing mechanism in the cloud computing platform," in *Proc. IEEE 15th Int. Symp. Consum. Electron. (ISCE)*, Jun. 2011, pp. 98–103. doi: 10.1109/ISCE.2011.5973792.
[36] A. Sarma, A. Matos, J. Girão, and R. L. Aguiar, "Virtual identity framework for telecom infrastructures," *Wireless Pers. Commun.*, vol. 45, no. 4, pp. 521–543, Jun. 2008. doi: 10.1007/s11277-008-9475-4.
[37] A. Matos, J. Girao, S. Sargento, and R. Aguiar, "Preserving privacy in mobile environments with virtual network stacks," in *Proc. IEEE Global Telecommun. Conf.*, Nov. 2007, pp. 1971–1976. doi: 10.1109/GLOCOM.2007.378.
[38] S. Clauß, D. Kesdogan, and T. Kölsch, "Privacy enhancing identity management: Protection against re-identification and profiling," in *Proc. Workshop Digit. Identity Manage.*, Fairfax, VA, USA, Nov. 2005, pp. 1–10.
[39] Z. Chen, "A privacy enabled service authorization based on a user-centric virtual identity management system," in *Proc. 2nd Int. Conf. Commun. Netw. China*, Shanghai, China, Aug. 2007, pp. 423–427. doi: 10.1109/CHINACOM.2007.4469418.
[40] W. Shen, J. Qin, J. Yu, R. Hao, and J. Hu, "Enabling identity-based integrity auditing and data sharing with sensitive information hiding for secure cloud storage," in *IEEE Trans. Inf. Forensics Security*, vol. 14, no. 2, pp. 331–346, Feb. 2019. doi: 10.1109/tifs.2018.2850312.
[41] A. Mehmood, I. Natgunanathan, Y. Xiang, H. Poston, and Y. Zhang, "Anonymous authentication scheme for smart cloud based healthcare applications," *IEEE Access*, vol. 6, pp. 33552–33567, 2018. doi: 10.1109/ACCESS.2018.2841972.
[42] W. Feng, Z. Yan, and H. Xie, "Anonymous authentication on trust in pervasive social networking based on group signature," *IEEE Access*, vol. 5, pp. 6236–6246, 2017. doi: 10.1109/ACCESS.2017.2679980.
[43] M. Barisch, "Modelling the impact of virtual identities on communication infrastructures," in *Proc. 5th ACM Workshop Digit. Identity Manage.*, New York, NY, USA, Nov. 2009, pp. 45–52. doi: 10.1145/1655028.1655040.
[44] S. Shunmuganathan, R. Saravanan, and Y. Palanichamy, "Secure and efficient smart-card-based remote user authentication scheme for multiserver environment," *Can. J. Elect. Comput. Eng.*, vol. 38, no. 1, pp. 20–30, 2015.
[45] S. Jangirala, S. Mukhopadhyay, and A. K. Das, "A multi-server environment with secure and efficient remote user authentication scheme based on dynamic ID using smart cards," *Wireless Pers. Commun.*, vol. 95, no. 3, pp. 2735–2767, Aug. 2017.
[46] S. S. Sahoo, S. Mohanty, and B. Majhi, "An improved and secure two-factor dynamic ID based authenticated key agreement scheme for multiserver environment," *Wireless Pers. Commun.*, vol. 101, no. 3, pp. 1307–1333, Aug. 2018.
[47] X. Wu, J. Xu, and B. Fang, "Lightweight mutual authentication scheme for protecting identity in insecure environment," *China Commun.*, vol. 15, no. 6, pp. 158–168, Jun. 2018. doi: 10.1109/cc.2018.8398512.
[48] P. Joshi and C.-C. J. Kuo, "Security and privacy in online social networks: A survey," in *Proc. IEEE Int. Conf. Multimedia Expo*, Jul. 2011, pp. 1–6. doi: 10.1109/ICME.2011.6012166.
[49] B. Möller, "Provably secure public-key encryption for length-preserving chaumian mixes," in *Proc. RSA Conf. Cryptographers' Track*, Berlin, Germany, Apr. 2003, pp. 244–262.
[50] E. Käsper, "Fast elliptic curve cryptography in OpenSSL," in *Financial Cryptography and Data Security* (Lecture Notes in Computer Science), vol. 7126, G. Danezis, S. Dietrich, and K. Sako, Eds. Berlin, Germany: Springer, 2012.
[51] (Feb. 2019). (AVISPA). [Online]. Available: http://www.avispa-project.org/
[52] (Feb. 2019). *OpenStack*. [Online]. Available: https://www.openstack.org/

IBRAHIM GOMAA received the B.Sc. degree in electrical engineering (Communication section), from Cairo University, Egypt, in 2002, and the M.Sc. degree in electronics engineering from the Computers and Systems Department, Helwan University and National Telecommunication Institute, Egypt, in 2011. He is currently pursuing the Ph.D. degree in computer science with Helwan University. Actually, he spent 13 years as a Network Security Administrator with the National Telecommunication Institute, from 2005 to 2018, where he is currently a Research Assistant. His current research interests include information security, network security, virtualization and cloud computing, big-data science, and Internet of Things.



EMAD ABD-ELRAHMAN received the B.Sc. degree in electronics engineering from Mansoura University, Egypt, in 1999, and the M.Sc. degree in electronics engineering from the Computers and Systems Department, Mansoura University and National Telecommunication Institute, Egypt, in 2004. In 2008, he joined the University of UPMC-France (Paris-6) and IMT (Institute Mines-Telecom) Telecom SudParis, where he received the Ph.D. thesis degree in computer science and telecommunication, in 2012. Actually, he spent three years as a Guest Researcher with the RST Department, Telecom SudParis (IMT)-CEA Saclay-France (2014–2016). He has been an Associate Professor with the National Telecommunication Institute, Cairo, Egypt, since 2018. His current research interests include networking, optimization, multimedia, multimodal traffic in ITS, virtualization SDN/NFV, and cloud computing. He is involved in many European and French projects, including the UP-TO-US, DVD2C, and CA-ITS.

ELSAYED SAAD received the B.Sc. degree in electrical engineering (communication section), Cairo University, in 1967, the M.Sc. degree from the Electronic and Communication Engineering Department, Cairo University, in 1974, and the Dipl.Ing. and Dr. Ing. degrees in electrical engineering from Stuttgart University, in 1977 and 1981, respectively. He has served in military, from 1969 to 1972. He is currently a Professor of electronic circuits with the Faculty of Engineering, University of Helwan. He has authored and/or co-authored 188 Papers. He is an International Scientific Member of the ECCTD, in 1983, and a member of the National Radio Science Committee. He is also a member of the Egyptian Engineering Syndicate, a member of the European Circuit Society (ECS), and a member of the Society of Electrical Engineering (SEE). He is an Inventor of the Saad's Single Amplifier SC Structure. He has been an Engineering Consultant for the Supreme Council of Universities, since 2002. He was a member of the Helwan University Council for the Award of Scientific Research. He is the Judge for the National Scientific Award (Egypt National Level).

ADLEN KSENTINI received the Ph.D. degree in computer science from the University of Cergy-Pontoise, in 2005. From 2006 to 2016, he was an Assistant Professor with the University of Rennes 1. In 2016, he joined the Communication Systems Department, EURECOM, as an Assistant Professor. He has been working on network slicing in the context of two European projects on 5G, H2020 projects 5G!Pagoda, and 5GTransformer. He is an IEEE COMSOC Distinguished Lecturer.