International Journal of Scientific Research in Computer Science, Engineering and Information Technology
© 2018 IJSRCSEIT | Volume 3 | Issue 3 | ISSN : 2456-3307

Large Data Access with Efficient Attributes Access Policy in Cloud Computing

Raja Ashok Kumar, M. Suresh Babu
Department of CSE, Assistant Professor, AITS, RAJAMPET, Andhra Pradesh, India

ABSTRACT

How to management the access of the massive quantity of massive knowledge becomes a awfully difficult issue, particularly once huge knowledge are keep within the cloud. Cipher text-Policy Attribute primarily based coding (CP-ABE) may be a promising coding technique permits end-users to inscribe their knowledge below the access policies outlined over some attributes of knowledge customers and solely allows data customers whose attributes satisfy the access policies to rewrite the info[1]. In CP-ABE, the access policy is connected to the cipher text in plaintext type, which can additionally leak some personal info regarding end-users. Existing strategies solely partly hide the attribute values within the access policies, whereas the attribute names are still unprotected. During this paper, we have a tendency to propose Associate in Nursing economical and fine-grained huge knowledge access management theme with privacy-preserving policy[3]. In cloud computing environment, there are many users of cloud. They stores there data and accessing of large data stored on cloud. But this users face some of major issue causing loss of data in cloud and facing a problem in authority and privacy of users. Cipher text-Policy Attribute based Encryption (CP-ABE) is a promising encryption technique that enables end-users to encrypt their data under the access policies defined over some attributes of file and upload encrypted file with encrypted attribute with, key provided by attribute authority. Cloud consumers want to download any file so it only allow data consumers whose attributes satisfy the access policies to decrypt the data. In CP-ABE, the access policy is attached to the cipher text in plaintext form, which may also leak some private information about end-users. Existing methods only partially hide the attribute values in the access policies, while the attribute names are still unprotected, these issues are modify in this scheme to provide more security. In this scheme attribute authority assign public key to user while uploading files on cloud and also files secret key and private key to data consumer are used while uploading and downloading respectively.

Keywords: Big Data, Access Control ,CP-ABE , Privacy-preserving Policy, Encrypted Index

I. INTRODUCTION

In the era of massive information, an enormous quantity of information is generated quickly from numerous sources (e.g. good phones, sensors, machines, social networks etc.). Towards these massive information, standard pc systems don't seem to be competent to store and method these information[1]. Owing to the versatile and elastic computing resources, cloud computing could be a natural suitable storing and process massive information. With cloud computing, end-users store their information into the cloud, and consider the cloud server to share their information to alternative users (data consumers). So as to solely share end-user's information to licensed users, it's necessary to style access management mechanisms in step with the necessities of end-users. Once outsourcing information into the cloud[2], end-users lose the

physical management of their information. Moreover, cloud service suppliers don't seem to be fully-trusted by end-users that build the access management tougher [3]. For instance, if the standard access management mechanisms square measure applied, the cloud server becomes decide to gauge the access policy and build access call. Thus, end-users might worry that the cloud server might build wrong access call on purpose or accidentally, and disclose their information to some unauthorized users. So as to change end-users to manage the access of their own information, some attribute-based access management schemes square measure projected by investment attribute-based encoding. In attribute-based access management, end-users first outline access policies for his or her information and code the information underneath these access policies. Solely the users whose attributes will satisfy the access policy square measure eligible to decode the information[4]. In an efficient and fine-grained massive information access management scheme with privacy-preserving policy. Specifically, we tend to hide the total attribute (rather than solely its values) within the access policies. However, once the attributes square measure hidden, not solely the unauthorized users however additionally the licensed users cannot grasp that attributes square measure concerned within the access policy, that makes the secret writing a difficult downside. To help information secret writing, we tend to additionally style a completely unique Attribute Bloom Filter. to gauge whether or not AND attribute is within the access policy and find the precise position within the access policy if it's within the access policy[5]. Security analysis and performance analysis show that scheme will preserve the privacy from any LSSS access policy while not using abundant overhead. Big data is a term that refers to data sets or combinations of data sets whose size (volume), complexity (variability), and rate of growth (velocity) make them difficult to be captured, managed, processed or analyzed by conventional technologies and tools, such as relational databases and desktop statistics or visualization packages, within the time necessary to make them useful. While the size used to determine whether a particular data set is considered big data is not firmly defined and continues to change over time, most analysts and practitioners currently refer to data sets from 30- 50 terabytes(10 12 or 1000 gigabytes per terabyte) to multiple petabytes (1015 or 1000 terabytes per petabyte) as big data.[4] The analysis of Big Data involves multiple distinct phases as shown in the figure below, each of which introduces challenges. Many people unfortunately focus just on the analysis/modeling phase: while that phase is crucial, it is of little use without the other phases of the data analysis pipeline. Even in the analysis phase, which has received much attention, there are poorly understood complexities in the context of multi-tenanted clusters where several users' programs run concurrently. Many significant challenges extend beyond the analysis phase. For example, Big Data has to be managed in context, which may be noisy, heterogeneous and not include an upfront model. Doing so raises the need to track provenance and to handle uncertainty and error: topics that are crucial to success, and yet rarely mentioned in the same breath as Big Data. Similarly, the questions to the data analysis pipeline will typically not all be laid out in advance. It may need to figure out good questions based on the data. Doing this will require smarter systems and also better support for user interaction with the analysis pipeline. In fact, there is a major bottleneck in the number of people empowered to ask questions of the data and analyze it. It can drastically increase this number Big knowledge may be a term that refers to knowledge sets or mixtures of knowledge sets whose size (volume), quality (variability), and rate of growth (velocity) build them troublesome to be captured, managed, processed or analyzed by standard technologies and tools, like relative databases and desktop statistics or image packages, among the time necessary to form them helpful. whereas the dimensions accustomed verify whether or not a selected knowledge set is taken into account huge knowledge isn't firmly outlined and continues to vary over time, most analysts and practitioners presently talk to knowledge sets from 30-50 terabytes(10 twelve or a

thousand gigabytes per terabyte) to multiple petabytes (1015 or a thousand terabytes per petabyte) as huge knowledge. The analysis of massive knowledge involves multiple distinct phases as shown within the figure below, every of that introduces challenges. many folks sadly focus simply on the analysis/modeling part: whereas that phase is crucial, it's of very little use while not the opposite phases of the info analysis pipeline. Even within the analysis part, that has received a lot of attention, there square measure poorly understood complexities within the context of multi-tenanted clusters wherever many users' programs run at the same time. several important challenges extend on the far side the analysis part. for instance, huge knowledge should be managed in context, which can be reedy, heterogeneous Associate in Nursingd not embody an direct model. Doing therefore raises the requirement to trace place of origin and to handle uncertainty and error: topics that square measure crucial to success, and nevertheless seldom mentioned within the same breath as huge knowledge. Similarly, the inquiries to the info analysis pipeline can generally not all be arranged move into advance. it should have to be compelled to understand smart queries supported the info. Doing this may need smarter systems and additionally higher support for user interaction with the analysis pipeline. In fact, there's a significant bottleneck within the range of individuals authorised to raise queries of the info and analyze it. It will drastically increase this range by supporting several levels of engagement with the info, not all requiring deep information experience. Solutions to issues like this may not come back from progressive enhancements to business as was common like trade may build on its own. fortuitously, existing process techniques may be applied, either as is or with some extensions, to a minimum of some aspects of the massive knowledge drawback. for instance, relative knowledge bases have faith in the notion of logical data independence: users will trust what they require to work out, whereas the system (with adept engineers coming up with those systems) determines the way to work out it with efficiency. Similarly, the SQL normal and also the relative knowledge model offer a consistent, powerful language to specific several question desires and, in essence, permits customers to decide on between vendors, increasing competition. The challenge previous Maine is to mix these healthy options of previous systems. Map scale back has emerged as a preferred thanks to harness the ability of huge clusters of computers. Map scale back permits programmers to assume in a very data-centric fashion: they concentrate on applying transformations to sets of knowledge records, and permit the main points of distributed execution, network communication and fault tolerance to be handled by the Map scale back framework. Map scale back is often applied to massive batch-oriented computations that square measure involved primarily with time to job completion. The Google Map scale back framework and ASCII text file Hadoop system reinforce this usage model through a batch-processing implementation strategy: the whole output of every map and scale back task is materialized to a neighborhood file before it may be consumed by subsequent stage. Materialization permits for an easy and chic checkpoint/restart fault tolerance mechanism that's vital in massive deployments, that have a high likelihood of slowdowns or failures at employee nodes .

II. RELATED WORK

1) Title: Privacy-Preserving Data Publishing: A Survey of Recent Developments Written By: BENJAMIN C. M. FUNG, KE WANG, RUI CHEN, PHILIP S. YU.

The collection of digital info by governments, companies, and people has created tremendous opportunities for knowledge- and information-based higher cognitive process. Driven by mutual advantages, or by laws that need sure knowledge to be printed, there's a requirement for the exchange and publication of knowledge among varied parties. knowledge in its original type, however, usually contains sensitive info regarding people, and commercial enterprise such knowledge can violate individual privacy. this apply in knowledge commercial enterprise depends principally on policies and tips on what sorts of knowledge will be

printed and on agreements on the utilization of printed knowledge. This approach alone might cause excessive knowledge distortion or short protection. Privacy-preserving knowledge commercial enterprise (PPDP) provides ways and tools for commercial enterprise helpful info whereas protective knowledge privacy. Recently, PPDP has received respectable attention in analysis communities, and plenty of approaches are projected for various knowledge commercial enterprise situations. during this survey, we'll consistently summarize and value totally different approaches to PPDP, study the challenges in sensible knowledge commercial enterprise, clarify the variations and needs that distinguish PPDP from different connected issues, and propose future analysis directions.

2) Title: APPLET: a privacy-preserving framework for location-aware recommender system Written By: Xindi Ma,HuiLI, Jianfeng MA, Qi JIANG, Sheng GAO, Ning XI &DiLU

Location-aware recommender systems that use location-based ratings to provide recommendations have recently intimate a speedy development and draw vital attention from the analysis community. However, current work principally centered on high-quality recommendations whereas underestimating privacy problems, which may cause issues of privacy. Such n issues are a lot of distinguished once service suppliers, WHO have restricted machine and storage resources, leverage on cloud platforms to suit in with the tremendous number of service necessities and users. During this paper, we have a tendency to propose a unique framework, specifically applications programmer, for shielding user privacy info, together with locations and recommendation results, inside a cloud surroundings. Through this framework, all historical ratings are hold on and calculated in cipher text, permitting US to firmly cipher the similarities of venues through Paillier secret writing, and predict the advice results supported Paillier, independent, and comparable secret writing. we have a tendency to conjointly on paper prove that user info is non-public and can not be leaked throughout a recommendation. Finally, empirical results over a real-world dataset demonstrate that our framework will with efficiency suggest POIs with a high degree of accuracy in a very privacy-preserving manner.

3) Title:Efficient Discovery of De-identification Policies Through a Risk-Utility Frontier Written By: Weiyi Xia, Raymond Heatherly, Xiaofeng Ding Modern data technologies modify organizations to capture giant quantities of person-specific knowledge whereas providing routine services. several organizations hope, or area unit de jure needed, to share such knowledge for secondary functions (e.g.validation of analysis findings) during a de-identified manner. In previous work, it had been shown de-identification policy alternatives might be sculpturesque on a lattice, that might be looked for policies that met a prespecified risk threshold (e.g., chance of re-identification). However, the search was restricted in many ways that. First, its definition of utility was syntactical supported the extent of the lattice - and not linguistics - based mostly on the particular changes evoked within the ensuing knowledge. Second, the edge might not be famous beforehand. The goal of this work is to create the optimum set of policies that trade-off between privacy risk (R) and utility (U), that we have a tendency to ask as a R-U frontier. To model this drawback, we have a tendency to in-troduce a linguistics definition of utility, supported scientific theory, that's compatible with the lattice illustration of policies. To unravel the matter, we have a tendency to at first build a group of policies that outline a frontier. We have a tendency to then use a probability-guided heuristic to go looking the lattice for policies possible to update the frontier. To demonstrate the effectiveness of our approach, we have a tendency to perform associate degree empirical analysis with the Adult dataset of the UCI Machine Learning Repository. We show that our approach will construct a frontier nearer t o optimum than competitive approaches by looking a smaller range of policies. additionally, we have a tendency to show that a often followed de-identification policy (i.e., the porcupine provision customary of the HIPAA Privacy Rule) is suboptimal as

compared to the frontier discovered by our approach. In Cipher text policy attribute base encryption scheme provides an efficient scheme for encrypting files and assign attribute access policy to file while uploading file on cloud but this cause problem while uploading files with attribute access policy. Its attributes are not fully encrypted, while uploading only its name is encrypted but value of attributes remain unencrypted. [1] If unauthorized user gets this value then he may get file and access that file so security concern arises. Also data owner having more direct control on access policy and it is difficult to directly apply existing CP-ABE schemes to data access control for cloud storage systems because of the attribute revocation problem. [2]

In this scheme file is upload on cloud without entering any keywords of file. File upload on cloud only with attribute access policy for access of file. While cloud consumer want to download file from cloud then consumer enter only attributes and user get resulted file. This resulted file contains many files matching attributes but this is not exact matching result.[5] Also this file are once upload, remain for long time on cloud, this cause wastage of space on cloud and cloud consumers get this file as a result each and every time and this file is of no use after long time. File uploading on cloud are in encrypted format so many difficulty occur searching over an encrypted data.[4] The cloud server is not fully trusted authority, if users sensitive data or files remain for long time on cloud then file are not secure.[3]

III. PROPOSED ARCHITECTURE

1) We propose an efficient and fine-gained big data access control scheme with privacy-preserving policy, where the whole attributes are hidden in the access policy rather than only the values of the attributes.

2) We also design a novel Attribute Bloom Filter to evaluate whether an attribute is in the access policy and locate the exact position in the access policy if it is in the access policy.

3) We further give the security proof and performance evaluation of our proposed scheme, which demonstrate that our scheme can preserve the privacy from any LSSS access policy without employing much overhead.

The main goal of the project is to study, design and

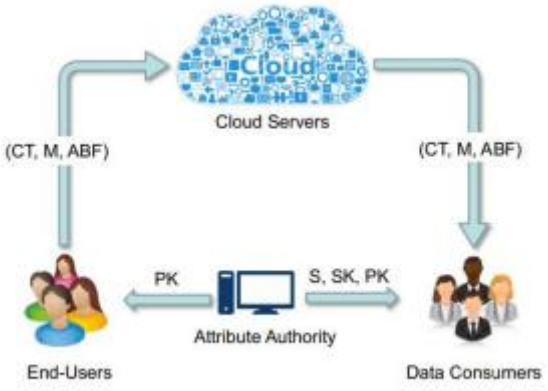

Fig.1: System Architecture

implement performance optimizations for big data frameworks. This work contributes methods and techniques to build tools for easy and efficient processing of very large data sets. It describes ways to make systems faster, by inventing ways to shorten job completion times.

- ✓ Another major goal is to facilitate the application development in distributed data-intensive computation
- ✓ platforms and make big-data analytics accessible to non-experts, so that users with limited programming
- ✓ experience can benefit from analyzing enormous datasets.
- ✓ To generate faster results.
- ✓ It reduces the complexity of data access and retrieval. When we have to dealing with big data.
- ✓ The alternative to this is apache Hadoop, which deals with big data with efficiency.
- ✓ Hadoop itself consists of Map Reduce and HDFS.
- ✓ It runs on Hadoop cluster

IV. TECHNIQUE PRELIMINARIES

In many distributed systems a user ought to solely be able to access knowledge if a user posses a definite set of credentials or attributes. Currently, the sole technique for imposing such policies is to use a trustworthy server

to store the info and mediate access management. However, if any server storing the info is compromised, then the confidentiality of the info are compromised. In CPABE we tend to gift a system for realizing complicated access management on encrypted knowledge that we tend to decision Ciphertext-Policy Attribute-Based coding. By victimization our techniques encrypted knowledge are often unbroken confidential although the storage server is untrusted ; what is more, our ways square measure secure against collusion attacks. Previous Attribute-Based coding systems used attributes to explain the encrypted knowledge and designed policies into user's keys; whereas in our system attributes square measure wont to describe a user's credentials, and a celebration encrypting knowledge determines a policy for United Nations agency will decode. Attribute-based encryption (ABE) is a new approach that include public-key cryptography concept . In public-key cryptography ,by using receiver's public -key, message is encrypted for particular receiver. Attribute based encryption can define set of attribute and by using subset of attributes(Key-policy attribute based encryption -KP-ABE) or policies defined over set of attribute(Ciphertext-policy attribute based encryption-CP-ABE), message can be encrypted.The main issue is, only authorized user can decrypt a ciphertext those who have key for "matching attributes"and that key is received by trusted party only[1]. A user's private key is associated with a set of attributes in ciphertext-Policy attribute-based encryption(CP-ABE) and an access policy is specifies by a ciphertext over a defined universe of attributes within the system. If user's attributes satisfy the policy of the respective ciphertext then user will be able to decrypt ciphertext. Using conjunctions, disjunctions and(k,n)(k, n)-threshold gates policies may be defined over attributes i.e., kk out of nn attributes have to b present(there may also be constructions for policies defined as arbitrary circuits and meanwhile with additional negations there may also be non-monotone access policies). For instance, let us assume that the universe of attributes is defined to be {P, Q, R, S}{P, Q, R, S} and user 1 receives a key to attributes {P, Q}{P, Q} and user 2 to attribute {S}{S}. If a ciphertext is encrypted with respect to the policy (P∧R)∨S(P∧R)∨S, then user 2 will be able to decrypt, while user 1 will not be able to decrypt. In this paper propose a mechanism for cloud computing. In cloud users upload their files and also access files from cloud .So scheme provides an efficient encryption scheme for security of data stored on cloud and then efficient access policy on data files. In public-key cryptography,by using receiver's public-key, message is encrypted for particular receiver. . If user's attributes satisfy the policy of the respective ciphertext then user will be able to decrypt ciphertext.

V. CONCLUSION

In this paper, we've got planned associate economical and fine-grained information access management theme for large information, wherever the access policy won't leak any privacy data. completely different from the present strategies that solely part hide the attribute values within the access policies, our technique will hide the complete attribute (rather than solely its values) within the access policies. However, this could result in nice challenges and difficulties for legal information shoppers to decode information. To address this downside, we've got additionally designed associate attribute localization formula to judge whether or not associate attribute is within the access policy. so as to enhance the potency, a unique Attribute Bloom Filter has been designed to find the precise row numbers of attributes within the access matrix. we've got additionally incontestible that our theme is by selection secure against chosen plaintext attacks. Moreover, we've got enforced the ABF by victimisation MurmurHash and also the access management theme to indicate that our theme will preserve the privacy from any LSSS access policy while not using abundant overhead. In our future work, we'll specialise in the way to affect the offline attribute idea attack that check the idea "attribute strings" by regularly querying the ABF

VI. FUTURE SCOPE

We might want to thank the analysts and also distributers for making their assets accessible. We additionally appreciative to commentator for their significant recommendations furthermore thank the school powers for giving the obliged base and backing.

VII. REFERENCES

[1]. Kan Yang, Qi Han, "An Efficient and Fine-grained Big Data Access Control Scheme with Privacy-preserving Policy" Citation information: DOI 10.1109/JIOT.2016.2571718, IEEE Internet of Things Journal

[2]. K. Yang and X. Jia, "Expressive, efficient, and revocable data access control for multi-authority cloud storage," IEEE Trans. Parallel Distrib. Syst., vol. 25, no. 7, pp. 1735-1744, July 2014. 3K. Yang, Z. Liu, X. Jia, and X. S. Shen, "Time-domain attribute-based access control for cloud-based video content sharing: A cryptographic approach," IEEE Trans. on Multimedia (to appear), February 2016.

[3]. B. Waters, "Ciphertext -policy attribute-based encryption: An expressive, efficient, and provably secure realization," in Proc. of PKC'11. Berlin, Heidelberg: Springer-Verlag, 2011, pp. 53-70. 5H. Li, Y. Yang, T. Luan, X. Liang, L. Zhou, and X. Shen, "Enabling fine-grained multi-keyword search supporting classified sub-dictionaries over encrypted cloud data," IEEE Trans. on Dependable and Secure Computing DOI: 10.1109/ TDSC.2015. 2406704, 2015.

[4]. K. Frikken, M. Atallah, and J. Li, "Attribute-based access control with hidden policies and hidden credentials," IEEE Trans. on Computers, vol. 55, no. 10, pp. 1259-1270, 2006.

[5]. J. Lai, R. H. Deng, and Y. Li, "Expressive cp-abe with partially hidden access structures," in Proc. of ASIACCS'12. ACM, 2012, pp. 18-19.

[6]. J. Hur, "Attribute-based secure data sharing with hidden policies in smartgrid," IEEE Trans. Parallel Distrib. Syst., vol. 24, no. 11, pp. 2171-2180,2013.

[7]. A. Beimel, "Secure schemes for secret sharing and key distribution,"Ph.D. dissertation, Israel Institute of Technology, Technion, Haifa, Israel,1996.

[8]. B. H. Bloom, "Space/time trade-offs in hash coding with allowable errors," Communications of the ACM, vol. 13, no. 7, pp. 422-426, 1970.

[9]. Arti Arun Mohanpurkar, Madhuri Satish Joshi, "A Traitor Identification Technique for Numeric Relational Databases with Distortion Minimization and Collusion Avoidance" International Journal of Ambient Computing and Intelligence Volume 7 • Issue 2 • July-December 2016

[10]. Arti Mohanpurkar, Madhuri Joshi, " The Effect of the Novel Anti-Collusion Fingerprinting Scheme on the Knowledge from Numeric Databases" International Journal of Scientific & Engineering Research, Volume 6, Issue 12, December-2015 ISSN 2229-5518

[11]. Arti Mohanpurkar, Madhuri Joshi, "Fingerprinting Numeric Databases with Information Preservation and Collusion Avoidance" International Journal of Computer Applications (0975 - 8887) Volume 130 - No.5, November2015

[12]. H. Lin, Z. Cao, X. Liang, and J. Shao, "Secure threshold multi authority attribute based encryption without a central authority," in Proc. of INDOCRYPT'08. Springer, 2008, pp. 426-436.

[13]. T. Nishide, K. Yoneyama, and K. Ohta, "Attribute-based encryption with partially hidden encryptor-specified access structures,"

in Applied cryptography and network security. Springer, 2008, pp. 111-129.

[14]. J. Li, K. Ren, B. Zhu, and Z. Wan, "Privacy-aware attribute-based encryption with user accountability," in Information Security. Springer, 2009, pp. 347-362.

[15]. D. Boneh and B. Waters, "Conjunctive, subset, and range queries on encrypted data," in Theory of cryptography. Springer, 2007, pp. 535-554.

[16]. J. Katz, A. Sahai, and B. Waters, "Predicate encryption supporting disjunctions, polynomial equations, and inner products," in Advances in Cryptology-EUROCRYPT'08. Springer, 2008, pp. 146-162.

[17]. J. Lai, R. H. Deng, and Y. Li, "Fully secure cipertext-policy hiding cpabe," in Information Security Practice and Experience. Springer, 2011, pp. 24-39.

[18]. L. Lei, Z. Zhong, K. Zheng, J. Chen, and H. Meng, "Challenges on wireless heterogeneous networks for mobile cloud computing," IEEE Wireless Communications, vol. 20, no. 3, pp. 34-44, 2013.

[19]. K. Zheng, Z. Yang, K. Zhang, P. Chatzimisios, K. Yang, and W. Xiang, "Big data-driven optimization for mobile networks toward 5g," IEEE Network, vol. 30, no. 1, pp. 44-51, 2016.

[20]. Z. Su, Q. Xu, and Q. Qi, "Big data in mobile social networks: a qoeoriented framework," IEEE Network, vol. 30, no. 1, pp. 52-57, 2016.

[21]. H. Li, D. Liu, Y. Dai, and T. H. Luan, "Engineering searchable encryption of mobile cloud networks: when qoe meets qop," IEEE Wireless Communications, vol. 22, no. 4, pp. 74-80, 2015.

[22]. H. Li, Y. Yang, T. Luan, X. Liang, L. Zhou, and X. Shen, "Enabling fine-grained multi-keyword search supporting classified sub-dictionaries over encrypted cloud data," IEEE Trans. on Dependable and Secure Computing DOI: 10.1109/TDSC.2015.2406704], 2015.

[23]. K. Frikken, M. Atallah, and J. Li, "Attribute-based access control with hidden policies and hidden credentials," IEEE Trans. on Computers, vol. 55, no. 10, pp. 1259-1270, 2006.

[24]. S. Yu, K. Ren, and W. Lou, "Attribute-based content distribution with hidden policy," in Secure Network Protocols (NPSec'08 Workshop). IEEE, 2008, pp. 39-44.

[25]. J. Lai, R. H. Deng, and Y. Li, "Expressive cp-abe with partially hidden access structures," in Proc. of ASIACCS'12. ACM, 2012, pp. 18-19.

[26]. J. Hur, "Attribute-based secure data sharing with hidden policies in smart grid," IEEE Trans. Parallel Distrib. Syst., vol. 24, no. 11, pp. 2171-2180, 2013.

[27]. A. Beimel, "Secure schemes for secret sharing and key distribution," Ph.D. dissertation, Israel Institute of Technology, Technion, Haifa, Israel, 1996.

[28]. B. H. Bloom, "Space/time trade-offs in hash coding with allowable errors," Communications of the ACM, vol. 13,no. 7, pp. 422-426, 1970.

[29]. K. Yang, X. Jia, and K. Ren, "Secure and verifiable policy update outsourcing for big data access control in the cloud," IEEE Trans. Parallel Distrib. Syst., vol. 26, no. 12, pp. 3461-3470, Dec 2015.

[30]. C. Dong, L. Chen, and Z. Wen, "When private set intersection meets big data: an efficient and scalable protocol," in Proc. of CCS'13. ACM, 2013, pp. 789-800.