International Journal of Research (IJR)
e-ISSN: 2348-6848, p- ISSN: 2348-795X Volume 2, Issue 10, October 2015
Available at http://internationaljournalofresearch.org

Result Paper on Security in Hybrid P2p Networks Using Saas and Multicast Key Management

[1*] Nikhil Sawarkar & [2] Prof.Roshani Talmale

[1] Department of Computer Science and Engineering, RTMNU University, TGPCET Nagpur, Maharashtra, India

* Nikhil Sawarkar Email: nikhil.sawarkar01@gmail.com
Telephone: +91 9623296318

ABSTRACT

Cloud computing is the innovation that uses the web and focal remote servers to keep up information and applications. Cloud computing permits buyers and organizations to utilize applications without establishment and access their individual records at any machine with web access. This engineering takes into consideration significantly more productive processing by concentrating stockpiling, memory, and preparing and transmission capacity. In this security is a paramount issue to give a security to this cloud we present a novel system for securing cloud by giving multicast key to every client. It will be an element session key which will fluctuate in the time of period. At whatever point another client enters into the cloud the new key will be produced .It will withstand for a period .After that time period the client ought to restore the key for the further use of the cloud.

KEYWORDS: Cloud; Multicast Key Management; Encryption; SaaS

INTRODUCTION

Distributed computing shows an opportunity for pervasive frameworks to power computational and stockpiling assets to achieve errands that would not typically be conceivable on such asset obliged gadgets. Distributed computing can empower fittings architects to construct lighter frameworks that last more and are more versatile. Notwithstanding the preferences distributed computing offers to the originators of pervasive frameworks, there are a few impediments of leveraging distributed computing that must be tended to.

Distributed computing, or in less complex shorthand simply "the cloud", additionally concentrates on expanding the adequacy of the imparted assets. Cloud assets are typically imparted by numerous clients as well as progressively reallocated for every interest. This can work for assigning assets to clients. For instance, a cloud machine office that serves European clients amid European business hours with a particular application (e.g., email) may reallocate the same assets to serve North American clients amid North America's business hours with an alternate application (e.g., a web server). This methodology ought to boost the utilization of processing power therefore lessening ecological harm too since less power, cooling, and so forth are needed for an assortment of capacities. With distributed computing, numerous clients can get to a solitary server to recover and redesign their information without obtaining licenses for distinctive applications.

In this security is a paramount issue to give a security to this cloud we present a novel technique for securing cloud by giving multicast key to every client. It will be an element session key which will differ in the time of period. At whatever point another client enters into the cloud the new key will be created .It will withstand for a period .After that time period the client ought to recharge the key for the further utilization of the cloud.

BRIEF LITERATURE SURVEY:

Information must be secure when it goes between your site and the cloud and must be secured in the cloud, venture the whole time is verifying that the information is additionally ensured amid exchanges, for example, if a representative or client has the capacity access information in an application exchange transforming Especially for exchange handling, this implies experiencing the procedure of verifying information is secure and believing the supplier, yet retreating to check the security. With this set philosophy of secure multicast key administration on cloud is been ensured .The cloud clients are assembled as indicated by their investments for (e.g. business, news, diversion and so forth.). For each one gathering an alternate set of keys been accommodated every clients .Each gathering is been structurized as tree (K.Sriprasadh 2013).

Another way to secure is to use 2 way hash functions. Cryptographic hash capacities have been broadly utilized as a part of a different security applications, for example, trustworthiness insurance and confirmation. Beneath demonstrates to, proper methodologies to utilize two hash fastens to lessen key administration overhead in BMS.(Shweta M. Kulkarni 2013).

(Wenjun Luo 2012) introduced a various leveled personality based signcryption key administration plot in distributed computing. Their answer receives character based signcryption engineering. Personality based signcryption gives security insurance and unforgeability as well as is more proficient way than a piece of an encryption plan with a mark plan. The character of substances which executes as open key, can improves key administration in distributed computing. By our various leveled arrangement, the versatility in cloud computing additionally is unraveled.

PROPOSED SYSTEM

The proposed work is planned to be carried out in the following manner

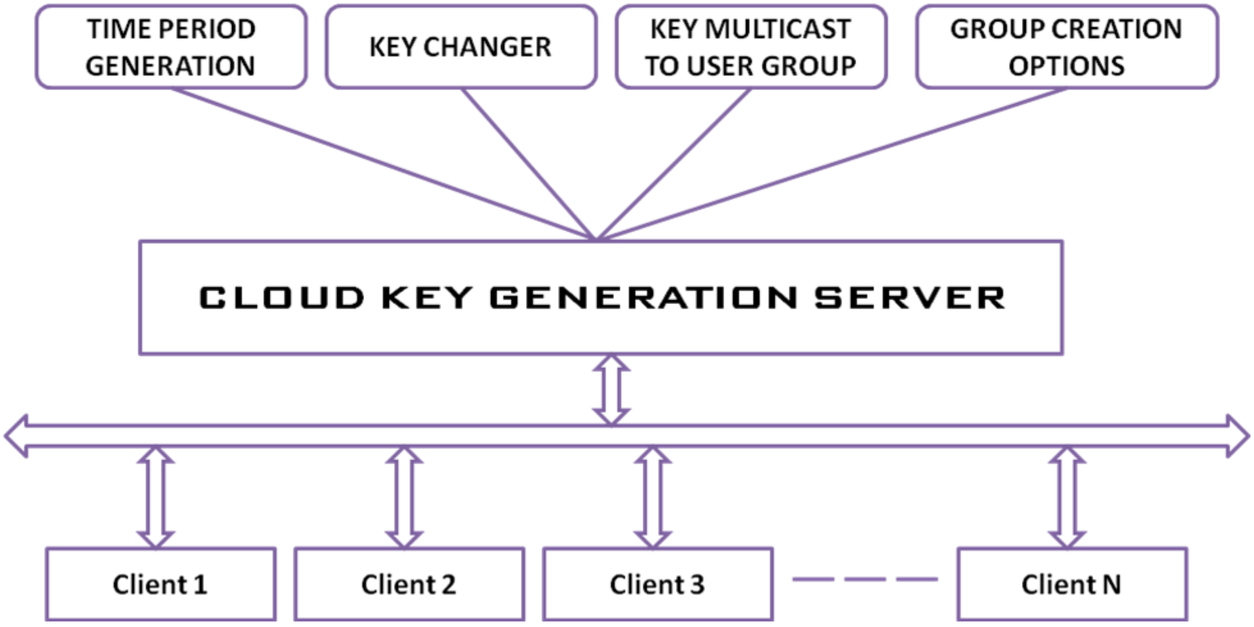


Figure.1: Basic system architecture

1. Keys:
The dynamic parts of the gathering get security emphasized affiliations that incorporate encryption keys, verification/honesty keys, cryptographic arrangement that depicts the keys, and characteristics, for example, a record for referencing the security affiliation (SA) specific articles contained in the SA.

2. GCK Srole:
Notwithstanding the approach connected with gathering keys, the gathering holder or the Group Controller and Key Server (GCKS) may characterize and authorize bunch enrollment, key administration, information security, and different arrangements that could possibly be imparted to the whole participation.

3. Periodic refresh of keys:
The determined survival of the keys are periodically refreshed

4. Maintenance protocol during addition and removal of group members:
The convention ought to encourage expansion and evacuation of gathering parts. Parts who are Included may alternatively be denied access to the key material utilized before they joined the gathering, and evacuated parts ought to lose access to the key material after their flight.

5. The convention ought to help an adaptable gathering rekey operation without unicast trades in the middle of parts and a Group Controller and Key Server (GCKS), to abstain from overpowering a GCKS dealing with a huge gathering.

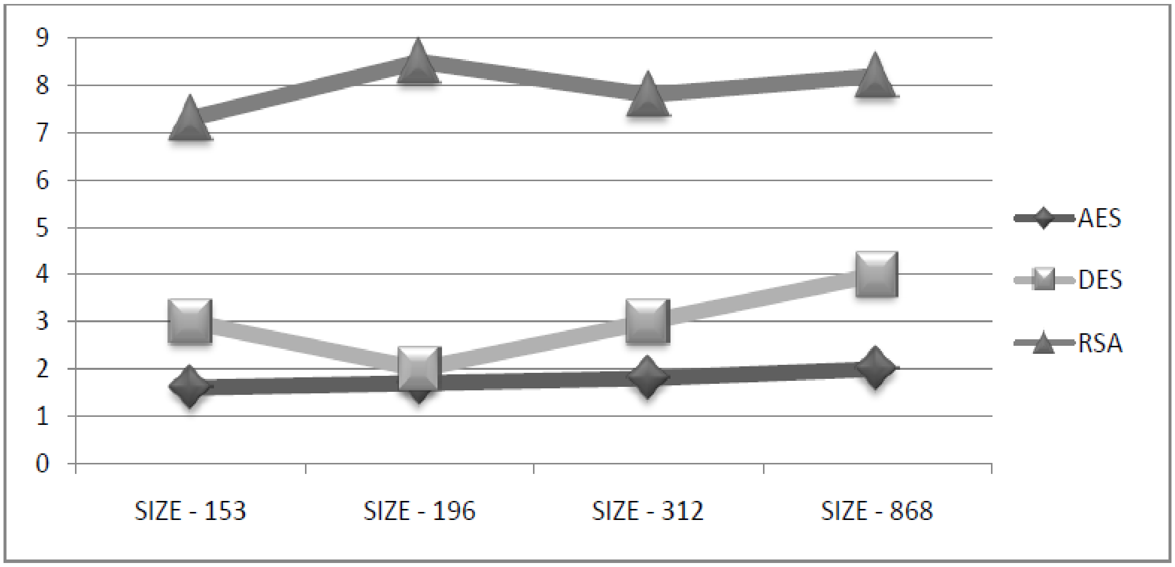
6. The key administration convention ought to offer a structure for supplanting or recharging changes, approval framework, and verification frameworks.

Result Analysis

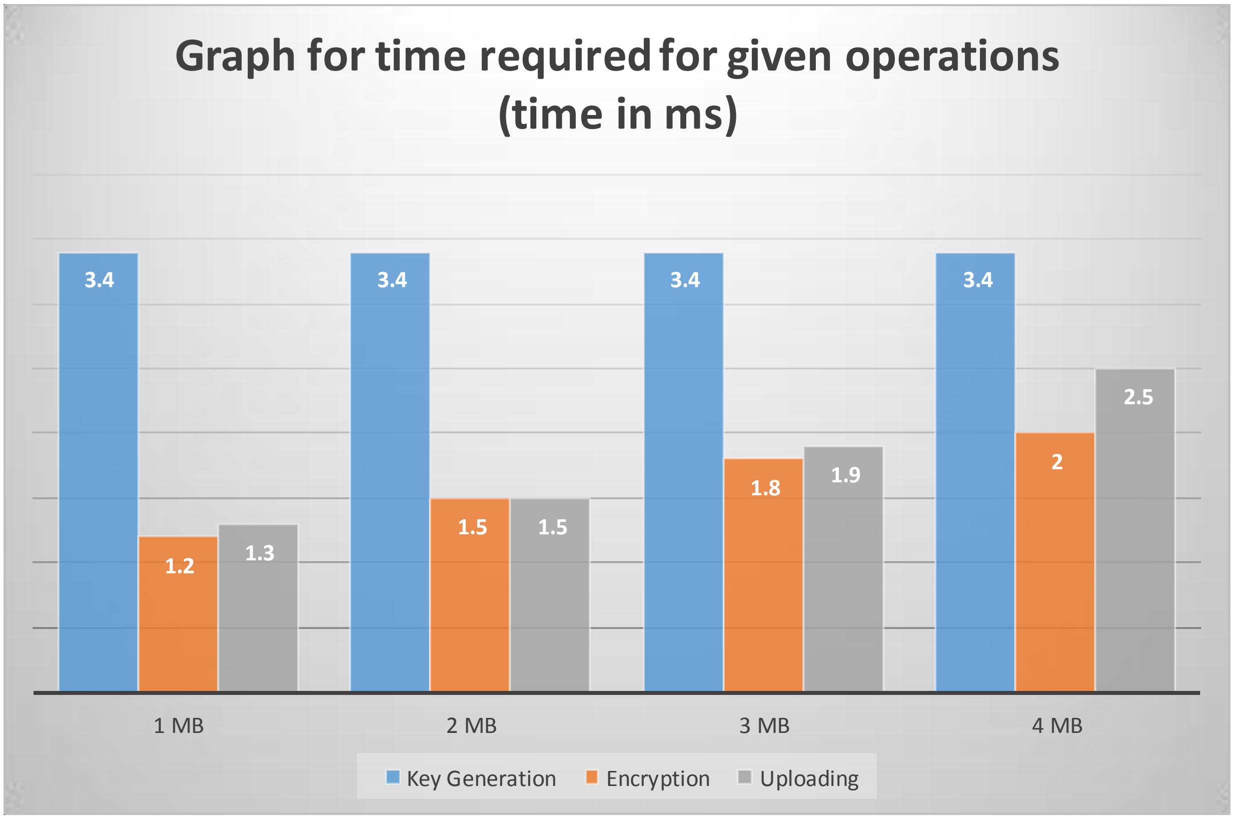
Comparison between Symmetric Algorithms

Input	**AES**	**AES Cloud**	DES	DES Cloud	BLOWFISH	BLOWFISH Cloud	Desede	Desede Cloud
10 Kb	11.5	1.5	7.5	2	4	2	12	4.5
13 Kb	14.7	2	10	2.5	4.7	2	15.5	5.25
39 Kb	21	3	31.5	6.5	8.25	2.75	47.25	10.25
56 Kb	24.5	3.75	50.25	9.25	15.7	3	70.5	14.5

Graph based Comparison of AES DES and RSA



Encryption Time



Conclusion

Multicast key management will provide better security for the cloud forthe secure data transaction, through keying and rekeying process. The security of the cloud can extend by applying some batch rekeying methods which will avoid further complexity in rekeying. The algorithm use for data encryption is Advanced Encryption Algorithm with 256 bit keying. With encryption we also provide a random key generation algorithm that will be generated by key server using a random key generation algorithm. The security is further extended by providing text and file encryption algorithms at the same time. The system can be used to encrypt any type of file and share within the group.

Future Scope

The file size in the proposed system is limited to 10 MB. We plan to increases the file size and at the same time we will use multiple encryption algorithms for each group. Again we plan to reduce the time complexity of rekeying again and again for each group. We plan to generate an aggregate key which can be used to reduce rekeying.

REFERENCES:

[1] A Novel Method to Secure Cloud Computing Through Multicast Key Management K.Sriprasadh Saicharansrinivasan O.Pandithurai A.saravanan International Conference On Information Communication And Embedded Systems Year 2013

[2] Generation of Shorter Length Keys for Broadcast and Multicast Services Using 2-way Hash Chain Schemes Shweta M. Kulkarni, Shubhada S. Kulkarni International Journal of Inventive Engineering and Sciences (IJIES) ISSN: 2319–9598, Volume-1, Issue-10, September 2013

[3] Hierarchical Identity-based Key Management in Cloud Computing Wenjun Luo, Min Xu Journal of Convergence Information Technology(JCIT) Volume 7, Number 20, Nov 2012

[4] Efficient Key Management Scheme for Secure Multicast in MANET J. Lakshmanaperumal, K.Than ushkodi, N.M.Saravana kumar, K.Saravanan, D.Vigneshwaran, T.Purusothaman IJCSNS International Journal of Computer Science and Network Security, VOL.10 No.11, November 2010

[5] Publicly Verifiable Secret Sharing for Cloud-Based Key Management Roy D'Souza1, David Jao,_, Ilya Mironov, and Omkant PandeyD.J. Bernstein and S. Chatterjee (Eds.): INDOCRYPT 2011, LNCS 7107, pp. 290–309, 2011. Springer-Verlag Berlin Heidelberg 2011

[6] (U.S.) Nicholas. Carr, fresh Yan Yu, "IT is no longerimportant: the Internet great change of the high ground cloud computing," The Big Switch:Rewining the World,from Edison to Google, , ITIC Publishing House, October 2008 1-1

[7] Ya-Qin Zhang, the future of computing in the "cloud - Client", The Economic Observer reported,http://www.sina.com.cn, 2008 Nian 07 Yue 12 Ri 14:30

[8] http://searchcloudcomputing.techtarget.com/sDefinition/0,,sid201_gci1287881,00.html

[9] http://www.boingboing.net/2009/09/02/cloudcomputing-skep.html