The Journal of Supercomputing (2021) 77:1693–1713
https://doi.org/10.1007/s11227-020-03313-y

A lightweight anonymous authentication scheme for secure cloud computing services

Hamza Hammami[1] · **Sadok Ben Yahia**[1,2] · **Mohammad S. Obaidat**[3,4,5]

Published online: 24 May 2020

Abstract

Cloud computing represents the latest technology that has revolutionized the world of business. It is a promising solution giving companies the possibility of remotely storing their data and accessing services whenever they are needed and at a lower cost. However, outsourcing IT resources also brings risks, especially for sensitive information in terms of security and privacy, since all data and resources stored in the cloud are managed and controlled by cloud service providers. On the other hand, cloud users would like cloud service providers not to know what services being accessed and how often they are using them. Therefore, designing mechanisms to protect privacy is a major challenge. One promising research area is via authentication mechanisms, which has attracted many researchers in this delicate subject. For this, several solutions have been devised and published recently to tackle this problem. Nevertheless, these solutions often suffer from different types of attacks, high computing and communication costs, and the use of complex key management schemes. To address these shortcomings, we propose an approach that ensures the optimal preservation of the privacy of cloud users to protect their personal data including identities. The suggested approach gives the cloud user the ability to access and use the services provided by cloud service providers anonymously without the providers of those services knowing their identity. We demonstrate the superiority of our proposed approach over several anonymous authentication solutions in terms of computation and communication costs.

Keywords Cloud computing · Security · Attacks · Privacy · Anonymous · Authentication.

✉ Hamza Hammami
hamzahammamii@gmail.com

Extended author information available on the last page of the article

1 Introduction

Undeniably, Internet technology has been growing exponentially since its inception. Cloud computing, as a new emerged trend in the world of data and communication technologies, is a computing paradigm in which businesses can store their data and access applications remotely [1]. This is how the cloud has attracted much attention in both academia and industry, with its scalability, collaboration, agility, availability, and cost reduction, besides offering a compelling alternative to IT solutions in-house [2]. However, by outsourcing the IT infrastructure, a number of security issues have been introduced due to the fact that all resources are remotely located and managed by third-party cloud service providers (CSPs) [2]. One crucial and automatic point when using outsourced cloud services is the presence of a good authentication mechanism. More precisely, the key issue of the cloud, being a common IT platform, is that it has to allow for strong mechanisms to properly establish the authenticity of its users and mitigate as many vulnerabilities as possible [2]. The power of this authentication system is related to the need for confidentiality required by users. However, the critical secure identity management can even bring in a more complex dimension when it comes to cloud computing with the need for appropriate online authentication, including comprehensive protection for both the user and sensitive data [2].

In this context, the main motivation of our approach is to propose an anonymous authentication scheme in order to better protect the personal data of users which is equivalent to hiding the maximum personal data regarding CSPs. The protection of personal data is an essential property in our proposed scheme. The particularity will be the adaptability of the scheme to the users' requirements allowing them to better refine the level of anonymity and untraceability. In fact, anonymity represents a property that ensures that the identity of the cloud user who uses a service or resource cannot be disclosed and untraceability is the inability of an unauthorized cloud user to link a task that has been performed to the user who performed it. The adoption of our approach will ensure the preservation of the privacy of its users in terms of protection of their personal data, including identity. Thus, they will be able to access and proceed to the consumption of the services in an anonymous and legitimate way without the CSP knowing their identities apart from the awareness of services that have been consumed.

The main contributions of the paper are the authentication scheme providing the anonymous use of cloud services through anonymous access generated during each service consumption request. The characteristics of our scheme are:

- The adaptive personal data security policy defined for each user, allowing them to provide a required level of anonymity.
- The anonymous use of cloud services, where the only information the CSP will know is that a legitimate user has requested a service.
- The anonymous credentials, where anonymous access allows users to make anonymous requests without disclosing other credentials.

The paper is organized as follows. In Sect. 2, we give the general description of cloud computing, with its features, service models, and deployments. In Sect. 3, we first highlight the adversary model, and then, we describe the security requirements and the design goals of our proposed approach. In Sect. 4, we review the state of the art work on anonymous authentication schemes that have been proposed to address the issue of access control and privacy of data stored in the cloud environment. Subsequently, we carry out a comparative study of these schemes, from which we try to inspire ourselves to be able to elaborate and make our contribution in this field. In Sect. 5, we describe the details of the proposed solution to deal with the limitations of the existing anonymous authentication schemes. We illustrate the performed security analysis in Sect. 6 to show the effectiveness and reliability of our solution. Finally, this paper ends with a general conclusion evaluating the performance.

2 Cloud computing framework

In this section, we give details of cloud computing technologies. We first address their essential characteristics. Then, we present their different service and cloud-deployment models.

2.1 Essential characteristics

Cloud computing has the following five key features [3]:

- Self-service on demand: The use of services and resources is entirely automated, and it is the user, by means of a control console, who sets up and manages the configuration remotely.
- Broad network access: Services are accessible from the Internet via traditional and heterogeneous equipment, light or heavy.
- Resource pooling: The provider's computing resources are gathered and used for serving multiple clients under one co-residence model, with resources dynamically allocated as a function of requests. Generally, the client does not know the exact localization of resources provided to them, even though they can specify this location at some more abstract levels (like the country, the region, and the data center).
- Rapid elasticity: Resources have the ability to be provisioned and released flexibly and automatically, with the objective of responding rapidly and extensively to demand. For the customer, resources appear unlimited and are capable of being allocated at any time and in any quantity.
- Pay-per-use: Cloud systems automatically control and optimize the use of resources by means of measurement at certain abstraction levels appropriate to the service type. The use of resources is in fact supervised, controlled, and reported to provide transparency for CSPs and customers.

2.2 Service and deployment models

A cloud infrastructure is a collection of hardware and software making the five essential characteristics of cloud computing possible. It can be seen as containing a physical layer and an abstraction one. The physical layer consists of the hardware resources necessary to support the provided cloud services, including servers, storage, and network components. Conceptually, the physical layer is under the abstraction one. It comprises the software deployed on the physical layer, which presents the essential characteristics of the cloud and enables the provider to maintain different types of services. Accordingly, there are different service and deployment models that allow the implementation of services on a cloud infrastructure [3].

The cloud service can be clustered into three service provisioning models, which define the type of offered service [3]:

- Software as a service (SaaS): Clients are able to use providers' applications running on the infrastructure of the cloud. These applications are accessible via light interfaces like Web browsers or program interfaces. As a matter of fact, clients do not manage the underlying cloud infrastructure including the storage, operating systems, servers, network, or even the application functions except for parameters of limited user configuration.
- Platform as a service (PaaS): Clients can deploy cloud infrastructure applications through the use of provider-supported languages, tools, services, and libraries. Clients do not manage the underlying cloud infrastructure including the storage, operating systems, servers, or network, but control the deployed applications and potentially the configuration parameters of the environment hosting the applications.
- Infrastructure as a Service (IaaS): Customers are capable of accessing the networks, storage, processing, and other fundamental computing resources through which customers can deploy and run any software type, including applications and operating systems. In addition, clients do not manage any underlying cloud infrastructure. On the other hand, they control the deployed applications, the storage, and the operating systems, and they potentially monitor some network components to a limited extent.

The cloud has four deployment models, which define how to manage the cloud infrastructure on which the services are made use of [3].

- Public cloud: The cloud infrastructure is shared by the general public. The cloud infrastructure is physically remotely placed on the premises of the CSPs and managed by them. It can be utilized and configured by an industrialist, an academician, a governmental organization, or a combination of several organizations.
- Private cloud: The cloud infrastructure is used exclusively by one organization and can be managed by it. It may be also managed by a third party or a combination of the two. Such an infrastructure can be physically placed on the premises of the organization or outside.

– Community cloud: The cloud infrastructure is used exclusively by a community of organization customers with common interests. It can be managed by one or several community organizations, a third party, or a combination of both. It is physically placed on the premises of one or several organizations in the community or outside.
– Hybrid cloud: The cloud infrastructure is comprised of two or several distinct cloud infrastructures (private, community, or public) which remain fully fledged entities, but are interlinked by standardized or proprietary technologies to enable the portability of data and applications.

Figure 1 illustrates the cloud paradigm architecture, which summarizes the features, different service and deployment models explained above.

3 Adversary model, security requirements, and design goals

In this section, we first present a threat model that identifies the capabilities of attackers in the cloud computing environment. Second, we describe the security requirements and the design goals of the proposed security scheme.

3.1 Threat model

Cloud computing represents an IT infrastructure in which software and data are stored and processed remotely in the data center of a cloud computing provider or in interconnected centers using an excellent bandwidth essential for the fluidity of the system; accessible as a service via the Internet. However, this system immediately highlights a major security problem, the resolution of which constitutes a real challenge [4]. The security problem linked to the sent or received transmission of confidential data between the remote user and the cloud computing environment through

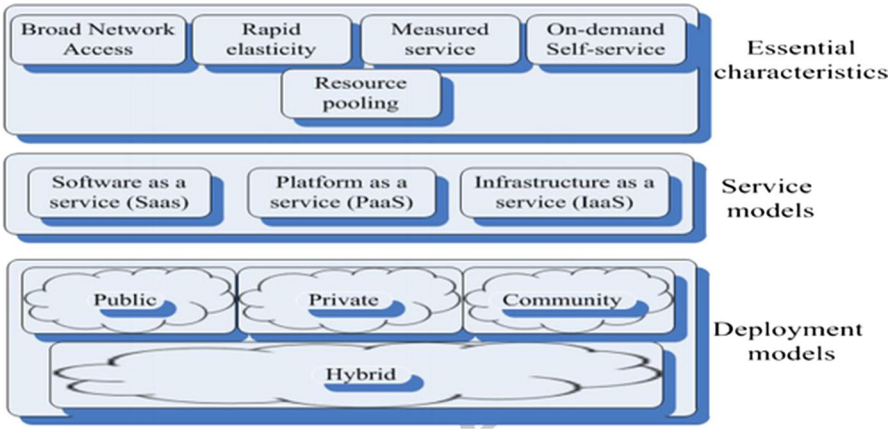

Fig. 1 Cloud computing architectural framework

a network which is not always secure effectively makes these data vulnerable to numerous threats and gives the opportunity for adversaries to exploit these threats in order to compromise confidential data and to invade users' privacy by accessing or taking the possession of all or part of their personal data [5]. In addition, this vulnerability opens the way for adversaries to compromise the confidentiality of personal data of the cloud users, as well as sensitive information that can be exploited by these adversaries in order to disclose personal data [6]. Figure 2 illustrates the security issues related to the cloud computing environment.

Therefore, it has become essential to introduce the protection of personal data of remote users in order to guarantee them more security. This requires the implementation of a strong mechanism to correctly authenticate users and mitigate as many vulnerabilities as possible. This has been the subject of several research approaches that have been developed to address the security issues that will be mentioned in Sect. 4.

3.2 Security requirements in cloud computing environment

Although the cloud is a fast-growing technology adopting the principle of outsourcing the IT infrastructure, there are still challenges to overcome in terms of security. These challenges will need to be addressed so that cloud users can enjoy all the benefits of the cloud and place their absolute trust in them. Indeed, enhanced security and privacy practices will attract more users and businesses to the world of cloud computing. The biggest security challenge is related to the loss of control over some personal data, data leaks, and identity protection when migrating applications and sensitive data to the cloud [2, 7].

Security, protection of personal data "privacy," and trust are the main concerns that prevent the massive adoption of the cloud. In a survey conducted by the Fujitsu Research Institute on cloud users [8], it was found that 88% of them were worried about who had access to their data and required more digital privacy. The reasons were, among other things, that cloud users did not trust the security mechanisms and

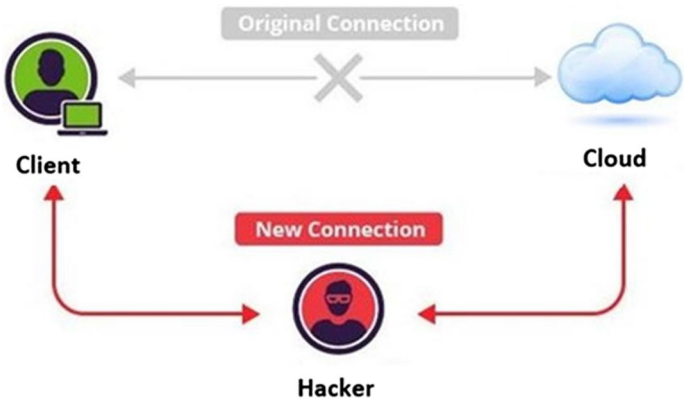

Fig. 2 Cloud computing security issues

the service provider (CSP) itself. However, one of the major questions that cloud users must answer is: Do they trust the CSP not to disclose their personal data or not to change or delete them?

Since the user's identity and sensitive information are regularly used in the authentication process when accessing cloud services, it becomes important to protect them [2]. In other words, how can the CSP provide authentication while remaining anonymous? This assurance of anonymity authentication necessitates the presence of a system that must have the ability to hide the identities of the two communicating parties [2]. It must also provide a robust and secure procedure to authenticate each party. This motivates users to access services provided by the CSP with greater confidence and ability to control their personal information. Anonymous authentication seems to be usually a contradictory statement, because anonymity requires hiding the identity, as opposed to authentication which requires revealing identity in order to be verified. The use of anonymous accreditations makes it possible to prove its legitimacy without having to reveal its identity explicitly. The compromise will be to be able to verify the authenticity of a user without knowing their identity [2].

To sum up, it seems that the protection of data in the cloud is insufficient, that is why even the identity of the cloud user must be protected against the cloud provider and other customers. One of the most important goals we want to achieve in cloud computing security is the privacy of users. This can be done by protecting personally identifiable information against the service provider, so our problem is: How can we ensure anonymous authentication of users without having to provide their real identities to the service provider?

3.3 Design goals

In this context, the present work is part of the research theme on security challenges including the protection of personal data during the authentication process, posed in cloud environments. Our goal is to propose an approach that will provide a complete architecture, in order to ensure an optimal privacy of the cloud user. Privacy is considered a key element in the cloud environment, so the proposed anonymous authentication will have to guarantee the anonymous consumption of cloud and on-demand services. The CSP adopting our approach will ensure the preservation of the privacy of its users in terms of protecting their personal data, including identity. They will therefore be able to access and proceed to the consumption of the services in an anonymous and legitimate way without the CSP knowing their identity.

4 Related work

In this section, we delve into some recent work to circumvent infrastructure security issues related to cloud computing. Particularly, we detail the approaches that have been based on the anonymous authentication mechanisms proposed to

assure data security, especially access management and remote users' identities in the cloud. We conclude this section by comparing the different approaches studied in this section.

The authentication approach depends essentially on its desired and adequate use, for example, the authentication of users in the cloud environment is different from that of other environments. Since the identity of the user is sensitive information regularly used in the authentication process when accessing cloud services, a critical need is to protect and prevent users from disclosing their personal information to the CSP [2, 9].

In the same vein, some research work has been carried out to define security mechanisms for the protection of personal data, and only some schemes have been designed by integrating anonymity as a basic element of interest to us. For this, several solutions have been proposed to remedy this problem. For instance, the authors in [10] proposed a solution based on elliptic curve cryptography in order to ensure secure authentication to the remote server. This authentication process relied primarily on the use of two-factor authentication with a key agreement between the server and the user making the authentication.

Furthermore, the authors in [11] suggested an authentication scheme which consisted in giving a remote user secure access to the remote server. The propounded security scheme was based on its operation with the use of cryptography on elliptic curves.

Moreover, the authors in [12] devised a security approach that would meet essential security requirements and provide mutual authentication between the cloud and its devices. This approach was primarily based on elliptic curve cryptography to provide secure communication between the cloud and its connected devices.

In addition, the authors in [13] proposed an effective and improved authentication solution based primarily on the use of identity and cryptography on elliptic curves to provide a password authenticated key exchange authentication scheme that could be extended.

Moreover, the authors in [14] suggested an authentication scheme with a key agreement between the Telecare Medical Information Systems (TMIS) and their users. The proposed authentication scheme provided an efficient authentication scheme that would ensure patient security and privacy in the TMIS. In addition, this authentication scheme would verify the legality of users and the TMIS server during remote access.

Furthermore, the authors in [15] put forward an authenticated key exchange solution based on a two-factor anonymous dynamic identifier. This proposed protocol would support smart card revocation and password update without centralized storage.

In addition, the authors in [16] proposed a two-factor anonymous authenticated key agreement scheme to ensure a secure logon process using elliptic curve cryptography.

Moreover, the authors in [17] suggested an authentication approach that would meet all security requirements and resist various attacks. This devised solution for connecting integrated devices to the cloud server using cryptography based on elliptic curves.

Besides, the authors in [18] suggested a solution that aimed to randomize the transmitted data in a way that would complicate the opponent's tasks on the channel and make them unable to link the various conversations. It also allowed the interconnected parties to recognize the received messages.

Furthermore, the authors in [19] proposed an anonymous and efficient two-factor authentication protocol to properly authenticate users to the mobile cloud computing environment. This suggested authentication protocol was based on the use of cryptography on elliptical curves to provide mutual authentication between mobile devices and cloud computing.

Table 1 summarizes the advantages and limitations of each proposed security scheme.

After focusing on anonymous authentication schemes [10–19] fitting in the same trend as our scheme. All these anonymous authentication schemes have led us to opt for our solution whose main objective is to be able to use the cloud services while being anonymous and while proving its legitimacy regarding the CSP. In addition, the originality will be to ensure this level of anonymity and respect the privacy of cloud users, while being independent of the CSP without any constraints at the level of confidence, it claims to provide. In the next section, our contribution is presented, where we present a new anonymous authentication protocol that ensures the privacy of users regardless of the concept of trust imposed in such an environment.

5 Proposed solution

We take advantage here of the security mechanisms that we have studied before [10–19]. The anonymous authentication scheme we have suggested has used elliptic curve cryptography to ensure performance, reliability, and robustness against various types of attacks. Furthermore, based on the limitations of the approaches, we have studied in the literature regarding their limited resources, and they are unable to make the necessary calculations. In this regard, we propose an anonymous authentication scheme that operates with inexpensive functions, namely: (i) the hash function, (ii) the concatenation, and (iii) the or-exclusiveness. These functions are used to reduce any computational cost. Moreover, we utilize a session key in our scheme to encrypt and decrypt the messages exchanged between the cloud and its users.

Table 2 summarizes the list of symbols used in our proposed scheme.

The operation of the proposed scheme is based on some security operations which are presented in three phases: setup, registration, and authentication. Each phase is detailed as follows:

5.1 Setup phase

In this phase, cloud users generate a list of parameters. These latter will allow the other phases to operate securely. The details are as follows:

Table 1 Advantages and limitations of each suggested security scheme

Schemes	Advantages	Limitations
Qu et al. [10]	- It is mainly based on the use of an elliptic curve cryptosystem in combination with two-factor authentication with a key agreement between the server and the user performing the authentication	- It does not support user untraceability - It is susceptible to the man-in-the-middle attack - It requires a high execution time during the authentication process
Chaudhry et al. [11]	- It is based on its operation with the use of cryptography on elliptic curves to give a remote user secure access to the remote server.	- It is vulnerable to the known-key-security attack on the session key - It does not support user untraceability - It does not provide security against the man-in-the-middle attack
Chang et al. [12]	- It takes advantage of the opportunities offered by elliptic curves in order to provide mutual authentication between the cloud and its connected devices	- It does not support the anonymity and untraceability of users - It does not ensure a perfect forward secrecy property - It does not resist against the known-key-security attack
Farash et al. [13]	- It provides a two-part authentication key exchange mechanism based on identity and elliptical curves	- It is vulnerable to the man-in-the-middle attack - It does not provide the anonymity and untraceability of users
Chaudhry et al. [14]	- It provides an efficient authentication scheme to ensure patient security and privacy in the Telecare Medical Information Systems (TMIS) - It verifies the legality of users and the TMIS server during remote access	- It does not support user untraceability - It is susceptible to the known-key-security attack on session key
Xie et al. [15]	- It provides an authenticated key exchange solution based on a two-factor anonymous dynamic identifier	- The major drawback of this solution is that it is vulnerable to the man-in-the-middle attack
Lu et al. [16]	- It provides a two-factor anonymous authenticated key agreement scheme to ensure a secure logon process using elliptic curve cryptography	- It does not ensure user untraceability - It is vulnerable to the man-in-the-middle attack
Kumari et al. [17]	- It securely connects integrated devices to the cloud server using cryptography based on elliptic curves	- It does not provide user untraceability - It does not ensure security against the known-key-security attack
Xiangxue et al. [18]	- It is based on a data randomization trick complicating the adversary's tasks and limiting their capacities on the communication channel	- The major drawback of this solution is that it does not provide a perfect forward secrecy property
Jiaqing et al. [19]	It is based on the use of cryptography on elliptical curves in order to provide mutual authentication between mobile devices and cloud computing	- It does not provide user untraceability

Table 2 List of symbols

Symbol	Description
E	Elliptic curve under reference
p and q	Long prime integers
e(.)	Bilinear pairing function
G_1	Multiplicative group of order q
G_2	Additive group of order q
$H_1(.), H_2(.)$	One-way hash functions
x_{UC}	The secret key to the user cloud
x_{CP}	The secret key to the cloud
P	Group generator
a, b, n, d	Random numbers
t_{UC}, t_{CP}	Time stamps
ID_{UC}	The identifier of the cloud user
ID_{CP}	The anonymous identifier of the cloud
AID_{UC}	The anonymous identifier of the cloud user
AID_{CP}	The anonymous identifier of the cloud
$\oplus$	Bitwise XOR operation
$\|\|$	Bitwise concatenation operation
SK	Session key
Enc, Dec	Encryption and decryption functions

1. At the beginning, they arbitrarily produce two large prime integers p and q. After that, they choose an elliptic curve E(F_p) on F_p.
2. 2. Then, they firstly generate two groups of order q: a first additive group G_1 and a second multiplicative G_2. Secondly, they generate (P; *e:* $G_1 \times G_1 \longrightarrow G_2$). We note here that P represents a generator of the additive group and e denotes a bilinear pairing.
3. Next, the cloud user chooses two secure hash functions:
   - H_1: $\{0, 1\}^* \times G_1 \longrightarrow G_1$
   - H_2: $\{0, 1\}^* \times G_2 \longrightarrow Z_{q*}$
4. After that, they generate a random number. The latter will be considered as a secret key $x_{UC} \in Z_{q*}$. Then, we find: $Y_{UC} = x_{UC} \cdot \mathrm{P}$
5. Finally, they send { E(F_p), G_1, G_2, $H_1(.)$, $H_2(.)$, Y_{UC} } to the cloud and keep its secret x_{UC}.

5.2 Registration phase

Once the setup phase is completed, during which the cloud user has generated a list of parameters, these parameters will allow the other phases to operate in the best safety conditions. During the registration phase, cloud computing securely records its users so that they can receive and store them safely. The stages of registration between the cloud and its users are detailed as follows:

1. After receiving the parameters generated by the cloud user terminal, the cloud will generate a random number that will be considered as its secret key $x_{CP} \in Z_{q*}$. Then it will calculate $Y_{CP} = x_{CP} \cdot \mathrm{P}$. Once the calculation is complete, the cloud sends its user ID_{CP} identity with Y_{CP}. This sending is done via a secure communication channel while using a Secure Socket Layer (SSL). We indicate by UC cloud user and CP cloud remote platform.
2. Once ID_{CP} with Y_{CP} is received by the cloud user, the latter will check the validity of the received cloud identity. In case the validity check result is not correct, the user will declare that it is a conflict. Otherwise, the user will produce a t_{UC} time stamp as well as two ephemeral(lasts for a very short time) secrets **a** and $\mathbf{b} \in Z_{q*}$. After that, the user computes $A_{UC} = a \cdot P$, $B_{UC} = b \cdot P$, $Q_1 = A_{UC} \oplus Y_{CP}$, $Q_2 = B_{UC} \oplus Y_{CP}$.
3. Subsequently, thanks to the secret numbers generated and the secret keys calculated, the users will hide their real identity as well as the cloud. Subsequently, they will calculate their corresponding anonymous identities in the following way:

   – $AID_{UC} = H_1(ID_{UC} \| t_{UC} \| x_{UC} \| A_{UC} \| B_{UC})$ and
   – $AID_{CP} = H_1(ID_{CP} \| Q_1 \| Q_2)$

   Afterwards, the cloud user calculates $C_{CP} = \mathrm{a} + \mathrm{b} + AID_{CP} \cdot x_{UC}$ and sends to the cloud $\{ AID_{CP}, AID_{UC}, A_{UC}, B_{UC}, C_{CP} \}$
4. After having received $\{ AID_{CP}, AID_{UC}, A_{UC}, B_{UC}, C_{CP} \}$ by the cloud, the latter will produce a time stamp t_{CP} and computation $Q_1 = A_{UC} \oplus Y_{CP}$, $Q_2 = B_{UC} \oplus Y_{CP}$ and $AID'_{CP} = H_1(ID_{CP} \oplus Q_1 \oplus Q_2)$. Next, the cloud will send AID'_{CP} and t_{CP} to its user.
5. Once AID'_{CP} and t_{CP} are received by the cloud user, the latter will check the freshness and validity of t_{CP} and then check whether $AID_{CP} = AID'_{CP}$ and $C_{CP} \cdot \mathrm{P} = A_{UC} + B_{UC} + AID'_{CP} \cdot Y_{UC}$. If the result of the check is verified by the cloud user as invalid, there will be an error message returned to the cloud. Otherwise, the registration phase is performed successfully.

Figure 3 depicts the progress of the registration phase.

5.3 Phase of authentication

As soon as the registration step is completed, the utilizer will become a cloud user and can perform anonymous authentication. The details of this phase are described by the following steps:

1. First, the cloud generates a second time stamp t'_{CP}. After that, it generates $\mathrm{n} \in Z_{q*}$, which is an arbitrary number to be used once. Then, the cloud calculates $N_{CP} = \mathrm{n} \cdot \mathrm{P}$, $M_{CP} = \mathrm{n} \cdot Y_{UC}$, $K_{CP} = H_1(N_{CP} \| M_{CP} \| t'_{CP})$, $U_{CP} = \mathrm{e}(M_{CP}, K_{CP})$, $Z_{CP} = x_{CP} + H_1(AID'_{CP} \| U_{CP} \| t'_{CP})^{n \cdot x_{CP} mod q}$ and cipher $= \mathrm{Enc}(AID'_{CP} \| Z_{CP})$. Subsequently, the cloud sends $\{ N_{CP}, \text{cipher}, t'_{CP} \}$ to its user.
2. Once $\{ N_{CP}, \text{cipher}, t'_{CP} \}$ are received by the user, the latter will check both the validity and the freshness of t'_{CP}. After that, the user will calculate $M'_{CP} = x_{UC} \cdot$

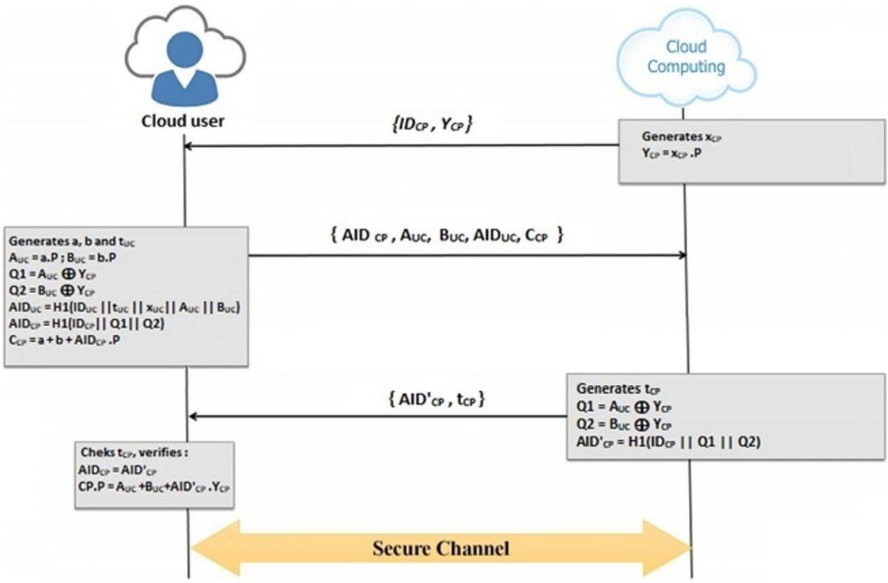

Fig. 3 Registration phase

N_{CP}, K_{UC}= $H_1(N_{CP} \| M'_{CP} \| t'_{CP})$ and $U'_{CP} = \mathrm{e}(K_{UC}, M'_{CP})$. Using the K_{UC} key, the user decrypts the cipher to get the clear = $Dec_{K_{UC}}$(cipher). Next, this user calculates Z'_{CP} = clear $\oplus$ AID_{CP} and checks whether the following equation holds: $Z'_{CP} \cdot \mathrm{P} = Y_{CP}$+P$(H_1(AID_{CP} \| U'_{CP} \| t'_{CP}))^{M'_{CP} \cdot Y_{CP}/Y_{UC}}$. If the result of the equation is verified by the user as incorrect, the authentication phase will be stopped, and an authentication error message will be sent to the cloud. Otherwise, the user has successfully passed the authentication phase. Next, the cloud user will generate a variable d $\in Z_{q*}$ and will calculate D_{UC} = d · P, Pass = $H_2(D_{UC} \| M'_{CP} \| Z'_{CP} \cdot \mathrm{P} \| t'_{CP})$, and the session key SK= H_2(Pass ‖ d · N_{CP}). Subsequently, the user will send { Pass, D_{UC} } to the cloud.

3. Finally, the cloud will calculate $H_2(D_{UC} \| M_{CP} \| Z_{CP} \cdot \mathrm{P} \| t'_{CP})$. Afterwards, it will check the result of the calculation with Pass. If the verification result sent by the user is not correct, then the session will be suspended. Otherwise, the calculation of the session key is done in the following way: SK= H_2(Pass ‖ n · D_{UC}).

The progress of the authentication and key agreement phase is depicted in Fig. 4.

6 Experiment results and discussion

In this section, we describe the experimental part of our approach. It is mainly based on two parts. First, we illustrate our approach through the evaluation of its performance to ensure anonymity, untraceability, persistent privacy and its ability to stem the man-in-the-middle attack, replay, and known-key-security attacks, while

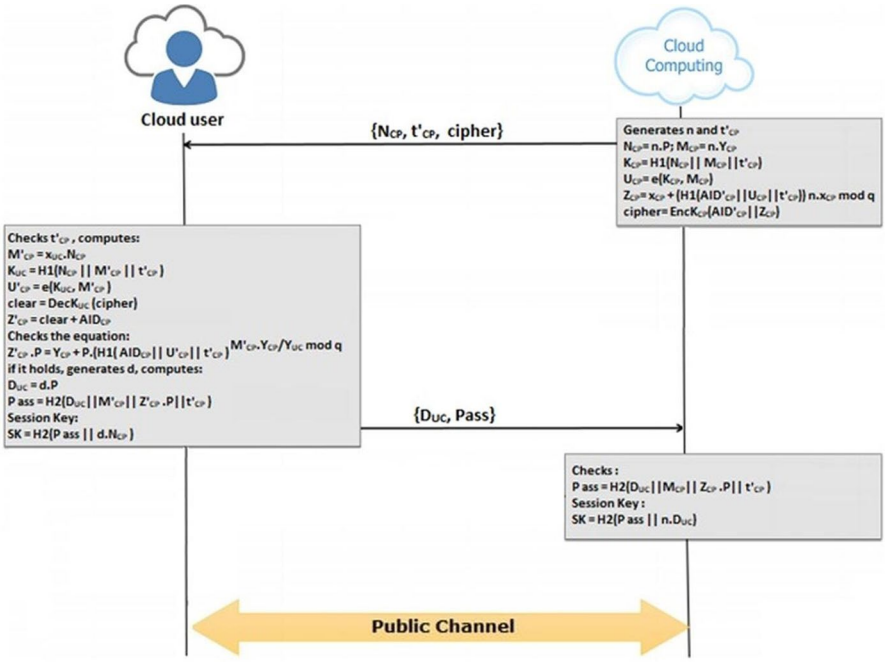

Fig. 4 Authentication and key agreement phase

showing the techniques and tools used. Second, we will show the performance of the proposed solution. To do this, we perform a series of simulation. The objective of simulation is to compare the performance of our proposed scheme to other approaches bearing the same trend in terms of calculation costs and execution time. In what follows, we present and analyze the results of each component.

6.1 Security analysis

Our security analysis will take into consideration anonymity, untraceability, perfect forward secrecy, known-key-security, man-in-the-middle, and replay attacks.

6.1.1 Anonymity

The verifier, regardless of whether there is one or not, must not have the means to identify an authentication requestor [20]. This authentication is provided by our solution, because in the proposed solution, the cloud user's real identity must be masked to be an anonymous identity: $AID_{UC} = H_1(ID_{UC} \parallel t_{UC} \parallel x_{UC} \parallel A_{UC} \parallel B_{UC})$ where $A_{UC} = \mathrm{a} \cdot \mathrm{P}$ and $B_{UC} = \mathrm{b} \cdot \mathrm{P}$. As we have mentioned before, a and b are two random numbers intended to be utilized only once, in order to ensure freshness and randomization. We note also the fact that AID_{UC} is protected by a hash function. Hence, using this function, a possible attacker who may intercept communication

between the cloud and its user will have no way of revealing the real identity of the user. In addition, A_{UC} and B_{UC} are produced utilizing both a and b nonces, which are unknown to the attacker, who does not know the efficient algorithm for calculating the discrete logarithm and hence further protect the anonymity.

6.1.2 Untraceability

It is a fact that an identity provider cannot know the services that one of the cloud users has access to [20]. If a cloud provider cannot know the origin of the access request and its path to reach its destination, any possible attacker cannot listen to the messages exchanged for each session, so he cannot collect all the anonymous identities of the cloud user (AID_{UC}). If the user utilizes the same AID_{UC} value, the attacker can guess that the same value that contains a user's identity may subsequently be used without recognizing its real value, i.e., an attacker sees the same value persistently being applied in the same position during the authentication phase. Therefore, in our proposed solution, we resort to the utilization of secret ephemeral generated arbitrarily as well as the unique time stamp to make all anonymous identities generated from the remote user differently. In this case, the attacker cannot trace the user by monitoring the network activities. As a consequence, the proposed solution ensures the untraceability of cloud users.

6.1.3 Perfect forward secrecy

This is a property assuring past communication could not be decrypted, even if the long-term key is revealed or stolen [21]. This property is verified by our solution; thanks to the session key SK= H_2(Pass ‖ n · d ·P). As mentioned earlier, d and n are secret numbers generated arbitrarily and intended to be used only once via the cloud and its user. These two secret numbers guarantee the freshness of the keys utilized for each session. Therefore, for a potential attacker to have the secret keys generated by the cloud and its user, it cannot become the used session key, since it must compute (n · d · P) from N_{CP} and D_{UC}. We note that N_{CP}= n · P and D_{UC}=d · P, so it will not be able to do it because it does not know any efficient algorithm for the calculation of a discrete logarithm.

6.1.4 Known key security

On condition that a generated session key is compromised by an opponent, this situation should not have influence on other session keys [22, 25]. This property is ensured by the fact that a possible attack cannot identify any session key from a compromised one. This is verified in our solution by using session keys that are computed independently, thanks to secret numbers d and n generated arbitrarily and intended to be used for one session. This clearly shows that our solution guarantees known key security.

6.1.5 Man in the middle

An attack by an attacker who intercepts a communication between the cloud and its users is dangerous because the aggressor pretends to be the original sender [23, 26]. When possessing the original message, the attacker can trap the recipients by making them believe that the message they receive is legitimate. In our scheme, we curb this type of attack by using an authentication process that verifies whether $Z'_{CP} \cdot \mathrm{P} = Y_{CP} + \mathrm{P}(H_1(AID_{CP} \| U'_{CP} \| t'_{CP}))^{M'_{CP} \cdot Y_{CP}/Y_{UC}}$ holds. Accordingly, the attacker will not be able to generate N_{CP} and K_{CP} or calculate and cipher Z_{CP} without owning the private key (x_{CP}) of cloud service providers as well as the random secret numbers. On the other hand, the cloud authenticates the user by verifying whether equation $\mathrm{Pass} = H_2(D_{UC} \| M_{CP} \| Z_{CP} \cdot \mathrm{P} \| t'_{CP})$ is correct. However, without the secret key of the cloud user (x_{UC}), a possible attacker will not be able to calculate M'_{CP} from N_{CP}, and therefore, they will not be able to hide the exact value of the *Pass* variable. As a result, we may conclude through the presentation of this discussion that we can easily stem the man-in-the-middle attack.

6.1.6 Replay attack

This is an attack that consists in intercepting data packets and replaying them, i.e., retransmit them without any decryption to the cloud or to its users [23, 24]. In our solution, we have remedied this situation by the use of time stamps and ephemeral secrets, in such a way that an attacking event intercepts the messages exchanged between the cloud and its users, so it will not be able to replay them to authenticate itself with the cloud or its user. This is because the cloud and its users generate random nonces used for each authentication session and for the verification of the freshness of the time stamps.

Table 3 clearly shows that our proposed solution is resistant to any known attack, namely the replay, known-key-security, and man-in-the-middle attacks. Those solutions put forward by [10, 11, 13, 15, 16] and [11, 12, 14, 17] were vulnerable to the man-in-the-middle and known attacks. In addition, the solution proposed in [19]

Table 3 Security analysis

Security properties	[10]	[11]	[12]	[13]	[14]	[15]	[16]	[17]	[18]	[19]	Ours
SP_1	✓	✓	×	×	✓	✓	✓	✓	✓	✓	✓
SP_2	×	×	×	×	×	✓	×	×	✓	×	✓
SP_3	✓	✓	×	✓	✓	✓	✓	✓	×	✓	✓
SP_4	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
SP_5	✓	×	×	✓	×	✓	✓	×	✓	✓	✓
SP_6	×	×	✓	×	✓	×	×	✓	✓	✓	✓

SP_1: User anonymity; SP_2: User untraceability; SP_3: Perfect forward secrecy

SP_4: Resistance to replay attack; SP_5: Resistance to known key security

SP_6: Resistance to man-in-the-middle attack

did not provide user untraceability and the solutions suggested in [12, 18] did not verify the perfect forward secrecy of users either. Furthermore, only the solution propounded in [15] ensured untraceability, whereas our suggested solution provides user untraceability and perfect forward secrecy.

6.2 Performance evaluation

In this last section, we will show the performance of the proposed solution. To do this, we have performed a series of simulation for evaluating the performance of our anonymous authentication scheme against other existing anonymous authentication schemes as regards the criteria of computation and communication costs. These simulation series are performed using the MIRACL library (Multiprecision Integer and Rational Arithmetic C / C ++ Library) running on a Windows 7 Professional 64-bit machine with 2.5GHz Intel Core i5-2520M processor and 8 GB memory. This library is considered the gold standard for elliptical curve cryptography. It removes all obstacles to free unlimited connections between users and cloud applications.

6.2.1 Computation cost

To show the performance and effectiveness of our authentication scheme with other competing solutions proposed in the literature, we perform a series of tests. After simulating the different tests, we have obtained Fig. 5 which shows the comparison of the performance of our solution with the authentication solutions proposed in [10–17, 19] in terms of total calculation time consumed by the service requester and the CSP.

From this figure, we can say that our proposed security scheme requires a calculation cost on the client user side equal to 0.352 ms which is better than the other competing authentication schemes and which is followed by the solution proposed in [19] which requires 0.497 ms. In addition to that, our solution requires a cloud

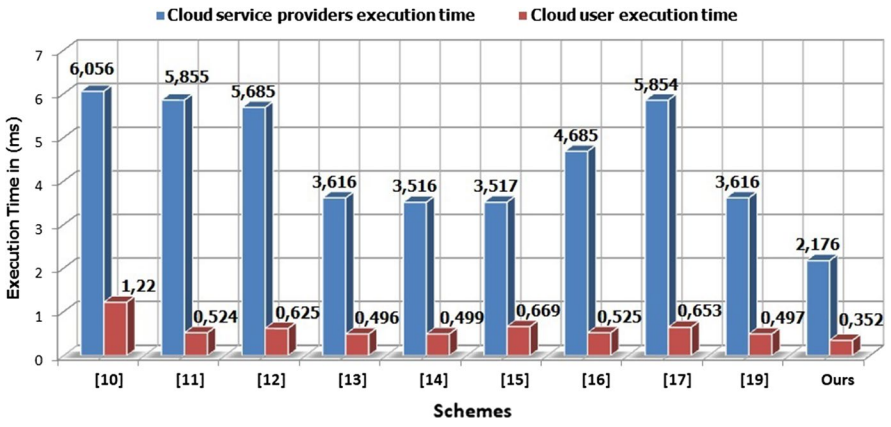

Fig. 5 Time consumption in comparison with schemes, respectively, proposed in [10–17, 19]

service providers calculation cost equal to 2.176 ms, which is also better than the other solutions and which is followed by the solution put forward in [14] which requires 3.516 ms. This illustrates that our suggested scheme is better than the proposed authentication schemes. We can conclude by stating that our suggested security scheme is always effective compared to other related schemes, whether on the client side or on the cloud service providers side.

6.2.2 Communication cost

Figure 6 illustrates the comparison of the performance of our proposed authentication scheme with other related competing authentication schemes put forward in [10–19] in terms of communication cost consumed by the service requester and the CSP.

According to Fig. 6, we can say that the cost of the communication message of our designed solution throughout the authentication process, where we perform two communication cycles which are the communication of User-Cloud ⟶ CSP: $< D_{UC}$, Pass> and the communication of CSP ⟶ User-Cloud: $< N_{CP}, T_{CP}$, Cipher >, is equal to 576-bit and 512-bit. Therefore, before illustrating the performance and reliability of our scheme in terms of communication costs compared to the other anonymous authentication schemes proposed in [10–19], we first mention the overall cost of communication by invocation and response messages from our scheme, which is equal to the sum of 576-bit and 512-bit = 1088 bits. In fact, it is more cost-effective than the authentication options of the other schemes. This is followed by the solution suggested in [18] which requires 2464 bits. Hence, by explaining the comparison result, we can conclude that our proposed authentication scheme outperforms all the other related authentication schemes in terms of cost of communication messages.

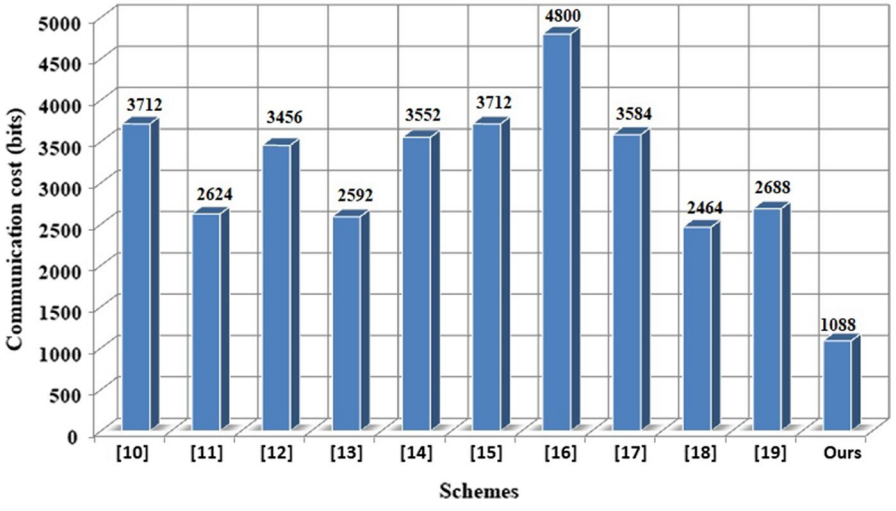

Fig. 6 Message size in comparison with schemes, respectively, in [10–19]

7 Conclusion

The concept of anonymity arises in many occasions on the Internet, especially for e-mail, browsing, and several applications that need to guarantee the anonymity property, in particular e-commerce. However, with the emergence of cloud computing, security and privacy have been addressed when using different services. Cloud technology, before being completely secure, will have to incorporate improvements that will better protect users, thus ensuring the confidentiality and the privacy of their personal data.

After presenting the state-of-the-art authentication mechanisms reported for the cloud, we have identified the weak points and the strengths of the different mechanisms studied in order to better establish our solution. We have proposed a security scheme to provide an anonymous authentication adaptive to the privacy requirements of cloud users, which is characterized by an adaptive policy of protection of personal data. This scheme takes advantage of opportunities offered by elliptic curve cryptographic functions and by the bilinear pairing to be able to offer an anonymous authentication system in which users can prove that they are legitimate, without revealing any sensitive information that can identify them. Our main contribution, therefore, has been to provide the cloud users with anonymous, efficient authentication that allows them to anonymously consume cloud services so that the only information a CSP will know is that a legitimate user has requested a service.

Finally, we have analyzed several attacking scenarios in which we have tried to present our solution advantages and performances concerning the fights against these scenarios of attacks. Then, we have illustrated the superior performance of our approach compared to other anonymous authentication schemes that exist in the literature against computation and communication costs.

References

1. Mansouri Y, Toosi AN, Buyya R (2019) Cost optimization for dynamic replication and migration of data in cloud data centers. IEEE Trans Cloud Comput 7(3):705–718
2. Djellalbia A, Boukerram A (2016) Authentification Anonyme dans un environnement Cloud (Doctoral dissertation, Université Abderrahmane Mira-Bejaia)
3. Probst T (2015) Évaluation et analyse des mécanismes de sécurité des réseaux dans les infrastructures virtuelles de cloud computing (Doctoral dissertation)
4. Karajeh H, Maqableh M, Masa'deh R (2020) Privacy and security issues of cloud computing environment. In: Proceedings of the 23rd IBIMA Conference Vision, pp 1–15
5. Sehgal N K, Bhatt P C P, Acken J M (2020) Cloud computing and information security. In: Cloud computing with security, Springer, Cham, pp 111–141
6. Raj A, Kumar R (2020) An exploration on cloud computing security strategies and issues. In: Inventive communication and computational technologies, Springer, Singapore, pp 549–562
7. Singh V, Pandey S K (2020) Cloud computing: vulnerability and threat indications. In: Performance management of integrated systems and its applications in software engineering, Springer, Singapore, pp 11–20
8. Fujitsu, (2010) Personal data in the cloud: A global survey of consumer attitudes. Available at:http://www.fujitsu.com/downloads/SOL/fai/reports/fujitsu_personal-data-in-the-cloud.pdf. Accessed 01 Nov 2019
9. Chia WY (2009) The classification of e-authentication protocols for targeted applicability (Doctoral dissertation, Monterey. California, Naval Postgraduate School)

10. Qu J, Tan XL (2014) Two-factor user authentication with key agreement scheme based on elliptic curve cryptosystem. J Electr Comput Eng 2014:16
11. Chaudhry SA, Naqvi H, Mahmood K, Ahmad HF, Khan MK (2017) An improved remote user authentication scheme using elliptic curve cryptography. Wireless Pers Commun 96(4):5355–5373
12. Chang CC, Wu HL, Sun CY (2017) Notes on "secure authentication scheme for IoT and cloud servers". Pervasive Mob Comput 38:275–278
13. Farash MS, Attari MA (2014) A secure and efficient identity-based authenticated key exchange protocol for mobile client-server networks. J Supercomput 69(1):395–411
14. Chaudhry SA, Naqvi H, Shon T, Sher M, Farash MS (2015) Cryptanalysis and improvement of an improved two factor authentication protocol for telecare medical information systems. J Med Syst 39(6):1–11
15. Xie Q, Wong DS, Wang G, Tan X, Chen K, Fang L (2017) Provably secure dynamic ID-based anonymous two-factor authenticated key exchange protocol with extended security model. IEEE Trans Inf Forensics Secur 12(6):1382–1392
16. Lu Y, Li L, Peng H, Yang Y (2017) An anonymous two-factor authenticated key agreement scheme for session initiation protocol using elliptic curve cryptography. Multimedia Tools and Applications 76(2):1801–1815
17. Kumari S, Karuppiah M, Das AK, Li X, Wu F, Kumar N (2018) A secure authentication scheme based on elliptic curve cryptography for IoT and cloud servers. J Supercomput 74(12):6428–6453
18. Li X, Qiu W, Zheng D, Chen K, Li J (2009) Anonymity enhancement on robust and efficient password-authenticated key agreement using smart cards. IEEE Trans Industr Electron 57(2):793–800
19. Mo J, Hu Z, Chen H, Shen W (2019) An efficient and provably secure anonymous user authentication and key agreement for mobile cloud computing. Wireless Commun Mob Comput. https://doi.org/10.1155/2019/4520685
20. Jiang L, Li X, Cheng L L, Guo D (2013, October). Identity authentication scheme of cloud storage for user anonymity via USB token. In: Anti-Counterfeiting, Security and Identification (ASID), 2013 IEEE International Conference on. IEEE, pp 1–6
21. Yang Y, Golshan A (2017) U.S. Patent No. 9,584,318. Washington, DC: U.S. Patent and Trademark Office
22. Krutz RL, Vines RD (2010) Cloud security: a comprehensive guide to secure cloud computing. Wiley Publishing, New Jersey
23. Subashini S, Kavitha V (2011) A survey on security issues in service delivery models of cloud computing. J Netw Comput Appl 34(1):1–11
24. Obaidat MS, Traore I, Woungang I (2019) Biometric-based physical and cybersecurity systems. Springer, Berlin, pp 165–187
25. Obaidat M, Boudriga N (2007) Security of E-systems and computer networks. Cambridge University Press, Cambridge
26. Hammami H, Brahmi H, Brahmi I, Yahia S B (2016) Security issues in cloud computing and associated alleviation approaches. In 2016 12th International Conference on Signal-Image Technology & Internet-Based Systems (SITIS). IEEE, pp 758–765

Affiliations

Hamza Hammami[1] · Sadok Ben Yahia[1,2] · Mohammad S. Obaidat[3,4,5]

Sadok Ben Yahia
sadok.benyahia@gmail.com

Mohammad S. Obaidat
msobaidat@gmail.com

[1] Faculty of Sciences of Tunis, University of Tunis El Manar, LIPAH-LR11ES14, Tunis 2092, Tunisia

[2] Department of Software Science, Tallinn University of Technology, Akadeemia tee 15a, 12618 Tallinn, Estonia

[3] College of Computing and Informatics University of Sharjah, Sharjah, UAE

[4] King Abdullah II School of Information Technology, Universality of Jordan, Amman, Jordan

[5] University of Science and Technology Beijing, Beijing, China