Secure Data Collaboration Services with Outsourced Revocation in Cloud Computing

Anshul Garg* and Rachna Jain**

*Research Scholar, Completed B.Tech in Computer Science from Bharati Vidyapeeth's College Of Engineering, IPU, India.

**Assistant Professor, Department of Computer Science, Bharati Vidyapeeth's College Of Engineering, IPU, India.

Abstract- Cloud computing is an emerging and promising technique for allowing users to handle and access data from remote locations. However, with the technology getting matured, the users' privacy and the security of user's statistical information is progressively challenged. The traditional centralized access control scheme uses a symmetric key approach and does not support validation. We aim to illustrate the vital issues of identity revocation in this paper. Here we introduce the concept of an instance of outsourcing computation into Identity-Based Encryption (IBE) which trails to a revocable IBE scheme in the server-aided0 setting. Most of the key generation related operations during key-update and key-issuing processes are removed with this scheme, leaving only an invariant number of elementary operations for Public Key Generation (PKG). To achieve this goal, we employ a technique that allows the use of an under crossed private key for each user, in which an AND gate is involved to fasten together and restrict the identity component and the time component. For this purpose, we give the encryptor full control over the access rights, providing viable key management even in the case of multiple freelance authorities, and enabling feasible user revocation, which is requisite in practice. Furthermore, we propose another construction which can be demonstrated under the recently formalized Refereed Delegation of Computation model (RDoC). Finally, we present a view of experimental results to establish the productivity of our model.

Keywords— Cloud Computing; Identity-based encryption; Data Security; Outsourced Data; Access-control; Refereed Delegation of Computation model; Revocation.

I. INTRODUCTION

Cloud computing technology has become the promising and prominent technology of the time. The companies are opting for the services of cloud service providers (CSPs) in place of maintaining their own data centers due to flexibility and cost savings in outsourcing their computing jobs to the experts. This allows them to concentrate on their own field of expertise of business. However, the recent trends of outsourcing data storage to CSPs raise the issue of security, which leads us to the necessity of encryption. Traditional crypto systems confidentially encoded data for a target recipient (e.g. from Davidson to Harley) which restricted the range of prospects and extensibility presented by the cloud environment. In a scenario in which companies are conjoining on a cryptography project and employees are working together on some tasks, suppose Davidson wants to share some data of a sub task with those who are working on it, and with the managers of the project from the different companies. With the traditional encryption approach, recipients must be determined in advance so that they are having their keys. Furthermore, either they have to share the same private key or numerous encrypted versions (with different keys) must be stored. These compromises the security, efficacy and the flexibility expected in a robust cloud environment.

Identity-Based Encryption (IBE) is an amazing substitute for public key encryption. It makes simpler key managing in a certificate-based Public Key Infrastructure (PKI). IBE uses a type of public-key encryption in which the public key of a user is some unique information about the identity of the user (e.g., IP address, unique name, email address, etc). This means that a sender can encrypt a message using the text-value of the receiver's specific identity as a key, who has access to the public parameters of the system. The receiver acquires its decryption key from a central authority, which is required to be trusted as it creates secret keys for every user [1]. Consequently, the receiver is able to decrypt this text by obtaining the private key connected with the resultant identity from Private Key Generator (PKG). IBE demands an efficient revocation mechanism as it allows an arbitrary string as the public key which is considered as an appealing advantage over PKI. Specifically, if the private keys of some users get compromised, there should exist a methodology to revoke such users from the system. In PKI setting, revocation mechanism is recognized by affixing legitimacy periods to certificates or using intricate combinations of procedures [2], [3], [4]. This is the primary drawback of the traditional PKI system.

In view of that, key-update efficiency at PKG can be substantially reduced from linear to the height of such binary tree. Though the binary tree introduction is competent to accomplish a relatively high performance, it will result in other problems as noted below:

1. For each and every node on the path i.e. from the identity leaf node to the root node, PKG has to generate a key pair which results in a logarithmic complexity that depends upon the number of users in the system for issuing a single private key.

2. The cultivating size of the private key which is logarithmic in the number of users in the system makes it problematic for the storage of user's private keys.

3. With increasing number of users in the system, PKG has to maintain a binary tree with a surplus number of nodes. This brings together one more tailback for the global system. If the revocation is analytically calculated in PKI, scarce revocation mechanisms are registered in IBE. The skill of cloud computing users for on-demand computing related to cloud-based services such as Amazon's EC2 and Microsoft's

Windows Azure or Brightcove video cloud has shown that they are not competent in using complex systems. The persons using the cloud services expect that IBE revocation to repair any disputes of productivity and storage overhead pronounced above should be simple. Simply transferring the PKG's master key to the Cloud Service Providers (CSPs) could be a more sophisticated approach. The CSPs then simply update all the private keys and transmit the private keys back to unrevoked users by using the traditional key update technique. However, this approach is less trustworthy as in this system the security depends upon the CSPs who are permitted to access the master key for IBE system.

4. The public clouds are exterior to the trusted sphere of users and are not devoted to users' distinct privacy. For this reason, it is not desirable to entrust a secure volatile IBE scheme to CSPs to reduce the overhead computation.

In this paper, we will examine the outsourcing reckoning into IBE revocation, and deliberate on the security description of outsourced revocable IBE. We propose a scheme to divest all the key generation connected maneuvers during key-issuing and key-update, leaving a constant number of simple maneuvers for PKG and qualified users to accomplish locally. In this scheme, as with the recommendation in [3], we realize revocation through updating the private keys of the unrevoked users. But unlike that work [3] which irrelevantly concatenates time period with identity for key generation/update and necessitates to re-issue the unabridged private key for unrevoked users, we suggest a unique collusion resistant key issuing process. For this, we shall employ a hybrid private key for each user, in which an AND gate is involved to fasten together and restrict two sub-components, namely the time component and the identity component. Initially, the user is able to achieve a default time component (i.e., for the current time period) and the identity component from PKG as his/her private key. Unrevoked users' need to request on the key-update component to a recently introduced entity named Key Update Cloud Service Provider (KU-CSP), in order to hold the ability to decrypt.

In contrast to the suggestion of the authors, D. Boneh and M. Franklin [3], in the arrangement we suggest here, KU-CSP just needs to update a frothy component of the key instead of the need to re-issue the complete private keys. We further come up with:

- The establishment of KU-CSP, the user needs no communication with PKG in key update.
- No secure passage or user authentication is vital during key-update between user and KU-CSP.
- A security enhanced edifice under the lately formalized Refereed Delegation of Computation (RDoC) model [9].
- Lastly, we provide extensive investigational results to determine the adeptness of our proposed model.

Let us deliberate on Identity-based Encryption (IBE) scheme which characteristically involves two entities, PKG, and users (both sender and receiver).

This consists of the succeeding four algorithms:

A. *Setup(λ)*: In this algorithm, a security parameter λ is taken as input and gives the public key PK and the master key MK. (master key is not revealed at PKG.)

B. *Keygen (ID, MK)*: PKG runs the private key generation algorithm, which takes the user's identity and master key MK as input and outputs a private key SKID.

C. *Encrypt (M, ID)*: Sender runs the encryption algorithm, which takes the receiver's identity ID_ and a message M to be encrypted as input and outputs the cipher text CT.

D. *Decrypt (CT, SKID):* Receiver runs the decryption algorithm, which takes the cipher text CT and his/her private key SKID_ as input and outputs a message M or an error.

II. RELATED WORKS

Shamir et al in 1984[1] talked in the paper about a type of cryptographic scheme, which allows users to communicate in a secure manner and also helps in verifying signatures without the use of any type of keys or third party involvement. Aiello in 1998[2] talk about the user to provide communication in a secure environment. It emphasizes on digital identification. Boneh in 2001[3] proposed a brand new scheme for identification which was called IBE. It follows the ciphertext security model and gives many applications for the given systems. Elwailly in 2004[4] provides two schemes for implementation, one being a tree system and another being an improvement in the certificate revocation process. It helps in the time and other complexities that exist in the model. Sahai in 2005[5] provided an IBE scheme that was called Fuzzy Identity-Based Encryption. It was based on descriptive models. It uses private key and ciphertext for attribute-based encryption. It deals with attacks from collusions and random errors. Goyal in 2007[6] presented an all new certificate revocation system and it made use of the hash chaining system. This scheme considerably helped in reducing costs in various areas. Huang in 2008[7] gave an attribute-based scheme in which each user is provided with a specific set of attributes. It basically works on encryption and decryption of ciphertext in the system. It is the first scheme to not take into account a central authority. Boldyreva in 2008[3] took forward the concept of IBE that is identity-based encryption.

The scheme suggested helps more users access this system by improving the efficiency from linear to logarithmic to secure it further. Hanaoka in 2010[9] proposed an efficient model for encryption that worked on parallel keys. It gave schemes which provide cheaper costs for computation. Canetti in 2011[10] looked into various protocols that work by a computational process to work on the verifiability and identification of system and its security.

Identity-Based Encryption (IBE) is a tool used to streamline the public key and certificate regulation at Public Key Infrastructure (PKI). It is an important alternative to public key encryption. However, one of the main disadvantage of IBE

is the overhead computation at Private Key Generator (PKG) during user revocation. Efficient revocation has been well studied in conventional PKI setting, but the difficult management of certificates is eliminated in IBE.

- *Revocable IBE***:** Introduced by and firstly implemented by Boneh and Franklin [3], IBE has been researched intensively in the cryptographic community in respect of construction and first schemes were validated secure in random oracle model. Subsequent systems were established securely in standard model under selective-ID Security or adaptive-ID security. In recent time, there have been multiple lattice-based constructions for IBE Systems. However, there is scope for ample work on revocable IBE. Hanaoka et al. proposed a way for users to periodically renew their private keys without communicating with PKG [10]. However, the authors propose a tamperresistant hardware device and mediator-aided revocation. If an identity is revoked then the mediator is asked to stop helping the user. Apparently, it is non-practical since all users are unable to decrypt on their own and they need to convey with mediator for each and every decryption. Lately, Lin et al. proposed space effective revocable IBE mechanism from nonmonotonic Attribute- Based Encryption (ABE), but their structure requires O(r) time's bilinear pairing operations for a single decryption where r is the number of revoked users.

- *Other Revocation Technique*: The authors examined proxy re-encryption to pose a revocable ABE scheme. In this scheme, confident authority only requires updating master key according to attribute revocation status in each time period and affect proxy re-encryption key to proxy servers. The proxy servers will then re-encrypt cipher text using the re-encryption key to make sure all the unrevoked users can perform successful decryption. A third-party service provider is presented in both Yu et al. and this work. Accordingly, Yu et al. utilized the third party (work as a proxy) to ascertain revocation through encrypting cipher text which only conforms to the special application that the cipher text is stored at the third party. However, in our formulation, the revocation is realized according to updating private keys for unrevoked users at cloud service provider which has no binding on the location of cipher text.

- *Outsourcing Computation:* The difficulty about how to securely outsource dissimilar variants of affluent computations has drawn attention from computer science community for a long time. Attalla et al. offered a framework for secure outsourcing of scientific computations for instance matrix multiplication and quadrature. The solution utilized the masking technique and thus led to escape of private information Chaum and Pedersen initially posed the concept of wallets with observers, a piece of secure hardware mounted on the client's computer to accomplish some expensive computations. Rosenberger and Lysyanskaya offered the first outsource-secure algorithm for modular exponentiations based on pre-computation and server aided computation. Atallah and Li researched the problematic computing domain regarding the edit distance amidst two sequences and presented a competent protocol to securely outsource sequence comparison with two servers.
  Furthermore, Benjamin and Atallah spoke about the problem of secure outsourcing for broadly pertinent linear algebraic computations. Even so, the offered protocol necessitates the expensive operations of homomorphism encryption. Attalla and Frikken further considered this problem and gave enhanced protocols based on the frail secret hiding postulation. Chen et al. Made an efficiency enhancement on the work and anticipated a new scheme for outsourcing single/simultaneous modular exponentiations.

- *Cryptographic Background*

a. *Definition 1.* (Bilinear map)
Let G, GT be cyclic groups of prime order q, writing the group action multiplicatively. g is a generator of G. Let e: G x G→ GT be a map with the following properties:

- Bilinearity: e(g1a , g2b) = e(g1,g2)ab for all g1 , g2 € G, and a,b €R Zq ;
- Non-degeneracy: There exists g1 , g2 € G with e(g1 , g2) ≠ 1 , in other words, the map does not send all pairs in G X G to the identity in GT ;
- Computability: There exists an algorithm to compute e(g1 , g2) for all g1 , g2 € G.

b. *Definition 2***.** (DBDH problem)
The decision Bilinear Diffie-Hellman (DBDH) problem is that, given g,gx,gy,gz € G for unknown random value x,y,z €R Zq , and T €R GT , to decide if T=e(g,g)xyz. We say that the (t, €)-DBDH assumption holds in G if no t –time algorithm has probability at least + € in solving the DBDH problem for non-negligible €.

III. RESEARCH ELABORATIONS

We propose a system model for outsourced revocable IBE in Figure.1. In comparison with typical IBE scheme, a KU-CSP is convoluted to comprehend revocation for negotiated users. Basically, the KU-CSP can be anticipated as a public cloud run by a third party to supply basic computing capabilities to PKG as homogenous services over the network. Normally, the KU-CSP is hosted away from users and the PKG. Also, we have provided a technique to cut down on the storage cost and computation of PKG by proposing a flexible and provisional leeway to the infrastructure.

When revocation is provoked, instead of requesting private keys from PKG again in [3], unrevoked users have to ask the KU-CSP for updating a trivial component of their private keys. Though many credentials are involved in KU-CSP's deployment, in this paper we just logically envisage it as a computing service provider. We are concerned about how to design secure scheme with an untrusted KU-CSP. Based on the system model proposed, we are capable of

defining the outsourced revocable IBE scheme. Equated with the customary IBE definition, the KeyGen Encrypt and KeyGen Decrypt algorithms are redefined to assimilate the time component (This could be the system time). Note that two lists RL and TL, are used in our definition, where RL captures the identities of revoked users and TL is a linked list for the past and current time period.

A. *KeyGen (MK,ID,RL,TL)*:
The key generation algorithm route by PKG takes as input–a master key MK, an identity ID, a revocation list RL and a time list TL. If ID € RL, the algorithm is abandoned, otherwise, it sends the private key SKID = (IK [ID], TK [ID]Ti), to user where IK[ID] is the identity factor for private key SKm and TK[ID]T is its time factor for current time period Ti. Additionally, the algorithm leads an outsourcing key OKID to KU-CSP.

B. *Encrypt (M, ID,Ti,,PK):*
The encryption algorithm routed by sender takes as input-message M, an identity ID and a time period of Ti. It outputs CT which is the ciphertext.

C. *Decrypt(CT,SKID'):*
The decryption algorithm routed by receiver takes as input-a ciphertext CT encrypted under identity ID and time period Ti and a private key SKID'= (IK[ID'],TK[ID']Tj). It outputs the original message M if ID=ID' and Ti=Tj, otherwise outputs 1. Moreover, two algorithms are defined too to apprehend revocation at KU-CSP through updating the private keys of unrevoked users.

D. *Revoke (RL, TL, {ID1… IDi}:*
The revocation algorithm routed by PKG takes as input–a revocation list RL, a time list TL and the set of identities to be revoked is given by {ID1…IDi}. It results in an updated time period Ti+1 along with the updated revocation list RL' and time list TL'.

E. *KeyUpdate (RL,ID,Ti+!,OKid):*
The key update algorithm whose route is defined by KUCSP uses a revocation list RL, an identity ID, a time period Ti+1 and the outsourcing key OKID for identity ID as the inputs. It gives the user and his updated time component in private key TK[ID]Ti+1 as output if his identity ID is not held in RL, otherwise, outputs $\perp$.

In this paper, we deliberate user revocation likewise is the procedure, to deprive users of decryptability even if they have been issued their private keys. To this end, we implant a time period into private key for revocation.

For example, 'Harley' in our setting not only encrypts the message with Davidson's email address "davidson@company.com" but also with the current time period (e.g., "Oct 08, 2017"). When Harley receives the encrypted email, he then obtains his private key comprising of an identity factor and a time period factor from PKG. With the both appropriate factors, the email can be read.

Suppose Harley had approached KU-CSP. Then, the time factors of all the other users are updated by KU-CSP with a fresh time period (say, "Oct 19, 2017). After that, the message sent to Harley should be encrypted with Harley's email address and the updated time period. Since Harley does not have the time factor equivalent to the updated time period, the succeeding encrypted messages cannot be decrypted by Harley even if they are envisioned for him.

The challenge in scheming the outsourced revocable IBE scheme is how to avert a collusion between Harley and other unrevoked fraudulent users. Specifically, a fraudulent user (named Mark) can share his updated time factor (that is, Oct 19 2017) with Harley, and assist Harley to decrypt ciphertext even if Harley just has the previous one (i.e., "Oct 18, 2017"). We will show how to dodge such a collusion later.

IV. SECURITY DEFINITION

We presume that KU-CSP in the illustrated system model is semi-trusted. Specifically, it will trail our protocol but will attempt to search out as much secret information as possible based on its ownership. Hence, two types of adversaries are to be examined as follows.

1. *Type-I adversary:*
It is defined as a curious user with identity ID but revoked before time period Ti. Such adversary attempts to acquire beneficial information from cipher- text intended for him at or after Ti (e.g. time period Ti ,Ti+!, ...) through conniving with other users even if they are unrevoked. Therefore, it is permitted to enquire for private key including identity component and updated time component for complacent users. We postulate that under the assumption of KU-CSP semi-trust worthiness, type-I adversary cannot get outsourcing key for any users.

2. *Type-II adversary:*
It is defined as a curious KU-CSP which intends to acquire valuable information from cipher text intended for some goal identity at time period Ti. Such adversary not only retains outsourcing keys for all users in the system, but also is capable of getting user's private key through colluding with any other user with identity ID' .It is noted that to make such attack realistic, we must restrict ID' ≠ ID.

Under this scenario, we are able to define CCA security game for type-I and type-II adversary correspondingly to our setting in Fig. 1. Assume Ai is the type-i adversary where i= I, II. Then, its benefit in attacking the IBE with outsourced revocation scheme € is defined as

$$Adv€, Ai (\lambda) = |pr[bi = bi']-0.5| \quad \ldots(1)$$

c. *Definition 3*:
An identity-based encryption is reliable against ciphertext attack (IND-IDCCA) with outsourced revocation scheme, if no polynomially bounded adversary has a nonnegligible benefit against challenger in security game for both type-I and type-II adversary.

Lastly, away from the CCA security, we also postulate the following:

1) An IBE with outsourced revocation structure is IND-IDCPA secure (or semantically secure alongside chosen-plaintext attack) if no polynomial time adversary has nonnegligible benefit in modified games for both type-I and type-II adversary, in which the decryption oracle in both phase 1 and phase 2 is uninvolved;

2) An IBE is secure in selective model in which the test identity and time period is succumbed before setup if no polynomial time adversary has non-negligible improvement in modified games for both type-I and type-II adversary.

V. PROPOSED APPROACH

The application's success intended at tackling the significant matter of identity revocation, we initiate outsourcing subtraction into IBE for the first time and put forward a revocable IBE format in the server aided scenery. Our system off- loads all of the key making related operations throughout key-issuing and key-update processes to a Key Update Cloud Service Provider (KU-CSP), and takes only the invariable amount of simple functions for PKG and users to make locally. This goal is attained by operating a novel collusion-resistant technique. We hold a hybrid private key for each user, in which an AND gate is implicated to connect and vault the identity constituent and the time constituent. Furthermore, we recommend another assembly which is verifiable protected under a formalized Refereed Delegation of Computation model. Finally, we present general investigational consequences to make obvious the effectiveness of our proposed edifice.

- ADVANTAGES:

It achieves competence for both the private key size at the user and calculation at PKG. User does not need the PKG throughout key-update, in additional, PKG is permitted to be offline after conveying the revocation list to KUCSP, No protected canal or user confirmation is required during key-update among user and KU-CSP. The proposed approach is shown in Figure 1.

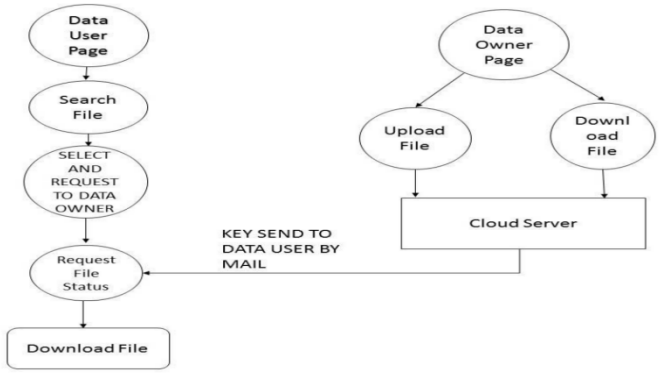

Fig.1. The Proposed approach for outsourcing subtraction into IBE.

a) *Data Users:* In this module, the data user can register with cloud server to search, upload and download files.
b) *Data owner:* In this module, the data owner can register to maintain their file into cloud server and allow access to data users to access the file.
c) *File search:* In this module user can search needed file to download with a proper key.
d) *File upload:* User can upload their file into cloud server with high-level security system.
e) *File download:* In this module, the user can download file with a proper key which provided by data owner.

1) *Input Design:*

The input design is an association between the information system and the user. It includes the functions of developing specifications and procedures for data preparation and those steps that are necessary to put transaction data into a usable form so that processing can be achieved by inspecting the computer to fetch data from a written or printed document or it can occur by keying the data directly into the system. The design of input concentrates on controlling the amount of input required, monitoring and controlling the errors, avoiding delay and extra steps and keeping the process simple.

2) Objectives:

Input Design is the process of converting a user oriented variety of the inputs into a computer-based system. This design is important to avoid bugs in the data input process and show the correct direction to the management. It will help for getting correct information from the computerized system. It is achieved by creating user-friendly interfaces for the data entry to handle large volume of data and their access. The purpose of designing input is to make data entry easier and to be free from bugs. The data entry screen is designed in such a way that all the data manipulations can be performed easily. It also provides log or record viewing facilities and check for its validity. The necessary coding is inbuilt for data validity. Data can be entered with the help of screens or user-interfaces. Suitable messages are provided as and when needed. The principle objective of input design is to create an input layout that is scalable and easy to follow.

3) Output Design:

A quality output design describes that the quality output is one, which meets the requirements of the end user and presents the information correctly and consistently. In any system results of processing are transmitted to the users and to other system managers through outputs. Output design determines how the information is to be displaced for instant need and also the hard copy output. It is the most significant and direct source of information to the user. Effective and intelligent output design improves the system's relationship to assist user decision-making. Designing computer outcome should go in a well-organized, well thought out manner; the correct output must be developed while ensuring that each output element is designed so that user will find the desired output easily and effectively. When analyzing design computer output, the programmer should figure out the specific

output that is needed to meet the user's requirements. It is essential to select ways for presenting user's information in the way management requires. The output form for an information system should fulfill one or more of the objectives namely, information about past activities, logs, current status or projections of the future, important events, problems, or warnings, triggers to an action etc.

VI. CONCLUSION

This paper emphasizes the basic issue of character repudiation, outsourcing calculation inculcated into IBE and a revocable plan in which the repudiation operations are assigned to CSP. With the aid of KU-CSP, the proposed scheme:

1) Realizes constant competence for both calculations at PKG and private key size at consumer.

2) Removes the requirement of user to contact the PKG after every key update, that is, PKG is permitted to be offline after sending the revocation list to KU-CSP.

3) Eliminates the need for protected channel or user verification in key-update between user and KUCSP.

In addition, the paper apprehends revocable IBE a strong contender of the encryption model of the future. The advanced construction presented in the paper shows that it is secure under RDoC model, in which not less than one of the KU-CSPs is assumed, to be honest. Therefore, if a revoked user and either of the KU-CSPs collide, it is unable to help such user re-obtain his/her decrypt ability. Finally, we offer general tentative results to present the competence of our anticipated construction.

REFERENCES

[1] ID-based encryption- Wikipedia at https://en.wikipedia.org/wiki/ID-based_encryption.

[2] Aiello, W., Lodha, S., & Ostrovsky, R. (1998). Fast digital identity revocation. In *Advances in Cryptology—CRYPTO'98*(pp. 137-152). Springer Berlin/Heidelberg.

[3] Goyal, V. (2007, February). Certificate revocation using fine grained certificate space partitioning. In *International Conference on Financial Cryptography and Data Security* (pp. 247-259). Springer, Berlin, Heidelberg.

[4] Elwailly, F. F., Gentry, C., & Ramzan, Z. (2004, February). Quasimodo: Efficient certificate validation and revocation. In *Public Key Cryptography* (Vol. 2947, pp. 375-388).

[5] Shamir, A. (1984, August). Identity-based cryptosystems and signature schemes. In *Crypto* (Vol. 84, pp. 47-53)..

[6] Boldyreva, A., Goyal, V., & Kumar, V. (2008, October). Identity-based encryption with efficient revocation. In *Proceedings of the 15th ACM conference on Computer and communications security* (pp. 417-426). ACM.

[7] Sahai, A., & Waters, B. (2005, May). Fuzzy identity-based encryption. In *Eurocrypt* (Vol. 3494, pp. 457-473).

[8] Boneh, D., & Franklin, M. (2001). Identity-based encryption from the Weil pairing. In *Advances in Cryptology—CRYPTO 2001* (pp. 213-229). Springer Berlin/Heidelberg.

[9] Canetti, R., Riva, B., & Rothblum, G. N. (2011). Two 1-Round Protocols for Delegation of Computation. *IACR Cryptology ePrint Archive*, *2011*, 518.

[10] Hanaoka, G., & Weng, J. (2010, September). Generic Constructions of Parallel Key-Insulated Encryption. In *SCN*(Vol. 6280, pp. 36-53).

[11] J. Li, J. Li, X. Chen, C. Jia and W. Lou, "Identity-Based Encryption with Outsourced Revocation in Cloud Computing," in *IEEE Transactions on Computers*, vol. 64, no. 2, pp. 425-437, Feb. 2015. doi: 10.1109/TC.2013.208

AUTHOR DETAILS

First Author – Anshul Garg, Research Scholar, completed Bachelors of technology(B.Tech) from Bharati Vidyapeeth's College Of Engineering, IPU, India, E-mail: ansh008.008@gmail.com.

Second Author – Mrs. Rachna Jain, Assistant Professor at Bharati Vidyapeeth's College Of Engineering, IPU, India, E-mail: rachna.jain@bharatividyapeeth.edu.

Correspondence Author- Anshul Garg, Research Scholar, completed Bachelors of technology(B.Tech) from Bharati Vidyapeeth's College Of Engineering, IPU, India, PH:+919717783400, E-mail: ansh008.008@gmail.com.