PAPER • **OPEN ACCESS**

Security on Cloud Revocation Authority using Identity Based Encryption

To cite this article: M N Rajaprabha 2017 *IOP Conf. Ser.: Mater. Sci. Eng.* **263** 042051

IOP Conf. Series: Materials Science and Engineering **263** (2017) 042051 doi:10.1088/1757-899X/263/4/042051

Security on Cloud Revocation Authority using Identity Based Encryption

Rajaprabha M N

VIT University, Vellore-632014, Tamilnadu, India
Email: mnrajaprabha@vit.ac.in

Abstract. As due to the era of cloud computing most of the people are saving there documents, files and other things on cloud spaces. Due to this security over the cloud is also important because all the confidential things are there on the cloud. So to overcome private key infrastructure (PKI) issues some revocable Identity Based Encryption (IBE) techniques are introduced which eliminates the demand of PKI. The technique introduced is key update cloud service provider which is having two issues in it and they are computation and communication cost is high and second one is scalability issue. So to overcome this problem we come along with the system in which the Cloud Revocation Authority (CRA) is there for the security which will only hold the secret key for each user. And the secret key was send with the help of advanced encryption standard security. The key is encrypted and send to the CRA for giving the authentication to the person who wants to share the data or files or for the communication purpose. Through that key only the other user will able to access that file and if the user apply some invalid key on the particular file than the information of that user and file is send to the administrator and administrator is having rights to block that person of black list that person to use the system services.

1. Introduction

Cloud computing means use a remote server with the help of network rather than using local server. Cloud refers to the space or storage over the remote server and the needy person can able to access the data with the help of internet. Now a day people uses cloud storage for saving documents over the one place and even can be retrieve from any geographic location through internet. Due to cloud storage dependencies over the devices are decreased because any person can able to access its cloud storage from anywhere and through any device. There are many more advantages of using cloud storage like cloud enables you to work with different person, it also facilitates you more and more space or we can say unlimited space or storage to save our files, cloud also provide backups, which is more beneficial for the business entity to continue their business. But all of the above is the security, which is the main part because everyone's data is saved over the cloud and every type of files like passwords, some important documents, business confidential files etc. are saved so to make it secure some security is also required.

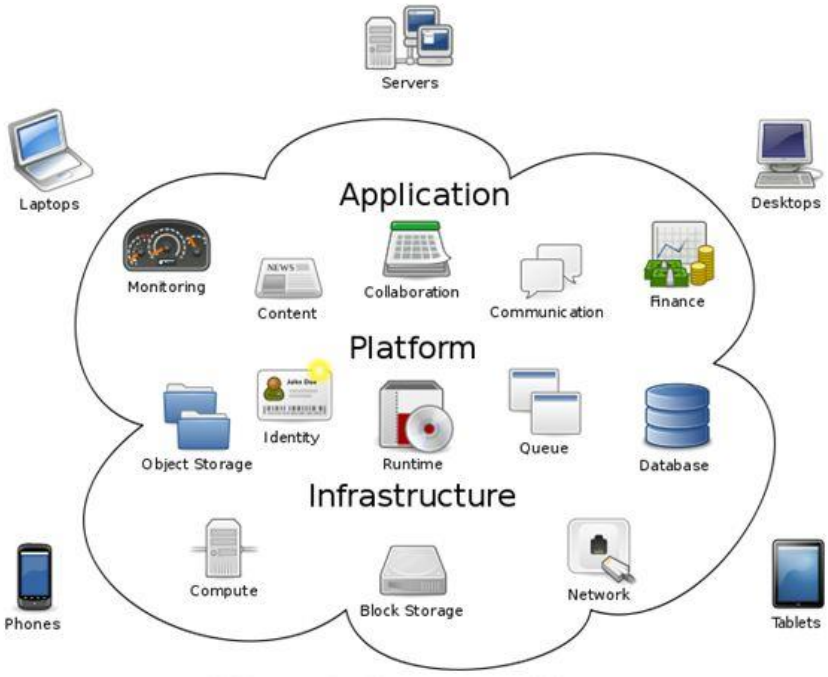

Fig. 1. Cloud Infrastructure

In current era security is the main aspect, because data is the more important in today's world and security on data is also more important. As we know that before few years one of the main cloud server got hacked and many of the data got corrupted that time, so to make data secure more securities are required and more encryption and decryption techniques are also required so after looking towards all this aspect we come with a project for making data more secure and our project is on 'Security On Cloud Revocation Authority Using Identity Based Encryption'. Before cloud technology was introduced the working of the system was different. Usually the data use to save on local server and the main disadvantage was as the new data introduced the space start decreasing, so every time more resources are required and which effect cost and also the complexity of the system. But after cloud was introduced all the data was stored over the cloud which means over the virtual space. The user first use to send request to the server then through server data is sent over the cloud and also even the time of fetching data, first the request is send to the server then server checking for the address where the data is saved over the cloud and then it is giving response back to the end user.

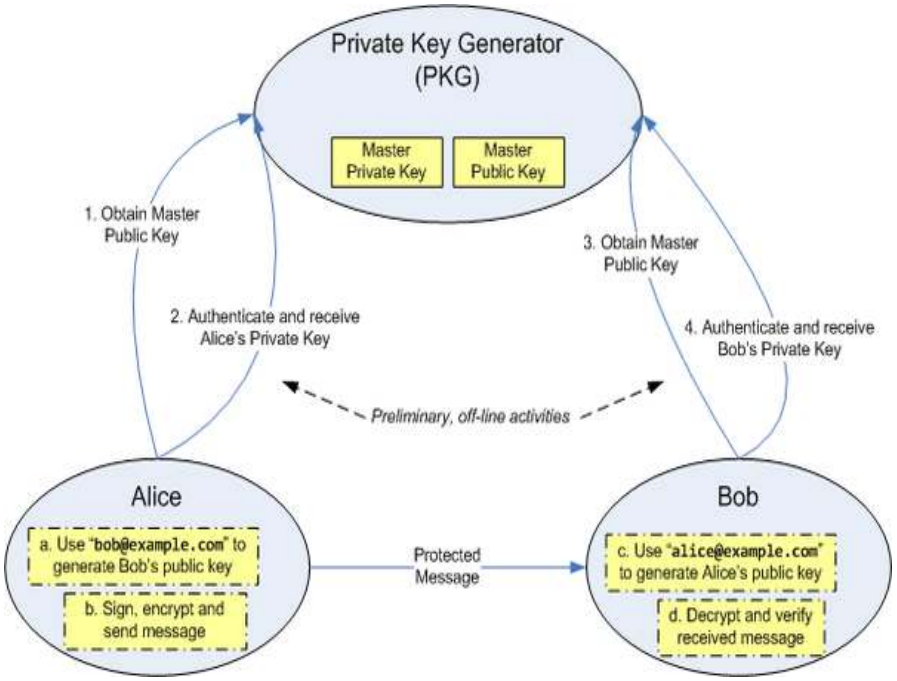

Fig. 2. Identity based Encryption

In our system we are doing the same thing but also applying the security and for the security we are using Identity based Encryption. In Identity based encryption usually the online process is going on for key generation and all the process. In Identity based encryption the person on both side either sender and the receiver having shared parameters so if someone wants to send message to some other person then he/she will going to encrypt the message with receiver's identity and identity may be anything like name, place, mail address etc. Then at the receiver's side message will be decrypted with the private key generated by the Private Key generator (PKG). But in our system along with that for more improvement we are also using the key update on time bases and along with that most of the process will be done offline only.

2. Main Idea

As the identity based encryption do not support the public key infrastructure and it have its own public key system. In identity based public key system there is requirement of user and one trusted party who will responsible to handle the secret key. So basic idea in this system is that the user who want to save its data to the cloud he/she have to first encrypt the data with some parameters of its own file and send It to the cloud but if the user want to send data to some person then he/she have to encrypt the file with the receiver's identity and send it to that person and after the file is encrypted and send to the next user then for decryption purpose the receiver will demand for the key to the sender and sender will send key to cloud service provide over the secure channel. Then Cloud service provider will going to send that key to receiver through its register mail id and at last the user will able to access that file using its appropriate secret key. One more thing is added is that whenever the person who wants to save data to the cloud he/she can save it and every time the data is send to the cloud, each time new time updated key is generated for that user.

3. Literature Survey

In this paper it is defined that the "X.509 v3 and X.502 v2" are the CRL which means Certificate Revocation List which are used into the web. In this research paper the brief overview of model and approaches are used in introduction. Information related to the "X.509 v3" certificate and Internet

name forms and there formats and semantics are described in detail. Along with two internet specific extensions, standard certificate extensions are also explained in this paper. This paper also gives information about the algorithm related to the X.509 certification path validation. In this paper also describes the "X.509 v2 format" and its related information in this paper.

Cloud computing is the system which gives a huge variety of client system and the distributed access to the hardware or software which is scalable and virtualized in nature over the internet. These cloud computing systems featuring us on demand provisioning of computation resources. Three service models are present in cloud computation system and they are "infrastructure as a service (IaaS), platform as a service (PaaS) and software as a service (SaaS)". IaaS provide us an infrastructure on cloud so that the user can able to install their own applications to use that cloud services. PaaS provide the platform to develop the application or anything else like in online web development. SaaS provides to install the application on the cloud so that all the users can able to access or use that services as like in mailing services. Cloud computing consist of four type of infrastructures. (i) Private cloud which is used by the organization for storing or accessing sensitive information. It is costly in nature and all the rights are owned by the organization. (ii) Public cloud which is used by anyone and everyone, it can be free and paid model example dropbox. (iii) Hybrid cloud which is combination of both public and private clouds. In this cloud provider offer shared storage as a public cloud and provides dedicated computing as a private cloud.

In this examination paper it was Showcase a Generalized Priority calculation for effective execution of assignment and correlation with FCFS and Round Robin Scheduling. The Algorithm is tried in cloud Sim toolbox and the outcomes gave better execution contrasted with other customary booking calculations. To start with Come First Serve will sit tight for the principal undertaking to originate from holding up line and after fruition of that lone the following errand will be taken for the further handling. Round Robin Scheduling will give a reasonable time stamp to every one of the errands. The cloud sim toolbox bolsters Round Robin system for interior planning of employments. The disadvantage of RR is that the biggest employment sets aside enough time for finishing. General Priority Algorithm in this the client characterize the need as per the client request the parameter of the cloudlet will be characterized like memory, size, transfer speed booking strategy, and many other things. In this proposed method, the undertakings are first of all developed by their size to such an extent that on the off chance that one of the errand having most elevated size then its positioning will be more impressive. "The Virtual Machines are" likewise positioned" (organized) as indicated by their "MIPS" (Million guidelines for each second) esteem with the end goal that the one who is having most impressive MIPS has the most higher rank. Along these lines, the main component for arranging assignments "is their size and for VM is their MIPS." This approach is performing much better than FCFS and Round Robin planning.

Pairings on elliptic bends are fast returning more developed as cryptological primitives for arrangement in new security applications, quite inside the setting of executions of Identity-Based Encryption (IBE)." In this paper it is having a tendency to depict the usage of differed pairings on breakthrough "32-Bits Smart-Card, the Philips Hipersmarttm, A portrayal of the MIPS-32 fundamentally based smartmipstm engineering". 3 sorts of matching are considered, starting the quality John Orley Allen Tate blending "On A nonsupersingular bend E(Fp), second the ate matching, conjointly on a nonsupersingular bend E(Fp), and inevitably the Ht Pairing an a supersingular Curve E(F2m)". we have a tendency to show that pairings are regularly ascertained as quickly as great cryptological primitives on this plan, with a count time of as next to no as zero.15 Seconds.

Now a day mobile devices are computing on low power so accordting to it protection theme style could be a significant acceptance. "The public key for Identity Based System along with linear pairs outlined on elliptic curves gives a versatile approach to realize simplifying the certificate

management." "Within the past, several user authentication schemes with linear pairings are planned. In 2009, Goriparthi Et Al. additionally planned a replacement user authentication theme for Mobile Client–Server surroundings. However, these schemes don't give mutual authentication and key exchange between the consumer and also the server that area unit necessary for mobile wireless networks." During this research paper, its have a tendency to gift a replacement user authentication and exchange the key protocol victimization linear pairings for surroundings of Client–Server of moble. "As compared with the recently planned pairing-based user authentication schemes, our protocol provides each Mutual Authentication and key exchange. Performance analysis is created to indicate that our conferred protocol is similar temperament for mobile Client–Server surroundings. Security Analysis is given to demonstrate that our planned Protocol is incontrovertibly secure against previous attacks.

We gift 2 new schemes for economical certificate revocation. Our 1st theme may be a direct improvement on a widely "known Tree-Based Variant Of The NOVOMODO System Of Micali [11]. Our second theme may be a direct improvement on a Tree-Based Variant Of A Multi-Certificate Revocation System By Aiello, Lodha, And Ostrovsky [1]. At The core of our schemes may be a novel construct termed a Quasimodo tree that is sort of a Merkle Tree however contains a length-2 chain at the leaves and conjointly directly utilizes interior nodes. This idea is of freelance interest, and that we believe such trees can have various different applications. The idea, whereas easy, directly provides a strict improvement within the relevant time and communication complexities over antecedently printed theme.

Identity Based Encryption (IBE) is an" energizing contrasting option "to Public-Key Encryption, as IBE" wipes out the requirement "for a Public Key Infrastructure (PKI)." "Any setting, PKI-Or Identity-Based, must give a way to repudiate clients from the framework. Viable repudiation is a Well-Studied issue in the conventional PKI Setting. However in the setting of IBE, there has been little work on concentrate the denial systems. " The most reasonable arrangement "requires the senders to likewise utilize eras when encoding, and every one of the beneficiaries (Regardless Of Whether Their Keys Have Been Compromised or Not) to refresh their private keys frequently by reaching the put stock in expert." "We come with an IBE conspire that essentially improve key-update effectiveness in the side of the put stock in gathering, where it is remaining gifted for the clients

4. Existing System

In the present era there are many systems proposed in the market which can able to secure the system or communication system using various encryption techniques. There are many encryption techniques which are present like RSA (Rivest, Shamir, and Adleman), Deffie Hellman Encryption, DES, Double DES, Triple DES, etc. so these are the techniques which are used for data encryption. So our existing system is like sending data to the server but simply sending data to the server and saving it by encrypting to the server. This is secure but it will going to create two problems and which are: First, whenever the users will increase then it will required of big server of more space which will create problem in scalability and if we increase server then it will increase more complexity. Second is that due to the increase in server it will also increase the maintenance cost of the system. So to overcome this problem cloud services are added to the system, in which data are saved directly to the cloud but it also came with some security issue. Then new security was introduced in which a trusted authority was there which was used to generate the keys to encrypt and decrypt the messages which helps to maintain secure and safe communication between the two parties but still it was not much secure and time consuming and even the sender and receiver should to be online, Which means both parties are to be online at the time of communication or sending data even for the encryption or decryption also they are compulsory to be online and which consumes much time for all this process. So to overcome all this drawbacks we come with new system in which we had come to overcome all the problems.

5. Proposed System

As due to the more and more issues related to the data encryption and its security we come with a new system which will secure our data over the cloud and server both. Working of our system in such manner, Suppose the person want to use our system then he/she have to first register with our system so that he/she able to enjoy our securities over the system. After the registration, suppose the user is data owner and he/she wants to save the confidential data over the cloud, then the person have login in into the system and upload there file over the cloud and through that data the server will generate the master key and send it to the CRA. And other key will be identity key which will be provided to the end user or the person who want to access data or file with the medium of a secure channel. And whenever the new data will be added to the cloud, everytime CRA will provide the time update key to the user. And if suppose in the scenario of two user when one of them want to access the data of the other then for the security purpose the receiver will request for the data to the data owner and only with the data owner permission only the receiver will able to access the file from the server. Suppose a normal user wants to fetch a file of any data owner then he have to select file and will going to send request then whenever data owner will come online he can see in request module of data owner and accept request for the file demand by the normal user. So for that the sender will accept the request and send private key to the cloud which was created with the combination of Plaintext, Receiver's ID and time period. Then the request will be send to the cloud and cloud administration will going to send private key of that file to the file seeker or data seeker through the mail or on its register mail address And at the receiver side the key will be decrypted and through that key he/she will able to access the requested file form the cloud. But if he/she is an unauthorized person then that person's information will be shown in hacker's detail at the cloud side. And may be later on person will be blacklisted from the server or database or blocked to access the data over the cloud. Now in this system more and more security was implemented as like at the time of uploading the file, the data owner upload file and time of sending it got encrypted and then send to the cloud for the storage. And also the time of download at receiver's side whenever the user got mail of secret key and when he enter the key and download at that time the file got decrypted.

6. Conclusion

This idea is related to the cloud security using Identity Based Encryption which will allow users to make their data more secure as compare to before. It will make data to travel secure over the network and even no unauthorized person will able to access without any permission of the data owner. This system also cares about the user's data which is stored and is in encrypted format so that it can achieve more security. All the uses can trust on this system for the storage and also for the access the data. Even this system will also show the details of hackers, the person who will try to access data illegally from the cloud, without any data owner's information.

For the future work, as soon as the new technology introduced and as the time spent new techniques are introduced and the current techniques are expired so to make this system for long lasting we will try to add more encryption techniques into the system so that the data will always be secure and valid for the long period of time. Along with that the details which are stored in the hacker details, so to make more secure we do some analysis part on that hacker who is trying to access the data illegally and monitor the activities of that person and according to that we will block that person form the system.

References

[1] J. Li, X. Chen, C. Jia, and W. Louue 2015, IEEE Tran. on Computers, vol. **64**, no. 2, pp. 425-437.

[2] J.-H. Seo and K. Emura 2013 Proc. CT-RSA'13, LNCS, vol. **7779**, pp. 343-358.
[3] J.H. Seo and K.L. Emura, 2015, Proc. CT-RSA'15, LNCS, vol. **9048**, pp. 106-123.
[4] Y.-M. Tseng. and T.-T. Tsai, 2012, Computer Journal, vol.**55**, no.4, pp. 475-486.
[5] S. Galbraith, K. Paterson, and N. P. 2008, Smart Discrete Applied Mathematics, vol. **156**, no. 16, pp. 3113-3121.
[6] T. Kitagawa, P. Yang, G. Hanaoka, R. Zhang, K. Matsuura, and H. Imai 2006, Proc. ACISP'06, LNCS, vol. **4058**, pp. 348-359.
[7] T.-Y. Wu and Y.-M. Tseng 2010, Computer Networks, vol. **54**, no. 9, pp. 1520-1530.
[8] B. Lynn 2015, Java Pairing Based Cryptography Library (JPBC).
[9] J. Li, Y. Shi, and Y. Zhang 2015, International Journal of Communication Systems vol **10** no 7, pp 3339-3352.
[10] C Kaufman, P. Hoffman, Y. Nir, P. Eronen, and T. Kivinen 2014 IETF, RFC 7296.
[11] A.Freier, P. Karlton, and P. Kocher 2011, IETF, RFC 6101, 2011.
[12] H.-S. Ju, D.-Y. Kim, D.-H. Lee, H. Park, and K. Chun 2006, Proc.APWeb2006, LNCS, vol.**3841**, pp. 720-725.
[13] A. Boldyreva, V. Goyal, and V. Kumar 2008, Proc. CCS'08, pp. 417-426.
[14] A. Sahai and B. Waters 2005 Proc. Eurocrypt'05, LNCS, vol. **3494**, pp. 557-557.
[15] B. Libert and D. Vergnaud 2009 Proc. CT-RSA'09, LNCS, vol. **5473**, pp. 1-15.
[16] J H Seo and K Emura, 2013 Proc. PKC'13, LNCS, vol. **7778**, pp. 216-234.