information

MDPI

Article

AES–CP–IDABE: A Privacy Protection Framework against a DoS Attack in the Cloud Environment with the Access Control Mechanism

Sonali Chandel [1,*], Geng Yang [1,2] and Sumit Chakravarty [3]

[1] School of Computer Science, Nanjing University of Posts and Telecommunications, Nanjing 210003, China; yangg@njupt.edu.cn

[2] Jiangsu Key Laboratory of Big Data Security & Intelligent Processing, Nanjing 210003, China

[3] Department of Electrical and Computer Engineering, Kennesaw State University, Marietta, GA 30060, USA; schakra2@kennesaw.edu

* Correspondence: f2015010102@njupt.edu.cn

Received: 10 June 2020; Accepted: 17 July 2020; Published: 22 July 2020

Abstract: Cloud computing technology has revolutionized the field of data management as it has enhanced the barriers of storage restrictions and high-cost establishment for its users. The benefits of the cloud have paved the way for its extensive implementation in large enterprises. However, the data in the cloud have succumbed to various security threats, and its privacy issues remain one of the biggest and topmost concerns for the data owners. Several techniques, such as Attribute-based Encryption (ABE), have been proposed by several researchers to preserve the privacy of the data. However, the issue of security still looms largely over the cloud. In the present work, we introduce the novel encryption model called "Advanced Encryption Standard–Cipher-text-Identity and Attribute-based Encryption" (AES–CP–IDABE) to preserve data privacy along with its access control. In the proposed scheme, the data have been double encrypted initially through the ABE, along with the attributes and the identity of the user. Secondly, the Advanced Encryption Standard (AES) is used to encrypt the encrypted data and provide it to the authorized users. The user access control is established using the digital signature with the help of user ID and security keys. Additionally, the set up includes Denial-of-Service (DoS) detection through IP address monitoring and control. The proposed scheme has also been evaluated for its performance in the communication between the user and the data owner, along with the user's execution time. From the outcome, it is evident that the proposed scheme was more effective than the existing scheme of ABE over execution, encryption, and decryption time. Additionally, the performance over DoS detection and impact of attribute numbers for the proposed scheme was also studied to prove its effectiveness.

Keywords: cloud security; cipher-text; attribute-based encryption; advanced encryption standard; access control; DoS detection; privacy

1. Introduction

With the advent of cloud computing technology, the domain of networking with data is on the rise. This technique has been accepted extensively around the world in recent times. The intense evolution and implementation of the cloud environment have happened due to its ability to handle massive data at a minimal cost, along with its flexible access policies. This has caused many public and private enterprises to establish a cloud network for their data management purpose and their users [1]. However, like any other technology, cloud computing also suffers from numerous privacy and security concerns that remain as a hindrance to its complete adoption [2]. If the existing problems related to cloud security are not addressed appropriately, the chances are that it might prevent the growth and extension of cloud-computing application areas in the future [3]. Among the most common security issues, maintaining the privacy of data stored on the cloud is a primary concern for most of the organizations/users before deciding to go for the adoption of cloud computing. When sensitive data is shared over the cloud, the concern of the data owners increases naturally, especially when it comes to the handling of the security and privacy of their data by the cloud service providers [4].

The traditional symmetric and asymmetric key encryption methods are employed to ensure the privacy of the data. The symmetric key is an identical key for both encryption and decryption process. The asymmetric key means that the public key and the private key used for both cryptic processes are different. However, these encryption methods only offer some privacy and zero access control [5]. Another critical issue is that several attacks like malware-injection, side-channel, and flooding can be easily conducted against cloud computing [6]. One of the most common security threats is the Denial-of-Service (DoS) attacks that refer to the malicious behavior of hackers, which prevents the cloud's capacity to perform adequately to its normal functions and services [7]. The main issues that need to be addressed for storing data on the cloud are user access control and data privacy [8], along with DoS detection.

Recently, Attribute-Based Encryption (ABE) has gained significant attention among researchers, as it can retain data privacy and realize access control in a fine-grained manner [9]. Notably, Cipher-text Policy–Attribute-based Encryption (CP-ABE) enables data owners to define the access policy through a set of attributes that the user needs to possess to decrypt the cipher-text, by which the confidentiality and access control of data can be guaranteed [10]. For addressing the issues in the existing CP-ABE, ABE, and Advanced Encryption Standard (AES), a novel algorithm is used in the present work to encrypt the data twice using the Cipher-text Policy-Identity–Attribute-Based Encryption (CP-IDABE) along with AES through the AES–CP–IDABE scheme. The attributes set of the user are defined to allow them to access the data in the cloud. Their identity is established through a set of five questions that are put forth randomly for verifying them during authentication. The AES is applied with a key size of 256-bits on the cipher-text obtained after data encryption through the proposed CP–IDABE.

The significant contribution that we have provided through our proposed scheme to ensure the security of the data on the cloud concerning its privacy and access control is as follows:

1. We developed a novel ABE model using AES cryptography and identity-based access control at the owner's side and the user's side in the cloud environment. We name the novel algorithm as "AES Cipher-text-Identity and Attribute-Based Encryption" or AES–CP–IDABE in short.
2. We provide the owner-side authentication with the necessary information of the owner. This becomes the attribute for their key generation through which they can access the cloud environment.
3. For the user-side, we provide two layers for generating the attributes that will be implemented during the authentication process. Initially, the user's basic information is employed for identity generation along with five random questions, which can ensure the credibility and validity of the authorized user.
4. The data in our model is encrypted using AES cryptography, and it is effectively decrypted with the independent keys of the user 6.
5. Along with securing the data, our model also shows reduced overhead and resource consumption, which is a crucial requirement for its real-time implementation.

Our paper is divided into different sections and subsections as follows: after the introductory section, Section 2 discusses the related works on the cloud environment and its security that are completed explicitly in the field of data privacy and access control. Section 3 discusses the proposed methodology for accomplishing the authentication along with the defense against DoS attacks. Section 4 highlights the working principle of the proposed system model. Section 5 describes the control mechanism and security model implementation. Section 6 presents the control of the proposed algorithm. Section 7 presents the evaluation of the proposed methodology, along with its comparison to the existing techniques. The final Section 8, summarizes the paper with a conclusion and provides insights for future work.

2. Related Work

An embryonic tool is proposed in [11] for updating the key and providing the zero-knowledge authentication for cloud privacy through data auditing. The approach reduced the cost of both computation and communication with essential security. The real-time verification is not carried out to understand the practical problems. The authors in [12] proposed the Hierarchical Predicate Encryption (HPE) technique for improving the privacy of the cloud data. They also used the Keyword Search with Access Control (KSAC), which provides the fine-grained access control under a multi-field query search. The proposed method has been validated with the real-time application and found to be effective. In [13], a novel and secure K-Nearest Neighbor (KNN) query scheme is proposed for protecting the privacy of the cloud data. The method has been validated for its security in a theoretical approach, and it is found to be effective after extensive trials. The authors of [14] proposed another KNN query scheme. They provided multiple keys for preserving the privacy of the encrypted data with a distributed Double Trapdoor Public-Key Cryptosystem (DT-PKC) and protocols set. From the extensive evaluation, the proposed method exhibited its effectiveness in both performances as well as security.

In [15], an attribute-based method has been established for the storage system in the cloud for protecting privacy. This method avoided the deduplication of data in it. It also provides the access policy without the usage of the decryption key. In [16], the attribute-based encryption has been implemented in the multi-publisher cloud environment in which the subscriber accesses the published data. In this approach, the outsourcing model provides the encryption method. In [17], the attribute-based scheme has been implemented to verify the attributes set along with the cipher-text under both the offline and online mode. The method is based on a weak decisional bilinear Diffie–Hellman method in a restricted resource environment. The main limitation of this method is the revocation of the attributes in data sharing. In [18], a cipher-text-ABE scheme is proposed with the use of access policies that are defined at the owner's side of the data. The evaluated outcome proves the effectiveness and performance. It is observed that the established method is feasible only under the limited resource environment.

In [19], a Security-enhanced Multi-Authority Attribute-based Encryption (SMA–ABE) is provided to attain access control of fine-grained order and efficient decryption with provable transformation and offload on the cloud. As a result, it provides storage efficiency, computation, and communication and completes the detection in a shorter time compared to other schemes with similar detection accuracy. In [20], a novel framework is proposed to monitor the synchronize packets flowing through the correlation engine or a flow traffic tool. For detecting the attack source, packet marking techniques and time-to-live (TTL) is used. A honeypot technique is also used for the prevention of attacks. In [21], another Fast-malformed Hypertext transfer protocol-message Detection Algorithm (FHDA) is proposed to provide priority to the recurrent malformed elements, and it enhances the priority of detection in each field based on the previous detection results. The presented scheme was able to complete the detection in a shorter time by maintaining the detection accuracy.

In [22], an intrusion detection model was proposed using the machine learning technique to detect the DoS attack. The signature-based approach is employed for classifying four benchmark datasets and accomplished the detection rate of 96%. In [23], a novel two-fold security scheme was proposed with the Public key Encryption Keyword Search (PEKS) and Role-based Access Control (RBAC). The proposed framework did not perform the bilinear mapping and achieved an efficiency of about 97%. The security proof of the proposed model is validated based on its different components through the available commercial datasets. In [24], an extensive survey of the different security frameworks that are employed to secure a patient's data in the cloud environment is studied. It highlighted the importance of preserving healthcare data effectively. The study suggested that future research on cloud security must provide a fool-proof privacy mechanism to secure data sustainably. In [25], a decentralized ABE with multiple authority for securing the cloud is proposed. The proposed mechanism provided the complete solution to the previously established security scheme of Lewko and Waters through an effective mechanism for key distribution.

In [26], a novel identity-based encryption with an equality test supporting flexible authorization is proposed for protecting the privacy of the cloud data. In this technique, the equality test is performed to verify whether two encrypted cipher-texts have the same message. The outcome of the experiments showed that the proposed scheme was effective in providing security. In [27], the improved form of CP-ABE is proposed for the secure sharing of data in the cloud environment. The comparison with the existing scheme showed that the proposed scheme is highly reliable and safe. In [28], a novel secure system is proposed with an algorithm of role re-encryption and convergent encryption. It was named the Secure Role Re-encryption System (SRRS). The proposed system supports the validation for both owners and users through the mapping between the keys and roles through the role authorization tree. The system encloses both the revocation and key updating mechanism to secure the data from any leakage. Simulation experiments validate the effectiveness of the proposed security system.

From the extensive survey of the related works, a comparison of which is given in Table 1, we observed that the ABE methods are being widely implemented for preserving data privacy and providing access control. However, some problems still exist for the data in the cloud environment. The following are the problem statements for the present work:

- When malicious users launch the cyber-attacks on cloud storage, resource consumption will increase.
- The cryptography-driven access control does not protect the cloud provider against many attacks.
- The cloud provider does not implement access control effectively and does not prevent access from unauthorized users effectively.

Table 1. Comparison of works on securing data and user privacy in the cloud.

Ref. No.	Contribution	Methodology	Performance	Future Scope/Limitation
[11]	In the Public Key Infrastructure system, the key expires with the digital certificate	Key updation technique developed for auditing the cloud data	New scheme was more effective than Shacham–Waters auditing scheme	Real-time implementation of the proposed scheme required to understand its effectiveness
[12]	Keyword search problem with access control is addressed	Novel scheme with KSAC is established with encrypted data	Proposed KSAC required 1.08s and 0.12s for generating per-capacity and match decision	Cost can be reduced by modifying the noise injection frequency
[13]	Traditional method of support processing and analysis of encrypted data	K-nearest neighbor (KNN) query scheme is proposed	Proposed scheme showed less overhead compared to the existing schemes	Access pattern for data has to be protected
[15]	Existing ABE system does not support a secure deduplication process	Attribute-based method established for the storage system with effective deduplication	Provided increased confidentiality and semantic security in sharing and deduplication of data	Supports the construction of a new ABE scheme that can be used in CP-ABE
[17]	Addressed the problem in achieving high-efficiency, fine-graininess on data owner’s side	Attribute-based scheme implemented to verify the attribute set along with the cipher-text under offline and online mode	Proposed method is robust against cipher-text attacks	Main limitation is the revocation of the attributes in data sharing

3. Preliminaries

The present work involves the usage of the cipher-text policy attribute-based encryption with the identity of a user (CP–IDABE) and the advanced encryption standards (AES). The preliminaries for the proposed dual encryption algorithm are given in the following subsections.

3.1. CP–IDABE

The CP–IDABE combines both the user ID and the attributes for the cryptic mechanism of the cipher data under the access policy. The user can employ the generated key to encrypt and decrypt the data in the cloud environment. The ID of the user comprises the username and password. The attribute set includes a set of answers for the questions that were used to validate the user from accessing the cloud.

- Attributes: In the proposed model, the attributes of the user can be one of the following items in the set of five:

  (i) First job;
  (ii) Last five digits of their credit card;
  (iii) Name of their hometown;
  (iv) Favorite team;
  (v) Favorite sports.

- Policy: Here, the access policy for the user has been designated by attribute A with the identity ID of the user U (A $\wedge ID \wedge U$). The user identity obtained from the user name and password is listed along with the attribute in formulating the access policy that is set in the cloud. Hence, CP–IDABE secures the data from unauthorized access. On satisfying the given condition, the access will be approved, or else it will be denied.

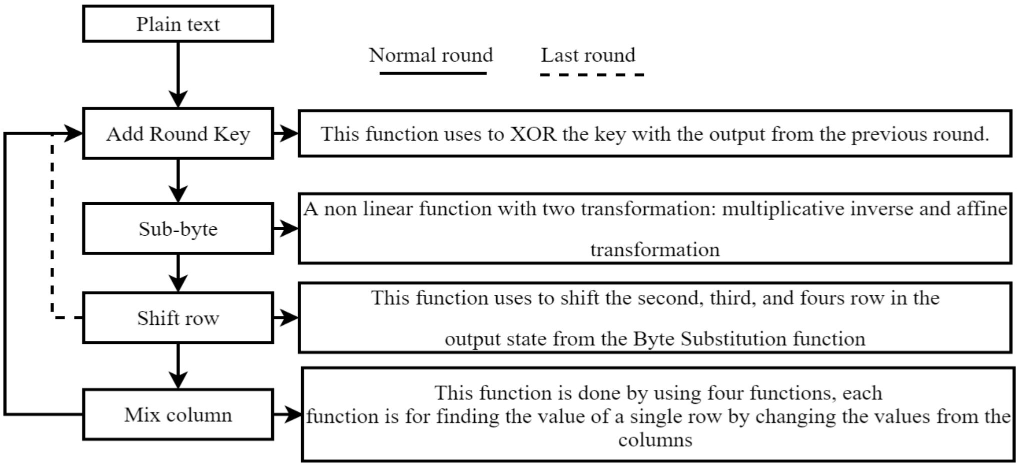
The CP–IDABE consists of attributes $\mathrm{A_i}$, the following steps as setup, key generating technique (KeyGen), encryption (Enc) and decryption (Dec) in performing the cryptic mechanism to the cloud data:

- Setup (1^{P}): P is the security parameter that provides the Public key ($\mathrm{P_k}$) and Master secret key ($\mathrm{M_k}$) from the cloud server (CS).
- KeyGen ($\mathrm{M_k}$, $\mathrm{A_i}$, $\mathrm{ID_u}$): Given attributes $\mathrm{A_i}$ and $\mathrm{M_k}$ and the identity of the user ($\mathrm{ID_u}$), this algorithm yields the private key of the user ($\mathrm{S_{ki}}$).
- Enc ($\mathrm{P_k}$, M, $\mathrm{ID_u}$, A): Given $\mathrm{P_k}$, the user identity ($\mathrm{ID_u}$), the message M and an access policy (A), the Enc algorithm yields an initial Encrypted cipher-text (Ect).
- Dec ($\mathrm{S_{ki}}$, Ect): Given the private key ($\mathrm{S_{ki}}$) and an initially encrypted cipher-text (Ect), the Dec algorithm yields the message M if the $\mathrm{ID_u}$ and $\mathrm{A_i}$ satisfy the access policy (A).

3.2. AES–Cryptology

The AES algorithm is implemented in the proposed model to perform another cryptic operation using the cipher-text that was encrypted through CP–IDABE with a 256-bit key with 14 rounds. The AES algorithm has the following mechanism for encryption after the key generation, as shown in Figure 1. The generated AES key is shared with the user, along with the CP–ID-ABE key.

- Enc (M′, K): Given the key (K), the message M′ yields the final cipher-text (Ect′) during encoding (Enc).
- Dec (K, Ect′): Given the key (K), this algorithm yields the message M′ from Ect′ during decoding (Dec).



This function uses to XOR the key with the output from the previous round.

A non linear function with two transformation: multiplicative inverse and affine transformation

This function uses to shift the second, third, and fours row in the output state from the Byte Substitution function

This function is done by using four functions, each function is for finding the value of a single row by changing the values from the columns

Figure 1. Advanced encryption standard.

3.3. *Digital Signature*

- SignGen (IDu, At, Mk): the identity of the user (IDu) and the access policy (At) along with the master key (Mk) yield the digital signature (SD) and the verifying message Mv.

3.4. *Dual Encryption of AES–CP–IDABE*

$$\left(\begin{array}{c} S_k \leftarrow_{\$} \{0,\ 1\}^{\lambda} \\ \text{Ect} \ \leftarrow \ \text{ABE.Enc}\,(P_k,\ S_{ki},\ A) \\ \text{SD} \ \leftarrow \ \text{SIG.Sign}\,(S_i,\ \text{Ect}) \\ \text{Ect}' \ \leftarrow \text{AES.ENC}(k, M_1) \\ \text{output}\,(\text{Ect},\ \text{SD}, \text{Ect}_1, \text{Ect}') \end{array}\right)$$

In the proposed method, the data in the cloud is encrypted using a double-encryption algorithm. Initially, the data in the cloud is encrypted (Ect) with a secret key (S_{ki}) and public key (P_k) obtained through the CP–IDABE algorithm based on its access policy (A), and the security parameter (λ). The digital signature (SD) is achieved with the signature key (S_i). The encrypted text is again encrypted with the AES algorithm to provide the double-encrypted cipher-text (Ect') with the secret key (K) and the message (M_1).

4. Working Principle of the Proposed System Model

The system model for the proposed algorithm, as seen in Figure 2, consists of three significant components, as explained below:

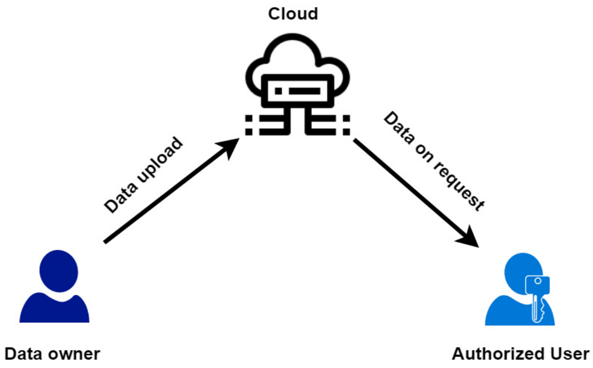


Figure 2. Components of the proposed scheme.

- Data owner: The data owner plays a vital role in any cloud environment. They are the ones who share and store the data on the cloud, which can be accessed by authorized users. They are also responsible for uploading the data into the specified cloud and encrypt it with the proposed AES–CP–IDABE. If any attack takes place in the cloud environment, then they are the ones who get affected the most.
- Data user: Data users utilize the data that are stored on the cloud. It also decrypts the encrypted data through the authentication keys provided by the data owner. The cloud server has to authorize them based on their identity and permission attributes to access the cloud and the stored data.
- Cloud server: The cloud server is an integral part of the proposed work in securing the cloud environment. All the data from the data owners and the users are stored on the server. It contains all the keys and the digital signature of all the users, along with their attributes and ID. Servers are designed to verify the difference between the user's access and the owner's access to the cloud environment. Besides authenticaticating the user, it also monitors resource utilization in the cloud.

5. Control Mechanism and Security Model

For providing adequate security to the data in the cloud environment, the proposed framework embraces three different forms of control mechanism for each of the components, as shown in Figure 3. The proposed framework also ensures the security of data through access control, data privacy, and mitigating the DoS attacks. The three different forms of control mechanism for the data access (control I), which ensures the privacy of the data, authentication, and attack resistance (control II), the security of the cloud and, finally, monitoring of the user (control III) for effective resource utilization are explained below:

- Control I: The data owner and the cloud service provider provide distinct authentication to access the cloud. The data owner takes the responsibility of assigning the access policy for the data in the cloud. Hence, the user who has the access policy privileges can only access the data by decrypting it.
- Control II: The cloud server performs the validation of the user before allowing them to access the data and decrypt them. This, in turn, provides resistance against the malicious DoS attacks.
- Control III: The data owner in this model can monitor the user in the cloud server for maintaining the usage of the resource.

Additionally, the DoS attack detection and mitigation system are incorporated to prevent it from accessing the cloud. The security of the cloud environment in the proposed methodology is explained as follows:

- Access control—Since the user attributes and their ID are both used for the authentication of the user; the attacker cannot breach the initial login process easily. In addition to this, while the user information is being processed for authenticating its access to the cloud, one of the five random questions connected to the attributes will pop up. The user can enter the cloud environment only after the verification of the answers to the random pop-up questions. Furthermore, in our model, we provide a separate authentication process for cloud service providers and the data owner.
- Data privacy—AES has never been cracked yet, and it is safe against any brute force attacks contrary to common beliefs and arguments. Additionally, even if the attacker somehow breaches the AES key because of its symmetry, they must know the novel CP–IDABE key as well to obtain the actual data, which is very complex with the well-defined access policies and random ID of the user. The double encryption process preserves data privacy as the encryption key, and a decryption key is a dual form of both AES and CP–IDABE. Hence, the data in the cloud is adequately protected.
- Against the DoS attacks—In general, DoS attacks occur with an increased number of fake requests from the external hacker's source. Once the attacker enters the cloud, the number of request

flow increases. Therefore, the cloud service provider in the proposed model initiates the attack detection and mitigation framework. It encloses the mechanism that captures the IP address and stores them in the cloud server to mitigate the attacker. If the attacker tries to access the cloud, it will block the user and protect the cloud environment from the DoS attack. In the present work, four common DoS attack forms that are considered are mentioned below:

- User datagram protocol (UDP) flood: In this type of DoS attack, a server is flooded with UDP packets. This makes it harder for defensive mechanisms to identify the attack.
- SYN flood: It is carried out when an attacker sends many SYN packets to the target server from spoofed IP addresses.
- Internet control message protocol (ICMP) flood: When a server is flooded with massive amounts of spoofed ICMP packets, its resources are exhausted in trying to process these requests. This overload reboots the server and has an enormous impact on its performance.
- HTTP flood: In an HTTP flood attack, the adversary floods massive spurious HTTP requests for downloading an online file from the target server.

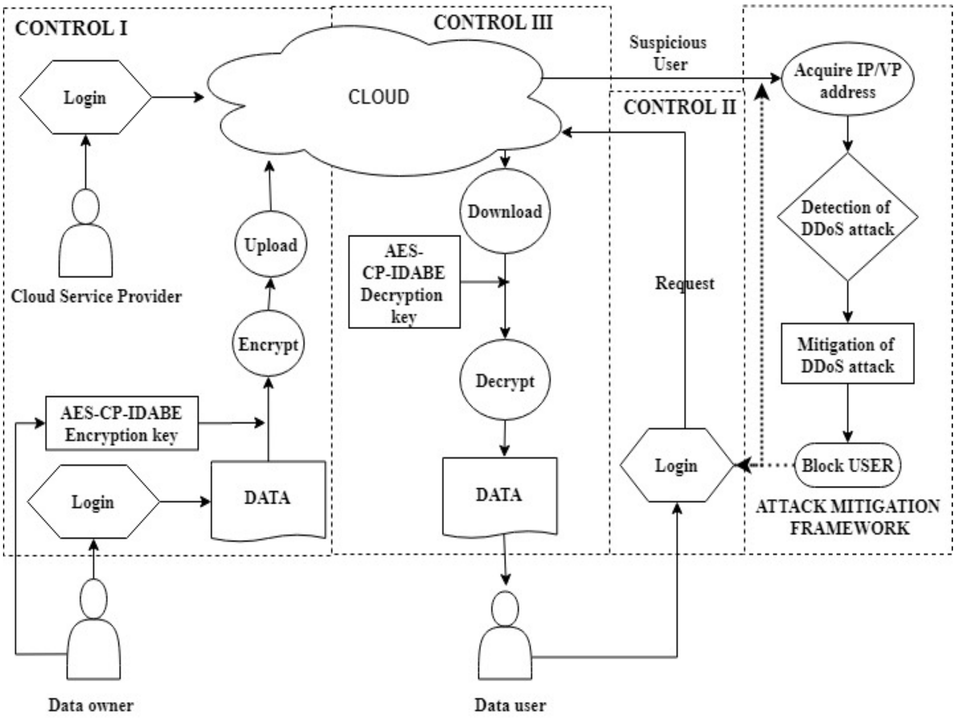


Figure 3. The proposed framework for securing data privacy and denial-of-service (DoS) mitigation.

We assume that in the cloud environment, the network flow is in a specified unit of time (T), source IP address (SI), destination IP address (DI), and the port (P) of the data packet, respectively. Based on the request information, the signature for the connection is generated. The classes of attacks are predefined with four classes, as discussed above. The class for each attack is denoted as S_A for a SYN attack, U_A for UDP attack, I_A for ICMP attack, and H_A for HTTP attack. The categorization of blocked users is given as follows:

If the cloud server accumulates SYN packets (SYN_{PCk}) without an acknowledgment packet, it overwhelms the cloud server. SYN flood is detected to be the attack (S_A)

$$\sum \mathrm{SYN}_{\mathrm{PCk}} \rightarrow \text{ SYN Flood} \rightarrow \mathrm{S}_{\mathrm{A}} \tag{1}$$

If the UDP packets $(\mathrm{UDP_{PCk}})$ accumulation increases and are sent back as destination-unreachable packets, it overwhelms the cloud server, and UDP flood is detected to be the attack $(\mathrm{U_A})$

$$\sum \mathrm{UDP_{PCk}} \rightarrow \mathrm{UDP\ flood} \rightarrow \mathrm{U_A} \tag{2}$$

If the number of ICMP $(\mathrm{ICMP_{Req}})$ echo-requests overwhelm the cloud server, ICMP flood is detected to be the attack $(\mathrm{I_A})$

$$\sum \mathrm{ICMP_{Req}} \rightarrow \mathrm{ICMP\ flood} \rightarrow \mathrm{I_A} \tag{3}$$

If the number of the HTTP requests $(\mathrm{HTTP_{req}})$ overwhelms the cloud server, HTTP flood is detected to be the attack $(\mathrm{H_A})$

$$\sum \mathrm{HTTP_{req}} \rightarrow \mathrm{HTTP\ flood} \rightarrow \mathrm{H_A} \tag{4}$$

The mitigation is carried out through the Firewall Inbound and Outbound (FIO) rules, where inbound rules deal with external attackers, and outbound rules deal with internal attacks. For all attackers, the IP and Virtual Port (VP) address are extracted and treated with FIO, as shown in the expressions below:

$$\textbf{SYN Attack}: \mathrm{S_{iA}} \rightarrow (\mathrm{IP_{is}}, \mathrm{VP_{is}}) \rightarrow \mathrm{FIO} \tag{5}$$

$$\textbf{UDP Attack}: \mathrm{U_{iA}} \rightarrow (\mathrm{IP_{iU}}, \mathrm{VP_{iU}}) \rightarrow \mathrm{FIO} \tag{6}$$

$$\textbf{ICMP Attack}: \mathrm{C_{iA}} \rightarrow (\mathrm{IP_{iC}}, \mathrm{VP_{iC}}) \rightarrow \mathrm{FIO} \tag{7}$$

$$\textbf{HTTP Attack}: \mathrm{H_{iA}} \rightarrow (\mathrm{IP_{iH}}, \mathrm{VP_{iH}}) \rightarrow \mathrm{FIO} \tag{8}$$

where $\mathrm{S_{iA}}$, $\mathrm{U_{iA}}, \mathrm{C_{iA}}, \mathrm{H_{iA}}$ are the attackers with SYN packets, UDP packets, ICMP and HTTP requests with IP and VP addresses of $(\mathrm{IP_{is}}, \mathrm{VP_{is}}), (\mathrm{IP_{iU}}, \mathrm{VP_{iU}}), (\mathrm{IP_{iC}}, \mathrm{VP_{iC}}), (\mathrm{IP_{iH}}, \mathrm{VP_{iH}})$, respectively.

6. The Flow of Control for the Proposed Algorithm

The proposed framework comprises three different phases with generating the cryptographic keys through CP–IDABE–AES algorithms and a digital signature in the cloud server (CS). The algorithm for each process is defined along with the input and output variables below:

6.1. Key Generation for CP–IDABE

- $\mathbf{P_k}$, $\mathbf{M_k} \leftarrow \mathbf{P}$: The cloud server runs the initial setup for the generated cloud data and provides the public key $(\mathrm{P_k})$ and the master key $(\mathrm{M_k})$ with the security parameter (P).
- $\mathbf{S_{ki}} \leftarrow \mathbf{M_k}, \mathbf{ID_u}, \mathbf{A_i}$: When the public and the master key are generated, and the user processes their request, the CS generates the secret key $(\mathrm{S_{ki}})$ with the master key $(\mathrm{M_k})$ along with the identity $(\mathrm{ID_u})$ and attribute set $(\mathrm{A_i})$.
- $\mathbf{Ect} \leftarrow \mathbf{P_k}$, $\mathbf{M}, \mathbf{ID_u}, \mathbf{A_i}$: The data in the cloud were encrypted before being uploading into the cloud with the encrypted key, which results in the generation of the encrypted cipher-text (Ect) with the public key $(\mathrm{P_k})$user identity $(\mathrm{ID_u})$ attribute policy (A) and the message M.
- $\mathbf{M} \leftarrow \mathbf{S_{ki}}$, $\mathbf{Ect}$: When the user provides the secret key for the encrypted cipher-text, the process of decryption begins, and the message M is obtained.

6.2. AES- ALGORITHM

- $\mathbf{Ect'} \leftarrow \mathbf{M'}, \mathbf{k}$: By providing the decrypted data as the input for the AES cryptography, the data will be encrypted again to result in Ect′ with the key (K) and the message M′.
- $\mathbf{M'} \leftarrow \mathbf{k}, \mathbf{Ect'}$: With the encrypted data Ect′ and the key (k), the data will be decrypted to produce the message M′.

6.3. Signature Generation

- $\mathbf{SD} \leftarrow \mathbf{ID_u}, \mathbf{A_i}, \mathbf{M_v}$: The CS picks the attributes and user identification ($\mathrm{ID_u}$) for generating the digital signature (SD) with the message.
- $\mathbf{Verify} \leftarrow \mathbf{SD}, \mathbf{M_v}$: For verifying the user, they must provide the digital signature SD along with the verification message $\mathrm{M_v}$.

7. Results and Discussion

The proposed security framework of the data in the cloud is implemented using Java, and the required data were accumulated in the drop-box. The interfaces in the cloud were achieved through the **Java** API for eXtensible Markup Language (XML) web services hosted with the help of Apache Tomcat. The Structured Query Language (SQL) database was updated on the server-side for storing the data. A Java-supporting Internet browser forms the client-side. The remaining basic configuration was to use an Intel processor with a memory of 16 GB at 2.45 GHz with a disk of 1 TB capacity.

The proposed approach was evaluated over three-parameters, namely:

- Cloud user communication: The amount of data that is consumed during the interaction of the user and the cloud server.
- User execution time: The measure of time taken for key generation and the response time in the cloud for the user.
- Data owner upload communication: The amount of data consumed to upload the data on the cloud from the data owners' end.

The proposed AES–CP–IDABE was compared with the existing basic ABE scheme for data security and attack detection with smart detection system [22] and shown in the following subsections.

7.1. Cloud User Communication and User Execution Time

In the evaluation of the user communication for the proposed method, it was observed to be around 1000 KB. The value was almost equal to the existing method of basic ABE. This shows that the enhancement in the basic ABE does not affect the data transmission in the cloud, as shown in Figure 4. The user data execution time was observed to be 178 ms, which was comparatively lower than that of the existing models with 189 ms. Hence, it was evident that the proposed method was 7.4% more efficient than the ABE method. Thus, by employing the proposed method, the data user execution time was reduced considerably, as shown in Figure 4.

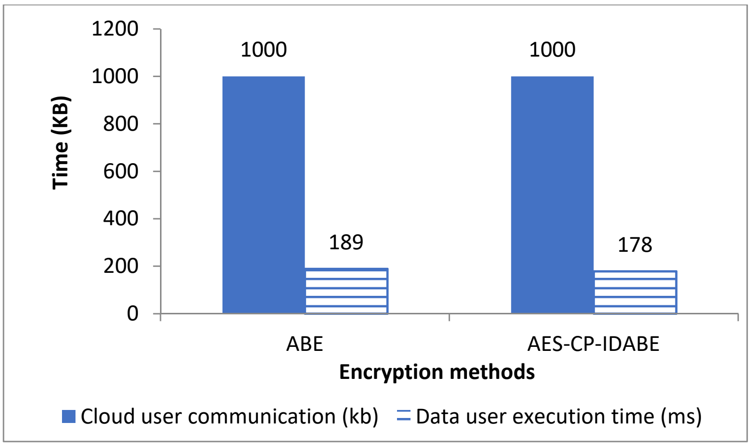


Figure 4. Comparison of the proposed and existing methods regarding user communication and data user execution time.

7.2. Communication of Data Owner

The data owner uploads the data in the cloud system that can be used by many authorized users. The proposed method was evaluated for upload communication with varying numbers of users. After the analysis, it was observed that the proposed data owner communication increases with an increase in the number of users. A typical pattern was observed in both the proposed and existing methods. However, the proposed method showed better performance with a value of 895 KB compared to the existing ABE methods with 990 KB, as shown in Figure 5.

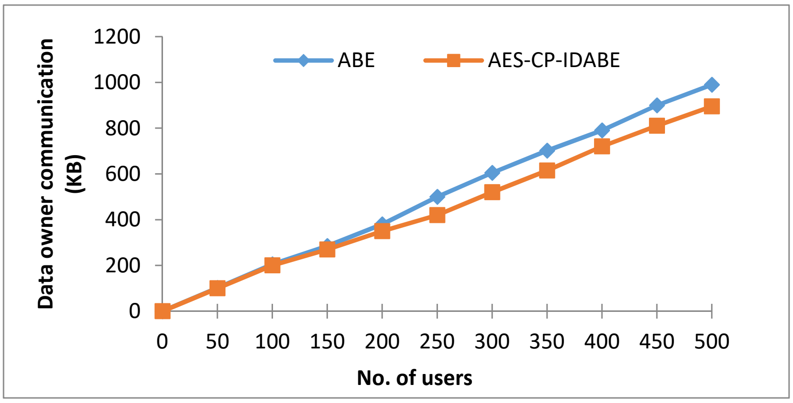


Figure 5. Comparison of the proposed and existing methods regarding the upload communication of the data owner.

7.3. Time Cost for Encryption and Decryption

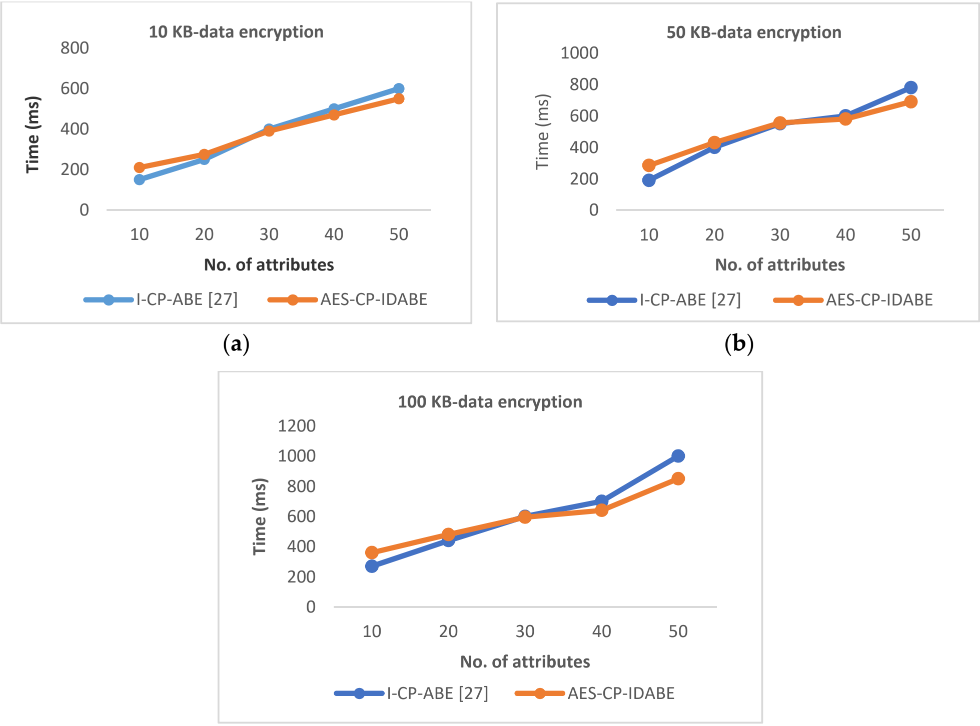
The time and costs involved in encrypting and decrypting different-sized data with an increasing number of cipher-text attributes are given in Tables 2 and 3. It was observed that both the encryption and decryption time of the proposed approach were higher than the Improved-CP-ABE (I-CP-ABE) [27] when the number of attributes was less. However, when there is an increase in the attributes, the difference between the times decreases. It was also observed that the proposed AES–CP–IDABE performs better with attributes of more than 40 KB. The comparison graph is plotted for the different data sizes in Figures 6 and 7.

Table 2. Encryption time of different data sizes.

Data Size	No. of Attributes	10	20	30	40	50
10 KB	I-CP–ABE [27]	150	250	400	500	600
	AES–CP–IDABE	210	275	390	470	550
50 KB	I-CP–ABE [27]	190	400	550	600	780
	AES–CP–IDABE	285	430	555	580	690
100 KB	I-CP–ABE [27]	270	440	600	700	1000
	AES–CP–IDABE	360	480	595	640	850

Table 3. Decryption time of different data size.

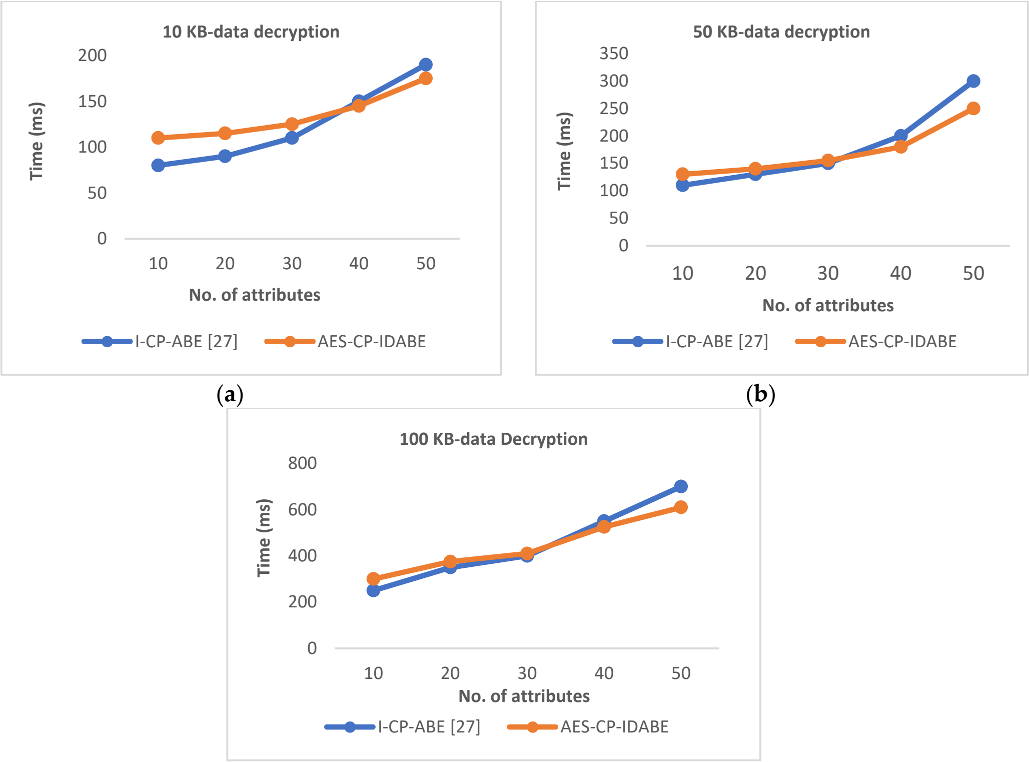
Data Size	No. of Attributes	10	20	30	40	50
10 KB	I-CP–ABE [27]	80	90	110	150	190
	AES–CP–IDABE	110	115	125	145	175
50 KB	I-CP–ABE [27]	110	130	150	200	300
	AES–CP–IDABE	130	140	155	180	250
100 KB	I-CP–ABE [27]	250	350	400	550	700
	AES–CP–IDABE	300	375	410	525	610



(**a**) (**b**)

(**c**)

Figure 6. (**a**) Comparison of the proposed and existing methods regarding the encryption of 10 KB data. (**b**) Comparison of the proposed and existing methods regarding the encryption of 50 KB data. (**c**) Comparison of the proposed and existing methods regarding the encryption of 100 KB data.



(**a**) (**b**)

(**c**)

Figure 7. (**a**) Comparison of the proposed and existing methods regarding the decryption of 10 KB data. (**b**) Comparison of the proposed and existing methods regarding the decryption of 50 KB data. (**c**) Comparison of the proposed and existing methods regarding the decryption of 100 KB data.

7.4. Performance of Different Attacks

The present security framework of AES–CP–IDABE has an attack mitigation system. For analyzing the system, the customized dataset [22] was employed in the security framework. The four frequent attacks are considered for the study, and their prevalence is detected and mitigated effectively. The performance metrics on the various attacks on the proposed security framework are shown in Table 4. The SYN flood was detected with an accuracy of 98.6% along with the precision and F1 measure value (tradeoff value of recall and precision) of 0.995.

Table 4. Performance of AES–CP–IDABE on various DoS attacks.

Attacks	F1 Measure	Precision	Accuracy
SYN flood	0.995	0.995	0.986
UDP flood	1	1	0.981
ICMP flood	0.988	1	0.978
HTTP flood	1	0.985	0.981

Similarly, the UDP flood, ICMP flood, and HTTP flood are detected with an accuracy of 98.1%, 97.8%, and 98.1%, respectively. The precision and F1 measure for the UDP attack is approximately 100%, whereas, for the ICMP attack, it is 98.8% and 100%, respectively. The HTTP flood is detected with a precision of approximately 98.5%, and F1 measures about 100%. The overall performance of the proposed AES–CP–IDABE is compared with the Smart Detection System (SDS) [22] regarding the detection of the DoS attacks. The F1 measure of the proposed framework is about 99.5%, similar to the existing SDS framework. However, the performance regarding precision indicated that the proposed framework is slightly better than the current SDS, with a variation of about 0.3%. Finally, the accuracy of the proposed framework is about 98%, which is better than the existing SDS framework with an accuracy of 96.5% of the customizable data, as shown in Figure 8.

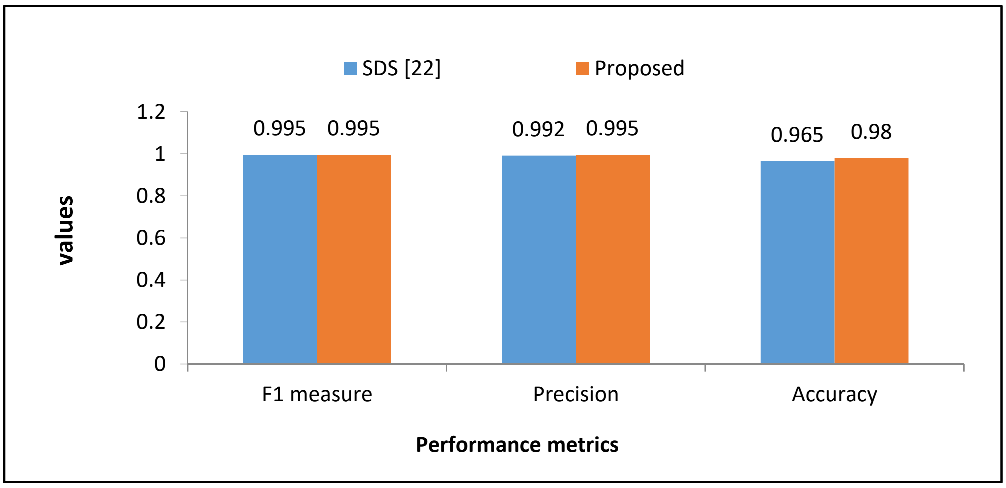


Figure 8. Comparison of the DoS attack detection process for the proposed and existing methods.

8. Conclusions and Future Work

The novel scheme of encryption, AES–CP–IDABE, was proposed to protect the privacy of data on the cloud storage space. The proposed scheme performed double encryption on the data stored in the cloud. The IDABE performed the initial encryption, followed by the secondary encryption through AES. The access control was provided based on the digital signature that was generated using the user ID and key from the cloud server. The authentication was provided for the owner and the user of data in the cloud environment. The attribute set was constructed with five questions that appear randomly as the user tries to access the cloud. Both user and owner evaluated the proposed scheme to find their performance for the communication with the standard ABE concerning the execution time for the user. From the comparison, it was evident that the novel scheme was better than the existing ABE scheme with reduced data owner communication and execution time of the data user. The scheme additionally provides information on the DoS attack through the IP address of the attacker. The performance of attack detection is evaluated and compared on metrics like accuracy, precision, and F1 measures. The comparison showed that the proposed framework has an accuracy of 98% regarding attack detection, which is significantly better than the existing model with enhanced attack mitigation.

Future work may involve establishing a novel scheme for a role-based multi-user cloud environment. The scheme can be enhanced to provide more security and robustness of the cloud environment. In recent times, the number of users in the cloud environment has increased tremendously, and there is a need for multi-owner clouds. Generally, the organizations have a different group of users, and their attributes vary from one to another. Henceforth, the proposed scheme can be improved to handle the multi-owner nature and user groups in the cloud more effectively and efficiently.

Author Contributions: Conceptualization, S.C. (Sonali Chandel); data curation, S.C. (Sumit Chakravarty); formal analysis, S.C. (Sumit Chakravarty); funding acquisition, G.Y.; project administration, G.Y.; software, S.C. (Sumit Chakravarty); supervision, G.Y.; validation, G.Y.; writing—original draft, S.C. (Sonali Chandel); writing—review and editing, S.C. (Sonali Chandel). All authors have read and agreed to the published version of the manuscript.

Funding: This work was supported in part by the National Natural Science Foundation of China under Grant 61972209, Grant 61572263, and in part by the China Postdoctoral Science Foundation under Grant 2019M651919.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Hashem, I.A.; Yaqoob, I.; Anuar, N.B.; Mokhtar, S.; Gani, A.; Khan, S.U. The rise of "big data" on cloud computing: Review and open research issues. *Inf. Syst.* **2015**, *47*, 98–115.
2. Singh, A.; Chatterjee, K. Cloud security issues and challenges: A survey. *J. Netw. Comput. Appl.* **2016**, *79*, 88–115. [CrossRef]
3. Yu, S.; Wang, C.; Ren, K.; Lou, W. Achieving secure, scalable, and fine-grained data access control in cloud computing. In Proceedings of the 2010 IEEE INFOCOM, San Diego, CA, USA, 14–19 March 2010; pp. 1–9.
4. Sun, W.; Yu, S.; Lou, W.; Hou, Y.T.; Li, H. Protecting your right: Verifiable attribute-based keyword search with fine-grained owner-enforced search authorization in the cloud. *IEEE Trans. Parallel Distrib. Syst.* **2014**, *27*, 1187–1198. [CrossRef]
5. Kumar, P.; Alphonse, P.J.A. Attribute based encryption in cloud computing: A survey, gap analysis, and future directions. *J. Netw. Comput. Appl.* **2018**, *108*, 37–52.
6. Grobauer, B.; Walloschek, T.; Stocker, E. Understanding cloud computing vulnerabilities. *IEEE Secur. Priv.* **2010**, *9*, 50–57. [CrossRef]
7. Kozlov, D.; Veijalainen, J.; Ali, Y. Security and privacy threats in IoT architectures. In Proceedings of the BODYNETS, Oslo, Norway, 24–26 September 2012; pp. 256–262.
8. Khan, A.R. Access control in cloud computing environment. *ARPN J. Eng. Appl. Sci.* **2012**, *7*, 613–615.
9. Zhu, W.; Yu, J.; Wang, T.; Zhang, P.; Xie, W. Efficient attribute-based encryption from R-LWE. *Chin. J. Electron.* **2014**, *23*, 778–782.
10. Wan, Z.; Deng, R.H. HASBE: A hierarchical attribute-based solution for flexible and scalable access control in cloud computing. *IEEE Trans. Inf. Forensics Secur.* **2011**, *7*, 743–754. [CrossRef]
11. Li, Y.; Yu, Y.; Yang, B.; Min, G.; Wu, H. Privacy preserving cloud data auditing with efficient key update. *Future Gener. Comput. Syst.* **2018**, *78*, 789–798. [CrossRef]
12. Shen, Z.; Shu, J.; Xue, W. Keyword search with access control over encrypted cloud data. *IEEE Sens. J.* **2016**, *17*, 858–868. [CrossRef]
13. Zhu, Y.; Huang, Z.; Takagi, T. Secure and controllable k-NN query over encrypted cloud data with key confidentiality. *J. Parallel Distrib. Comput.* **2016**, *89*, 1–12. [CrossRef]

14. Cheng, K.; Wang, L.; Shen, Y.; Wang, H.; Wang, Y.; Jiang, X.; Zhong, H. Secure k-nn query on encrypted cloud data with multiple keys. *IEEE Trans. Big Data* **2017**. [CrossRef]
15. Cui, H.; Deng, R.H.; Li, Y.; Wu, G. Attribute-based storage supporting secure deduplication of encrypted data in cloud. *IEEE Trans. Big Data* **2017**, *5*, 330–342. [CrossRef]
16. Liang, X.; Shetty, S.; Tosh, D.; Kamhoua, C.; Kwiat, K.; Njilla, L. Provchain: A blockchain-based data provenance architecture in cloud environment with enhanced privacy and availability. In Proceedings of the 17th IEEE/ACM International Symposium on Cluster, Cloud and Grid Computing (CCGRID), Madrid, Spain, 14–17 May 2017; pp. 468–477.
17. Li, J.; Zhang, Y.; Chen, X.; Xiang, Y. Secure attribute-based data sharing for resource-limited users in cloud computing. *Comput. Secur.* **2018**, *72*, 1–12. [CrossRef]
18. Huang, Q.; Yang, Y.; Shen, M. Secure and efficient data collaboration with hierarchical attribute-based encryption in cloud computing. *Future Gener. Comput. Syst.* **2016**, *72*, 239–249. [CrossRef]
19. Jiang, R.; Wu, X.; Bhargava, B. SDSS-MAC: Secure data sharing scheme in multi-authority cloud storage systems. *Comput. Secur.* **2016**, *62*, 193–212. [CrossRef]
20. Murugesan, V.; Shalinie, M.; Neethimani, N. A brief survey of IP traceback methodologies. *Acta Polytech. Hung.* **2014**, *11*, 197–216.
21. Wang, Y.; Wang, F.; Guo, J. A rapid detection algorithm for malformed H-DoS in the cloud platform. *Int. J. Adv. Comput. Technol.* **2013**, *5*, 474–481.
22. Filho, L.; De, F.S.; Silveira, F.A.F.; Junior, A.D.B.; Vargas-Solar, G.; Silveira, F.L. Smart Detection: An Online Approach for DoS/DDoS Attack Detection Using Machine Learning. *Secur. Commun. Netw.* **2019**. [CrossRef]
23. Rao, K.R.; Ray, I.G.; Asif, W.; Nayak, A.; Rajarajan, M. R-PEKS: RBAC Enabled PEKS for Secure Access of Cloud Data. *IEEE Access* **2019**, *7*, 133274–133289. [CrossRef]
24. Chenthara, S.; Ahmed, K.; Wang, H.; Whittaker, F. Security and privacy-preserving challenges of e-Health solutions in cloud computing. *IEEE Access* **2019**, *7*, 74361–74382. [CrossRef]
25. Tan, S.Y. Correction to Improving Privacy and Security in Decentralizing Multi-Authority Attribute-Based Encryption in Cloud Computing. *IEEE Access* **2019**, *7*, 17045–17049. [CrossRef]
26. Hongbo, L.; Huang, Q.; Ma, S.; Shen, J.; Susilo, W. Authorized equality test on identity-based cipher-texts for secret data sharing via cloud storage. *IEEE Access* **2019**, *7*, 25409–25421.
27. Shumin, X.; Ren, C. Security Protection of System Sharing Data with Improved CP-ABE Encryption Algorithm under Cloud Computing Environment. *Autom. Control. Comput. Sci.* **2019**, *53*, 342–350. [CrossRef]
28. Xiong, J.; Zhang, Y.; Tang, S.; Liu, X.; Yao, Z. Secure Encrypted Data with Authorized Deduplication in Cloud. *IEEE Access* **2019**, *7*, 75090–75104. [CrossRef]