IARJSET ISSN (O) 2393-8021, ISSN (P) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

ISO 3297:2007 Certified ⁜ Impact Factor 7.105 ⁜ Vol. 9, Issue 6, June 2022

DOI: 10.17148/IARJSET.2022.96108

SECURED DATA ACCESS TO DISTRIBUTED STORAGE USING CLOUD

Bhanuprasad C[1], M Usha[2]

[1]Student, Dept. of MCA, Bangalore Institute of Technology, Bengaluru, India

[2]Asst. professor, Dept. of MCA, Bangalore Institute of Technology, Bengaluru, India

Abstract-Secure distributed storage, a new cloud administration, is designed to provide cloud clients flexible information access while preserving the anonymity of re-evaluated information. CP-ABE is one of the most promising strategies for securing the help (Ciphertext-Policy Attribute-Based Encryption). Nevertheless, employing CP-ABE may invariably result in a security breach known as abuse of access accreditation. because the CP-inbuilt ABE has a "go big or go home" decoding option. In this paper, we examine two noteworthy cases of access qualification abuse, one on the side of an authority that is only hazily believed to exist and the other in support of cloud clients. To combat exploitation, we present CryptCloud+, the first networked storage framework based on CP-ABE with white-box discernibility and inspection. We also present the security investigation and employ analysis to demonstrate the effectiveness of our methodology.

Keywords: Ciphertext policy, unauthorised use of access credentials, traceability and revocation, auditing and secure cloud storage

• INTRODUCTION

The ubiquity of distributed computing may accidentally expose flaws in the confidentiality of appropriated data and the security of cloud clients. This is a specific test to make sure that crucial authorised customers may access the data that has been moved to the cloud continuously and from any location. One security approach is to encrypt data before sending it to the cloud. However, manage and exchange information as much as is practical. This is so that a data owner can distribute encrypted data without first having to download encrypted data from the cloud and re-encode it (assume the information proprietor has no nearby duplicates of the information). A fine-grained admission control over scrambled information is beneficial for remote computing. A powerful technique for guaranteeing information confidentiality and offering granular access control is CPABE (Ciphertext-Policy Attribute-Based Encryption). It is possible to first define an access strategy based on the characteristics of the anticipated cloud user (e.g., students, faculty, and visiting researchers of the college). In addition to offering a safe solution to safeguard data saved in the cloud, CP-potent ABE's one-to-many encryption technology also enables fine-grained access control. The possibility of access certification misuse is frequently disregarded by distributed storage architectures based on CP-ABE. A college might, for instance, use a CPABE-based distributed storage framework to reacquire encoded student information to the cloud under specific circumstances that abide by important information sharing and protection laws (such as the government's Health Insurance Portability and Accountability Act of 1992 and the Family Educational Rights and Privacy Act (FERPA)) (HIPAA). After authorization, authorised cloud users are sent access credentials (i.e., unscrambling keys) that are customised to their characteristic sets (e.g., understudy job, employee job, or guest job), enabling them to examine the re-evaluated data. We are all aware that the organisation and its members could suffer a number of drawbacks if any sensitive student data stored in the cloud were to be lost (e.g., suit, loss of upper hand, and criminal accusations). The CP-ABE could help us avoid a security compromise caused by outside attackers. However, when "wrongdoings" involving the redistribution of decoding rights and the covert transit of student data for illicit financial gain are suspected, how can we be certain that an insider of the organisation is accountable? Can you still maintain the compromised access privileges? In addition to the previous inquiries, we also have one that relates to a significant age authority. In the case of a cloud client, the entrance certification (i.e., decoding key) is often issued by a semi-trusted power. Personality traits of the client. How can we be certain that this authority won't be used to shift the established entrance requirements to another party? For instance, a pariah Bob is given access to teacher Alice's important documents by a college security guard (who is not a campus employee). Using a diversity of expertise is one way to respond to the question. In any event, this drives up the cost of letters and mailings to foundations, and the problem of detrimental business intrigue persists. Therefore, we believe that implementing a responsible power plan is the best course of action for resolving the entrance certification escrow issue.

IARJSET ISSN (O) 2393-8021, ISSN (P) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

ISO 3297:2007 Certified ⁜ Impact Factor 7.105 ⁜ Vol. 9, Issue 6, June 2022

DOI: 10.17148/IARJSET.2022.96108

To prevent access credential abuse, we advise using CryptCloud+, a CP-ABE-based cloud storage system with white-box tracability, examination, accountable power, and revocation. This seems to be the first practical approach to granularly controlling access to secure cloud-based data. We explicitly offer a distributed storage solution based on CP-ABE in our article. We offer two responsible power and revocable CP-ABE frameworks (with white box recognizability and assessment), known as ATER-CP-ABE and ATIR-CPABE, respectively, based on this (traditional) structure. We discuss the creation of CryptCloud+, which provides the accompanying benefits, in light of the two frameworks.

1) locating malicious cloud users whereas, Customers who reveal their admission credentials risk being located and identified.

2) Responsive power. A semi-confident person in a position of authority who creates and then grants access certifications to unauthorised users can be located (without the proper authorisation). This makes it possible to attempt other activities (for example criminal examination or common case for harms and break of agreement).

3) Accounting. If a (thought) cloud customer is compelled to divulge their entrance qualifications, that decision will be made by the reviewer.

4) "Almost exactly" 0 capacity is required for the next action. In order to detect malicious cloud users, we use a Paillier-like encryption as an extractable commitment. More practically, we can do without keeping a client profile database. The fifth is to reject dangerous cloud clients. Individual access accreditations may be rejected if they don't "split the difference" entirely in stone. We have two strategies to effectively denounce the "traitor(s)". While the ATER-CP-ABE offers an express renouncement mechanism in which a disavowal list is expressly specified in the calculation Encrypt, the ATIRCP-ABE offers a verifiably renouncement mechanism in which the encryption does not need to realise the denial list but a key update activity is intermittently required. This study builds on our past research, as demonstrated below.

• RELATED WORK

This content that has been posted "in the neighbourhood" does not belong only to the owner of the information since cloud archiving considers new uses for information hoarding. Because of the unique nature of the cloud's administration of ownership and access to information, cloud-based organisations must be responsible for the management of information, programming, physical equipment, and stages. The cloud's approach to data ownership and access necessitates this step, as opposed to traditional computer environments. This type of authority over virtual computers will only provide a limited amount of control. We've seen a number of cloud-based, fine grained admission control systems described in this research as a means of protecting personally identifiable data in cloud computing settings. Accessible encryption enables catchphrases to be used to search for ciphertexts in a secure manner. Customers may analyse the validity of rethought material and minimise capacity overt repetition to a minimum using information evaluation and deduplication. Since that time, a growing number of ABE concepts may be found in works. Some ideas are provided here to improve safety, expressiveness, and effectiveness, but not to address difficulties such as disavowal. Safety, expressiveness, and efficiency are the primary objectives of these devices. Using responsible CP-ABE, as advocated by Li et al., prevents the spread of unauthorised keys among the participating clients. It has been decided that a multi-authority CP-ABE framework should be implemented for the benefit of clients. Capability for white and black box detection are provided 1 Liu and his colleagues' CP-ABE frameworks allow any droning access structure to convey strategy. In spite of the fact that some CP-ABE frameworks make use of white boxes and others do so in black, Ning et al. provide a fascinating assortment of both types of frameworks.

• OUR METHOD

1. To summarise, this is how we find and evaluate cloud clients that may pose a threat to our business, and then decide whether or not to engage alongside. In order to accomplish white-box discernibility and identify malicious cloud clients that are spewing out access credentials, an extraction process similar to Paillier's is used, as detailed above. Taking responsibility away from customers allows us to fulfil their needs for a personalised experience.
2. When we uncover cloud clients who may pose a danger for our organisation, we do an evaluation of their influence on our operations, and then determine whether or not to continue working with them. A similar encryption process to Paillier's may be used as an extractable responsibility to accomplish white-box discernibility and identify malicious cloud clients spewing out access credentials. This is the way to fulfil both of these objectives. This was finished

IARJSET ISSN (O) 2393-8021, ISSN (P) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

ISO 3297:2007 Certified ⁜ Impact Factor 7.105 ⁜ Vol. 9, Issue 6, June 2022

DOI: 10.17148/IARJSET.2022.96108

in the section that came before it. As a result of our ability to relieve our clients of some of the burdens connected with their personality, we are able to satisfy the desire of certain of our customers to instantly give up their identity.

3. As an extra back-up check for the entrance accreditation process, v2 contains a deterministic computation. In order to determine whether or not a credential is valid, this computation is performed during decoding. Keeping track of our qualities is a duty that we are required to do, rather than a choice that we are forced to make. Because of this, the price of expanding the system's capacity may be "decreased." The power supplier and the client being compared must agree on an admittance certification before it is feasible to create responsible energy. This means that the authority has no ability to exercise “complete control” over the accreditations that are awarded. Depending on the client's credentials and personality, the authority may be able to give them with a UAC that fulfils their requirements. It's unclear how much power the client has, whilst the authority has no idea. The accreditation uac will almost certainly be altered if an authority (reallocates) a position with the client (with access qualification uac) without the customer's consent. Accreditations will offer a cryptographic proof of the destructive capability. An auditor may use this method to determine whether or not a client is to blame for a certification problem. We You don't need to know about the implicit renunciation list in order to use Encrypt. Each non-repudiated user gets a unique update key after the rest of the parameters remain unaltered. The expert mystery key is shared with the mystery key and the update key for access control and revocation, respectively, using a (random secret) first degree polynomial (f(w) = w+) and f(t). It is possible to limit and remove access using f(1) and f (t). Malicious actors in the real world cannot understand newly generated ciphertext because they lack the necessary update keys. A combination of repudiation and discernibility is required to meet this attribute's criteria. A client's name will be deleted from the denial list if the recognition system concludes that they are malevolent (such as credential leakers).

• THE DESIGN GOAL AND THE FRAMEWORK MODEL

Our CP-ABE-based distributed storage framework along with the following essential components:

Dos first need to obfuscate and then transport encoded data onto the public cloud in accordance with appropriate access controls (PC).

Customer requests for information are handled by the personal computer, which then saves the newly-coded data (DUs) To see the new data, DUs must have been given access (for example, by downloading and decoding it).

A semi-trusted authority (AT) is granted access accreditations by decentralised units (DU) for the system parameters (unscrambling keys). The auditor (AU) is in responsibility of returning follow-up tasks and DUs, as well as overseeing the review and denial processes. A broad spectrum of stakeholders look to the auditor for guidance and assurance (AU). While adhering to established norms, the computer may also take in additional information about the text that has been rethought (jumbled) (for example accurately executing undertakings allotted by DOs). To some extent, the general public does not trust AT because of its ability to (rearrange) access certificates for unauthorised users and set framework limits (to be shared with AU). The same rules apply to an AU as an AT when it comes to total trust. On DOs, encrypting data keeps it safe from unauthorised access. Authorized DUs may intentionally leak their access credentials by selling them to a third party. To speed up the process of finding a framework double-crosser.

It is important to provide the following security assurances:

1) Security guarantees must ensure that scrambled data may be accessed with a wide range of permissions while still maintaining the data's secrecy.

2) Revocability calculations should be as inexpensive as feasible, and the calculations themselves should be equitable. It is also important that the computation be fair.

3) To be effective, the audit, follow-up, and disavowing processes must all be done effectively.

Preliminaries

• CONTEXT

Assuming that s is randomly selected from S, we define [l] = 1, 2 [l] as l N and [0, l] = [l]0 for s R S.

Definition 1 :

This is a collection of various things. Each one in turn, in a monotonous collection. An entrance structure (also referred to as a single access structure) on S consists of 2S of non-void property configurations. If B A and B C, C A are identical, then the phrase "if B,C A" is valid. However, this is very rare. As long as it's a component of another set, a set is OK.

IARJSET ISSN (O) 2393-8021, ISSN (P) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

ISO 3297:2007 Certified ⁜ Impact Factor 7.105 ⁜ Vol. 9, Issue 6, June 2022

DOI: 10.17148/IARJSET.2022.96108

Definition 2: This page uses the words "prime" and "universe" interchangeably. high-security exchange of personal information Based on the very same number of pieces and segments as M, Q has a networking that generates offers based on M. This network connects every component of the S entry system. If both of the following requirements are satisfied, Zp will accept S authentication: (3) an input element An on S for each distinctive structure across Zp in a single section of the intriguing s Zp In contrast to Zp, Row I of M will be the result of a function that receives a characteristic from S and returns the row I of M. This topic is far from over. A segment vector v = s Zp's common key is found in analysis. r2.rn0 Despite Zp's random picks, each one has the same secret key.

Initially, the private share's vector was agreed upon as Mv Zl1 p. For the sake of this example, we'll refer to the attribute (Mvj) as "home" (j). The composite request's bilinear groupings will be submitted to us soon. It is expected that the bilinear representations of the source security boundary will be produced by the G gathering generator. A cyclic collection of the request N = p1 p2 p3 is G's result (p1, G, GT, and e). GG GT is a map with the properties of (1) bi-linearity : u, v G, and (2) nondegeneracy: g G, in order to have a request N. There is a greater variety of options to pick from.
Complicacy assumes two things: (Subgroup Decision Problem with 3 Primes)

Assumption 1:
Define the distribution shown below given a group generator G: R = (G,g,X3), T1 R = Gp1p2, T2 R = Gp1, and G = (N = p1p2p3,G,GT,e). The following are some advantages of demonstrating this
presumption:

If Adv1G,A() = |Pr, then A(D,T1) and Pr[A(D,T2) = 1] are both 1. Assuming Adv1G. A() is the capacity of any PPT technique, we may prove that G meets the requirement. Using a G-based group generator, identify the mode of transportation in issue. "D" = (G,g); "X1X2 and Y3R Gp3); "T" = (G,g); "T2" and "R" P

Following are some of the benefits that come from disputing this assumption:
For the condition to be met, Adv2G,A() has to equal Pr, A(D,T1) must equal 1, and Pr[A(D,T2) must equal 1]. This assumption can be met if Adv2G,A() has no impact on G's capacity. Suspicions A audience sourcer's accompanying technique should be described in detail. This is how the letter G appears on a keyboard: (N = p1p2p3,G,GT,e), G = (R G,,s, R ZN,g, R Gp1,X2,Y2,Z2), R Gp2,X3, and R Gp3; R Gp2,X3 (G,GT,e). Building this for An has a variety of benefits, including the following: Pr[A(D,T1)=1] The Adv3G,A() stored procedure formula is A(D,T2) = 0. The hypothesis that G is a constant if Adv3G,A() is an inconsequential ability of any PPT algorithm A is compatible. It's feasible that a hypothesis may be true. the hypotheses [7, 13] of l-SDH "The G Strong Diffie-Hellman (l) issue," according to this definition, is " Using G as a group generator, create a bilinear array of primal requests (p). Sources of information (g and GX) produce a (l + 1)-tuple for the Zp G combination (c,g1/(C+x) Zp G. In the equation for l-SDHinGifPr, l-probability SDHinGifPr's is larger than the random collection of x and A's consumption of arbitrary pieces in Zp. Since there's no time-based strategy to solving the l-SDH issue in G., the (l,t,)-SDH assumption is legitimate. That's only the beginning.

1. Knowledge of a Log in Secrecy

It is based on nothing. Proving the discontinuous log of a collection component T using the zero information validation of material (ZK-POK) feature of discrete log convention (DLC) is possible. ZK-POK is the name given to this functionality. Conventions like these provide a number of advantages, including the following: A secure protocol can't be established without proof that a test system can construct a verifier's view without access to the observer's knowledge (for instance, showing that an information extractor Ext can connect with the prover to separate the observer via rewinding procedure).

2. Binary Tree Terminologies

The zero-information confirmation of information in the discreet log convention may be used by a prover to demonstrate a verifier that it possesses the discrete log t of a certain collection component T. (ZK-POK). The following features would be present in such a gathering: S may create an observer's viewpoint on a protocol verifier, for example, when information attributes and zero-information are both confirmed (for example demonstrating that an information extractor can connect with the prover to separate the observer by means of rewinding procedure).

IARJSET ISSN (O) 2393-8021, ISSN (P) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

ISO 3297:2007 Certified ⁜ Impact Factor 7.105 ⁜ Vol. 9, Issue 6, June 2022

DOI: 10.17148/IARJSET.2022.96108

- **THE ATER-CP-ABE MODEL**

Definition 1

In the system known as ATER-CPABE (Fully accountable Authority and Openly Revocable CPABE with White-Box Track and trace and Auditing), spiteful clients are explicitly rejected, maliciously misbehaving authority is held responsible, and the poisoned client is traced via an unscrambling key. Setup, encryption, and decryption calculations in the conference form [35] were examined, and a repudiation rundown was developed in order to effectively finish the process of enunciating risky customers.

The following calculations are included in our ATER-CP-ABE figure, which we will now display:

• the installation's pp and msk files When an algorithm is given a device known and a trait universal representation U, it returns the public boundary pp as well as the expert secret key msk. Additionally, a list of null values is used to begin the implementation of RL.

• Skid,S Authentication and client-side standardisation are both served by KeyGen(pp,msk,id). There may be some overlap between AT and U and the client's pp and a set of personality qualities. As far as we know, no one has identified S. msk's contribution to AT. If AT and U want to spill the beans, they may simply flip a coin. The mysterious key slide isn't provided to U until the conclusion of the meeting.

"ct:Oninput pp," "plain-text message," and "entry structure" are all examples of these terms. A repudiate list, also known as an over the galaxy of attributes, is used to create ciphertext (ct).

The m or m may be unlocked. Given an input, an unknown key, and an encrypted message, it determines whether or not the sk's S characteristic set fits the encrypted message and id/RL entry structure before providing the plaintext m. It's an excellent idea no matter what the circumstances are.

It is recommended to utilise KeySanityCheck (pp,sk) Secretkeysk does a keysanity check and returns 1 or 0 depending on whether it is successful. Anything that happens will inevitably lead to a negative result. When deciphering the jumbled text, an algorithm must receive the secret key in a form that it can understand. Take a second look to be sure you're on the right track.

discover or keep track of (pp,msk,sk) Sk frames in the setting of the PP, MSK, and the Mystery Key SK are determined. Decides to choose whether or not follow the sk. at this point A result of 1 from the KeySanityCheck(sk, pp) function indicates that the security key sk is in good health. You can tell the difference between your own traits and your profession. Later, the SK is captivated by its character and adds it to their Renunciation List of Absolution (RL). At the absolute least, it shows that the sk protocol is not rigorously observed.

Re-examine and re-examine (pp,skid,sk id) This convention was devised by U and AU to determine whether a client is to fault. To find out whether the customer is being honest or if they are to fault, this question is posed.

Definition 2

Security

If the three criteria listed below are satisfied, the ATER-CP-ABE plot is secure.

1) Crypt text meaning must be lost in response to specific plaintext assaults, as defined by the CP-ABE standard. Common public Key Verified Encryption (CP-ABE) is an abbreviation for CP-ABE (IND-CPA).

2) A character id cannot be generated from decoding the key, thus neither Trace nor Audit can determine the appropriate customer's role in the incident. The location is unable to do so since it uses sk as an input in both calculations.

3) Clients never reveal the decoder key, which is required for the auditing technique to determine whether or not a user is speaking the truth. The ATER-CPABE IND-CPA game and this exam have many similarities, but they also have substantial differences. Variations in each of the key issues' aggressive and explicit personas are the most relevant ones. In the Challenge stage, A makes a list of renunciations public. The game operates as follows.

• Once Setup is complete, the challenger will transmit the public limits pp toA. (,U).

• As a first step, the challenger is asked a series of adaptive questions about the secret keys associated with the configurations of various characteristics. After executing KeyGen(pp,msk,idi,Si), the opponent sends skidi,Si to A. (idi,Si).

IARJSET ISSN (O) 2393-8021, ISSN (P) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

ISO 3297:2007 Certified ⁜ Impact Factor 7.105 ⁜ Vol. 9, Issue 6, June 2022

DOI: 10.17148/IARJSET.2022.96108

• Both the RL and A disavowal lists and entry structures carry the same amount of data as the messages they accompany (m0,m1). But none of the quality sets (idi, Si) in issue can meet A's specifications. iQ1. The Encrypt(pp,m,A,RL) method is used to produce random test results by tossing a coin. The ct command will be sent to ToA.
Whether or whether they've offered a distinctive key to the sets of quality that satisfy A is up to each challenger to respond. I The answer to [Q1+1, Q] In this case, we have no information. To assist A, the challenger dials KeyGen (ppmsk) and then dispatches Skidi and Si (idi,Si).
• Hypothesis: Provides a 0 0 1,1 value for An's win in this game is specified as Adv = |Pr[0 =]1/2|.

Definition 3
PPT Because the ATER-CP-ABE guarantees the IND-CPA in the game outlined above, player A has a little advantage. The Dishonest Authority's game. Here, a corrupt authority will attempt to produce an unencrypted key that will lead them to a customer. The winner of a fight between a challenger and an attacker is referred to as "it."
• A's initial actions are to set boundaries and hand the competitor over to A (who is portraying a hostile authority figure) (id,S). The challenger uses the backup check as a fallback if the primary check fails on pp (id,S).
• To generate a decoding key bundle based on the customer's ID and S, An and the challenge both must address the KeyGen conference. Client data is used in this method.
• When both Trace (pp) and Debug (pp) are set to true, an id for the deciphering key is returned. It is possible for An to acquire an advantage over the other players by using Adv = |Pr[A succeeds]|. In this situation, it is possible to keep record of all of the coins, including challengers, audits, trace, and A. an extra meaning, which is a major benefit. The ATER-CP-ABE is acceptable to utilise if every PPTA has a little benefit in the game outlined above.

• THE ATIR-CP-ABE MODEL

Definition 1
ABE concepts have been in literature for some time, but they've become increasingly common in recent years. Several ways have been offered to increase security, expressiveness, and efficiency, but not to tackle concerns like disavowal. To prevent the distribution of non-authorized keys among participants, Li et al. advocate the usage of CP-ABE. According to new study, the use of CP-ABE structures with multiple authors has been advocated. being able to distinguish between white and black boxes 1 The CP-ABE frameworks were established by Liu et al. in order to communicate strategy. A new CP-ABE framework might be discovered in Ning and colleagues' research using both white-box and black-box approaches.
A plaintext message (m), an input data structure (pp), and an output data structure (A,x) are all part of a secure communication mechanism (x). One of the features of the cipher-text, ct, is that it includes the current feature x.

Definition 2

On the ATER network, the security requirements for CP-ABE and CP-ABE are the same. Our definition of security games includes the IND-CPA and IND-CPA. Do an investigation to see if there are any dishonesty amongst the three parties engaged in the transaction Although security rounds are employed in ATIR-CP ABEs to check for dishonest users and users, unlike in ATER-CP, the Adversary does not provide a list of disavowals during Challenge phase.

• CONCLUSION AND FUTURE WORK

Because of CP-ABE-based cloud storage systems' leaking of user credentials, CryptCloud+ was designed. CryptCloud+, a dependable, trustworthy, and revocable CryptCloud system, incorporates transparency and auditing. A white box transparency, responsible authorities, auditing, and effective revoke only this cloud storage option provides are available. CryptCloud+ makes it easier to identify and ban unauthorised cloud users (leaking credentials). As a result, our approach is effective regardless of who has access to a user accounts in question. Unlike white-box traceability, black-box traceability may be required by CryptCloud. One of our next projects will focus on black box audit and tracing. CryptCloud+ and AU always operate as expected when using each other. There is, however, the chance that this is not the case. It's probable that AU's faith in others has been eroded by this. In order to find a solution, it's important to consider all possible angles. There are several similarities between threshold systems. As a consequence, deployment and communication expenses will rise. The opposite is true: Increasing output may create issues in the long term. We want to decentralise trust amongst autonomous units in the future to maintain the same degree of security and effectiveness (AUs).

DOI: 10.17148/IARJSET.2022.96108

The same security level will be in place throughout the transaction. In white-boxed applications, encryption techniques such as Paillier's are utilised to ensure traceability. White-box traceability may take use of any and all commitments that can be extracted from a corporation. In order to improve traceability, it is feasible to loosen the standards for commitments that may be extracted. Through the deployment of CryptCloud+, white-box monitoring of malicious cloud users has never been easier. This capability is critical to white-box cloud user tracking.

• REFERENCES

[1] Mazhar Ali, Revathi Dhamotharan, Eraj Khan, Samee U. Khan, Athanasios V. Vasilakos, Keqin Li, and Albert Y. Zomaya. Sedasc: Secure data sharing in clouds. IEEE Systems Journal, 11(2):395–404, 2017.
[2] MazharAli,SameeU.Khan,andAthanasiosV.Vasilakos. Security in cloud computing: Opportunities and challenges. Inf. Sci., 305:357–383, 2015.
[3] Michael Armbrust, Armando Fox, Rean Griffith, Anthony D Joseph, Randy Katz, Andy Konwinski, Gunho Lee, David Patterson, Ariel Rabkin, Ion Stoica, et al. A view of cloud computing. Communications of the ACM, 53(4):50–58, 2010.
[4] Nuttapong Attrapadung and Hideki Imai. Attribute-based encryption supporting direct/indirect revocation modes. In Cryptography and Coding, pages 278–300. Springer, 2009.
[5] Amos Beimel. Secure schemes for secret sharing and key distribution. PhD thesis, PhD thesis, Israel Institute of Technology, Technion, Haifa, Israel, 1996.
[6] Mihir Bellare and Oded Goldreich. On defining proofs of knowledge. In Advances in Cryptology-CRYPTO'92, pages 390–420. Springer, 1993.
[7] Dan Boneh and Xavier Boyen. Short signatures without random oracles. In EUROCRYPT - 2004, pages 56–73, 2004.
[8] Hongming Cai, Boyi Xu, Lihong Jiang, and Athanasios V. Vasilakos. Iot-based big data storage systems in cloud computing: Perspectives and challenges. IEEE Internet of Things Journal, 4(1):75–87, 2017.

