Improving Security of Cloud Using Inter cloud Identity Management Protocol

Ms. Snehal Gaikwad
Department of Information Technology
Abha Gaikwad-Patil College of Engineering
Snehalgaikwad2709@gmail.com

Prof. Pragati Patil Bedekar
Department of Computer Science and Engineering
Abha Gaikwad-Patil College of Engineering
Pragatimit@gmail.com

Abstract- Cloud computing is the new era to providing various services to the customer at low cost. Many companies start to provide various cloud computing services for users at the same time these services also go with some security problems. Now most of cloud computing systems provide digital identity for users to access their services; this will bring some difficulty for a hybrid cloud that includes multiple private clouds or inter clouds system. Today most cloud computing system use asymmetric and conventional public key cryptography techniques to provide more data security and authentication. Identity-based cryptography has provided the new characteristics that seem to fit well the requirements of cloud computing. In this paper we are implementing the high security measures to the inter cloud system using the AES encryption techniques.

Keywords-*Cloud computing, cryptography, digital identity, intercloud.*

_____*****_____

1. Introduction

Cloudcomputing is another registering and deliberate model that gives the Cloud computing administrations and a lot of figuring assets to the clients. Clients can procure processing asset, storage room and different sorts of programming administrations as indicated by their requirements [2]. In Cloud computing, with a lot of different registering assets, clients can undoubtedly comprehend their issues with the assets gave by a cloud. This brings extraordinary adaptability for the clients. Cloud computing has run with new difficulties and open doors for verification to the cloud. There is expanding request that ready to verification for get to administrations in cloud and information for both association and customers. Personality administration is a standout amongst the most unfavorable variables that impact the accomplishment of Internet business applications [3]. Private mists, additionally called interior mists, are the private systems that give Cloud computing administrations to the arrangement of clients inside inner system. Personality administration offers the high security in a mixture cloud that comprising various specialist co-ops has troublesome particularly for key conveyance and shared validation. Clients to get to the administrations in a cloud, a client computerized character is expected to deal with the get to control in cloud. Personality based cryptography is an open key innovation that are utilized to distinguish the approved client utilizing open key [2]. In this paper we are propose the cryptography based calculation to give the high security and take care of the issue of character to entomb cloud framework.

1.1. Background details

1. SafiriyuEludioraet. al. propose user identity management protocol for cloud computing customers and cloud service providers. This protocol will authenticate and authorize customers/providers in other to achieve global security networks. The protocol will be developed to achieve the set global security objectives in cloud computing environments. Confidentiality, integrity and availability are the key challenges of web services' or utility providers. A layered protocol design is proposed for cloud computing systems, the physical, networks and application layer [1].

2. Liang Yan et. al. proposed the federated identity management in the cloud such that each user and each server will have its own unique identity, and the identity is allocated by the system hierarchically. With this unique identity and hierarchical identity based cryptography (HIBC), the key distribution and mutual authentication can be greatly simplified [2].

3. Pankaja A. Hadoleet. al. proposes a system which is designed to improve the communication protocol in mobile computing. By improving means just to overcome the limitations of existing protocols. The Improved identity management protocol will minimize the network overhead for network companies which ultimately maintain the balance between profit and investment for network companies. In proposed scheme, authors has successfully improve upon IDM3G to design a fair and secure digital rights management of multimedia over 3G networks, which makes our proposed scheme more practical and easy to

implement in the future [3]

4. Bharat Bhargava et. al. proposed and to extend the Microsoft's CardSpace identity management tool, to include more robust security tokens using the zero knowledge proof concept. These security tokens are in the form of SAML token supported by Windows Communication Foundation (WCF) and authors can prove interoperable with the existing security platforms [5].

1.2 Identity Management:

Character management is a vast authoritative level territory that arrangements with recognizing people in a client in association and make control over their entrance to the assets under that framework by partner client rights and confinements with the built up personality. Character management have many difficulties, for example, provisioning, validation and the utilization of solid confirmation and to guarantee the responsibility of outsiders recovering touchy data and computerized marks to offers non-renouncement of online exchanges. Confirmation will require an association to have the way to give qualifications and to oversee them in simple way for their utilization in standard web situations. In the event that an association needs to guarantee that the client is the correct client before giving any accreditations, then it should either utilize a genuine information source, for example, an administration information source or individual face to face, getting ID data. For Strong confirmation, it must be require that advanced ID endorsement and numerous verification elements to ensure the data and information of any association. Some particular association environment take the fingerprints for confirmation [4].

1.3 Need Of Identity Management

What is a risks? In terms of security, identity management in cloud computing is one area that will require increased attention if those benefits are to be fully realized. In order to access the sensitive data or information and resources, all the organizations monitors which person are accessing the resources or data in cloud and to ensure that they are accessing the data or resources in an appropriate manner.

Confidentiality: Preserving authorized restrictions on access and disclosure, including means for protecting personal privacy and proprietary information.

Integrity: Guarding against improper information modification or destruction; includes ensuring information non-repudiation and authenticity.

Availability: Ensuring timely and reliable access to and use of information to the users.

Security is not a component; it is a property of a framework. It comes about because of careful investigation of security necessities, sound engineering and plan, and secure coding hones [12]. Staff security likewise improve these elements associations need to agree to standards and controls set around the cloud specialist organizations for the cloud clients

The asset bookkeeping issue has been examined by various specialists. Have perceived the issue and proposed a component, TastefulCloud Interposition, for sharing the application setting data crosswise over multi-layered servers to bolster activities, for example, upholding asset quantity.

They characterized the setting reflection that incorporated the personality of the customer and accomplished the formation of the unique situations and spread of them crosswise over server through change of OS and applications. Clients are required to recompile the application in the wake of augmenting.

Depicted design, for following the vitality utilization of implanted gadgets. To accomplish the objective of vitality following, they have built up a structure for asset bookkeeping of Clouddevices. Since their objective surroundings is inserted frameworks, they could bolster the situation in which they make changes to the OS piece and require the engineers to compose applications that tell the OS of the proprietor of different exercises.

2. Methodology Used

In the existing systems, the cloud designers have tried a lot of variations in security approaches to secure the cloud from any unwanted usage. But due to intercloud systems, identity management has been a major issue, which needs to be solved for providing security to the system. In the current systems, this is not done because of which the current cloud systems pose a higher security threat. To avoid the problem of identity management, we propose a 3 layered security system, which is based on,

a. Sending request for an operation.
b. SMS based security to prove request is legitimate
c. User permission based model to accept/reject the request and perform an action.

2.1 System Description

First the user will send a request to the cloud to perform an action, this action can be modification/addition or removal

of data from the system. The request code will be sent to the registered user's cell phone via SMS, if the user is legitimate then the code will be entered on the system, after which the request can be accepted or rejected by the creator of the particular data. This 3 layered model will allow the cloud to be extremely secure and will reduce attacks happening on the cloud. For the security issue we implement a standard AES algorithm.

The following things are done by the system,

1. Android service for OTP sending, only to registered numbers.
2. Request generation for download/delete the files.
3. Report of users who are trying to sneak into our files.
4. File security for upload and download.

The system modules includes user login, application encryption process, decryption processand message sending API functionality that help to achieve security. Whenever user download any file from cloud it send message to user registered mobile number and secret key to user.

Same way it also send message to user if other user want to access the data or file that uploaded by user .the user has privilege to accept or reject the on other user request.

We have developed a model, where security workload is totally separated from the service logic and also observed that it is possible to separate security functions from business activities, encapsulate them into services, a reusable secured service, and a business service, then combine or merge them to achieve secured services without burdening the developer from coding the security code over and over again, so the developer of the service will concentrate on the business logic of the service itself not the security issues. To sum up, one time security service is done, but used several times with many services independent from each other. So developed model is satisfying and targeting developers who are building cloud-based services where they can implement directly the security logic in order to get a secured cloud services. However, as the number of users using the security service increase, accessing this centralized service can experience delays.

3. Result Analysis

In this section we are analyze the system working and to shows the various snapshots.

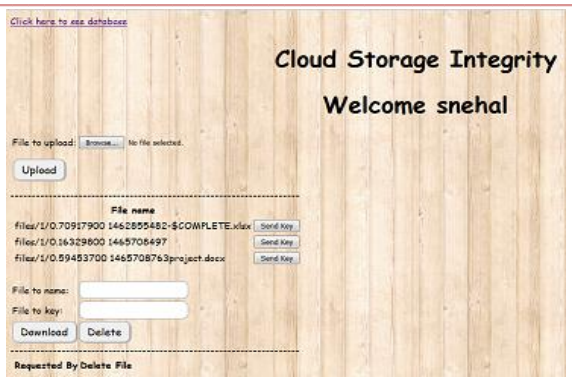

Fig. 1 (a) Upload/Download file

Fig. 1(a) shows the windows of Upload/Download file the file from inter cloud. If user want to upload the any file from computer to the cloud, first user will browse the file from computer and the attach after that user will be upload the file to cloud.

Fig 1 (b) Upload/Download file

Fig. 1 (b) shows user has successfully upload the file to cloud. If user want to download any file from cloud, user request for the code/key. If the user are registered code/key will be sent via sms to user's mobile number. User must enter the file name and associate file key to the text field and then download the file.

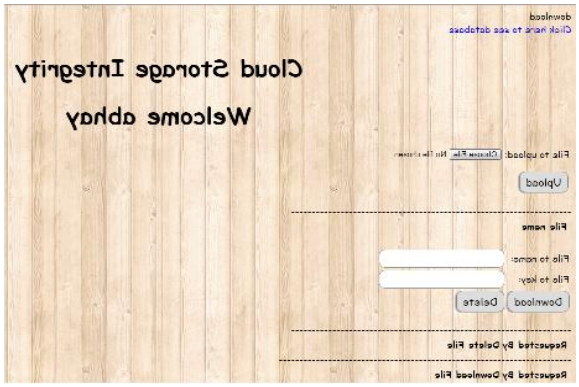

Fig. 1 (c) Upload/Download file

Fig. 1 (c) shows if another user try to upload/download the file from cloud but he is not registered user. System will automatically sent the sms to registered user and shows the

user is legitimate then the code will be entered on the system, after which the request can be accepted or rejected by the creator of the particular data

Fig. 2 User log record

Fig. 2 showsthe window of user log record. The number of registered user are upload/download the to/from cloud. The system maintains the log record for each registered user and show the log record on screen.

4. Conclusion

In this paper we need to ponder on the issue of asset bookkeeping and control inside an IT stage that offers shared administrations. Keeping in mind the end goal to comprehend the way of the issue and discover bearings for successful arrangement we will investigate two diverse bookkeeping procedures worked with various adjust of accentuation. One of them is a model asset bookkeeping and control system that works at the hypervisor. It joins the observing unit that gathers fine-grained string level information and the induction unit that applies light-weight surmising.

5. References

[1] Safiriyu Eludiora, Olatunde Abiona, AyodejiOluwatope, AdeniranOluwaranti, Clement Onime, Lawrence Kehinde, “A User Identity Management Protocol for Cloud Computing Paradigm”, Int. J. Communications, Network and System Sciences, 2011, 4, 152-163, doi:10.4236/ijcns.2011.43019 Published Online March 2011.

[2] Liang Yan, ChunmingRong,Gansen Zhao “Strengthen Cloud Computing Security with Federal Identity Management Using Hierarchical Identity-Based Cryptography”, CloudCom 2009, LNCS 5931, pp. 167–177, 2009. © Springer-Verlag Berlin Heidelberg 2009.

[3] PankajaA.Hadole, Prof. JayantRohankar, Prof. PriyankaAmbatkar, Prof.ArunKatara, “ Development of Secure Mobile Cloud Computing Using Improved Identity Management Protocol”, International Journal on Recent and Innovation Trends in Computing and Communication, 645 – 650, Volume: 2 Issue: 3, March 2014.

[4] “Identity and risk management: Preparing for a new world”, CGI Group Inc., © 2012.

[5] Bharat Bhargava ,Noopur Singh , Asher Sinclair, “Privacy in Cloud Computing Through Identity Management”.

[6] Antonio Celesti, FrancescoTusa ; Massimo Villari ; Antonio Puliafito, “Security and Cloud Computing: InterCloud Identity Management Infrastructure”, Enabling Technologies: Infrastructures for Collaborative Enterprises (WETICE), 2010 19th IEEE International Workshop on, 263 – 265, 28-30 June 2010.

[7] S. Agarwala, F. Alegre, K. Schwan, and J. Mehalingham. E2eprof Automated end-to-end performance management for enterprise systems.In*Proceedings of 37th Annual IEEE/IFIP Intl. Conf. on Dependable*

[8] *Systems and Networks*, DSN ’07, pages 749–758. IEEE, 2007.[3] Amazon SimpleDB. http://aws.amazon.com/simpledb/.

[9] G. Banga, P. Druschel, and J. C. Mogul. Resource containers: a new facility for resource management in server systems. In *Proceedings of the 3rd symposium on OSDI*, pages 45–58, Berkeley, CA, USA, 1999.USENIX Association.

[10] P. Barham, A. Donnelly, R. Isaacs, and R. Mortier. Using magpie for request extraction and workload modelling. In *Proceedings of the 6th conference on Symposium on OSDI*, Berkeley, CA, USA, 2004.

[11] [M. Y. Chen, A. Accardi, E. Kiciman, J. Lloyd, D. Patterson, A. Fox, and E. Brewer. Path-based faliure and evolution management. In *Proceedings of the 1st conference on Networked Systems Design and Implementation*,Berkeley, CA, USA.

[12] Bernstein, D., Vij, D., Intercloud Directory and Exchange Protocol Detail using XMPP and RDF, Proceedings of IEEE 2010 International Workshop on Net-Centric Service Enterprises: Theory and Application (NCSE2010) (2010)

[13] [B. F. Cooper, A. Silberstein, E. Tam, R. Ramakrishnan, and R. Sears. Benchmarking cloud serving systems with ycsb. In *Proceedings of the1st ACM symposium on Cloud computing*, SoCC ’10, pages 143–154,New York, NY, USA, 2010. ACM.

[14] A. Dinaburg, P. Royal, M. Sharif, and W. Lee. Ether: malware analysis via hardware virtualization extensions. In *Proceedings of the 15th ACM conference on Computer and communications*

security, CCS '08, pages 51–62, New York, NY, USA, 2008. ACM.

[15] R. Fonseca, P. Dutta, P. Levis, and I. Stoica. Quanto: tracking energy in networked embedded systems. In *Proceedings of the 8th USENIX conference on Operating systems design and implementation*, OSDI'08, pages 323–338, Berkeley, CA, USA, 2008. USENIX Association.

[16] S. Ghemawat, H. Gobioff, and S.-T. Leung. The google file system. In Proceedings of the nineteenth ACM symposium on Operating systems principles, SOSP '03, pages 29–43, New York, NY, USA, 2003. ACM.

[17] D. Gupta, L. Cherkasova, R. Gardner, and A. Vahdat. Enforcing performance isolation across virtual machines in xen. In Proceedings of the ACM/IFIP/USENIX 2006 Intl. Conference on Middleware, Middleware '06, pages 342–362. Springer-Verlag New York, Inc., 2006.

[18] E. M. Haber, E. Kandogan, and P. Maglio. Collaboration in system administration. Queue, 8(12):10:10–10:20, Dec. 2010.

[19] B. Hindman, A. Konwinski, M. Zaharia, A. Ghodsi, A. D. Joseph, R. Katz, S. Shenker, and I. Stoica. Mesos: A platform for finegrained resource sharing in the data center. In Proceedings of the 8th

[20] USENIX Conference on Networke Systems Design and Implementation, NSDI'11, pages 295–308, Berkeley, CA, USA, 2011.

[21] Introducing the Windows Azure Paltform. http://go.microsoft.com/?linkid=9752185.

[22] A. John Levon. Oprofile. http://oprofile.sourceforge.net/credits/.

[23] Peer to Peer, http://en.wikipedia.org/wiki/Peer-to-peer

[24] W3C Semantic Web Activity, http://www.w3.org/2001/sw/

[25] Aberer, K., Cudr´e-Mauroux, P., Hauswirth, M., and Van Pelt, T.:GridVine: Building Internet-Scale Semantic Overlay Networks,International Semantic Web Conference, volume 3298 ofLecture Notes in Computer Science, pages 107–121. Springer(2004).

[26] Cai, M. and F. Martin.: RDFPeers: a scalable CloudRDFrepository based on a structured peer-to-peer network.,WWW '04: Proceedings of the 13th international conference onWorld Wide Web, pages 650–657, New York, NY, USA. ACMPress (2004).

[27] Tatarinov, I., Ives, Z., Madhavan, J., Halevy, A., Suciu, D., Dalvi,N., Dong, X., Kadiyska, Y., Miklau, G., and Mork, P., ThePiazza Peer Data Management Project. SIGMOD Record, 32(2003).