Cloud Data Security by using Blowfish Algorithm

K.Manoj Kumar Reddy[1], G.Ananthnath[2]
[1,2]*KMM Institute of PG Studies*

Abstract- **Cloud computing has nice potential of providing sturdy procedure power to the society at reduced value. It enables customers with restricted procedure resources to source their giant computation workloads to the cloud, and economically relish the large procedure power, bandwidth, storage, and even applicable code which will be shared in a pay-per-use manner. Storing knowledge in a very third party's cloud system causes serious concern over knowledge confidentiality. General encryption schemes defend knowledge confidentiality, however conjointly limit the practicality of the storage system as a result of many operations are supported over encrypted knowledge. Constructing a secure storage system that supports multiple functions is difficult once the storage system is distributed and has no central authority. We have a tendency to propose a threshold proxy re-encryption theme and integrate it with a localized erasure code specified a secure distributed storage system is developed. The distributed storage system not only supports secure and sturdy knowledge storage and retrieval, however conjointly lets a user forward his knowledge within the storage servers to another user while not retrieving the info back. The most technical contribution is that the proxy re-encryption theme supports encoding operations over encrypted messages yet as forwarding operations over encoded and encrypted messages. Our method totally integrates encrypting, encoding, and forwarding. We analyze and suggest appropriate parameters for the amount of copies of a message sent to storage servers and also the variety of storage servers queried by a key server.**

Index Terms- **Cloud computing, encryption, re-encryption, encoding.**

INTRODUCTION

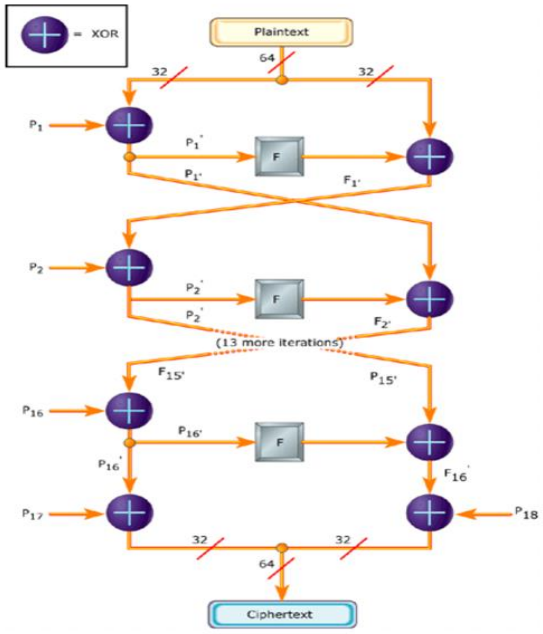
Cloud Computing provides convenient on-demand network access to a shared pool of configurable computing resources that can be rapidly deployed with great efficiency and minimal management overhead. One fundamental advantage of the cloud paradigm is computation outsourcing, where the computational power of cloud customers is no longer limited by their resource constraint devices. By outsourcing the workloads into the cloud, customers could enjoy the literally unlimited computing resources in a pay-per-use manner without committing any large capital outlays in the purchase of hardware and software and/or the operational overhead there. Despite the tremendous benefits, outsourcing computation to the commercial public cloud is also depriving customer's direct control over the systems that consume and produce their data during the computation, which inevitably brings in new security concerns and challenges towards this promising computing model. High-speed networks and ubiquitous Internet access become available in recent years, many services are provided on the Internet such that users can use them from anywhere at any time. For example, the email service is probably the most popular one. Cloud computing is a concept that treats the resources on the Internet as a unified entity, a cloud. Users just use services without being concerned about how computation is done and storage is managed.

Cloud computing is a developing example, exchanging the capacity abilities to autonomous specialist co-ops. As a result of the loss of direct control on outer information, clients are disinclined for tolerating cloud administrations. To construct a sheltered cloud computing system, service stages and application programming levels must be considered for ensured cloud computing framework. Data encryption is one of the sufficient intends to accomplish cloud computing data security. Users can encode information that is put away or handled inside the cloud to anticipate unapproved access. Traditionally, the primary point of convergence is scrambled data on determined stage, for example, information encryption. For cloud computing, a framework level plan must be executed. Cryptography was the uncommon area of military and administrative mystery benefits, and has been

given security properties, for example, information secrecy and information root authentication. A essential contrast between cryptographic plans determines the connection between the match of keys, incorporated into message encryption and unscrambling calculations. Symmetric or ordinary cryptography rely on upon the key between two imparting elements Alice and Bob. The premise of symmetric cryptography, and additionally lopsided cryptography, is on utilizing two comparative calculations for message encryption and unscrambling In spite of, basic operations of encryption and decryption, cryptography in cloud computing likewise supplies numerous security related capacities.

BLOWFISH ALGORITHM

Diagram for Blowfish Algorithm:



Blowfish is a symmetric encryption algorithm, meaning that it uses the same secret key to both Encrypt and decrypt messages. Blowfish is also a block cipher, meaning that it divides a message up into fixed length blocks during encryption and decryption. The block length for Blowfish is 64 bits; messages that aren't a multiple of eight bytes in size must be padded. Blowfish consists of two parts: key-expansion and data encryption. During the key expansion stage, the inputted key is converted into several sub key arrays total 4168 bytes. There is the P array, which is eighteen 32- bit boxes, and the S-boxes, which are four 32-bit arrays with 256 entries each. After the string initialization, the first 32 bits of the key are XOR ed with P1 (the first 32-bit box in the P-array). The second 32 bits of the key are XOR ed with P2, and so on, until all 448, or fewer, key bits have been XOR ed Cycle through the key bits by returning to the beginning of the key, until the entire P-array has been XOR ed with the key. Encrypt the all zero string using the Blowfish algorithm, using the modified P-array above, to get a 64 bit block. Replace P1 with the first 32 bits of output, and P2 with the second 32 bits of output (from the 64 bit block). Use the 64 bit output as input back into the Blowfish cipher, to get a new 64 bit block. Replace the next values in the P array with the block. Repeat for all the values in the P-array and all the S boxes in order.

Encrypt the all zero string using the Blowfish algorithm, using the modified P-array above, to get a 64 bit block. Replace P1 with the first 32 bits of output, and P2 with the second 32 bits of output (from the 64 bit block). Use the 64 bit output as input back into the Blowfish cipher, to get a new 64 bit block. Replace the next values in the P-array with the block. Repeat for all the values in the P-array and all the S boxes in order.

Algorithm

Divide x into two 32-bit halves: xL, xR
For i = 1to 32:
xL = XL XOR Pi
xR = F(XL) XOR xR
Swap XL and xR
Swap XL and xR (Undo the last swap.)
xR = xR XOR P17
xL = xL XOR P18
Recombine xL and xR

CONCLUSION

In this paper, various security issues are raised in cloud computing. Lack of high security and privacy are drawbacks in cloud. In proposed model we are use blowfish algorithm. By this algorithm we can enhanced level of security and privacy in cloud computing.

REFERENCES

[1] F. Shaikh and S. Haider, "Security threats in cloud computing," in Internet Technology and

Secured Transactions (ICITST), 2011 International Conference for, 2011, pp. 214–219.

[2] R. B. Uriarte and C. B. Westphall, "Panoptes: A monitoring architecture and framework for supporting autonomic clouds," in Network Operations and Management Symposium (NOMS), 2014 IEEE. IEEE, 2014, pp. 1–5.

[3] D. Fernandes, L. Soares, J. Gomes, M. Freire, and P. Incio, "Security issues in cloud environments: a survey," International Journal of Information Security, vol. 13, no. 2, 2014, pp. 113– 170. [Online]. Available: http://dx.doi.org/10.1007/s10207-013-0208-7 [retrieved: Sept, 2014]

[4] T. T. W. Group et al., "The notorious nine: cloud computing top threats in 2013," Cloud Security Alliance, 2013.

[5] M. Mukhtarov, N. Miloslavskaya, and A. Tolstoy, "Cloud network security monitoring and response system," vol. 8, no. Special Issue on Cloud Computing and Services. sai: itssa.0008.2012.020 ITSSA, 2012, pp. 71–83.

[6] B. Grobauer, T. Walloschek, and E. Stocker, "Understanding cloud computing vulnerabilities," Security Privacy, IEEE, vol. 9, no. 2, marchapril 2011, pp. 50 –57.

[7] X. Tan and B. Ai, "The issues of cloud computing security in high-speed railway," in Electronic and Mechanical Engineering and Information Technology (EMEIT), 2011 International Conference on, vol. 8, 2011, pp. 4358–4363.

[8] F. Sabahi, "Cloud computing security threats and responses," in Communication Software and Networks (ICCSN), 2011 IEEE 3rd International Conference on, 2011, pp. 245–249.

[9] K. Vieira, A. Schulter, C. Westphall, and C. Westphall, "Intrusion detection for grid and cloud computing," IT Professional, vol. 12, no. 4, 2010, pp. 38–43.

[10] S. de Chaves, C. Westphall, and F. Lamin, "Sla perspective in security management for cloud computing," in Networking and Services (ICNS), 2010 Sixth International Conference on, 2010, pp. 212–217.

[11] D. dos Santos, C. Merkle Westphall, and C. Becker Westphall, "A dynamic risk-based access control architecture for cloud computing," in Network Operations and Management Symposium (NOMS), 2014 IEEE, May 2014, pp. 1–9.

[12] P. Silva, C. Westphall, C. Westphall, M. Mattos, and D. Santos, "An architecture for risk analysis in cloud," in ICNS 2014, The Tenth International Conference on Networking and Services, 2014, pp. 29–33.

[13] M. Isard, M. Budiu, Y. Yu, A. Birrell, and D. Fetterly, "Dryad: distributed data-parallel programs from sequential building blocks," in EuroSys '07: Proceedings of the 2nd ACM SIGOPS/EuroSys European Conference on Computer Systems 2007. New York, NY, USA: ACM, 2007, pp. 59–72. [Online]. Available: http://dx.doi.org/10.1145/1272996.1273005

[14] L. Kaufman, "Data security in the world of cloud computing," IEEE SECURITY & PRIVACY, vol. 7, no. 4, July-August 2009.

[15] A. A. Nyre and M. G. Jaatun, "Privacy in a semantic cloud: ˚ What's trust got to do with it?" in The First International Conference on Cloud Computing, 2009, pp. 107–118.

[16] S. Pearson, Y. Shen, and M. Mowbray, "A privacy manager for cloud computing," in The First International Conference on Cloud Computing, 2009, pp. 90–106.

[17] B. Ramsdell, "RFC 3851 - Secure/Multipurpose Internet Mail Extensions (S/MIME) Version 3.1 Message Specification," Network Working Group, Request For Comment, July 2004. [Online]. Available: http://www.faqs.org/rfcs/rfc3851.html

[18] L. Yan, C. Rong, and G. Zhao, "Strengthen cloud computing security with federal identity management using hierarchical identity-based cryptography," in The First International Conference on Cloud Computing, 2009, pp. 167–177.

[19] Y. Yu, M. Isard, D. Fetterly, M. Budiu, u. Erlingsson, P. K. ´ Gunda, and J. Currey, "DryadLINQ: A System for GeneralPurpose Distributed Data-Parallel Computing Using a HighLevel Language," in Proceedings of the 8th Symposium on Operating Systems Design and Implementation (OSDI '08), San Diego, CA, December 2008.

[20] G. Zhao, J. Liu, Y. Tang, W. Sun, F. Zhang, X. ping Ye, and N. Tang, "Cloud computing: A statistics aspect of users." in The First

International Conference on Cloud Computing, ser. Lecture Notes in Computer Science, M. G. Jaatun, G. Zhao, and C. Rong, Eds., vol. 5931. Springer, 2009, pp. 347–358.

[21] DeyanChen,Hong Zhao," Data Security and Privacy Protection Issues in Cloud Computing, " 2012 IEEE International Conference on Computer and Electronics engineering.

[22] Priyanka Ora and Dr.P.R.Pal, "Data Security and Integrity in Cloud Computing Based On RSA Partial Homomorphic and MD5 Cryptography" IEEE International Conference on Computer 2015.

[23] Shakeeba S. Khan ,Prof.R.R. Tuteja, Security in Cloud Computing using Cryptographic Algorithms, Vol. 3, Issue 1, January 2015

[24] ZhaoYong-Xia and Zhen Ge ,"MD5 Research," Second International Conference on Multimedia and Information Technology, 2010

[25] Dai Yuefa, Wu Bo, Gu Yaqiang, Zhang Quan and Tang Chaojing, "Data Security Model for Cloud Computing," Proceedings of the 2009 International Workshop on Information Security and Application (IWISA 2009) Qingdao, China, November 21-22, 2009.

[26] P. Druschel and A. Rowstron, "PAST: A Large-Scale, PersistentPeer-to-Peer Storage Utility," Proc. Eighth Workshop Hot Topics in Operating System (HotOS VIII), pp. 75-80, 2001.

[27] A. Adya, W.J. Bolosky, M. Castro, G. Cermak, R. Chaiken, J.R. Douceur, J. Howell, J.R. Lorch, M. Theimer, and R. Wattenhofer, "Farsite: Federated, Available, and Reliable Storage for an Incompletely Trusted Environment," Proc. FifthSymp.Operating System Design and Implementation (OSDI), pp. 1-14, 2002.

[28] A . Haeberlen, A. Mislove, and P. Druschel, "Glacier: Highly Durable, Decentralized Storage Despite Massive Correlated Failures,Proc. Second Symp. Networked Systems Design and Implementation (NSDI), pp. 143- 158, 2005.

[29] Z. Wilcox-O'Hearn and B. Warner, "Tahoe: The LeastAuthority Filesystem,"Proc. Fourth ACM Int'l Work shop Storage Security and Survivability (StorageSS), pp. 21- 26, 2008.

[30] H.-Y. Lin and W.-G. Tzeng, "A Secure Decentralized Erasure Code for Distributed Network Storage," IEEE Trans. Parallel and Distributed Systems, vol. 21, no. 11, pp. 1586-1594, Nov. 2010.