IJCSE International Journal of Computer Sciences and Engineering Open Access

Survey Paper Volume-4, Issue-4 E-ISSN: 2347-2693

A Survey on Outsourced Attribute-Based Encryption Technique

Hadiya Rafiq Mir [1*] and U. A. Jogalekar [2]

[1*,2] Dept. of Computer Engineering,
Savitribai Phule Pune University, India

www.ijcseonline.org

Received: Mar/22/2016 Revised: Apr/01/2016 Accepted: Apr/14/2016 Published: Apr/30/ 2016

***Abstract*— In the modern times, more sensitive data is being stored on third party servers which are untrusted, so data on these sites need to be in encrypted form. Every now and then new encryption techniques are put forward. Attribute Based Encryption (ABE) is one such cryptographic technique that secures the data and provides fine-grained access control. However, The Computational complexities of ABE key issuing and decryption are getting too high due to the high expressiveness of ABE approach which affects the efficiency of ABE. To tackle this, many Outsourced Variants of ABE have been proposed to improve the efficiency of ABE such that it could be widely deployed. In this paper, a survey is done on various ABE techniques that have been proposed and their advantages and disadvantages are also discussed.**

Keywords- Attribute-based encryption; Key Generation Service Provider; Decryption Service Provider; Access control; Outsourcing computation; Key issuing; Checkability.

I. INTRODUCTION

Traditionally, we have viewed encryption as a method for one user to encrypt data to another specific targeted party, such that only the target recipient can decrypt and read the message. However, in many applications a user might often wish to encrypt data according to some policy as opposed to specified set of users. Trying to realize such applications on top of a traditional public key mechanism poses a number of difficulties. For instance, a user encrypting data will need to have a mechanism which allows him to look up all parties that have access credentials or attributes that match his policy. These difficulties are compounded if a party's credentials themselves might be sensitive or if a party gains credentials well after data is encrypted and stored.

In an ABE system, a user's keys and cipher texts are labelled with sets of descriptive attributes and a particular key can decrypt a particular cipher text only if there is a match between the attributes of the cipher text and the user's key. First time, ABE enables efficient public key-based fine-grained sharing. In Key-Policy Attribute-Based Encryption (KP-ABE), the access structure is specified in the private key, while the cipher texts are simply labelled with a set of descriptive attributes. Cipher text Policy Attribute-Based Encryption (CP-ABE) schemes were proposed to facilitate key management and cryptographic access control in an expressive and efficient way. Under the construction of CP-ABE, an attribute is a descriptive string assigned to (or associated with) a user and each user may be tagged with multiple attributes. Multiple users may share common attributes, which allow message encryptions to specify a data access policy by composing multiple attributes through logical operators such as "AND", "OR", etc. To decrypt the message, the decryptor's attributes need to satisfy the access policy.

Cloud computing is an emerging computing paradigm, in which IT resources and capacities are provided as services over the Internet while hiding platform and implementation details. Promising as it is, this paradigm also brings forth new challenges for data security and privacy when users outsource sensitive data for sharing on cloud servers, which are likely outside of the same trusted domain of data owners. These concerns are originated from the fact that sensitive data resides in a public cloud, which is maintained and operated by untrusted cloud service provider (CSP).

ABE gives a secure way that permits information proprietor to share outsourced information on the untrusted stockpiling server rather than trusted server with determined gathering of clients. This point of preference makes the technique engaging in distributed storage that requires secure access control for countless having a place with diverse associations. By and by, one of the principle proficiency downsides of ABE is that the computational expense in decoding stage develops with the entrance's intricacy recipe. Along these lines, before generally sent, there is an expanding need to enhance the proficiency of ABE. To address this issue, outsourced ABE, which gives an approach to outsource escalated figuring assignment amid unscrambling to CSP without uncovering information or private keys, was presented. It has an extensive variety of uses. The heavy decryption outsourced, we watch that the ascribe power needs to manage a ton of overwhelming calculation in a versatile framework. More precisely, the characteristic power needs to issue private keys to all clients, however yet era of private key ordinarily requires huge secluded exponentiation calculation, which becomes directly

with the intricacy of the predicate equation. At the point when an extensive number of clients require their private keys, it may over-burden the property power. Besides, key administration system, key denial specifically, is essential in a safe and adaptable ABE framework. In the majority of existing ABE plans, the disavowal of any single private key requires key-upgrade at property power for the remaining unrevoked keys which impart regular ascribes to the one to be disavowed. These substantial errands brought together at power side would make it a proficiency bottleneck in the entrance control framework

II. RELATED WORK

In [1], they present another sort of Identity-Based Encryption (IBE) plan that they call Fuzzy Character Based Encryption. In Fuzzy IBE, they see a way of life as set of graphic qualities. A Fluffy IBE plan takes into account a private key for a personality, w, to decode a cipher text scrambled with a personality, w', if and just if the characters w what's more, w' are near one another as measured by the "set cover" separation metric. A Fuzzy IBE plan can be connected to empower encryption utilizing biometric inputs as personalities; the lapse resistance property of a Fuzzy IBE plan is accurately what takes into account the utilization of biometric personalities, which characteristically will have some clamor every time they are inspected. Furthermore, they demonstrate that Fuzzy-IBE can be utilized for a kind of application that they term "quality based encryption". In this paper they show two developments of Fuzzy IBE plans. Their developments can be seen as an Identity-Based Encryption of a message under a few qualities that create a (fluffy) character. Their IBE plans are both mistake tolerant and secure against plot assaults. Furthermore, our fundamental development does not utilize arbitrary prophets. We demonstrate the security of their plans under the Selective-ID security model.

In this [2] paper, Attribute-based encryption (ABE) is another vision for open key encryption that permits clients to scramble and unscramble messages taking into account client characteristics. For instance, a client can make a cipher text that can be unscrambled just by different clients with characteristics fulfilling ("Faculty" OR ("PhD Student" AND "Quals Completed")).Given its expressiveness, ABE is presently being considered for numerous distributed storage and processing applications. Be that as it may, one of the principle productivity downsides of ABE is that the measure of the cipher text and the time required to unscramble it develops with the multifaceted nature of the entrance recipe. In this work, they propose another worldview for ABE that to a great extent wipes out this overhead for clients. Assume that ABE cipher texts are put away in the cloud. They indicate how a client can furnish the cloud with a solitary change key that permits the cloud to decipher any ABE cipher text fulfilled by that client's traits into a (steady size) El Gamal-style cipher text, without the cloud having the capacity to perused any piece of the client's messages. To unequivocally characterize and exhibit the upsides of this methodology, they give new security definitions to both CPA and replayable CCA security with outsourcing, a few new developments, an execution of their calculations and itemized execution estimations. In a run of the mill setup, the client spares altogether on both data transfer capacity and decoding time, without expanding the number of transmissions.

In [3], distributed computing is a promising innovation, which is changing the customary Internet processing worldview and IT industry. With the improvement of remote access advances, distributed computing is relied upon to grow to versatile situations, where cell phones and sensors are utilized as the data accumulation hubs for the cloud. In any case, clients' worries about information security are the principle deterrents that obstruct distributed computing from being generally embraced. These worries are begun from the way that delicate information dwells in broad daylight mists, which are worked by business administration suppliers that are not trusted by the information proprietor. Accordingly, new secure administration architectures are expected to address the security worries of clients for utilizing cloud processing systems. In this paper, they exhibit a comprehensive security structure to secure the information stockpiling out in the open mists with the uncommon core interest on lightweight remote gadgets store and recover information without uncovering the information substance to the cloud administration suppliers. To accomplish this objective, their answer concentrates on the accompanying two research bearings: First, they exhibit a novel Privacy Preserving Cipher Policy Attribute-Based Encryption (PP-CP-ABE) to secure clients' information. Utilizing PP-CP-ABE, light-weight gadgets can safely outsource overwhelming encryption and unscrambling operations to cloud administration suppliers, without uncovering the information content also, utilized security keys. Second, they propose an Attribute Based Data Storage (ABDS) framework as a cryptographic access control component. ABDS accomplishes data hypothetical optimality in terms of minimizing calculation, stockpiling and correspondence overheads. Particularly, ABDS minimizes cloud administration charges by decreasing correspondence overhead for information administrations. Their execution appraisals exhibit the security quality and effectiveness of the exhibited arrangement as far as calculation, correspondence, and capacity.

In this [4] paper, computationally costly undertakings that can be parallelized are most proficiently finished by circulating the calculation among an expansive number of processors. The Internet's development has made it conceivable to welcome the support of pretty much any PC in such disseminated calculations. This presents the potential

for conning by untrusted members. In a business setting where members get paid for their commitment, there is motivation for exploitative members to claim credit for work they didn't do. In this paper, they propose security plans that protect against this danger with next to no overhead. Their weaker plan disheartens ensuring so as to con that it doesn't pay off, while their more grounded plans let members demonstrate that they have done the greater part of the work they were doled out with high likelihood.

In [5], touchy information is shared and put away by outsider locales on the Internet, there will be a need to scramble information put away at these locales. One disadvantage of scrambling information is that it can be specifically shared just at a coarse-grained level (i.e., giving another party your private key). They build up another cryptosystem for fine-grained sharing of scrambled information that we call Key-Policy Attribute-Based Encryption (KP-ABE). In their cryptosystem, cipher texts are named with sets of traits and private keys are connected with access structures that control which cipher texts a client has the capacity decode. They show the appropriateness of their development to sharing of review log data what's more, telecast encryption. Their development bolsters appointment of private keys which subsumes Hierarchical Identity-Based Encryption (HIBE).

In [6] a few circulated frameworks a client ought to just be ready to get to information if a client forces a sure arrangement of credentials or traits. As of now, the main strategy for authorizing such arrangements is to utilize a trusted server to store the information and intervene access control. Be that as it may, if any server putting away the information is traded off, then the classification of the information will be traded off. In this paper they introduce a framework for acknowledging complex access control on scrambled information that they call Cipher text-Policy Characteristic Based Encryption. By utilizing our systems scrambled information can be kept private regardless of the fact that the storage server is untrusted; in addition, our techniques are secure against intrigue assaults. Past Attribute- Based Encryption frameworks utilized credits to depict the scrambled information and incorporated strategies with client's keys; while in their framework credits are utilized to depict a client's certifications, and gathering encoding information determines an approach for who can decode. Along these lines, their methods are theoretically closer to customary access control systems, for example, Role-Based Access Control (RBAC). Furthermore, their give a usage of our system and give execution estimations.

In [7] cipher text strategy trait based encryption (CP-ABE), each mystery key is connected with an arrangement of traits, and each cipher text is connected with an entrance structure on traits. Unscrambling is empowered if and just if the client's trait set fulfills the cipher text access structure. This gives fine-grained access control on shared information in numerous down to earth settings, including secure databases and secure multicast. In this paper, they think about CP-ABE plans in which get to structures are AND doors on positive and negative characteristics. Their fundamental plan is ended up being picked plaintext (CPA) secure under the decisional bilinear Diffie-Hellman (DBDH) suspicion. They then apply the Canetti-Halevi- Katz system to get a picked cipher text (CCA) secure augmentation utilizing one-time marks. The security evidence is a lessening to the DBDH supposition and the solid existential unforgeability of the mark primitive. Likewise, they acquaint various leveled characteristics with streamline their fundamental plan decreasing both cipher text size and encryption/unscrambling time while keeping up CPA security. At last, they propose an augmentation in which get to approaches are discretionary edge trees, and they close with a talk of handy uses of CP-ABE.

In this [8] paper, they address the issue of utilizing untrusted cryptographic assistants. They give a formal security definition to safely outsourcing calculations from a computationally restricted gadget to an untrusted assistant. In their model, the antagonistic environment composes the product for the assistant, yet then does not have direct correspondence with it once the gadget begins depending on it. Notwithstanding security, they likewise give a structure to measuring the proficiency what's more, checkability of an outsourcing usage. They exhibit two pragmatic outsource secure plans. In particular, they demonstrate to safely outsource measured exponentiation, which presents the computational bottleneck in most open key cryptography on computationally constrained gadgets. Without outsourcing, a gadget would require O(n) measured augmentations to do measured exponentiation for n-bit types. The heap lessens to O(log2 n) for any exponentiation-based plan where the legitimate gadget may utilize two untrusted exponentiation programs.

In this [9] paper they think about intuitive verifications for tractable languages. The prover ought to be efficient and keep running in polynomial time. The verifier ought to be super-efficient and keep running in about straight time. These verification frameworks can be utilized for assigning calculation: a server can run a calculation for a customer and intelligently demonstrate the outcome's rightness. The customer can confirm the result's rightness in about straight time. Already, related inquiries were considered in the Holo-realistic Proof setting by Babai, Fortnow, Levin and Szegedy, in the contention setting under computational presumptions by Kilian, and in the arbitrary prophetic model by Micali. Their concentrate, on the other hand, is on the first intuitive evidence model where no suspicions are made on the computational force then again adaptiveness of exploitative provers. Their fundamental specialized

hypothesis gives an open coin intuitive confirmation for any dialect process-able by a log-space uniform Boolean circuit with profundity d and info length n. The verifier keeps running in time (n+d).Polylog(n) and space O(log(n)), the communication many sided quality is d, Polylog(n) and the prover runs in time poly(n). Specifically, for dialects process-able by log-space uniform NC (circuits of polylog(n) profundity), the prover is efficient, the verifier keeps running in time n, Polylog(n) what's more, space O(log(n)), and the correspondence multifaceted nature is polylog(n).

In this [10] paper, they propose a completely homomorphic encryption plan i.e., a plan that permits one to assess circuits over scrambled information without having the capacity to unscramble. Their answer comes in three stages. To begin with, they give a general result – that, to develop an encryption plan that allows assessment of subjective circuits, it suffices to develop an encryption plan that can assess its own decoding circuit; they call a plan that can assess its (expanded) unscrambling circuit bootstrappable. Next, they depict an open key encryption plan utilizing perfect cross sections that are verging on bootstrappable. Grid based cryptosystems ordinarily have unscrambling calculations with low circuit many sided quality, frequently overwhelmed by an internal item calculation that is in NC1. Likewise, perfect grids give both added substance and multiplicative homomorphisms, as expected to assess general circuits. Lamentably, our introductory plan is not exactly bootstrappable i.e., the profundity that the plan can effectively evaluate can be logarithmic in the cross section measurement, much the same as the profundity of the decoding circuit, however the last is more prominent than the previous. In the last step, they demonstrate to change the plan to decrease the unscrambling's profundity circuit, and in this manner acquire a bootstrappable encryption plan, without decreasing the profundity that the plan can assess. Abdominal musclestractly, they perform this by empowering the encrypter to begin the unscrambling procedure, leaving less work for the decrypter, much like the server leaves less work for the decrypter in a server-helped cryptosystem.

In [11], they depict a working execution of a variation of Gentry's completely homomorphic encryption plan (STOC 2009),like the variation utilized as a part of a prior execution exertion by Smart what's more, Vercauteren (PKC 2010). Brilliant and Vercauteren actualized the basic "to some degree homomorphic" plan, however were not ready to actualize the bootstrapping usefulness that is expected to get the complete plan to work. They demonstrate various advancements that permit them to actualize all parts of the plan, including the bootstrapping usefulness. Their fundamental advancement is a key-era technique for the basic to some degree homomorphic encryption that does not require full polynomial reversal. This lessens the asymptotic many-sided quality from ˜O(n2:5) to ˜O (n1:5) when working with measurement n grids (and for all intents and purposes lessening the time from numerous hours/days to a few moments/minutes). Different enhancements incorporate a bunching system for encryption, a watchful investigation of the unscrambling level polynomial, and some space/time exchange offs for the completely homomorphic plan. They tried our execution with cross sections of a few measurements, comparing to a few security levels. From a "toy" setting in measurement 512, to "little," "medium," and "huge" settings in measurements 2048, 8192, and 32768, individually. General public key size reaches in size from 70 Megabytes for the "little" setting to 2.3 Gigabytes for the "huge" setting. The opportunity to run one bootstrapping operation (on a 1-CPU 64-bit machine with huge memory) ranges from 30 seconds for the "little" setting to 30 minutes for the "huge" setting.

In this[12] paper, distributed computing gets to be predominant, more sensitive information is being incorporated into the cloud for sharing, which brings forward new difficulties for outsourced information security and protection. Attribute based encryption (ABE) is a promising cryptographic primitive, which has been generally connected to plan fine grained access control framework recently. In any case, ABE is being censured for its high plan overhead as the computational expense develops with the many-sided quality of the entrance equation. This drawback turns out to be more genuine for cell phones in light of the fact that they have obliged processing assets. Going for handling the test above, they exhibit a nonexclusive and efficient answer for actualize quality based access control framework by bringing secure outsourcing systems into ABE. All the more unequivocally, two cloud administration suppliers (CSPs), specifically key generation cloud service provider (KG-CSP) and decoding cloud service provider (D-CSP) are acquainted with perform the outsourced key-issuing and decoding on sake of quality power and clients individually. Keeping in mind the end goal to outsource overwhelming calculation to both CSPs without private data spillage, they formulize a basic primitive called outsourced ABE (OABE) what's more, propose a few developments with outsourced decoding and key- issuing. At last, broad investigation shows that with the assistance of KG-CSP and D-CSP, efficient key-issuing and unscrambling are accomplished in their developments.

III. CONCLUSON

In this paper, we have surveyed various outsourced ABE plans. Further we plan to provide a more efficient ABE system that achieves consistent efficiency at authority and client sides with help of KGSP and DSP. Not at all like the best in class are outsourced ABE, checkability and User Revocation upheld by this development. We have analysed the security of proposed plans and found that our construction is efficient and practical based on experimental results.

Sr.no	Paper	Technique	Advantage	Disadvantage	Result
1	Fuzzy Identity Based Encryption	Fuzzy IBE, private key for an identity, to decrypt a cipher text encrypted with an identity	To perform authentication checks before delivering a document.	It is interactive. . It requires two rounds of additional communication overhead to perform decryption.	Hides the public key that was used to encrypt the cipher text is intriguing, uses set-overlap as a similarity measure between identities
2	Outsourcing the Decryption of ABE Cipher texts	New security definitions for both CPA and replayable CCA security with outsourcing, saves significantly on both bandwidth and decryption time, without increasing the number of transmissions.	Decrease the size of the trusted code base, removing thousands of lines of complex parsing code	It can be selectively shared only coarse grained level that means private key shared with another party	Outsourcing as a tool to harden ABE implementations in platforms with code isolation, used in systems containing hardware security modules
3	Attribute-Based Encryption for Fine-Grained Access Control of Encrypted Data	Cipher texts are labeled with sets of attributes and private keys are associated with access structures that control which cipher texts a user is able to decrypt.	Preventing unauthorized data access	Ability of users to selectively share their encrypted data at a fine grained level	To sharing of audit-log information and broadcast encryption, delegation of private keys which subsumes Hierarchical Identity-Based Encryption
4	Cipher text Policy Attribute Based Encryption	System for realizing complex access control on encrypted data,	Secure against collusion attacks.	The Length of cipher text is depends on the number of attributes.	In their system attributes are used to describe a user's credentials, and a party encrypting data determines a policy for who can decrypt.
5	Provably Secure Cipher text Policy ABE	Canetti-Halevi-Katz techniques to obtain a chosen cipher text (CCA) secure extension using one-time signatures.	Reducing both cipher text size and encryption/ decryption time while maintaining CPA security.	Not expressive, Length of cipher text is depends on the number of attributes.	CP-ABE, use AND gate on positive and negative attributes on cipher text, to obtain CCA security

ACKNOWLEDGMENT

We would like to express thanks to researchers for making their work available and professors for their worthy guidance. We are thankful to the college for their support and for rendering us the required infrastructure. We would also like to express gratitude to Savitribai Phule Pune University and also to concerned members of IJCSE committee, for their valuable reviews.

REFERENCES

[1] A. Sahai and B. Waters, ''Fuzzy Identity-Based Encryption,'' in Proc. Adv. Cryptol.-EUROCRYPT, LNCS 3494, R. Cramer, Ed., Berlin, Germany, 2005, pp. 457-473, Springer-Verlag.

[2] M. Green, S. Hohenberger, and B. Waters, ''Outsourcing the Decryption of ABE Ciphertexts,'' in Proc. 20th USENIX Conf. SEC, 2011, p. 34.

[3] Z. Zhou and D. Huang, ''Efficient and Secure Data Storage Operations for Mobile Cloud Computing,'' in Cryptology ePrint Archive, Report 2011/185, 2011.

[4] P. Golle and I. Mironov, ''Uncheatable Distributed Computations,'' in Proc. Conf. Topics Cryptol., CT-RSA, 2001, pp. 425-440.

[5] V. Goyal, O. Pandey, A. Sahai, and B. Waters, ''Attribute-Based Encryption for Fine-Grained Access Control of Encrypted Data,'' in Proc. 13th ACM Conf. Comput. Commun. Security, 2006, pp. 89-98.

[6] J. Bethencourt, A. Sahai, and B. Waters, ''Ciphertext-Policy Attribute-Based Encryption,'' in Proc. IEEE Symp. Security Privacy, May 2007, pp. 321-334.

[7] Mewada, Shivlal, Pradeep Sharma, and S. S. Gautam. "Classification of Efficient Symmetric Key Cryptography Algorithms." International Journal of Computer Science and Information Security 14.2 (2016): pp(105-110).

[8] S. Hohenberger and A. Lysyanskaya, ''How to Securely Outsource Cryptographic Computations,'' in Proc. Theory Cryptogr., LNCS 3378, J. Kilian, Ed., Berlin, Germany, pp. 264-282, Springer- Verlag.

[9] S. Goldwasser, Y.T. Kalai, and G.N. Rothblum, ''Delegating Computation: Interactive Proofs for Muggles,'' in Proc. 40th Annu. ACM STOC, 2008, pp. 113-122.

[10] C. Gentry, ''Fully Homomorphic Encryption Using Ideal Lattices,'' in Proc. 41st Annu. ACM STOC, 2009, pp. 169-178.

[11] C.Gentry and S.Halevi, ''ImplementingGentry's Fully-Homomorphic Encryption Scheme,'' in Proc. Adv. Cryptol.-EUROCRYPT, LNCS 6632, K. Paterson, Ed., Berlin, Germany, 2011, pp. 129-148, Springer-Verlag.

[12] J. Li, X. Chen, J. Li, C. Jia, J. Ma, and W. Lou, ''Fine-Grained Access Control System Based on Outsourced Attribute-Based Encryption,'' in Proc. 18th ESORICS, 2013, pp. 592-609.

[13] M.J. Atallah, K. Pantazopoulos, J.R. Rice, and E.E. Spafford, ''Secure Outsourcing of Scientific Computations,'' in Trends in Software Engineering, vol. 54, M.V. Zelkowitz, Ed. Amsterdam, The Netherlands: Elsevier, 2002, pp. 215-272.

[14] R. Gennaro, C. Gentry, and B. Parno, ''Non-Interactive Verifiable Computing: Outsourcing Computation to Untrusted

Workers,'' in Proc. Adv. Cryptol.-CRYPTO, LNCS 6223, T. Rabin, Ed., Berlin, Germany, 2010, pp. 465-482, Springer-Verlag

[15] K.-M. Chung, Y.Kalai, F.-H. Liu, and R. Raz, ''MemoryDelegation,'' in Proc. Adv. Cryptol.-CRYPTO, LNCS 6841, P. Rogaway, Ed., Berlin, 2011, pp. 151-168, Springer-Verlag.

[16] D. Zeng, S. Guo, and J. Hu, ''Reliable Bulk-Data Dissemination in Delay Tolerant Networks,'' IEEE Trans. Parallel Distrib. Syst. http://doi.ieeecomputersociety.org/10.1109/TPDS.2013.221.