ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 5, May 2017

Analysis of Attacks and its prevention using Encryption in Cloud Computing

Anmol Bhatia[1], Gaurav Garg[2]

M. Tech, Dept. of CSE, Advanced Institute of Technology and Management, Palwal, India[1]

Assistant Professor, Dept. of CSE, Advanced Institute of Technology and Management, Palwal, India[2]

ABSTRACT: Attacks in cloud computing are becoming more dangerous problem in the globe. Analysis of attacks is more important to understand the bad impact on cloud by these attacks.Without knowing the attacks behaviour prevention is not possible.There are various encryption techniques to prevent the cloud from attacks. In this paper we are discussing the various attacks in cloud and its prevention technique that is more effective to save the cloud from attacks. On the behalf of different attacks we are also analysing some real world issues that will help us to clear the main focus of attacks prevention using encryption.

KEYWORDS: cloud computing; data security problems; real attacks; key sharing mechanism

I. INTRODUCTION

Cloud computing includes a bunch of computers that are put together wont to give completely different computations and tasks. Cloud computing is one in every of the foremost necessary IT paradigms within the previous few years. one in every of the key advantages that's offered from this IT technology for the businesses is reduced time and prices on the market. Cloud computing is providing firms and organizations to use shared storage and computing resources. it's higher than to develop and operate with the own infrastructure. Cloud computing conjointly provides organizations and firms to own a versatile, secure, and efficient IT infrastructure. It is compared with the national electrical grids that allow organizations and houses to plug into a centrally managed, economical and efficient energy supply. Main companies as well as Google, Amazon, Cisco, IBM, Sun, Dell, Intel, HP, Oracle, and Novell have invested with in cloud computing and propose a spread of cloud-based solutions to people and businesses.

There are numerous varieties and models in cloud computing relating to the various provided services. So, the cloud computing involves public cloud, personal cloud, hybrid cloud, and community cloud. Service delivery models, on the opposite hand, can be classified as SaaS (Software as a service), PaaS (Platform as a Service), and IaaS (Infrastructure as a Service). Cloud computing can be typically classified by 2 ways: by cloud computing location, and by the offered forms of services.

Cloud computing is that the terribly notable technology that gives the facilities of enormous knowledge storage and the use of computer code by paying for that [1]. Cloud computing provides the computer code as a service, platform as a service and infrastructure as a service facilities. although several options are provided by cloud computing however there ar still some holes relating to security. Among these holes we tend to take the DoS attack [2] into the thought within which associate degree wrongdoer sends pretend requests once more and once more to consume all the resources and once a legitimate request attempt to execute the method then system denies process constant request due to international organisation convenience of resources [3]. during this paper, associate degree integrated approach is introduced to forestall the pretend request by double coding of knowledge therefore the taking ofknowledge may be build tough. Two algorithms, RSA and AES are used for that integrated approach. Before discussing

DOI: 10.15680/IJIRCCE.2017. 0505215

each algorithms, easy coding and decipherment ought to be understanding. coding could be a technique within which an obvious text is reborn into a secrete text with the assistance of special key [4]. Key could also be public or personal. The secrete text is termed as cipher text. And within the same means decipherment could be a technique within which the cipher text is decoded and the original message is obtained with the assistance of key.

There are several algorithms offered for the coding and decipherment however the foremost economical technique is RSA and AES by the performance and reaction time. AES formula is that the advance coding commonplace that was developed by Joan Deaman and Vincent Rijmen [5]. Advance coding commonplace is legendary for its speed in each hardware and computer code implementation. With relation to AES, most likely the foremost powerful single-key recovery strategies designed up to now are not possible differential cryptology [6] and sq. attacks [7]. The AES technique may be used for the info blocks of 128, 192, 256 bits in ten to fourteen rounds [8]. the quantity of rounds depends upon the dimensions of the key. It will with efficiency run on the little devices. This formula may be enforced in numerous steps. 1st of all a block of knowledge is encrypted and the cipher is then settled to travel through the number of rounds. At that time, the ultimate spherical is dead that corresponds to cipher text output of ultimate spherical steps [9]. The next technique used for the encrypting the info is RSA formula. this method was developed by Ron Rivest, Adi Shamir, and author Adleman in 1977. during this technique, the message sender generates a public key to encode the message and a personal secret is generated by the receiver by victimization the secured info [10].

The wrongdoer may be confused by this method because of the inaccurate personal key will still decode the knowledge however that data are going to be in another type i.e. that may be not original message. This is often a far advanced technique. once generating the public and personal keys, the method of coding is started. In each coding and decipherment strategies the functions are created associated with the worth of public and personal keys [11].

The focus of this paper is to mix these each technique in such how that the cipher created by the AES is may be used as encrypted knowledge. And here a unique approach introduced here to shield the info on the cloud in such how that the personal key that's accustomed decode the info also will be encrypted victimization the RSA formula. consecutive step can cowl the performance comparison of all the techniques coated during this paper on the idea of various parameters and technique is called as hybrid technique.

II. RELATED WORK

In [25] the author focuses on technical security problems arising from the usage of Cloud services and particularly by the underlying technologies accustomed build these cross-domain Internet-connected collaborations. Denial of service (DoS) attacks has become a significant threat to current laptop networks. To possess a much better understanding on DoS attacks, this text provides a summary on existing DoS attacks and major defence technologies within the web and wireless networks. particularly, we tend to describe network based mostly} and host based DoS attack techniques let's say attack principles. In [26] DoS attacks are classified in line with their major attack characteristics. Current counterattack technologies also are reviewed, together with major defence merchandise in readying and representative defence approaches in analysis.

In [27] authors enforced 3 inscribe techniques like AES, DES and RSA algorithms and compared their performance of inscribe techniques supported the analysis of its stirred time at the time of coding and secret writing. Experiments results are given to analyses the effectiveness of every formula.
In [28] paper provides a summary of current cryptology analysis on the AES scientific discipline formula. Discussion is provided on the impact by every technique to the strength of the formula in national security applications. The paper is finished with a trial at a forecast of the usable lifetime of AES in these applications.

In [29] paper introduces the conception and implementation of RSA formula for security purpose and to reinforce the performance of software exploitation this formula. during this article study has done regarding RSA formula.

This study includes what's RSA formula and why they're employed in the sphere of Cryptography & Network Security.

III. Real world issues analysis

There square measure several samples of planet privacy and security problems that have affected the Cloud. These problems have provided a barrier to the worldwide adoption of the cloud. We tend to gift these problems as a listing. In 2007, Salesforce.com leaked client contact lists once AN worker disclosed the list to a phisher, and successively allowed scammers to focus on phishing attacks against Salesforce customers [12].

- In Apr 2011, Sony was concerned in an exceedingly huge security blunder that probably gave away one hundred million master card numbers. Hackers claimed to own taken uncountable master card numbers from Sony's PlayStation Network [13].
- Google disclosed in June 2011 that hackers from China scarf passwords and tried to interrupt into email accounts to steal data [14]. over one hundred individuals were affected and enclosed senior governance. individuals began to argue whether this, and the Sony incident was beginning of the downfall of Cloud computing [15].
- Hotmail and Yahoo Mail users were additionally targeted in phishing attacks [16, 17]. The attacks concerned a user either clicking a malicious link within the email or maybe viewing the e-mail itself which might then run malicious code and conceive to compromise the user's account.
- Google Docs contained a flaw that unwittingly shared user docs with unauthorised users [24]. alternative users may access and edit docs while not the Google docs owner permission.
- There was additionally the problem of Mega transfer going its uncountable legitimate users in cyber-limbo [18]. Mega transfer was a web site wherever individuals may share files. Sadly, because of the quantity of bootleg content like pirated films and tv shows, the positioning was forced to finish off in early 2012.
- A Distributed Denial-of-Service (DDoS) attack on Amazon net Services forced several firms to finish off briefly, like Bitbucket [19].
- Facebook was the target of phishing attacks in early 2012 that tried to steal user accounts and learn monetary data [20]. Once accounts were taken, the user's profile would be fastened out and the profile image would amendment. In fact, Facebook has been the target of the many phishing attacks like Rammit [21] which affected up to 45,000 users. Each of those attacks contributes heavily to user suspicion and trust of storing sensitive information within the cloud. From this list, it's clear why users square measure apprehensive regarding storing their most sensitive information within the Cloud and to achieve trust of exploitation the Cloud to store vital information, mechanisms got to be enforced to ensure information is unbroken each confidential and secure from unauthorised users.

IV. Proposed work

The Main objective of this analysis is to spice up the key management and data security in cloud computing supported secret key sharing management formula. Our projected technique helps to convey higher fault tolerance against Byzantine attacks, server colluding and data modification attack. Byzantine failure is implausibly fracture in cloud servers, within that a storage server can fail in discretionary ways that during which. On incidence of a byzantine failure system responds in random suggests that. At the aim once a Byzantine failure goes on, the framework would possibly react in any erratic suggests that, unless it's meant to method Byzantine fault tolerance. The cloud is to boot inclined to info modification and server colluding attack among that the storage servers is also compromised by the individual, as a results of that info files is also changes if they're internally consistent. Some vital entities area unit there in our planned system that area unit given below:

1. Cloud User: User will produce, Update, Delete his/her information.
2. Cloud Storage Server: It's a server wherever the information is hold on in encrypted kind.
3. Key Management Server: It'll split the key completely in several ways and store them on different share holder servers.
4. Share Holder Server: It'll store the keys from totally different users. It is additionally to blame Renewal of shares sporadically.

DOI: 10.15680/IJIRCCE.2017. 0505215

5. Log Editor: It checks the shareholder server sporadically if the share isn’t obtaining changes.
6. Security Server: Will coding and decipherment factor.

V. Conclusion and Future Work

Data Sharing and Collaboration within the Cloud is quick changing into offered within the close to future as demands for knowledge sharing continues to grow speedily. during this chapter, we presented a review on enabling secure and confidential knowledge sharing and collaboration using Cloud computing technology. We tend to examine definitions associated with Cloud computing and privacy. We tend to then check out privacy and security problems moving the Cloud followed by what's being done to deal with these problems. Security is extremely necessary feature for any technology. victimization any technology won't be value if it's not secure. However, if any technology is secured then some compromises also can be done. On more discussion and additional work may be done to lower the execution time. The main goal of this work was to investigate and judge the protection techniques for knowledge protection within the cloud computing. For that purpose, we tend to analysed and evaluated the foremost necessary security techniques for knowledge protection that area unit already accepted from the cloud computing suppliers. we tend to classify them in four sections in line with the protection mechanisms that they provide: authentication, confidentiality, access management and authorization. So, we tend to with success answered on the key queries within the cloud technology, or just aforesaid ought to cloud computing be trusty in knowledge protection. We can conclude that if all suggested measures are taken into consideration providing authentication, confidentiality, access management and authorization, then the cloud computing may be trusty in knowledge protection. We conjointly cantered on the protection problems that ought to be taken into consideration exhaustive so as to own correct knowledge security within the cloud. we tend to suggest necessary security measures regarding knowledge protection within the cloud that must be taken into consideration. We tend to conjointly projected lots of problems that ought to be thought-about so as to own improved knowledge security within the cloud computing, like correct usage of body privileges, wireless access management of the info in systems that use wireless networks, knowledge recovery and boundary defines within the cloud.

References

1. M. Zhou, R. Zhang, W.Xie, W. Qian& A.Zhou, “Security and privacy in cloud computing: A survey. In Semantics knowledge and grid (SKG)”, 2010 sixth international conference, **(2010)**; Beijing, China.
2. M. Zhou, R. Zhang, W.Xie, W. Qian, & A.Zhou, “Security and privacy in cloud computing: A survey. In Semantics knowledge and grid (SKG)”, 2010 sixth international conference, **(2010)**; Beijing, China:IEEE.”
3. Z. Muda, W. Yassin, M.N. Sulaiman, and N.I. Udzir, “Intrusion detection based on K-Means clustering and Naïve Bayes classification”, 7th International Conference on Information Technology in Asia: Emerging Convergences and Singularity of Forms (CITA), 2011
4. D.Delfs., and K. Helmut, " Introduction To Cryptography: Principles and applications", Second Edition, Springer Science & Business Media, **(2007)**; Germany.
5. G.N.Shindeand H.S. Fade War, “Faster RSA algorithm for decryption using Chinese remainder theorem”, ICCES, vol. 5, no. 4, **(2008)**, pp. 255-261.
6. E.Biham, A. Biryukov and A. Shamir, “Miss in the middle attacks on IDEA and Khufu”, *FSE’99*, volume 1636 of *Lecture Notes in Computer Science*, **(1999)**, pp. 124–138.
7. J.Daemen, L. R. Knudsen, and V. Rijmen, “The Block Cipher Square”, *FSE’97*, volume 1267 of *Lecture Notes in Computer Science*, **(1997)**, pp. 149–165.
8. R.Pahal, V. Kumar in “Efficient Implementation of AES” Dept. ECE, SGISamalkha, Haryana, India, International Journal of Advanced Research in Computer Science and Software Engineering
9. C.Ritika, S. Kuldeep, “Efficiency and Security of Data with Symmetric Encryption Algorithms”, International Journal of Advanced Research in Computer Science and Software Engineering,vol. 2, no. 8, **(2012)**, p. 1
10. N. Y. Goshwe, Department of Electrical/Electronic Engineering University of Agriculture, Makurdi “Data Encryption and Decryption Using RSA Algorithm in a Network Environment” IJCSNS International Journal of Computer Science and Network Security, vol.13, no.7, **(2013)**.
11. R.S.Jamgekar, G. Shantanu Joshi, “File Encryption and Decryption Using Secure RSA”, International Journal of Emerging Science and Engineering (IJESE), vol. 1, no. 4, **(2013)**.
12. Andy P (2007) Salesforce.com Scrambles To Halt Phishing Attacks.
13. Charles A (2011) PlayStation Network: hackers claim to have 2.2m credit cards. TheGuardian Technology Blog. Source: http://www.guardian.co.uk/technology/blog/2011/apr/ 29/playstation-network-hackers-credit-cards. Accessed on Oct 2012

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 5, May 2017

14. Whitney L (2011) Feds investigate alleged attacks on Gmail accounts. CNetnews. Source: http://news.cnet.com/8301-1009_3-20068229-83/feds-investigate-allegedattacks- on-gmail-accounts. Accessed on Oct 2012
15. Jim C, Chyen Yee L (2011) Hacker attacks threaten to dampen cloud computing's prospects. Reuters article. Source: http://www.reuters.com/article/2011/06/03/uscloudcomputing-idUSTRE7521WQ20110603. Accessed on Oct 2012
16. Dominguez K (2012) Trend micro researchers identify vulnerability in hotmail. Trend Micro. Source: http://blog.trendmicro.com/trendlabs-security-intelligence/trend-micro-researchersidentify- vulnerability-in-hotmail/. Accessed on Oct 2012
17. Choney S (2011) Hotmail, Yahoo Mail users also targets in attacks. NBC News. Source: http://www.nbcnews.com/technology/technolog/hotmail-yahoo-mail-users-also-targets-attacks- 123078. Accessed on Oct 2012
18. Galvin N (2012) File-sharing service users in cloud over access to data. The Age.
19. Hulme G (2009) Amazon web services DDoS attack and the cloud. InformationWeek.Source: http://www.informationweek.com/security/amazon-web-services-ddos-attack-andthe/229204417. Accessed on Oct 2012
20. Hachman M (2012) New facebook phishing attack steals accounts, financial information. PC Mag. Source: http://www.pcmag.com/article2/0,2817,2398922,00.asp. Accessed on Oct 2012
21. Albanesius C (2012) Ramnit computer worm compromises 45K facebook logins. PC Mag. Source: http://www.pcmag.com/article2/0,2817,2398432,00.asp. Accessed on Oct 2012.
22. Ruhr (2011) Cloud computing: Gaps in the 'cloud'. NewsRx Health Sci.
23. Zunnurhain K, Vrbsky SV (2010) Security attacks and solutions in clouds. CloudCom2010 Poster.
24. Huang R, Gui X, Yu S, ZhuangW(2011) Research on privacy-preserving cloud storage framework supporting ciphertext retrieval. International conference on network computing and information security 2011:93–97.
25. M. Jensen and N.Gruschka,On "Technical Security Issues in Cloud Computing", IEEE International Conference on Cloud Computing, **(2009)**.
26. Q.Guand P. Liu"Denial of Service Attacks", Department of Computer ScienceTexas State University; School of Information Sciences and TechnologyPennsylvania State UniversityUniversity.
27. P. Mahajan & A.Sachdeva, "A Study of Encryption Algorithms AES, DES and RSA for Security", Global Journal of Computer Science and Technology Network, Web & Security vol. 13, no. 15,**(2013)**.
28. A. Kaminsky1, M. Kurdziel2, S. Radziszowski1, 1Rochester Institute of Technology, Rochester, NY 2Harris Corp., RF Communications Div., Rochester, "An Overview of Cryptanalysis Research for the Advanced Encryption Standard".
29. P. S. Yadav, P. Sharma, K. P Yadav, "Implementation of rsa algorithm using elliptic curve algorithm for security and performance enhancement", International Journal of Scientific & Technology Research, vol. 1, no. 4, **(2012)**.