ISSN (e): 2250 – 3005 || Volume, 08 || Issue, 9|| Sepetember – 2018 ||
International Journal of Computational Engineering Research (IJCER)

A Comprehensive Review On Identity Based Encryption In Cloud Computing

Dr. Chinthagunta Mukundha, Veeramalli Bhanu Chander,
Associate Professor, Dept of IT, Sreenidhi Institute of Science & Technology, Hyderabad.
PG Student, Dept of IT,Sreenidhi Institute of Science & Technology, Hyderabad.
Corresponding Author; Dr. Chinthagunta Mukundha

ABSTRACT:*Identity-based encryption (IBE), which easier to do or understand the public key and certificate management at public key infrastructure (PKI) is an important one of two or more available possibilities, to public key encryption.one of the main efficiency drawbacks of IBE suggested that users renew their private keys periodically and senders use the receivers' identities concatenated with current time period. But this mechanism would result in an overhead load at PKG. All the users regardless of whether their keys have been revoked or not, have to contact with PKG periodically to prove their identities and update new private keys. It requires that PKG is online and the secure channel must be maintained for all transactions, which will become a bottleneck for IBE system as the number of users grows, We propose a scheme to offload all the key generation related operations during key-issuing and key-update, leaving only a constant number of simple operations for PKG and eligible users to perform locally, Our scheme does not have to re-issue the whole private keys, but just need to update a lightweight component of it at a specialized entity KU-CSP With the aid of KU-CSP, user needs not to contact with PKG in key-update, in other words, PKG is allowed to be offline after sending the revocation list to KU-CSP, No secure channel or user authentication is required during key-update between user and KU-CSP. Further-more we propose another construction which is secure under the recently formulized refereed delegation computation model. Finally, I added bloom filter encryption technique, while uploading file the data will be encrypted using both IBE propose technique and extension bloom filter technique and their encryption time will be recorded for comparison.*

KEYWORDS: *Identity based encryption (IBE), Outsourced, Revocation, KU-CSP, Cloud-computing.*

Date of Submission: 03-11-2018 Date of acceptance: 17-11-2018

I. INTRODUCTION

This study to focus on identity-based encryption understand the public key and certificate management at public key infrastructure (PKI) is an important one or more available possibilities. We bring outsourcing activity into IBE demonstration of review and endorsement the protected meaning of outsourced revocable IBE out of the blue to the best of our insight. We propose a plan to offload all the key age-related tasks amid key-issuing and key-refresh, leaving just a consistent number of basic activities for PKG and qualified clients to perform locally. In our plan, we understand renouncement through refreshing the private keys of the unrevoked clients. Subsequently, keeping in mind the end goal to keep up decode capacity, unrevoked clients' needs to intermittently ask for on key-refresh for time part to a recently presented substance named Key Update Cloud Service Provider (KU-CSP). we don't need to re-issue the entire private keys, however simply need to refresh a lightweight part of it at a specific element KU-CSP. With the guide of KU-CSP, the client needs not to contact with PKG in key-refresh, at the end of the day, PKG is permitted to be disconnected in the wake of sending the disavowal rundown to KU-CSP. No safe channel or client validation is required amid key-refresh amongst client and KU-CSP. When a large number of users call for their private keys, it may over-burden the quality specialist. Additionally, key management mechanism, key revocation in particular, is necessary in a secure and scalable ABE system. In the majority of existing ABE scheme, the repudiation of any single private key requires key-refresh at a quality specialist for the rest of the unrevoked keys which share normal attributes with the one to be denied. characteristic expert. In addition, all of these heavy tasks centralized at authority side would make it an efficiency bottleneck in the access control system. going at eliminating the most overhead estimation at both the characteristic specialist and the client sides, an outsourced ABE conspire is prescribed that sponsorships

outsourced decryption and also enables appointing key generation. In addition, it is observed that when experiencing commercial cloud computing services, the CSPs may be selfish in order to save its computation or bandwidth, which may cause results returned incorrectly Keeping in mind the end goal to manage this issue, checkability is done on comes about came back from both KGSP and DSP.

When using public-key cryptography over the Internet, the main issue is the ability to associate the right public-keys to the right individuals/organizations. The overall strategy for doing so is as follows. In its simplest form, we assume one or more trusted Certificate-Authority (CA) centers which initially run the signature key generation algorithm to compute its own public and secret keys. Each CA holds its secret key under great security but widely distributes. Furthermore, we consider to realizing revocable IBE with a semi-honest KU-CSP. To achieve this goal, we present a security enhanced construction under the recently formalized Refereed Delegation of Computation (RDoC) model. In this manner, key-update proficiency at PKG can be fundamentally decreased from straight to the stature of such paired tree (i.e. logarithmic in the quantity of clients). By the by, we bring up that however the parallel tree acquaintance is capable with accomplish a relative superior, it will bring about different issues Nevertheless , we point out that though the binary tree introduction is able to achieve a relative high performance, it will result in other problems:1) PKG has to generate a key pair for all the nodes on the path from the identity leaf node to the root node, which results in complexity logarithmic in the number of users in system for issuing a single private key. 2) The size of private key grows in logarithmic in the number of users in system, which makes it difficult in private key storage for users. 3) As the quantity of clients in framework develops, PKG needs to keep up a double tree with a lot of hubs, which presents another bottleneck for the worldwide framework. Pair with the improvement of distributed computing.

II. REVIEW ON IDENTITY BASED ENCRYPTION TECHNIQUES.

1) Security in Cloud Using Cipher text Policy Attributes-Based Encryption With Check ability

(CP-ABE) is quality as a ability amongst the most suitable proposal for information get to rule in sharing storage. It can offload some serious processing concentrated to an outsider, the undisputed status of results came back from the outsider presently can't seem to be frequently to. Going for handle the test overall, another Secure Outsourced ABE framework is proposed, which support both secure outsourced key-issuing and decoding. At the point when encryption gives information privacy, it likewise incredibly restriction the adaptability of information activity. To mark this issue, it is expected to join ABE with cryptographic natives, s

2) Efficient Identity-Based Threshold Decryption Scheme From Bilinear Pairings

Identity based cryptography was suggestion by Shamir in 1984 to similar key management and take way the public key certificates. In identity-based cryptography, the identity of a user, such as his/her e-mail address, is taken as the public key and so the certificate for requirements the public key is not required our IBTD scheme is very efficient and hence is suitable for some resource-restricted applications. We suggestion a new identity-based threshold decryption (IBTD) plan from bilinear pairings. With this plan, the user can by himself distribute the private key among 17 decryption servers, without bother PKG in the sharing procedure. ss

3) Secure Identity Based Encryption Without Random Oracles

(IBE) provides a public key encryption machinery where a public key is an random string such as an email address or a telephone number. The corresponding secret key can only be generated by a Private Key Generator (PKG)who has idea of a master secret. it is only recently that the first working implementations were proposed a security model for identity-based encryption and gave a construction based on the Bilinear Diffie-Hellman (BDH) problem the present system is not very practical and mostly serves as an existence proof. It is still a great problem to find a practical IBE system with a tight security reduce without random oracles, based on Decision BDH or a comparable assumption.

4) Ciphertext-Policy Attribute-Based Encryption

In this paper we existing a system for discern complex access control on encrypted data that we call Ciphertext-Policy Attribute-Based Encryption. By using our capability encrypted data can be kept confidential even if the storage server is untrusted; moreover, our methods are secure against collusion attacks. Thus, our techniques are conceptually closer to trend access control methods such as Role-Based Access Control (RBAC). Finally, we provide an implementation of our system, which included several optimization abilities. In the future, it would be interesting to consider attribute-based encryption systems with different types of expressibility. While, Key-Policy ABE and Ciphertext-Policy ABE seize two interest and complimentary types of systems there certainly exist other types of systems

5) Fusion-Identity Based Encryption with the Outsourced Withdraw in the Cloud Computing:
Now a day's cloud is the delivery of on the demand computing resources everything from the applications to data centers above an internet on pay for use. User or multi user data sharing should be secure and integrity should be derived on cloud, there are two main research problems for cloud computing security such as security improvement using IBE and efficient ABE withdraw process. new fusion cloud security method is proposed in order to deliver both efficient withdraw and enhanced security. This fusion approach is combination of two well know security techniques such as IBE and ABE. we recommend to take a shot at in detail down to earth examination and testing to check the possible outcomes.

6) Two 1-Round Protocols for Delegation of Computation
In this paper consider a weak client that wishes to delegate computation to an untrusted server and be able to succinctly verify the correctness of the result, all within one round of interaction. We provide results for two relaxed varients of this problem. Specifically, where the client delegates the computation to two or more servers, and is guaranteed to output the correct answer as long as even a single server is honest, with a non-succinct offline stage and pubic verifiability the client has to maintain some secret local information pertaining to the offline stage so allows delegating the offline stage to a "some-trusted" outside third party that is quality used by more clients, even felt same suspicious unknown ones

7) Efficient selective-id secure identity-based encryption without random oracles:
In this model the adversary must commit ahead of time to the identity that it intends to attack, whereas in the standard model the adversary is allowed to choose this identity adaptively. The first system is based on the decisional bilinear Diffie-Hellman assumption, and extends to give a selective identity Hierarchical IBE secure without random oracles. The second system is based on a related assumption called the bilinear Diffie-Hellman inversion assumption, the same technique converts both our constructions into efficient CCA2-secure public key systems without random oracles that are almost as efficient as the Cramer-Shoup public key system.

8) Fast Digital Identity Revocation
Computerized characters are fundamental for business, private and government utilization of the web. they requirement for on-line shopping, business-to-business exchanges, on-line managing an account code validation, organization inside personalities While the general plan of every one of these plans is comparatives, and depends on open key cryptography and Certificate Authority administrations, To lessens the CA to catalogs correspondence costs significantly. It can be prove that the normal day by day cost is propositional to at most (R/365) log (365 N/R) this lessening the picked up at the costs of an expansive correspondence prerequisite for the verifier. This exclusive expanding the normal day by day correspondence cost of the CA by a factor[1].

9) Certificate Revocation Using Fine Grained Certificate Space Partitioning
A certificate is a digitally signed statement binding the key holder's name to a public key and various other feature. At the point when an endorsement is issued, the CA announces the timeframe for which the authentication is legitimate. However, there may be situations when the certificate must unusual to be declared invalid prior to its expiration date. Each partition contains the status of a set of certificates, our scheme is more efficient than the three well known certificate revocation techniques: CRL, CRS and CRT., The above approach may be worth analyze in environments where the number of directories or updates per day is high. This is because it may reduce the CA to directory communication costs which are quite high in such environments, though at the price of increasing the query costs.

10) Private and Cheating-Free Outsourcing Of Algebraic Computations
We give protocols for the secure and private outsourcing of straight variable based math calculations, that expert a customer to safely outsource broad arithmetical calculations to two remote servers, such that the servers learn nothing about the customer's private input or the result of the computation and any attempted corruption of the answer by the servers is identify the presence with high probability. large-scale problems in the physical and life sciences are being radically by internet computing technologies, in future work we will extend these results to different algebraic structures, such as the closed semi as grid computing, a weak computational device, once connected to such a grid, is no longer limited by its slow speed, small local storage.

11) Secure and Practical Outsourcing Of Linear Programming In Cloud Computing
The privacy cheating reduction‖ Sec-cloud‖ is used for courage the greater aspects of security. Although the cloud computing is being used to obtain large-scale computations to the cloud, data privacy has become a major issue, the modern cryptographic techniques in secure outsourcing along with the research work, which has been proposed in past years has been presented so that the customers/clients can outsource their complex problem to

the cloud for computation, they have also viewed several real time problems for secure outsourcing of complex matrix multiplication and quadrature scientific computations.

12) Attribute Based Data Sharing With Attributes Revocation
In CP-ABE, every client is related with an arrangement of properties and information are encoded with get to structures on characteristics. A client can unscramble a ciphertext if and just if his qualities fulfill the ciphertext get to structure, Specifically, we settle this testing issue by considering more pragmatic situations in which semi-trustable on-line intermediary servers are accessible One fascinating future work is to join a safe calculation strategy with our development to ensure the trustworthiness of intermediate servers to refresh client secret key without unveiling client property data.

13) Efficient and Secure Data Storage Operations for Mobile Cloud Computing:
In this paper, we present dealing security framework to secure the data storage in public clouds with the special focus on less weight wireless devices store and retrieve data without showing the data content to the cloud service providers(csp). To achieve this goal, our solution focuses on the following two research directions. ABDS achieves information theoretical optimality in terms of minimizing computation, storage and communication overheads. Another important future work will be implementation of a user space secure file system based on popular public cloud storage such that users can secure their cloud storage transparently.

14) Fine-Grained Access Control System based on Outsourced Attribute-based Encryption:
In this paper As, more and more sensitive data is being centralized into the cloud for sharing, which brings forth new challenges for outsourced data security and privacy, one of the main issue of ABE is that the computational cost in private key phase grows with the number of attributes specified in the access policy. to perform the outsourced key-issuing and decryption on behalf of attribute authority and users respectively Finally, extensive experiment demonstrates that with the help of KG-CSP and D-CSP, efficient key-issuing and decryption, Finally, through extensive experiments, it demonstrates that our OABE construction achieves efficient key-issuing and decryption at AA and user sides respectively.

15) Efficient Certificate Validation and Revocation
In this paper they are two new schemes for efficient certificate revocation. Our first scheme is a direct improvement on a well-known tree-based variant of the NOVOMODOO, second scheme is a direct improvement on a tree-based variant of a multi-certificate revocation system. At the core of our schemes is a novel construct termed a Quasimodo tree. use we must have a public-key infrastructure (PKI)that constitutes the policy, procedures, personnel, components, and facilities for binding public keys to identities or authorizations for the purposes of offering desired security services. this concept is of independent interest, and we believe such trees will have numerous other applications. Our Quasimodo single-certificate and multi-certificate revocation systems are quite regulation in terms of both computation and communication.

16) New Algorithms for Secure Outsourcing of Modular Exponentiations:
In this paper, we propose a new secure outsourcing algorithm for exponent modular a prime in the one-malicious model. the most expensive operation in discrete-logarithm based cryptographic protocols Therefore, an interesting open statement is whether there is an efficient algorithm for secure outsourcing modular exponent using only one untrusted cloud sever. The problem of secure outsourcing expensive computations has been well studied in the cryptography community, the proposed algorithm is superior in both efficient and check-ability. We then utilize this algorithm as a subroutine to achieve outsource-secure Cramer-Shoup encryptions and Schnorr signatures, the algorithms can achieve the desired security notions.

17) Identity-based hierarchical strongly key-insulated encryption and its application
In this paper, we discuss non-interactive updating of decryption keys in identity-based encryption when it comes to having to manage revocation of decryption keys without losing its merits in efficiency where a decryption key can be renewed without having to make changes to its public key, does not achieve our goal as such a scheme is completely insecure under our attack model. In extraction to this, we show another method of constructing a partially collusion resistant HIBE from arbitrary IBE in the random oracle model. By combining both results, we can construct an IBE with non-interactive key update from only an arbitrary IBE. the resultant IKE guarantees security against an adversary who has limited access to helper keys but still has unlimited access for the number of times he can query the decryption keys.

18) Secure outsourcing of scientific computations

we examine the outsourcing of numerically and scientific computation This currently arises in many practical situations, including the financial services and petroleum services industries. The general idea is for the customer to do some carefully designed local preprocessing of the problem and/or data before sending it to the agent These disguise techniques can be embedded in a very high level, easy-to-use system that hides their complexity. our methods are geared towards scientific computations that may be solvable in polynomial time, whereas the customer needs only to decrypt the data from the external agent's repository to obtain from it the real data.

III. CONCLUSION

We introduced outsourcing computation into IBE and propose a revocable conspire in which the disavowal tasks are designated to CSP. With the guide of KU-CSP, the proposed conspire is full-included:1) It accomplishes steady effectiveness for both calculation at PKG and private key size at client; 2) User needs not to contact with PKG amid key-refresh, as it were, PKG is permitted to be disconnected subsequent to sending the disavowal rundown to KU-CSP; 3) No protected channel or client validation is required amid key-refresh amongst client and KU-CSP.

FUTURE WORK

We added bloom filter encryption technique, while uploading file the data will be encrypted using both IBE propose technique and extension bloom filter technique and their encryption time will be recorded for comparison.

REFERENCES

[1]. W. Aiello, S. Lodha, and R. Ostrovsky, "Fast digital identity revocation," in Cryptology – CRYPTO'98 springer, 1998.

[2]. V. Goyal, "Certificate revocation using fine grained certificate space partitioning," in Financial Cryptography and Data Security ser. Lecture Notes in Computer Science, S. Dietrich and R. Dhamija, Eds. Springer Berlin / Heidelberg, 2007, vol. 4886, pp. 247–259.

[3]. D. Benjamin and M. J. Atallah, "Private and cheating-free outsourcing of algebraic computations," in Proceedings of the 2008 Sixth Annual Conference on Privacy, Security and Trust, ser. PST '08. Washington, DC, USA: IEEE Computer Society, 2008, pp. 240–24

[4]. C. Wang, K. Ren, and J. Wang, "Secure and practical outsourcing of linear programming in cloud computing," in Proc. IEEE Int. Conf. Comput. Commun. (INFOCOM), 2011, pp. 820–828.

[5]. S. Yu, C. Wang, K. Ren, and W. Lou, "Attribute based data sharing with attribute revocation," in Proceedings of the 5th ACM Symposium on Information, Computer and Communications Security, ser. ASIACCS '10. New York, NY, USA: ACM, 2010, pp. 261–270.

[6]. M. Green, S. Hohenberger, and B. Waters, "Outsourcing the decryption of ABE ciphertexts," in Proc. 20th USENIX Conf. Security (SEC'11), 2011, pp. 34–34.

[7]. B. Libert and J.-J. Quisquater, "Efficient revocation and threshold pairing based cryptosystems," pp. 163–171, 2003.

[8]. "Secure identity based encryption without random oracles," in Advances in Cryptology – CRYPTO 2004, ser. Lecture Notes in Computer Science, M. Franklin, Ed. Springer Berlin / Heidelberg,2004, vol. 3152, pp. 197–206

[9]. R.Canetti, B. Riva, and G. N. Rothblum, "Two 1-round protocols for delegation of computation, " Cryptology ePrint Archive, Report 2011/518, 2011

[10]. J. Bethencourt, A. Sahai, and B. Waters, "Ciphertext-policy attribute-based encryption," in Proceedings of the 2007 IEEE Symposium on Security and Privacy , ser. SP '07. Washington, DC, USA: IEEE Computer Society, 2007, pp. 321–334.

[11]. A. Sahai and B. Waters, "Fuzzy identity-based encryption," in Advances in Cryptology EUROCRYPT 2005, ser. Lecture Notes in Computer Science, R. Cramer, Ed. Springer Berlin / Heidelberg, 2005, vol. 3494, pp. 557–557.

[12]. D. Boneh and X. Boyen, "Efficient selective-id secure identity-based encryption without random oracles," in Advances in Cryptology- EUROCRYPT 2004, ser. Lecture Notes in Computer Science, C. Cachin and J. Camenisch, Eds. Springer Berlin / Heidelberg, 2004, vol. 3027, pp. 223–238

[13]. Z. Zhou and D. Huang, "Efficient and secure data storage operations for mobile cloud computing," in Proc. 8th Int. Conf. Netw. Service manage., 2012, pp. 37–45.

[14]. 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 18th European Symposium on Research in Computer Security (ESORICS), 2013.

[15]. X. Chen, J. Li, J. Ma, Q. Tang, and W. Lou, "New and secure outsourcing algorithms of modular exponentiations," in Proc. 17th Eur. Symp. Res. Comput. Security (ESORICS), 2012, pp. 541–556.

[16]. M. J. Atallah, K. Pantazopoulos, J. R. Rice, and E. E. Spafford, "Secure outsourcing of scientific computations," in Trends in Software Engineering, ser. Advances in Computers, M. V. Zelkowitz, Ed. Elsevier, 2002, vol. 54, pp. 215 – 272.

[17]. F. Elwailly, C. Gentry, and Z. Ramzan, "Quasimodo: Efficient certificate validation and revocation," in Public Key Cryptography(PKC'04), F. Bao, R. Deng, and J. Zhou, Eds. Berlin, Germany:Springer, 2004, vol. 2947, pp. 375–388.

[18]. Y. Hanaoka, G. Hanaoka, J. Shikata, and H. Imai, "Identity-based hierarchical strongly key-

[19]. insulated encryption and its application," in Advances in Cryptology (ASIACRYPT'05), B. Roy, Ed. Berlin,Germany: Springer, 2005, vol. 3788, pp. 495–514.

Dr. Chinthagunta Mukundha "A Comprehensive Review On Identity Based Encryption In Cloud Computing "International Journal of Computational Engineering Research (IJCER), vol. 08, no. 09, 2018, pp 68-72