Analysis of attribute-based cryptographic techniques and their application to protect cloud services

Sana Belguith, Nesrine Kaaniche, Mohammad Hammoudeh

Received: | Revised: | Accepted:

DOI:

ARTICLE TYPE

Analysis of Attribute Based Cryptographic Techniques and their Application to Protect Cloud Services

Sana Belguith*[1] | Nesrine Kaaniche[2] | Mohammad Hammoudeh[3]

[1] School of Computing, Science and Engineering, University of Salford, Manchester, UK
[2]Department of Computer Science, University of Sheffield, Sheffield, UK
[3]School of Computing, Mathematics & Digital Technology, Manchester Metropolitan University, Manchester, UK

Correspondence
*Sana Belguith. Email: s.belguith@salford.ac.uk

Summary

Recent technological advances such as the Internet of Things (IoT), fog computing, cloud applications lead to exponential growth in the amount of generated data. Indeed, cloud storage services have experienced unprecedented usage demand. The loss of user control over their cloud stored data introduced several security and privacy concerns. To address these concerns, cryptographic techniques are widely adopted at the user side. Attribute based cryptography is commonly used to provide encrypted and/or authenticated access to outsourced data in remote servers. However, the use of these cryptographic mechanisms often increase the storage and computation costs; consequently, the energy consumption in the entire cloud ecosystem. In this paper, we provide a comparative analysis of different attribute based cryptographic mechanisms suitable for cloud data sharing services. we also provide a detailed discussion of different reviewed schemes, w.r.t. supported features, namely security, privacy and functional requirements. In addition, we explore the limitations of existing attribute based cryptographic mechanisms and propose future research directions to better fit the growing needs of this cloud environment in terms of energy-savings, processing and storage efficiency and availability requirements.

KEYWORDS:
Cloud computing, Internet of Things, attribute based encryption, attribute based signature, attribute based signcryption, encrypted access control, authentication, privacy preservation.

1 | INTRODUCTION

In the last few decades, there has been a proliferation in the use of distributed computing systems. Today, most distributed applications are built-in pervasive, autonomic while relying on cloud infrastructures. Cloud computing is a large distributed network of processing and storage resources that aims at releasing users from hardware requirements and deployment complexities. This paradigm introduces several benefits such as on-demand self-service, unlimited resource pooling, broad network access and dynamic scalability in a pay per use business model. Based on a pay-as-you-go model, it enables hosting of pervasive applications from users, scientific, and business domains. These benefits encourage individual users and organisations to externalise their data storage to remote servers hosted by a Cloud Server Provider (CSP) [1,2].

The rapid transition toward cloud services raised many concerns in relation to the security of cloud data sharing activities [3,4]. In addition, data centers hosting Cloud applications consume huge amounts of energy, mainly needed for processing huge amounts of data and enforcing suitable security mechanisms, thus contributing to high operational costs and carbon footprints to the environment.

A cloud is considered as an untrusted environment due to its main intrinsic characteristics, namely the availability of its services for public use in a multi-tenant model, use of an untrusted network (i.e., the Internet) and the trust/reliance on third parties, i.e., CSP. Although, outsourcing data storage and processing to a CSP releases users from the burden of maintaining and securing a hardware architecture, they loose control over their data as they delegate these tasks to non fully trusted entity.

In cloud computing, curious CSPs and unauthorized users may attempt both accessing outsourced data as well as revealing and deducing clients' sensitive information, considered as valuable to conduct main recent data leakage attacks. This is mainly acknowledged with the successive revelations about the abuse of sensitive data collection and processing, starting from the US NSA spy program, revealed by E. Snowden in May 2013[1], until the last Cambridge Analytica and Facebook scandal disclosed in April 2018[2].

Consequently, in order to protect data outsourced in remote cloud servers, efficient and fine-grained access to the shared data among a large number of users with different access privileges must be provided. To alleviate users security and privacy concerns, leading CSPs, e.g., Amazon, Google and Microsoft, implemented different security solutions to prevent data disclosure and unauthorized access. Most of CSPs encrypt users data using a symmetric encryption algorithm, such as AES-256 algorithm, before storing enciphered data on remote servers while applying user-based access policies to enforce data access control [3] [4]. However, these approaches can not fully support flexible and scalable data sharing, user's privacy preservation and secure computation. When adopting these CSPs solutions, data owners have to outsource their data contents to the cloud in plaintext. Thus, the CSP is in charge of encrypting the data and handling data sharing among different groups of users. As secret encryption keys are generated, managed and stored at the cloud side, data owners must put full trust on the CSP.

The application of encryption mechanisms at the client side has been advocated in the literature to further address cloud trust and security issues. In this paradigm, the cloud client keeps the secret decrypting keys out of reach of the CSP. Even though the use of encryption schemes ensures data confidentiality, conventional encryption mechanisms such as symmetric and asymmetric encryption schemes are not sufficient to support the enforcement of fine-grained access control policies as key management mechanisms need to be applied to share secret keys among authorised users. The requirement of flexible data sharing among users that have different access privileges while belonging to different dynamic groups [5,6] further complicates the task of providing data confidentiality in the cloud. Consequently, enforcing fine grained encrypted data sharing at the client side is considered as a promising solution, permitting to enforce main security and privacy requirements. This idea led to the use of attribute based cryptographic techniques, including Attribute Based Encryption (ABE), Attribute Based Signature (ABS) and Attribute Based SignCryption (ABSC). In a nutshell, these techniques permit to associate an access structure and/or signing policy to outsourced data contents. This allows authorised users to decrypt and/or sign the data relying on his access rights with no need to share secret keys with the data owner.

Contributions — This paper presents a comprehensive review of the most recent attribute based cryptographic schemes that have been applied to ensure fine-grained and authenticated access control to encrypted and outsourced cloud data, shared among different groups of users. It provides a detailed discussion of different reviewed schemes, w.r.t. supported features, namely security, privacy and functional requirements. It also explores research directions and discusses further extensions of attribute-based mechanisms to better fit the growing needs of this dynamic environment, a.k.a. cloud, in terms of energy-savings, processing and storage efficiency and availability requirements.

Position of Our Paper — Several ABE, ABS and ABSC mechanisms were proposed in the literature and applied to different settings. Lee et al. [7] presented a comparison between ciphertext policy, key policy and hierarchical ABE schemes, based on the formal construction of the different schemes. A similar survey was introduced by Ruj, in 2018 [8], such that reviewed ABE schemes are classified based on the number of supported attribute authorities. Hence, single-authority and multi-authority ABE schemes are examined and their application to secure cloud services is investigated. A summary of the main features of ABE schemes is introduced by Pang et al. [9]. This paper reviews user/attribute revocation in ABE schemes, accountability and proxy re-encryption. Yang et al. [10] introduced , in 2015, the first survey paper on ABS schemes. This paper presents the main security challenges related to an authentication scheme in distributed environments. Furthermore, several constructions of ABS schemes have been investigated and compared w.r.t. functional and design requirements. Recently, Al-Dahhan et al. [11] studied the revocation challenge in ABE schemes. The authors reviews different revocation techniques applied to attribute based cryptographic techniques such as proxy re-encryption and key update. Compared to most closely related surveys, this paper classifies attribute based techniques under two categories based on main supported security features, namely fine-grained access control and authentication in clouds. ABE is the first attribute based technique introduced to provide one-to- many encrypted access control to shared data contents. Afterwards, ABS schemes have been first designed to assure the verifier that a signer, whose set of attributes satisfies an access structure has endorsed the message. ABS schemes are then extended to support privacy-preserving authentication. Attribute based signcryption was introduced to ensure data encryption and authentication in a one logical step. Since their appearance, attribute based mechanisms have witnessed several enhancements such as multi-authority setting to enhance strong security features and manage dynamic and decentralised architectures, accountability to deal with the key abuse issues, policy-hidden technique to enhance user's privacy as well as outsourcing decryption to reduce computation costs.

[1] http://www.bbc.com/news/world-us-canada-23123964
[2] http://fortune.com/2018/04/10/facebook-cambridge-analytica-what-happened/
[3] https://aws.amazon.com/security/
[4] https://azure.microsoft.com/en-us/overview/trusted-cloud/

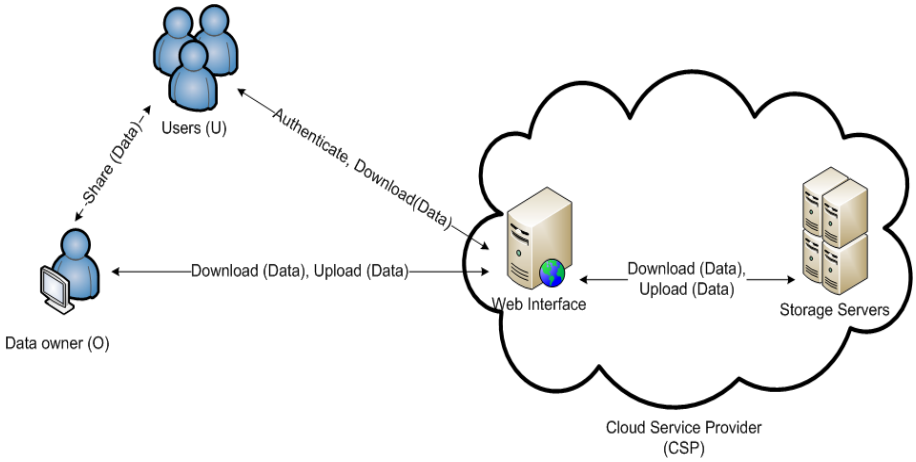

FIGURE 1 A cloud data sharing scenario.

Paper Organisation — The remainder of this paper is organised as follows. Section 2 presents security and privacy challenges in cloud data sharing services, system model and threat model. Attribute attribute access control solutions applied in the cloud are presented in Section 3. Section 4 surveys attribute based authentication schemes in the cloud. In section 5, we discuss the open issues in attribute based cryptography and we present applied enhancements, before concluding in Section 6.

2 | CLOUD DATA SHARING: THREAT MODELS AND SECURITY REQUIREMENTS

In this section, we identify the entities involved in a cloud data sharing service and we detail the threat model. Then, we present the security requirements to fulfill in order to secure data shared on cloud servers.

A cloud data storage service involves three main entities: a CSP, a data owner and a data user. CSP is responsible for storing data owners' outsourced data and sharing these data among authorised users. The data owner outsources their data to the cloud servers. The data user is a cloud client who requests access to the outsourced data by presenting their access rights to the CSP. From the viewpoint of cloud users, security threats to cloud data service are posed from two main types of adversaries, external (e.g., hackers) and internal (e.g., curious CSP). An external adversary is a malicious cloud user who uses attack techniques, such as network eavesdropping, vulnerability scanning and/or malware attacking, to gain unauthorized access to data stored in the cloud. An internal adversary is the CSP entity, who can not be fully trusted. For instance, in most existing cloud security solutions, the CSP is considered as *honest but curious* [12,13]. CSP is assumed to be honest as it provides proper inputs or outputs, while properly performing any processes expected from them, but it is curious such that it tries to gain extra knowledge from inferred information. In the following, we provide a structured overview of the security requirements for cloud data storage from a client's point of view, with respect to his outsourced data.

- Data confidentiality – Outsourcing data to remote servers is effectively delegating control over data to a CSP, thus making data potentially accessible to different parties and consequently increasing the risk of data breaches. Only authorized users should be able to access outsourced data, with respect to their granted privileges, while others, including the CSP, should not gain any knowledge about outsourced contents [14].

- Access control – Aims at giving the data owner the ability to enforce selective restriction of access to his outsourced data contents on remote cloud servers. Enhancing fine-grained access control is very important and complex in cloud storage environments. This is because different users may be granted different access privileges with regard to different data contents outsourced by the same data owner [15,16].

- Authentication – Refers to enabling a user to prove his credentials in order to access data outsourced in cloud. Privacy preserving authentication is authenticating a user without disclosing personal information about himself. In a cloud environment, users are more conscious about their privacy protection when they access cloud data or use cloud services [17,18].

TABLE 1 Comparison of ABE Schemes

Scheme	*Type*	*Access policy*	*Constant Ciphertext Size*	*Multi-authority*	*Revocation*	*Security Models*
Sahai et al. (2005) [23]	Fuzzy	Threshold	✗	✗	✗	CPA-Security
Bethencourt et al. (2007) [20]	CP-ABE	Monotone	✗	✗	✗	CPA-Security
Chase et al. (2007) [24]	KP-ABE	Monotone	✗	✓	✗	CPA-Security
Wang et al. (2010) [25]	CP-ABE	Monotone	✓	Hierarchical	✗	CPA-Security
Yu et al. (2010) [26]	KP-ABE	Monotone	✗	✓	✓	CPA-Security
Waters (2011) [27]	CP-ABE	Monotone	Short	✗	✗	CPA-Security
Lewko et al. (2011) [28]	CP-ABE	Monotone	✗	✓	✗	CPA-Security
Ruj et al. (2011) [29]	CP-ABE	Monotone	✗	✓	✗	CPA-Security
Li et al. (2013) [30]	KP-ABE	Monotone	✗	✓	✓	CPA-Security
Yang et al. (2014) [31]	CP-ABE	Monotone	✗	✓	✗	CCA2-Security
Canard et al. (2015) [32]	CP-ABE	Monotone	✓	✗	✗	CPA-Security
Xhafa et al. (2015) [33]	CP-ABE	Threshold	✗	✗	✗	CPA-Security
Wang et al. (2016) [34]	CP-ABE	Monotone	✗	✗	✗	CCA2-Security
Horvath et al (2015) [35]	CP-ABE	Monotone	✗	✓	✓	CPA-Security
Rahulamathavan e et al. (2016) [36]	KP-ABE	Monotone	✗	✓	✗	CPA-Security
Belguith et al. (2016) [12]	CP-ABE	Monotone	Short	✗	✗	CPA-Security
Belguith et al. (2016) [12]	CP-ABE	Monotone	Short	✗	✗	CPA-Security
Li et al. (2017) [37]	CP-ABE	Monotone	✗	✗	✓	CPA-Security
Huang et al. (2017) [38]	CP-ABE	hierarchical	✗	✗	✗	CPA-Security
Yang et al. (2018) [39]	CP-ABE	Monotone	✗	✓	✗	CPA-Security
Ramu et al. (2019) [40]	CP-ABE	Monotone	✗	✗	✓	CPA-Security

3 | ATTRIBUTE-BASED ACCESS CONTROL IN THE CLOUD

ABE is a promising cryptographic technique that provides fine grained access control for data stored in third parties servers. The first construction of ABE was presented as an extension of Identity Based Encryption (IBE) [19], called Fuzzy IBE, where identities are substituted by a set of descriptive attributes. Unlike traditional public key cryptography, ABE consists of encrypting ciphertext to a group of authorized users rather than to only one user. In ABE, both the ciphertext and the user's secret keys embed a set of attributes or a structure over attributes [20]. Consequently, a user is able to decrypt a ciphertext if her private key satisfies the access policy embedded in the ciphertext. Formally, ABE allows a user who holds a set of attributes, S, to encrypt a ciphertext generated w.r.t a set S', if and only if S and S' are close to each other. In other words, if S reaches a threshold $t \subset S'$ where $S' - t < \epsilon$ and ϵ is a negligible value. Hence, this ABE scheme is defined as a the first threshold ABE scheme. The threshold semantics lacks expressiveness in defining access rights. To provide fine grained access control, an ABE scheme supporting monotone access structure has been proposed by Goyal et al. [21]. This scheme embeds a set of attributes in the ciphertext while the user secret keys are associated with an access structure. This scheme is the first instantiation of the Key Policy ABE scheme (KP-ABE). A user can decrypt the ciphertext if there is a match between their access structure and the set of attributes included in the ciphertext. In the same paper, Goyal et al. have instantiated the Ciphertext Policy ABE (CP-ABE). Contrarily to KP-ABE, CP-ABE defines the user access rights using a set of attributes and encrypting data w.r.t an access structure. Generally, attribute based cryptographic techniques are suitable to data outsourcing scenarios, as they permit data owners to define fine-grained access to their data based on generated access trees over selected attributes [22]. Due to this flexibility in specifying different access rights for individual users belonging to different groups, ABE mechanisms are considered as the most suitable public key primitives for one-to-many communications with no need for support from an external entity. As the data is encrypted w.r.t a set of attributes, key management becomes much simpler as the encryption/decryption does not require the involvement of secret keys. Instead, the users who hold the required attributes may request the related secret keys that allow them to decrypt data. Each authorised user can decrypt the ciphertext using the required match between the access policy included in the ciphertext and their required attributes. As data encryption is performed before outsourcing, access control is performed without relying on the cloud storage server.

Table 1 presents a comparison between different ABE schemes, in terms of their provided features and security models.

3.1 | CP-ABE Schemes

In CP-ABE, a trusted attribute authority is responsible for issuing user's private keys based on their attributes set [6]. Based on the number of attribute authorities, ABE schemes are classified into two types: Single-Authority ABE (SA-CP-ABE) and Multi-Authority ABE (MA-CP-ABE).

SA-CP-ABE relies on a central attribute authority to generate user's attributes and the related secret keys. However, this centralised key management can limit system scalability. In addition, a central authority introduces a single point of failure. To mitigate this limitation, CP-ABE schemes relying on multi-attribute authorities were proposed [41]. In MA-CP-ABE schemes, several attribute authorities generate secret keys related to one attribute or a set of attributes.

3.1.1 | SA-CP-ABE Schemes

The first CP-ABE scheme was introduced by Bethencourt et al., [20]. This scheme relies on a central authority to generate the public parameters and the master secret key that is used to derive the user's secret keys. In addition, this central authority is responsible for issuing user's attributes and related secret keys. As shown in Figure 2 , the central trusted authority first issues public parameters and generates a master key. Then, using these generated parameters, it issues the user secret keys related to their set of attributes. Afterwards, a data owner encrypts a message w.r.t an access policy. Finally, a data user is able to decrypt the ciphertext if their set of attributes satisfies the access policy embedded in the ciphertext.

One key limitation of the SA-CP-ABE scheme is that the ciphertext's size increases exponentially with the size of the access policy which is equal to the number of attributes. To solve this problem, Herranz et al. [42] proposed a SA-CP-ABE scheme that generates a constant ciphertext size independent of the access policy's size. This scheme allows encrypting a message w.r.t a threshold access policy, which does not define expressive access rights. Waters et al. presented a SA-CP-ABE scheme with short ciphertext that uses an expressive access policy [27]. The ciphertext size increases linearly with the access structure's size. In addition, this scheme introduces an encryption and decryption overhead that increase linearly with the size of the encryption access policy. Canard and Trinh proposed a SA-CP-ABE scheme [43] which outputs a constant ciphertext size while using an expressive access policy. In this scheme, the decryption overhead is constant and independent from the size of the encryption access policy. In addition, this scheme offers high flexibility for the definition of access policies which supports general forms of Boolean expressions, i.e., Conjunctive Normal Form (CNF) and Disjunctive Normal Form (DNF). Wang et al. [25] developed a hierarchical CP-ABE scheme to enforce encrypted access control in cloud services. This scheme is an enhancement of the SA-CP-ABE scheme introduced by Bethencourt et al. [20] which applies hierarchical Identity Based Encryption (IBE) [44]. Although this scheme involves several attribute authorities organised in a hierarchical way, it is based on the use of a central master authority to administer this hierarchy. Xhafa et al. [33] designed an Electronic Health Records (EHR) system based on cloud services. In order to ensure EHR sharing between patients and physicians, this scheme uses the fuzzy-ABE introduced by Sahai and Waters [23]. Based on the SA-CP-ABE scheme introduced by Bethencourt et al. [20], Wang et al. [34] introduced a hierarchical SA-CP-ABE scheme to ensure secure cloud data sharing. This proposal introduces the use of layered access structures integrated in a single access tree that allows users to decrypt data based on their authorization level. For instance, a user with a lower authorization level can only access a small amount of data while a user with the highest authorization rights can access all the encrypted data. Li et al. [45] proposed an extension to parallelise and accelerate CP-ABE scheme [20] to enable its practical use. As such, main algorithms such as key generation, encryption, and decryption algorithms are executed in parallel using multi-threading techniques. In 2017, Zhao et al. [46] proposed a SA-CP-ABE scheme that supports non-monotonic access-structures, i.e., an access structure that supports NOT conjunctions. This scheme was applied to mobile health-care systems to provide fine grained access control to encrypted data.

SA-CP-ABE schemes have been widely applied to securely share outsourced data in clouds. However, the reliance on a central trusted authority to issue user's attributes and to generate their secret keys creates a single point of failure. A central attribute authority can attract key escrow attacks as it manages all the secret keys used in the system.

3.1.2 | MA-CP-ABE Schemes

The first MA-CP-ABE scheme was proposed by Lewko et al. [28]. In this scheme, several attribute authorities issue attributes and the related secret keys (see Figure 3) where each attribute authority administers only one attribute and generates the attribute's secret key. This avoids the reliance on a central trusted authority to handle attributes and users' secret keys, except for generating the public parameters. However, issuing attributes from different attribute authorities may lead to a collusion attack. For example, two users may combine two different attributes received from two different attribute authorities. One of these two users may use the attributes combination to access a ciphertext that can not be accessed using his attribute only. To defeat this collusion attack, this MA-CP-ABE scheme applied a Unique Global Identifier (GID) for each user. Each user must communicate their GID to the attribute authority which embeds it in the attribute secret key. Therefore, each user can only combine his own attributes to access a ciphertext.

Based on Lewko et al. MA-CP-ABE [28], several cloud access control solutions were proposed to ensure secure data sharing in cloud environments. Ruj et al. [29] proposed a revocable attribute based encryption scheme, called DACC, for cloud environments. In DACC, several attribute authorities issue users secret keys related to their attributes. A data owner enciphers his data with respect to a defined access policy and outsources the

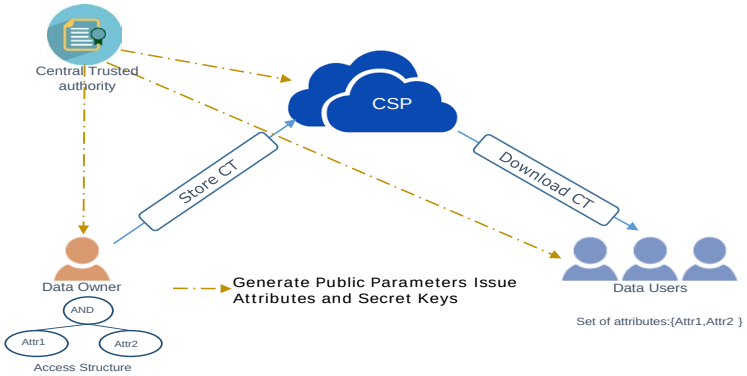

FIGURE 2 An example of SA-CP-ABE. CTA publishes public parameters to all system entities. Then, the data owner encrypts the data according to the access policy and using the received public parameters before outsources the ciphertext to the cloud. The data users download the ciphertext and decrypt it using their secret keys generated out of their attributes.

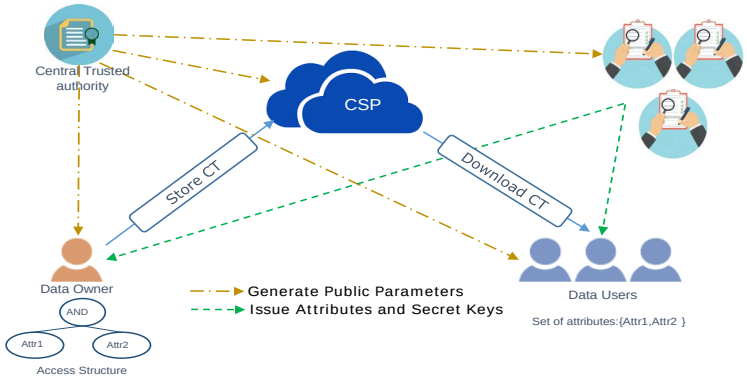

FIGURE 3 An example of MA-CP-ABE. CTA publishes public parameters to all system entities. Then, the data owner encrypts the data with respect the access policy and using the received public parameters before outsourcing the ciphertext to the cloud. The data users request their secret keys from the attribute authorities managing each attribute. Then, the users download the ciphertext and decrypt it using their secret keys generated based on their attributes.

ciphertext to the cloud. DACC also supports revocation of users by re-encrypting data using a new access policy before re-outsourcing them to the cloud.

Yang et al.[31] extended the SA-CP-ABE scheme introduced by Lewko et al.[47] to achieve a multi-authority setting. This scheme has been applied to ensure flexible access control over data stored in the cloud while providing efficient revocation of users.

A MA-CP-ABE scheme for cloud data sharing data is presented by Horvath et al.[35]. This scheme ensures users revocation by applying an identity based revocation mechanism. To update users access rights, the attribute authorities generate a revocation list including the identifiers of the revoked users. The data owner embeds these revoked identifiers in the ciphertext to prevent revoked users from decrypting the data.

Another revocable MA-CP-ABE scheme based in the work presented by Lewko et al. [28] was introduced by Zhou et al.[48]. This scheme achieves users revocation by re-issuing users secret keys. The attribute authorities are responsible for reissuing users' secret keys while excluding revoked users.

3.2 | Key Policy ABE

KP-ABE was first designed by Goyal et al.[21] in 2006. In KP-ABE, data are encrypted with respect to the set of attributes embedded in the ciphertext. The user's secret key is derived based on his access policy. The ciphertext can only be decrypted if its embedded set of attributes satisfies the user's access policy. Similar to CP-ABE, KP-ABE schemes are categorised into Single Authority KP-ABE (SA-KP-ABE) (c.f., Figure 4) and Multi Authority KP-ABE (MA-KP-ABE) schemes based on the number of authorities involved in the system.

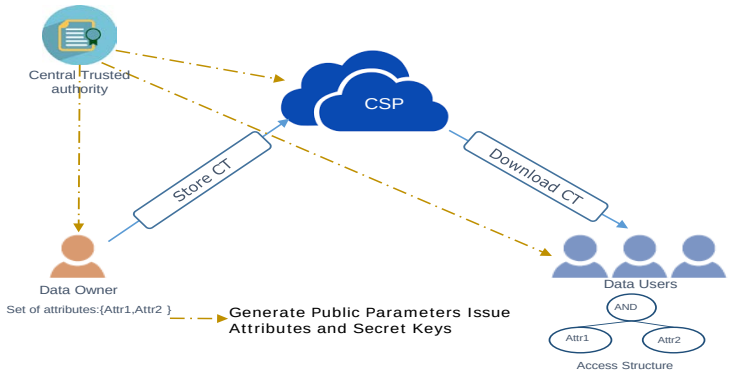

FIGURE 4 An example of SA-KP-ABE. CTA publishes public parameters to all system entities. Then, the data owner encrypts the data using a set of attributes and the received public parameters before outsourcing the ciphertext to the cloud. The data users download the ciphertext and decrypt it using their secret keys generated from their access policy.

3.2.1 | SA-KP-ABE Schemes

Ostrovsky et al.[49] designed a SA-KP-ABE that supports any type of access structure including non-monotonic boolean formula. A non-monotonic access policy can be expressed by AND, OR, NOT or threshold boolean operations. Attrapadung et al.[50] presented a SA-KP-ABE scheme with non-monotonic access policy. This scheme generates a ciphertext whose size does not increase with the access policy size.

A SA-KP-ABE with lightweight decryption overhead was presented by Hohenberger et al.[51]. To decrypt the ciphertext, the decrypting entity executes a limited number of pairing functions independently from the number of the involved attributes. Takashima[52] designed a SA-KP-ABE scheme that is characterised by an expressive access policy that generates a constant ciphertext size. This scheme introduces a constant number of pairing functions during the decryption process.

Liu et al.[53] proposed a SA-KP-ABE scheme adapted for cloud application. This scheme is proved to achieve semantic security against adaptive Chosen Ciphertext Attacks (CCA). Similarly, Lai et al.[54] presented an expressive KP-ABE scheme. This scheme generates a constant size cipherext and reduces decryption overhead. A KP-ABE which supports revocation was presented by Shi et al.[55]. This scheme embeds a revocation list in the ciphertext to manage the users access rights. A revoked user whose identity appears in the revocation list can not decrypt the ciphertext.

3.2.2 | MA-KP-ABE Schemes

Chase[24] proposed the first MA-KP-ABE scheme (see Figure 5). This scheme involves several attribute authorities to maintain attributes and issue secret keys. This scheme relies on the use of a user global identifier to prevent users from performing successful collusion attacks. However, the use of a unique global identifier for each user allows the attribute authorities to violate users' privacy by combining users attributes to build a full user profile. To overcome this issue, Chase[56] proposed an enhancement to their first construction using the Anonymous Credentials (AC) mechanism[57].

A MA-KP-ABE scheme has been applied to cloud data storage services to achieve secure data sharing among authorised users by Yu et al.[26]. This scheme is based on exploiting and combining KP-ABE[21], and lazy re-encryption[58]. This scheme accomplishes users revocation by re-encrypting ciphertext only after a user revocation occurs and the same ciphertext is requested by a non-revoked user. Li et al.[30] proposed a Personal Health Records (PHR) system based on cloud services. The authors applied the MA-KP-ABE scheme introduced by Chase et al.[56] to secure PHR and protect the privacy of patients and physicians who access the stored PHR. A MA-KP-ABE scheme that provides collusion resistance is introduced by Rahulamathavan et al.[36]. This scheme extends the KP-ABE scheme proposed by Han et al.[59] using the anonymous key issuing protocol [56] to link the decryption keys to users identities while preserving their privacy.

3.3 | Policy Hidden ABE

ABE schemes have been extensively used to secure data in distributed systems, mainly in cloud services. ABE associates an access policy with the ciphertext outsourced to untrusted servers. The public sharing of access policies may lead to the disclosure of sensitive data about data owner as well as the data users. To address this issue, several solutions were proposed, referred to as policy-hidden ABE schemes. Table 2 provides a comparison between policy-hidden ABE schemes.

An access policy contains attributes that are usually defined by a name and a value. A partially hidden access policy means that the attribute value is hidden while the name can be published. However, in fully hidden ABE schemes, the attribute's name and value are both made private.

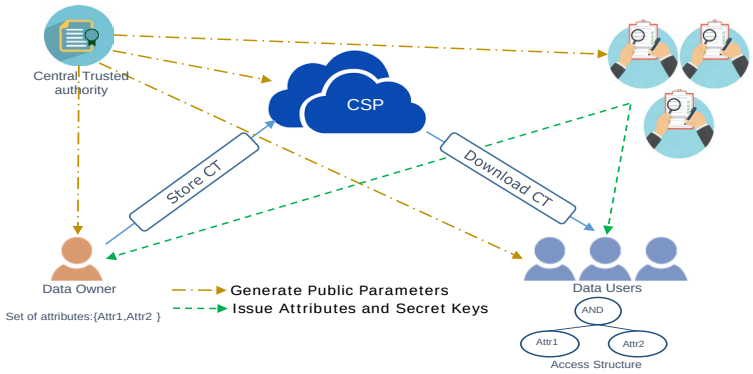

FIGURE 5 An example of MA-KP-ABE. CTA publishes public parameters to all system entities. Then, the data owner encrypts the data the access policy and the received public parameters before outsourcing the ciphertext to the cloud. The data user request their secret keys from the attribute authorities managing each attribute. Then, the user downloads the ciphertext and decrypts it using their secret keys generated from the associated access policy.

TABLE 2 Comparison of hidden policy ABE schemes

Representative schemes	*Type*	*Access Policy*	*Policy Hidden*	*Multi-Authority*	*Security Models*
Nishide et al. (2008) [60]	CP-ABE	Monotone	Partially hidden	✗	Selective CPA
Zhou et al. (2015) [67]	CP-ABE	Monotone	Fully Hidden	✗	Selective CPA
Xu et al. (2015) [63]	CP-ABE	Monotone	Fully Hidden	✗	Selective CPA
Phuong et al. (2016) [64]	CP-ABE	AND gates	Fully Hidden	✗	Selective CPA
Yundong et al. (2017) [68]	CP-ABE	Monotone	Fully Hidden	✓	Selective CPA
Belguith et al. (2018) [69]	CP-ABE	Monotone	Fully Hidden	✓	Selective CPA
Zhong et al. (2018) [70]	CP-ABE	Monotone	Fully Hidden	✓	Selective CPA
Xiong et al. (2019) [71]	CP-ABE	Monotone	Partially Hidden	✓	Selective CPA

Nishide et al. [60] proposed a partially hidden access control policy scheme which is based on the SA-CP-ABE proposed by Cheung et al. [61]. Another partially hidden access policy ABE scheme was proposed by Lai et al. [62]. This scheme is an extension of Water's SA-CP-ABE scheme [27].

Xu et al. [63] applied a hiding technique onto the access policy used in the SA-CP-ABE scheme presented by Bethencourt et al. [20] to achieve a fully hidden access policy. Phuong et al. [64] proposed another SA-CP-ABE scheme with hidden access policy. This scheme supports only AND gates access policy, which reduces the expressiveness of the defined access rights. The first MA-CP-ABE scheme with fully hidden access policy has been introduced by Zhong et al. [65]. This scheme extends Lewko et al.'s MA-CP-ABE scheme [28] by applying the one-way anonymous key agreement technique [66] to hide the access policy.

3.4 | Multi-Level ABE

Sharing data contents between different involved actors is often a challenging concern, due to the complexity of access control policies' management. As stated above, this issue becomes more complex when involved actors do not share the same access privileges to each part of the data file. Hence, different access levels need to be defined to allow authorized users to access different sub-parts of enciphered data. The translation of an access control structure into an equivalent multi-level policy remains one of the main challenging issues of encrypted access control mechanisms.

Huang et al. [72] proposed a data collaboration scheme, such that authorized users can share data in a collaborative manner. In fact, the data owner encrypts data with respect to a selected access policy based on CP-ABE, while the cooperative user re-encrypts the modified data and signs a collaboration request with his attributes. As such, only the users whose attributes satisfy the access policy can modify outsourced data. This scheme employs a delegation mechanism based hierarchical ABE, which contains a central authority and a number of independent domains. Each domain holds a domain authority that requests a secret parameter from the higher level authority and generates attribute secret keys for its domain users. Ruj et al. [73] presented a privacy preserving authenticated access control scheme for securing data in clouds based on an attribute based scheme. In this proposal, the cloud provider authenticates with the data owner without knowing his identity before storing information. Although these

schemes proposed efficient solutions to protect data contents from unauthorized access, they are still inefficient with multi-level access policies, where users have to share the same data content with different access rights to distinct parts of the data file.

The multi level access control policies in ABE schemes have been recently explored [34,74,75,76]. In these schemes, data files are encrypted using a multi level access policy where users can access parts of these data w.r.t. their access level.

Wang et al. [34] proposed an efficient file hierarchy attribute-based encryption scheme in cloud computing. The layered access structures are integrated into a single access structure, and then, the hierarchical files are encrypted with the integrated access structure. Kaaniche et al. [74] have introduced an encryption scheme based on attribute based mechanisms for multi-level access policies. This scheme ensures a selective access to data based on users' granted privileges. Practically, when a party encrypts a data file, she specifies an access structure and a certain number of security levels. Thus, a user is able to decrypt a sub-set of data blocks related to a security level k that user's private keys satisfy the sub-set of attributes related to the k-security level. EMA-LAB, a Multi Authorisation Level Attribute Based Access Control with short ciphertexts size [76] has been proposed. It relies on the usage of a constant-size threshold attribute based encryption scheme and permits a selective access to enciphered data w.r.t. different threshold levels. Thus, the size of the resulting ciphertext does not depend on the number of attributes involved in the access policy, which makes EMA-LAB suitable for bandwidth-limited applications. Kaaniche and Laurent [75] proposed a selective attribute based encryption mechanism, referred to as SABE, that enables the enciphering entity to encrypt the same data content, based on an ABE aggregate access tree, and the deciphering entity to decrypt the subsets of data blocks with respect to a security level k_l.

4 | ATTRIBUTE BASED AUTHENTICATED ACCESS TO CLOUDS

Signature schemes are usually applied to achieve user authentication while accessing cloud services. As a variant of ABE, the first Attribute Based Signature (ABS) scheme was designed by Maji et al. [77]. ABS allows a user to sign a message according to an access policy. The user is required to hold a set of attributes that satisfies the access policy to be able to sign a message. This allows a flexible access rights control over users who can sign a message. The user's attributes and secret keys are generated by an attribute authority. The verification entity verifies the generated signature by only using public parameters. ABS schemes need to fulfill two security requirements: privacy and unforgeability. An ABS scheme is privacy preserving as it maintains the anonymity of the signer's identity and the attributes used to generate the signature. An unforgeable ABS scheme means that a user can not generate a signature while their attributes do not satisfy the access policy even if he is colluding with other users [17]. Based on the number of authorities involved in the system, an ABS scheme can be a Single Authority ABS (SA-ABS) or a Multi Authority ABS (MA-ABS). Table 3 presents a comparison of ABS schemes.

4.1 | SA-ABS

Maji et al.'s [77] ABS scheme fulfills the unforgeability requirement as the signature can not be generated only by a a user whose attributes satisfy the defined access policy. Indeed, unauthorised users can not collude to generate a verifiable signature. In addition, ABS guarantee the signer's privacy, i.e., the signature does not compromise the signer's identity neither his attributes.

An efficient ABS construction supporting flexible threshold predicate was presented by Li et al. [78]. The authors prove that their scheme is secure in the random model while ensuring efficient computation and communication costs. Ge et al. [79] presented an ABS scheme based on the Water's SA-CP-ABE scheme [27]. Although this scheme introduces low computation and communication costs, it suffers from unforgeability attacks as users can pool their attribute and generate a valid signature.

ABS schemes has been applied to ensure data owners authentication and fine grained access control to outsourced data in cloud services. For instance, Zhao et al. [80] applied the Waters' CP-ABE scheme [27] to encrypt data, then the generated ciphertext is signed using the SA-ABS scheme introduced by Maji et al. [81]. This scheme allows the data users to verify that the data are outsourced by authorised data owners.

Liu et al. [82] extended the Bethencourt's SA-CP-ABE scheme [20] to implement a hierarchical setting. This scheme was combined with Maji's ABS scheme [81] to authenticate data owners who want to encrypt and outsource their data to the cloud.

A secure ABS scheme with externalised signature was proposed in [83]. In this scheme, a signer forwards an outsourced key to the CSP to use it for generating a partial signature over a given message. The signer can generate their valid signature using the received partial signature and their secret key.

4.2 | MA-ABS

Maji et al. [81] proposed the first instantiation of the MA-ABS schemes. Similar to MA-ABE schemes, MA-ABS allows the management of attributes and secret keys by several attribute authorities. However, in this construction, a central authority is required to manage communications between

attribute authorities. Okamoto et al.[84] proposed the first fully decentralized ABS scheme. This scheme relies on several attribute authorities where no central authority is required to manage their communication.

Ruj et al.[85] presented a privacy preserving authenticated access control scheme applied to cloud computing. In this proposal, the cloud provider verifies that the data were uploaded by an authorised data owner without inferring his identity. To this end, this scheme applies the MA-CP-ABE presented by Lewko et al[28] and the MA-ABS designed by Maji et al.[81].

In[12], the authors proposed an attribute based access control schemes that allows privacy preserving authentication of users accessing the cloud based on a MA-CP-ABS scheme. To authenticate users, the CSP forwards them a message to sign. The verification of the signature allows the CSP to know whether the user has the required attributes to access the data. Rao et al.[86] proposed a KP-ABS scheme with a constant signature size. Similar to the KP-ABE schemes, the user's key is derived using an access structure. Therefore, the signature is generated according to a set of attributes by a user whose access structure satisfies this set.

4.3 | Accountability in ABS

ABS schemes need to anonymise users identities. However, malicious users may use this feature to forge a signature while keeping their identities hidden. Therefore, it is necessary to introduce the accountability requirement to trace a malicious user identity by inspecting their presented signature. However, to prevent CSPs from using the accountability feature for their own benefits and trace clients, the accountability algorithm should be executed by a separate independent authority.

Accountability in ABS schemes was first presented by Khader et al.[87]. However, the proposed scheme only preserves the user identity while revealing their attributes used to generate the signature. To mitigate this limitation, Escala et al.[88] presented an accountable ABS scheme where both identities and attribute are hidden. These two ABS schemes rely on central authority to issue the attributes.

In 2014, El Kaafarani et al.[89] designed the first accountable MA-ABS. This scheme allows an inspection authority to reveal a user's identity when a misbehaving is detected. Kaaniche and Laurent[90] proposed an Anonymous Certification (AC) mechanism built on a traceable ABS. Their proposal provides a cryptographic tool that allows a user to authenticate with a CSP while revealing only the required information to keep their identify private.

A traceable signature scheme for mobile health-care applications was presented by Meng et al.[91]. This scheme allows the delegation of a doctor's signature to another party when this doctor is not able to sign. It applies a proxy signature which requires that a user first proves their access rights by decrypting a ciphertext to sign a message instead of the original signer.

A KP-ABS scheme was presented by Hong et al.[92] to deal with the presence of an untrusted authority. In this scheme, the signer requests a part of their signing key from the attribute authority. The second part of their secret signing key is derived privately by the signer himself. This scheme allows the attribute authority to trace compromised users based on their signing key's part which meets the accountability requirement.

4.4 | Attribute Based SignCryption (ABSC)

ABSC is a signcryption primitive that ensures fine grained access control, data origin authenticition and data confidentiality by combining ABE and ABS in one logic step. In 2010, Gagné et al.[98] proposed the first ABSC scheme which relies on a threshold access structure. This scheme allows defining an access structure to be used to encrypt the data. In addition, the generated ciphertext is signed by the data owner at the same time. A data user is able to verify the data owner's signature and decrypt the ciphertext using his attributes. This allows the data user to check whether the data was encrypted by an authorised data owner.

ABSC schemes incure lower computation overhead compared to encryption and signature schemes executed by the data owner. This ABSC scheme requires the use of two different access policies for the signature generation and the data encryption. Therefore, the size of the signcrypted data increases along with the complexities of both signing and encrypting access policies. Keita et al.[99] presented an ABSC scheme to support the update of the access structures used in the signature. This scheme allows the encryption to be updated without regenerating the user's secret keys. The size of the signcrypted message depends on the size of signing and encrypting access policies.

Liu et al.[100] introduced an ABSC scheme based on the SA-CP-ABE scheme presented by Water tet al.[27] and the ABS scheme proposed by Maji et al.[81]. This ABSC scheme has been used to design a secure EHR system based on cloud services. Therefore, a user may signcrypt data before outsourcing it to the cloud storage to be shared among other users. Users are able to verify the data origin to make sure that it was created by an authorised user. Due to the use of different access policies for signing and encrypting, the aforementioned ABSC scheme[100] introduces high communication and computation overheads. To countermeasure this drawback, Rao et al.[101] proposed the first KP-ABSC scheme with constant ciphertext size. The first CP-ABSC scheme with constant ciphertext size was proposed in 2017[102]. In this scheme, the data owner signcrypts his data with respect to a defined threshold access policy. The data user verifies and decrypts the received data only if the data were uploaded by an

TABLE 3 Comparison of ABS Schemes

Scheme	*Type*	*Access policy*	*Constant Signature Size*	*Multi-authority*	*Accountability*
Khader et al. (2007) [87]	KP-ABS	Monotone	✗	✗	✓
Maji et al. (2008) [77]	CP-ABS	Monotone	✗	✗	✗
Li et al. (2010) [77]	CP-ABS	Threshold	✗	✗	✗
Zhao et al. (2011) [80]	CP-ABS	Monotone	✗	✗	✗
Escala et al. (2011) [88]	CP-ABS	Monotone	✗	✗	✓
Maji et al. (2011) [81]	CP-ABS	Monotone	✗	✓	✗
Ge et al. (2012) [79]	CP-ABS	Monotone	Short	✗	✗
Liu et al. (2013) [82]	CP-ABS	Monotone	✗	✗	✗
El Kaafarani et al. (2014) [89]	CP-ABS	Monotone	✗	✓	✓
Ruj et al. (2014) [85]	CP-ABS	Monotone	✗	✓	✗
Liu et al. (2015) [83]	CP-ABS	Monotone	✗	✗	✗
Rao et al. (2016) [83]	KP-ABS	Monotone	✓	✗	✗
Kaaniche et al. (2016)	CP-ABS	Monotone	✗	✗	✓
Meng et al. (2016)	CP-ABS	Monotone	✗	✗	✓
Hong et al. (2016)	KP-ABS	Monotone	✗	✗	✓
Belguith et al. [12] (2016)	CP-ABS	Monotone	Short	✓	✗
Sun et al. (2017) [93]	CP-ABS	Monotone	✗	✗	✗
Gu et al. (2017) [94]	CP-ABS	Monotone	✗	✗	✗
Guo et al. (2018) [95]	CP-ABS	Monotone	✗	✓	✗
Cui et al. (2018) [96]	CA-ABS	Monotone	✓	✗	✗
Sun et al. (2019) [97]	CP-ABS	Monotone	✗	✗	✗

TABLE 4 Comparison of ABSC schemes

Representative Schemes	*Common Setup*	*Type*	*Access Policy*	*Constant Signcryption size*
Gagné et al. (2010) [98]	✗	CP-ABSC	Threshold	✗
Emura et al. (2012) [99]	✗	CP-ABSC	Monotone	✗
Rao et al. (2014) [101]	✗	KP-ABSC	Monotone	✓
Liu et al. (2015) [100]	✗	CP-ABSC	Monotone	✗
Rao et al (2017) [103]	✗	CP-ABSC	Monotone	Short
Belguith et al. (2017) [102]	✓	CP-ABSC	Threshold	✓
Liu et al. (2017) [104]	✗	KP-ABSC	Monotone	✗
Belguith et al. (2018) [105]	✗	CP-ABSC	Threshold	✓
Belguith et al. (2018) [106]	✗	CP-ABSC	Threshold	✓
Deng et al. (2018) [107]	✗	CP-ABSC	Monotone	✗
Xu et al. (2018) [108]	✗	CP-ABSC	Monotone	✗

authorised data owner. The size of the generated signcrypted message is constant and independent of the size of the access policy. Table 4 presents a comparison of ABSC schemes.

5 | ATTRIBUTE BASED CRYPTOGRAPHY CHALLENGES

In this section, we identify the key improvements applied to ABE in order to better apply these mechanisms to the cloud services.

TABLE 5 Comparison of OABE schemes

Representative schemes	*Type*	*Access Policy*	*Verifiability*	*Multi-authority*	*Security Models*
Green et al. (2011) [112]	CP-ABE	LSSS	✗	✗	RCCA
LAi et al. (2013) [116]	CP-ABE	LSSS	✓	✗	Selective CPA
Li et al. (2014) [119]	CP-ABE	LSSS	✓	✗	RCCA
Qin et al. (2015) [113]	CP-ABE	LSSS	✓	✗	RCCA
Lin et al. (2015) [120]	CP-ABE	LSSS	✓	✗	Selective CPA
Zuo et al. (2016) [121]	CP-ABE	LSSS	✗	✗	Selective CCA
Li et al. (2017) [118]	CP-ABE	AND gates	✓	✗	RCCA
Ma et al. (2017) [122]	CP-ABE	Montone	✓	✗	RCCA
Belguith et al. (2018) [69]	CP-ABE	LSSS	✓	✓	RCCA
Li et al. (2018) [123]	CP-ABE	LSSS	✓	✓	RCCA
Zhang et al. (2019) [124]	CP-ABE	LSSS	✓	✓	RCCA
Xiong et al. (2019) [71]	CP-ABE	LSSS	✓	✗	RCCA

5.1 | Efficiency in Attribute Based Techniques: Outsourcing ABE (OABE)

One key limitation of ABE schemes is the high decryption cost, which grows with the complexity of the access structures. For instance, the decryption cost is related to the execution of several pairing functions [109,110]. Several research efforts targeted ABE schemes with constant ciphertext size and/or constant number of pairing operations in the decryption phase [111]. However, such schemes only support threshold access policies or AND gates access policies which limits the expressiveness of the defined access rights. To mitigate this issue, Green et al. [112] proposed to outsource the execution of the decryption algorithm to a semi trusted server. To this end, a user needs to derive a pair of new keys called public and private transformation keys based on his own secret key. Then, the cipheretext and the public transformation key are forwarded to the semi trusted server that is able to partially decrypt the ciphertext using the received transformation key without accessing the plaintext. This partially decrypted ciphertext is then returned to the user who uses the private transformation key to fully decrypt the ciphertext by performing only one exponentiation operation. By applying this technique, users reduce the computation costs at their side. The delegation of the decryption algorithm to semi trusted server requires that the user verifies the correctness of the received partially decrypted ciphertext. A lazy server may try to forward previously partially decrypted ciphertext [113]. To overcome this limitation, several verifiable outsourced ABE schemes were proposed [114,115].

Lai et al. [116] proposed an outsourced ABE scheme where the user is able to verify the correctness of the partially decrypted ciphertext. This scheme encrypts two different messages, one is the original message and the other is a random message. The ciphertext involves a component $\tilde{C}$ generated using a combined hash functions over both messages. After receiving the partially decrypted ciphertext, the user decrypts the two messages and compare the result to $\tilde{C}$ to verify the correctness of the decryption performed by the server.

A SA-CP-ABE with both outsourced encryption and decryption algorithms was described by Wang et al. [117]. In this scheme, the data owner is assisted by a proxy server to partially encrypt the data. Then, the data owner uses the partially encrypted data to encrypt the message and generate the ciphertext to be outsourced to the cloud server. On the other side, users outsource the decryption algorithm to a semi-trusted server who partially decrypts the ciphertext. In 2017, Li et al. [118] proposed a SA-CP-ABE scheme that supports the verifiable outsourced decryption feature. Beyond reducing decryption overhead, this scheme incurs low communication costs as it generates a constant-size ciphertext.

All the above-mentioned outsourced ABE schemes are SA-CP-ABE schemes. Recently, PHOABE, the first MA-CPABE scheme with outsourced decryption has been introduced [69]. In this scheme, a user may delegate the decryption algorithm to be executed by a semi-trusted server while being able to verify the correctness of the partially decrypted ciphertext.

5.2 | Direct Revocation: Policy Update in ABE

One of the limitations of the current ABE techniques is the cost of updating access policies after generating a ciphertext, i.e., the addition or deletion of attributes from existing access policies requires re-encrypting entire data. Moreover, policy update often relies on a proxy re-encryption mechanism [125,108]. The re-encryption process is expensive in terms of communication costs and is particularly inefficient when the number of ciphertext elements grows [126,127]. Although some of the proposed algorithms, such as the scheme proposed by Xu et al. [108], are capable of revocation/addition of users, they still require sharing re-encryption keys with the proxy server which adds extra communication costs. In Hong's scheme [128], upon a revocation demand, the proxy is asked to re-encrypt all the ciphertext with respect to the new defined access policy. In addition, it updates the non-revoked users keys to ensure their ability to decrypt the ciphertext. A similar technique is applied by Liu et al. [104] to update a signcrypted data

TABLE 6 Comparison of Policy Update ABE schemes

Representative schemes	*Type*	*Access Policy*	*Policy Update*	*Security Models*
Jiang et al. (2016) [130]	CP-ABE	Threshold	Add and remove attributes	Selective CPA
Jiang et al. (2017) [129]	CP-ABE	Threshold	Add and remove attributes	Selective CPA
Hong et al. (2018) [128]	CP-ABE	Monotone	Proxy re-encryption	–
Belguith et al. (2018) [126]	KP-ABE	LSSS	Only add attributes	CCA
Belguith et al. (2018) [127]	KP-ABE	LSSS	Add and remove attributes	Selective CPA
Ge et al. (2018) [125]	CP-ABE	LSSS	Proxy re-encryption	Selective CPA

where a proxy server is used to update the data as well as users secret keys. Proxy re-encryption have few limitations as there is a need to rely on a third party to execute the re-encryption and re-distribute keys. Thus, a malicious proxy server can collude with users to not revoke their access rights. Moreover, the re-encryption process needs to be re-executed as many times as a user is revoked which limits the system scalability. Also, this technique does not solve the challenge of adding attributes to an access policy. Jiang et al. have instantiated the first policy update in CP-ABE schemes [129], in 2017. In this scheme, attributes can be added or removed efficiently without ciphertext re-encryption neither sharing users secret keys. Later, the first KP-ABE schemes supporting policy update is recently presented [126]. Both presented schemes [129,127] enable a cloud server to update the access policy associated with a ciphertext without relying on a proxy server to execute the re-encryption algorithm neither re-issuing users keys. The encrypting entity generates a ciphertext involving encrypted data combined with additional components required to perform the access policy update feature. These ciphertext additional components are simply a randomization of the ciphertext elements w.r.t. to the attributes universe. The cloud server uses the additional components to update the access policy on demand without decrypting ciphertexts neither re-issuing users secret keys.

6 | CONCLUSION

Cloud Computing is a popular computing architecture which allows a scalable data storage and computation. Despite the attractive features of cloud computing, this paradigm introduces several security and privacy concerns. Attribute based cryptography is commonly used to enhance data security and user's privacy in cloud services. In this survey, we systematically review ABE solutions in the literature. In particular, we discuss prominent ABE, ABS and ABSC schemes that provide data confidentiality, access control, authentication and privacy preservation for cloud data sharing services. Finally, we show that cloud data storage security is facing many challenges and many security problems remain to be identified and resolved. Future work avenues include the investigation of ABE, ABS and ABSC schemes in fog-enabled systems [131]. There is also an opportunity to investigate how these schemes can be used to address security threats to critical infrastructure [132] in specific.

References

1. Boddy Aaron, Hurst William, Mackay Michael, El Rhalibi Abdennour, Baker Thar, Montañez Casimiro A Curbelo. An Investigation into Healthcare-Data Patterns. *Future Internet*. 2019;11(2):30.

2. Aloraini Afnan, Hammoudeh Mohammad. A survey on data confidentiality and privacy in cloud computing. In: :10ACM; 2017.

3. Kaaniche Nesrine, Laurent Maryline. Data security and privacy preservation in cloud storage environments based on cryptographic mechanisms. *Computer Communications*. 2017;111:120–141.

4. Ahsan MA Manazir, Ali Ihsan, Idris Mohd Yamani Idna Bin, Imran Muhammad, Shoaib Muhammad. Countering Statistical Attacks in Cloud-Based Searchable Encryption. *International Journal of Parallel Programming*. 2018;:1–26.

5. Tariq Noshina, Asim Muhammad, Al-Obeidat Feras, et al. The Security of Big Data in Fog-Enabled IoT Applications Including Blockchain: A Survey. *Sensors*. 2019;19(8):1788.

6. Moffat Steve, Hammoudeh Mohammad, Hegarty Robert. A survey on ciphertext-policy attribute-based encryption (cp-abe) approaches to data security on mobile devices and its application to iot. In: :34ACM; 2017.

7. Lee Cheng-Chi, Chung Pei-Shan, Hwang Min-Shiang. A Survey on Attribute-based Encryption Schemes of Access Control in Cloud Environments.. *IJ Network Security.* 2013;15(4):231–240.

8. Bagyalakshmi C, Samundeeswari ES. A survey on attribute based encryption techniques in data security using cloud environment. 2018;.

9. Pang Liaojun, Yang Jie, Jiang Zhengtao. A survey of research progress and development tendency of attribute-based encryption. *The Scientific World Journal.* 2014;2014.

10. Yang Huihui, Oleshchuk Vladimir. Attribute-based authentication schemes: a survey. *International Journal of Computing.* 2015;14(2):86–96.

11. Al-Dahhan Ruqayah R, Shi Qi, Lee Gyu Myoung, Kifayat Kashif. Survey on Revocation in Ciphertext-Policy Attribute-Based Encryption. *Sensors.* 2019;19(7):1695.

12. Belguith Sana, Kaaniche Nesrine, Jemai Abderrazek, Laurent Maryline, Attia Rabah. PAbAC: a Privacy preserving Attribute based framework for fine grained Access Control in clouds. *13th International Conference on Security and Cryptography(Secrypt).* 2016;:133–146.

13. Kaaniche Nesrine, Laurent Maryline, El Barbori Mohammed. Cloudasec: A novel public-key based framework to handle data sharing security in clouds. *Security and Cryptography (SECRYPT), 2014 11th International Conference on.* 2014;:1–14.

14. Belguith Sana, Cui Shujie, Asghar Muhammad Rizwan, Russello Giovanni. Secure publish and subscribe systems with efficient revocation. In: :388–394ACM; 2018.

15. Belguith Sana, Gochhayat Sarada Prasad, Conti Mauro, Russello Giovanni. Emergency Access Control Management Via Attribute Based Encrypted QR Codes. In: :1–8IEEE; 2018.

16. Cui Shujie, Belguith Sana, De Alwis Pramodya, Asghar Muhammad Rizwan, Russello Giovanni. Malicious entities are in vain: Preserving privacy in publish and subscribe systems. In: :1624–1627IEEE; 2018.

17. Atwady Yahya, Hammoudeh Mohammed. A survey on authentication techniques for the internet of things. In: :8ACM; 2017.

18. Cui Shujie, Belguith Sana, De Alwis Pramodya, Asghar Muhammad Rizwan, Russello Giovanni. Collusion Defender: Preserving Subscribers' Privacy in Publish and Subscribe Systems. *IEEE Transactions on Dependable and Secure Computing.* 2019;.

19. Shamir Adi. Identity-based cryptosystems and signature schemes. *Workshop on the Theory and Application of Cryptographic Techniques.* 1984;:47–53.

20. Bethencourt John, Sahai Amit, Waters Brent. Ciphertext-policy attribute-based encryption. *IEEE Symposium on Security and Privacy, 2007..* 2007;:321–334.

21. Goyal Vipul, Pandey Omkant, Sahai Amit, Waters Brent. Attribute-based encryption for fine-grained access control of encrypted data. *The 13th ACM conference on Computer and communications security.* 2006;:89–98.

22. Li Wenmin, Wen Qiaoyan, Li Xuelei, He Debiao. Attribute-based fuzzy identity access control in multicloud computing environments. *Soft Computing.* 2018;22(12):4071–4082.

23. Sahai Amit, Waters Brent. Fuzzy identity-based encryption. In: Springer 2005 (pp. 457–473).

24. Chase Melissa. Multi-authority attribute based encryption. *Theory of Cryptography Conference.* 2007;:515–534.

25. Wang Guojun, Liu Qin, Wu Jie. Hierarchical attribute-based encryption for fine-grained access control in cloud storage services. *The 17th ACM conference on Computer and communications security.* 2010;:735–737.

26. Yu Shucheng, Wang Cong, Ren Kui, Lou Wenjing. Achieving secure, scalable, and fine-grained data access control in cloud computing. *Infocom, 2010 proceedings IEEE.* 2010;:1–9.

27. Waters Brent. Ciphertext-policy attribute-based encryption: An expressive, efficient, and provably secure realization. In: Springer 2011 (pp. 53–70).

28. Lewko Allison, Waters Brent. Decentralizing attribute-based encryption. In: Springer 2011 (pp. 568–588).

29. Ruj Sushmita, Nayak Amiya, Stojmenovic Ivan. Dacc: Distributed access control in clouds. *IEEE 10th International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom)*. 2011;:91–98.

30. Li Ming, Yu Shucheng, Zheng Yao, Ren Kui, Lou Wenjing. Scalable and secure sharing of personal health records in cloud computing using attribute-based encryption. *IEEE Transactions on Parallel and Distributed Systems*. 2013;24(1):131–143.

31. Yang Kan, Jia Xiaohua. Expressive, efficient, and revocable data access control for multi-authority cloud storage. *IEEE transactions on parallel and distributed systems*. 2014;25(7):1735–1744.

32. Canard Sébastien, Trinh Viet Cuong. Private Ciphertext-Policy Attribute-based Encryption Schemes With Constant-Size Ciphertext Supporting CNF Access Policy.. *IACR Cryptology ePrint Archive*. 2015;2015:891.

33. Xhafa Fatos, Li Jingwei, Zhao Gansen, Li Jin, Chen Xiaofeng, Wong Duncan S. Designing cloud-based electronic health record system with attribute-based encryption. *Multimedia Tools and Applications*. 2015;74(10):3441–3458.

34. Wang Shulan, Zhou Junwei, Liu Joseph K, Yu Jianping, Chen Jianyong, Xie Weixin. An Efficient File Hierarchy Attribute-Based Encryption Scheme in Cloud Computing. *IEEE Transactions on Information Forensics and Security*. 2016;11(6):1265–1277.

35. Horváth Máté. Attribute-Based Encryption Optimized for Cloud Computing. In: Springer 2015 (pp. 566–577).

36. Rahulamathavan Yogachandran, Veluru Suresh, Han Jinguang, Li Fei, Rajarajan Muttukrishnan, Lu Rongxing. User Collusion Avoidance Scheme for Privacy-Preserving Decentralized Key-Policy Attribute-Based Encryption. *IEEE Transactions on Computers*. 2016;65(9):2939–2946.

37. Li Jiguo, Shi Yuerong, Zhang Yichen. Searchable ciphertext-policy attribute-based encryption with revocation in cloud storage. *International Journal of Communication Systems*. 2017;30(1):e2942.

38. Huang Qinlong, Yang Yixian, Shen Mansuo. Secure and efficient data collaboration with hierarchical attribute-based encryption in cloud computing. *Future Generation Computer Systems*. 2017;72:239–249.

39. Yang Yan, Chen Xingyuan, Chen Hao, Du Xuehui. Improving privacy and security in decentralizing multi-authority attribute-based encryption in cloud computing. *IEEE Access*. 2018;6:18009–18021.

40. Ramu Gandikota, Reddy B Eswara, Jayanthi Appawala, Prasad LV Narasimha. Fine-grained access control of EHRs in cloud using CP-ABE with user revocation. *Health and Technology*. 2019;:1–10.

41. Božović Vladimir, Socek Daniel, Steinwandt Rainer, Villányi Viktória I. Multi-authority attribute-based encryption with honest-but-curious central authority. *International Journal of Computer Mathematics*. 2012;89(3):268–283.

42. Herranz Javier, Laguillaumie Fabien, Ràfols Carla. Constant size ciphertexts in threshold attribute-based encryption. *International Workshop on Public Key Cryptography*. 2010;:19–34.

43. Junod Pascal, Karlov Alexandre. An efficient public-key attribute-based broadcast encryption scheme allowing arbitrary access policies. *Proceedings of the tenth annual ACM workshop on Digital rights management*. 2010;:13–24.

44. Horwitz Jeremy, Lynn Ben. Toward hierarchical identity-based encryption. *Advances in CryptologyâĂŤEUROCRYPT 2002*. 2002;:466–481.

45. Li Lifeng, Chen Xiaowan, Jiang Hai, Li Zhongwen, Li Kuan-Ching. P-CP-ABE: Parallelizing Ciphertext-Policy Attribute-Based Encryption for clouds. *Software Engineering, Artificial Intelligence, Networking and Parallel/Distributed Computing (SNPD), 2016 17th IEEE/ACIS International Conference on*. 2016;:575–580.

46. Zhao Yang, Fan Pengcheng, Cai Haoting, Qin Zhiguang, Xiong Hu. Attribute-based Encryption with Non-Monotonic Access Structures Supporting Fine-Grained Attribute Revocation in M-healthcare.. *IJ Network Security*. 2017;19(6):1044–1052.

47. Lewko Allison, Waters Brent. New proof methods for attribute-based encryption: Achieving full security through selective techniques. In: Springer 2012 (pp. 180–198).

48. Zhou Junwei, Duan Hui, Liang Kaitai, et al. *Securing Outsourced Data in the Multi-Authority Cloud with Fine-Grained Access Control and Efficient Attribute Revocation.* 2017.

49. Ostrovsky Rafail, Sahai Amit, Waters Brent. Attribute-based encryption with non-monotonic access structures. *Proceedings of the 14th ACM conference on Computer and communications security.* 2007;:195–203.

50. Attrapadung Nuttapong, Libert Benoît, De Panafieu Elie. Expressive Key-Policy Attribute-Based Encryption with Constant-Size Ciphertexts.. *Public Key Cryptography.* 2011;6571:90–108.

51. Hohenberger Susan, Waters Brent. Attribute-based encryption with fast decryption.. *Public Key Cryptography.* 2013;7778:162–179.

52. Takashima Katsuyuki. Expressive attribute-based encryption with constant-size ciphertexts from the decisional linear assumption. *International Conference on Security and Cryptography for Networks.* 2014;:298–317.

53. Liu Weiran, Liu Jianwei, Wu Qianhong, Qin Bo, Zhou Yunya. Practical direct chosen ciphertext secure key-policy attribute-based encryption with public ciphertext test. *European Symposium on Research in Computer Security.* 2014;:91–108.

54. Lai Junzuo, Deng Robert H, Li Yingjiu, Weng Jian. Fully secure key-policy attribute-based encryption with constant-size ciphertexts and fast decryption. *Proceedings of the 9th ACM symposium on Information, computer and communications security.* 2014;:239–248.

55. Shi Yanfeng, Zheng Qingji, Liu Jiqiang, Han Zhen. Directly revocable key-policy attribute-based encryption with verifiable ciphertext delegation. *Information Sciences.* 2015;295:221–231.

56. Chase Melissa, Chow Sherman SM. Improving privacy and security in multi-authority attribute-based encryption. *Proceedings of the 16th ACM conference on Computer and communications security.* 2009;:121–130.

57. Camenisch Jan, Lysyanskaya Anna. An efficient system for non-transferable anonymous credentials with optional anonymity revocation. *International Conference on the Theory and Applications of Cryptographic Techniques.* 2001;:93–118.

58. Kallahalla Mahesh, Riedel Erik, Swaminathan Ram, Wang Qian, Fu Kevin. Plutus: Scalable Secure File Sharing on Untrusted Storage.. *Fast.* 2003;3:29–42.

59. Han Jinguang, Susilo Willy, Mu Yi, Yan Jun. Privacy-preserving decentralized key-policy attribute-based encryption. *IEEE Transactions on Parallel and Distributed Systems.* 2012;23(11):2150–2162.

60. Nishide Takashi, Yoneyama Kazuki, Ohta Kazuo. Attribute-based encryption with partially hidden encryptor-specified access structures. *International Conference on Applied Cryptography and Network Security.* 2008;:111–129.

61. Cheung Ling, Newport Calvin. Provably secure ciphertext policy ABE. *Proceedings of the 14th ACM conference on Computer and communications security.* 2007;:456–465.

62. Lai Junzuo, Deng Robert H, Li Yingjiu. Expressive CP-ABE with partially hidden access structures. *Proceedings of the 7th ACM symposium on information, computer and communications security.* 2012;:18–19.

63. Xu Runhua, Lang Bo. A CP-ABE scheme with hidden policy and its application in cloud computing. *International Journal of Cloud Computing.* 2015;4(4):279–298.

64. Phuong Tran Viet Xuan, Yang Guomin, Susilo Willy. Hidden ciphertext policy attribute-based encryption under standard assumptions. *IEEE Transactions on Information Forensics and Security.* 2016;11(1):35–45.

65. Zhong Hong, Zhu Wenlong, Xu Yan, Cui Jie. Multi-authority attribute-based encryption access control scheme with policy hidden for cloud storage. *Soft Computing.* 2016;:1–9.

66. Kate Aniket, Zaverucha Greg, Goldberg Ian. Pairing-based onion routing. *International Workshop on Privacy Enhancing Technologies.* 2007;:95–112.

67. Zhou Zhibin, Huang Dijiang, Wang Zhijie. Efficient privacy-preserving ciphertext-policy attribute based-encryption and broadcast encryption. *IEEE Transactions on Computers.* 2015;64(1):126–138.

68. Yundong Fan, Xiaoping Wu, Jiasheng Wang. Multi-authority attribute-based encryption access control scheme with hidden policy and constant length ciphertext for cloud storage. In: :205–212IEEE; 2017.

69. Belguith Sana, Kaaniche Nesrine, Laurent Maryline, Jemai Abderrazak, Attia Rabah. Phoabe: Securely outsourcing multi-authority attribute based encryption with policy hidden for cloud assisted iot. *Computer Networks.* 2018;133:141–156.

70. Zhong Hong, Zhu Wenlong, Xu Yan, Cui Jie. Multi-authority attribute-based encryption access control scheme with policy hidden for cloud storage. *Soft Computing.* 2018;22(1):243–251.

71. Xiong Hu, Zhao Yanan, Peng Li, Zhang Hao, Yeh Kuo-Hui. Partially policy-hidden attribute-based broadcast encryption with secure delegation in edge computing. *Future Generation Computer Systems.* 2019;.

72. Huang Qinlong, Yang Yixian, Shen Mansuo. Secure and efficient data collaboration with hierarchical attribute-based encryption in cloud computing. *Future Generation Computer Systems.* 2016;.

73. Ruj Sushmita. Attribute based access control in clouds: A survey. In: :1–6; 2014.

74. Kaaniche Nesrine, Laurent Maryline. Attribute based encryption for multi-level access control policies. *SECRYPT 2017: 14th International Conference on Security and Cryptography.* 2017;6:67–78.

75. Kaaniche Nesrine, Laurent Maryline. SABE: a Selective Attribute-Based Encryption for an efficient threshold multi-level access control. 2018;2:155–167.

76. Kaaniche Nesrine, Belguith Sana, Russello Giovanni. EMA-LAB: Efficient Multi Authorisation Level Attribute Based Access Control. 2018;:187–201.

77. Maji Hemanta K, Prabhakaran Manoj, Rosulek Mike. Attribute-Based Signatures: Achieving Attribute-Privacy and Collusion-Resistance.. *IACR Cryptology ePrint Archive.* 2008;2008:328.

78. Li Jin, Au Man Ho, Susilo Willy, Xie Dongqing, Ren Kui. Attribute-based signature and its applications. *Proceedings of the 5th ACM Symposium on Information, Computer and Communications Security.* 2010;:60–69.

79. Ge Aijun, Chen Cheng, Ma Chuangui, Zhang Zhenfeng. Short and Efficient Expressive Attribute-Based Signature in the Standard Model.. *IACR Cryptology ePrint Archive.* 2012;2012:125.

80. Zhao Fangming, Nishide Takashi, Sakurai Kouichi. Realizing fine-grained and flexible access control to outsourced data with attribute-based cryptosystems. In: Springer 2011 (pp. 83–97).

81. Maji Hemanta K, Prabhakaran Manoj, Rosulek Mike. Attribute-based signatures. In: Springer 2011.

82. Liu Xuejiao, Xia Yingjie, Jiang Shasha, Xia Fubiao, Wang Yanbo. Hierarchical attribute-based access control with authentication for outsourced data in cloud computing. *2013 12th IEEE International Conference on Trust, Security and Privacy in Computing and Communications.* 2013;:477–484.

83. Liu Zhusong, Yan Hongyang, Li Zhike. Server-aided anonymous attribute-based authentication in cloud computing. *Future Generation Computer Systems.* 2015;52:61–66.

84. Okamoto Tatsuaki, Takashima Katsuyuki. Decentralized attribute-based signatures. In: Springer 2013 (pp. 125–142).

85. Ruj Sushmita, Stojmenovic Milica, Nayak Amiya. Decentralized access control with anonymous authentication of data stored in clouds. *IEEE Transactions on Parallel and Distributed Systems.* 2014;25(2):384–394.

86. Rao Y Sreenivasa, Dutta Ratna. Efficient attribute-based signature and signcryption realizing expressive access structures. *International Journal of Information Security.* 2016;15(1):81–109.

87. Khader Dalia. Attribute Based Group Signature with Revocation. *IACR Cryptology ePrint Archive.* 2007;2007:241.

88. Escala Alex, Herranz Javier, Morillo Paz. Revocable attribute-based signatures with adaptive security in the standard model. In: Springer 2011 (pp. 224–241).

89. El Kaafarani Ali, Ghadafi Essam, Khader Dalia. Decentralized traceable attribute-based signatures. In: Springer 2014 (pp. 327–348).

90. Kaaniche Nesrine, Laurent Maryline. Attribute-based signatures for supporting anonymous certification. *European Symposium on Research in Computer Security*. 2016;:279–300.

91. Meng Dacheng, Wang Wenbo, Luo Entao, Wang Guojun. Attribute-Based Traceable Anonymous Proxy Signature Strategy for Mobile Healthcare. *Security, Privacy, and Anonymity in Computation, Communication, and Storage: 9th International Conference, SpaCCS 2016, Zhangjiajie, China, November 16-18, 2016, Proceedings*. 2016;:178–189.

92. Hong Hanshu, Sun Zhixin. An efficient and traceable KP-ABS scheme with untrusted attribute authority in cloud computing. *Journal of Cloud Computing*. 2016;5(1):1.

93. Sun Jiameng, Qin Jing, Ma Jixin. Securely outsourcing decentralized multi-authority attribute based signature. In: :86–102Springer; 2017.

94. Gu Ke, Jia Weijia, Wang Guojun, Wen Sheng. Efficient and secure attribute-based signature for monotone predicates. *Acta Informatica*. 2017;54(5):521–541.

95. Guo Rui, Shi Huixian, Zhao Qinglan, Zheng Dong. Secure attribute-based signature scheme with multiple authorities for blockchain in electronic health records systems. *IEEE Access*. 2018;6:11676–11686.

96. Cui Hui, Deng Robert H, Liu Joseph K, Yi Xun, Li Yingjiu. Server-aided attribute-based signature with revocation for resource-constrained industrial-internet-of-things devices. *IEEE Transactions on Industrial Informatics*. 2018;14(8):3724–3732.

97. Sun Jiameng, Su Ye, Qin Jing, Hu Jiankun, Ma Jixin. Outsourced Decentralized Multi-authority Attribute Based Signature and Its Application in IoT. *IEEE Transactions on Cloud Computing*. 2019;.

98. Gagné Martin, Narayan Shivaramakrishnan, Safavi-Naini Reihaneh. Threshold attribute-based signcryption. *International Conference on Security and Cryptography for Networks*. 2010;:154–171.

99. Emura Keita, Miyaji Atsuko, Rahman Mohammad Shahriar. Dynamic attribute-based signcryption without random oracles. *International Journal of Applied Cryptography*. 2012;2(3):199–211.

100. Liu Jianghua, Huang Xinyi, Liu Joseph K. Secure sharing of personal health records in cloud computing: ciphertext-policy attribute-based signcryption. *Future Generation Computer Systems*. 2015;52.

101. Rao Y Sreenivasa, Dutta Ratna. Expressive bandwidth-efficient attribute based signature and signcryption in standard model. *Australasian Conference on Information Security and Privacy*. 2014;:209–225.

102. Belguith Sana, Kaaniche Nesrine, Laurent Maryline, Jemai Abderrazek, Attia Rabah. Constant-size Threshold Attribute Based SignCryption for Cloud Applications. *14th International Conference on Security and Cryptography(Secrypt)*. 2017;.

103. Rao Y Sreenivasa. A secure and efficient Ciphertext-Policy Attribute-Based Signcryption for Personal Health Records sharing in cloud computing. *Future Generation Computer Systems*. 2017;67:133–151.

104. LIU Ximeng, Xia Yunhao, Sun Zhixin. Provably secure attribute based signcryption with delegated computation and efficient key updating. *KSII Transactions on Internet and Information Systems*. 2017;11(5):2646.

105. Belguith Sana, Kaaniche Nesrine, Mohamed Mohamed, Russello Giovanni. C-ABSC: cooperative attribute based signcryption scheme for internet of things applications. In: :245–248IEEE; 2018.

106. Belguith Sana, Kaaniche Nesrine, Mohamed Mohamed, Russello Giovanni. Coop-DAAB: Cooperative Attribute Based Data Aggregation for Internet of Things Applications. In: :498–515Springer; 2018.

107. Deng Fuhu, Wang Yali, Peng Li, Xiong Hu, Geng Ji, Qin Zhiguang. Ciphertext-Policy Attribute-Based Signcryption With Verifiable Outsourced Designcryption for Sharing Personal Health Records. *IEEE Access*. 2018;6:39473–39486.

108. Xu Qian, Tan Chengxiang, Fan Zhijie, Zhu Wenye, Xiao Ya, Cheng Fujia. Secure Data Access Control for Fog Computing Based on Multi-Authority Attribute-Based Signcryption with Computation Outsourcing and Attribute Revocation. *Sensors*. 2018;18(5):1609.

109. Al-khafajiy Mohammed, Baker Thar, Chalmers Carl, et al. Remote health monitoring of elderly through wearable sensors. *Multimedia Tools and Applications*. 2019;:1–26.

110. Al-khafajiy Mohammed, Baker Thar, Waraich Atif, Al-Jumeily Dhiya, Hussain Abir. IoT-Fog Optimal Workload via Fog Offloading. In: :359–364IEEE; 2018.

111. Attrapadung Nuttapong, Herranz Javier, Laguillaumie Fabien, Libert Benoît, De Panafieu Elie, Ràfols Carla. Attribute-based encryption schemes with constant-size ciphertexts. *Theoretical Computer Science*. 2012;422:15–38.

112. Green Matthew, Hohenberger Susan, Waters Brent, others . Outsourcing the decryption of abe ciphertexts. *USENIX Security Symposium*. 2011;(3).

113. Qin Baodong, Deng Robert H, Liu Shengli, Ma Siqi. Attribute-based encryption with efficient verifiable outsourced decryption. *IEEE Transactions on Information Forensics and Security*. 2015;10(7):1384–1393.

114. Chung Kai-Min, Kalai Yael, Vadhan Salil. Improved delegation of computation using fully homomorphic encryption. *Annual Cryptology Conference*. 2010;:483–501.

115. Gennaro Rosario, Gentry Craig, Parno Bryan. Non-interactive verifiable computing: Outsourcing computation to untrusted workers. *Annual Cryptology Conference*. 2010;:465–482.

116. Lai Junzuo, Deng Robert H, Guan Chaowen, Weng Jian. Attribute-based encryption with verifiable outsourced decryption. *IEEE Transactions on Information Forensics and Security*. 2013;8(8):1343–1354.

117. Wang Hao, Yang Bo, Wang Yilei. Server Aided Ciphertext-Policy Attribute-Based Encryption. *Advanced Information Networking and Applications Workshops (WAINA), 2015 IEEE 29th International Conference on*. 2015;:440–444.

118. Li Jiguo, Sha Fengjie, Zhang Yichen, Huang Xinyi, Shen Jian. Verifiable Outsourced Decryption of Attribute-Based Encryption with Constant Ciphertext Length. *Security and Communication Networks*. 2017;2017.

119. Li Jin, Huang Xinyi, Li Jingwei, Chen Xiaofeng, Xiang Yang. Securely outsourcing attribute-based encryption with checkability. *IEEE Transactions on Parallel and Distributed Systems*. 2014;25(8):2201–2210.

120. Lin Suqing, Zhang Rui, Ma Hui, Wang Mingsheng. Revisiting attribute-based encryption with verifiable outsourced decryption. *IEEE Transactions on Information Forensics and Security*. 2015;10(10):2119–2130.

121. Zuo Cong, Shao Jun, Wei Guiyi, Xie Mande, Ji Min. CCA-secure ABE with outsourced decryption for fog computing. *Future Generation Computer Systems*. 2016;.

122. Ma Hui, Zhang Rui, Wan Zhiguo, Lu Yao, Lin Suqing. Verifiable and exculpable outsourced attribute-based encryption for access control in cloud computing. *IEEE transactions on dependable and secure computing*. 2017;14(6):679–692.

123. Li Jing, Li Xiong, Wang Licheng, He Debiao, Ahmad Haseeb, Niu Xinxin. Fuzzy encryption in cloud computation: efficient verifiable outsourced attribute-based encryption. *Soft Computing*. 2018;22(3):707–714.

124. Zhang Jindan, Wang Baocang, Xhafa Fatos, Wang Xu An, Li Cong. Energy-efficient secure outsourcing decryption of attribute based encryption for mobile device in cloud computation. *Journal of Ambient Intelligence and Humanized Computing*. 2019;10(2):429–438.

125. Ge Chunpeng, Susilo Willy, Fang Liming, Wang Jiandong, Shi Yunqing. A CCA-secure key-policy attribute-based proxy re-encryption in the adaptive corruption model for dropbox data sharing system. *Designs, Codes and Cryptography*. 2018;86(11):2587–2603.

126. Belguith Sana, Kaaniche Nesrine, Russello Giovanni. PU-ABE: Lightweight Attribute-Based Encryption Supporting Access Policy Update for Cloud Assisted IoT. *2018 IEEE 11th International Conference on Cloud Computing (CLOUD)*. 2018;:924–927.

127. Belguith Sana, Kaaniche Nesrine, Russello Giovanni. Lightweight Attribute-based Encryption Supporting Access Policy Update for Cloud Assisted IoT. In: :135-146; 2018.

128. Hong Hanshu, Liu Ximeng, Sun Zhixin. A Fine-Grained Attribute Based Data Retrieval with Proxy Re-Encryption Scheme for Data Outsourcing Systems. *Mobile Networks and Applications*. 2018;:1–6.

129. Jiang Yinhao, Susilo Willy, Mu Yi, Guo Fuchun. Ciphertext-policy attribute-based encryption supporting access policy update and its extension with preserved attributes. *International Journal of Information Security*. 2017;:1–16.

130. Jiang Yinhao, Susilo Willy, Mu Yi, Guo Fuchun. Ciphertext-policy attribute based encryption supporting access policy update. *International Conference on Provable Security*. 2016;:39–60.

131. Baker Thar, Asim Muhammad, MacDermott Áine, et al. A secure fog-based platform for SCADA-based IoT critical infrastructure. *Software: Practice and Experience*. ;.

132. Ghafir Ibrahim, Saleem Jibran, Hammoudeh Mohammad, et al. Security threats to critical infrastructure: the human factor. *The Journal of Supercomputing*. 2018;:1–17.

AUTHOR BIOGRAPHY

Sana Belguith is a Lecturer at School of Computing, Science and Engineering, University of Salford, Manchester, UK. Previously, she used to be a Post-Doctoral Researcher in the Department of Computer Science at The University of Auckland, New Zealand. She received her engineering degree in Computer Science from the National Engineering School of Tunisia, in 2012 and her Ph.D. degree from the Tunisia Polytechnic School, Tunisia in 2017. As part of her Ph.D. programme, she was a Visiting Fellow at Télécom SudParis, France. Her major research interests include applied cryptography, distributed systems security, privacy enhancing techniques, access control, attribute-based encryption, and searchable encryption.

Nesrine Kaaniche is a Lecturer in Cybersecurity at the Department of Computer Science, University of Sheffield, co-affiliated with the Security of Advanced Systems Research Group. Previously, she was a research member of the chair Values and Policies of Personal Information, at Telecom SudParis, Institut Polytechnique de Paris, France and an International Fellow (Aug- Nov 2016) at SRI International, San Francisco, CA, USA. She received a PhD degree on cloud storage security jointly from Sorbonne University and Telecom SudParis, France, in 2014. Her major research interests include privacy enhancing technologies and applied cryptography for distributed systems and decentralised architectures, i.e., IoT, fog, cloud, and blockchains. She served as Technical Program Committee member for several conferences, and as referee for several outstanding international journals.

Mohammad Hammoudeh is the Head of the CfACS IoT Laboratory within the Department of Computing and Mathematics, Manchester Metropolitan University. He has been a researcher and publisher in the field of big sensory data communication, mining and visualisation. He is a highly proficient, experienced, and professionally certified cyber security professional, specialising in threat analysis, and information and network security management. His research interests include highly decentralised algorithms, communication, and cross-layered solutions to Internet of Things, and wireless sensor networks.