Reactive Security Measure On Trusted Cloud Computing

Meenu Bhati[1], Puneet Rani[2]
[1]M.tech, cse, srcem, mdu rohtak, India
[2]M.tech, cse, srcem, A.P, India

ABSTRACT

In the current era of digital world, various organizations produce a large amount of sensitive data including personal information, electronic health records, and financial data. The local management of such huge amount of data is problematic and costly due to the requirements of high storage capacity and qualified personnel. Therefore, Storage-as-a-Service offered by Trusted Cloud Service Providers emerged as a solution to mitigate the burden of large local data data storage and reduce the maintenance cost by means of outsourcing data storage. Since the data owner physically releases sensitive data to a remote Trusted Cloud Service Providers, there are some concerns regarding confidentiality, integrity and access control of the data. The confidentiality feature can be guaranteed by the owner via encrypting the data before outsourcing to remote severs. For verifying data integrity over cloud severs, researchers have proposed provable data possession technique to validate the intactness of data stored on remote sites. Commonly, traditional access control techniques assume the existence of possession in networked information systems such as those related to critical infrastructures (power facility, airports, data vaults, defence systems, and so forth) is a matter of crucial importance. Scalable and efficient provable data possession: storage outsourcing is a rising trend which promotes a number of interesting security issues, many of which has been extensively investigated in the past. Dynamic provable data possession: as storage-outsourcing services and resource-sharing networks have become popular, the problem of efficiently proving the integrity of data stored at un-trusted servers has received increased attention. In the provable data possession (PDP) model, the client pre-processes the data and then sends it to an un-trusted server for storage, while keeping a small amount of meta-data. The client later asks the server to prove that the stored data has not been tempered with or deleted (without downloading the actual data). Enabling public verifiability and data dynamics for storage security in cloud computing: Cloud Computing has been envisioned as a next-generation architecture of IT Enterprises. It moves the application software and databases to the centralized large data centers, where the management of the data and services may not be fully trustworthy. This work studies the problem of ensuring the integrity of data storage in Cloud Computing.

Keywords: Cloud Computing, Trusted Cloud Computing and Reactive Security Measures, Provable Data Possession.

I. INTRODUCTION

This paper focuses on the issues related to the data security aspects of cloud computing know are Reactive Security Measure. As a data and information will be shared with the third party, cloud computing users want to avoid and un-trusted cloud provider. Protecting private and important information, such as credit card details or a patient's medical records from attackers or malicious insiders is of critical importance. In addition, the potential for migration from a single cloud to a multi-cloud environment is examined and research related to security issues in single and multi-clouds in cloud computing is, we have proposed a cloud-based storage scheme which support outsourcing of dynamic data, where the owner is capable of not only archiving and accessing the data stored by the Trusted Cloud Service Providers, but also updating and scaling this data on the remote servers. The proposed schemes enables the authorized users to ensure that they are receiving the most recent version of the outsourced data. Moreover, in case of disputes regarding data integrity/newness, a Trusted Third Party is able to determine the dishonest party. The data owner enforces access control for the outsourced data by combining three cryptographic techniques: broadcast encryption, lazy revocation, and key rotation. We have studied the security features of the proposed scheme. We have investigated the overheads added by a scheme when incroported into a cloud storage model for *static* data with only *confidentiality* requirement. The storage overhead is ~0.4% of the outsourced data size, the communication overhead due to block-level dynamic changes on the data is ~1% of the block size, and the communication overhead due to retrieving the data is ~0.2% of the outsourced data size. For a large organization with 105 users, performing dynamic operations and enforcing access control add about 63 milliseconds of overhead. Therefore, important

ISSN: 2278 – 7798

features of outsourcing data storage can be supported without excessive overheads in storage, communication and computation. They must not be able to read updated/new blocks. Trusted Cloud Service Providers *defence:* the Trusted Cloud Service Providers must be safeguarded against false accusations that may be claimed by dishonest owner/users, and such a malicious behavior is required to be revealed.

II. RELATED WORK

A lot of papers are found proposing the approach to format in the cloud security and these are divided into the many benefits in terms of low cost and accessibility of data. Ensuring the security of cloud computing is a major factor in the cloud computing environment, as users often store sensitive information with cloud storage providers but these providers may be un-trusted which is under the trusted cloud computing. Dealing with "single cloud" providers is predicted to become less popular with customers due to risk of service availability failure and the possibility of malicious insiders in the single cloud. A movement towards "multi-clouds" or in other words, "inter-clouds" or "cloud-of-clouds" has emerged recently with the trust relationship models ensuring the trusted and trusting resource sharing. This paper surveys recent research related to single and multi-cloud security and addresses possible solutions. It is found that the research into the use of multi-cloud providers to maintain security has received less attention from the research community than has the use of single clouds. This work aims to promote the use of multi-clouds due to its ability to reduce security risks under the trusted clouds known as reactive security ensuring the data protection to the cloud computing user under the trusted cloud computing. This section provides a review of the literature on evolution of security protocols for Cloud over Passive Security Measure in order to achieve requirements of confidentiality, data integrity and authentication. The encryption/decryption process , limitations and the vulnerability of each protocol to various attacks have been provided in this section can be decrypted by a specific granted user, and thus enforces access control for the data.

III. DISCUSSION

some aspects related to outsourcing data storage are beyond the setting of both provable data possession, e.g., enforcing access control, and ensuring the newness of data delivered to authorized users. Even in the case of dynamic provable data possession, a verifier can validate the correctness of data, but the server is still able to cheat and return stale data to authorized users after the auditing process is done.

IV. EXISTING SYSTEM

Cloud Computing has been envisioned as the next-generation architecture of IT enterprise. In contrast to traditional solutions, where the IT services are under proper physical, logical and personnel controls, cloud computing moves the application software and databases to the large data centers, where the management of the data and services many not be fully trustworthy. This unique attribute, however, poses many new security challenges which have not been well understood. In this article, we focus on cloud data storage security, which has always been an important aspect of quality of service. To ensure the correctness of users' data in the cloud, we propose an effective and flexible distributed scheme with two salient features, opposing to its predecessors. By utilizing the homomorphic token with distributed verification of erasure-coded data, our scheme achieves the integration of storage correctness insurance and data error localization, i.e. the identification of misbehaving server(s). unlike most prior works, the new scheme further supports secure and efficient dynamic operations on data blocks, including: data update, delete and append. Extensive security and performance analysis shows that the proposed scheme is highly efficient and resilient against Byzantine failure, malicious data modification attack, and even server colluding attacks.

V. IMPLEMENTATION

In order to address the cloud security on passive or reactive measures vulnerabilities, algorithm based on stream cipher theory has been proposed. A pseudorandom keystream is used to generate cipher text by utilizing the Subsitution box values. This encryption algorithm is based on XOR operation and the steps for the algorithm are described below for reactive security measures:

Steps are as follows:

i. **Calculate Passkey Numeral For Encryption:**

- Random number is generated between 1024 and 999999.

ISSN: 2278 – 7798

- Length of number is calculated.
- Sum of ASCII value of digits of number are calculated.

Thus, passkey Numeral = Numeral Length+ Sum of ASCII value of digits.

ii.Calculate a0, a1, a2 and a3 parameters:

- a0= Sum of digits at even positions of passkey numeral
- a1= Sum of digits at odd positions of passkey numeral
- a2= Product of digits of passkey numeral
- a3= (Passkey numeral)mod(256).

	0	1	2	3
0	(EP1[b0] XOR c0)*c0	(EP1[b1] XOR c1]*c0	(EP1[b2] XOR c2]*c0	(Ep1[b3] XOR c3)*c0
1	(EP2[b0] XOR c0)*c1	(EP2[b1] XOR c1]*c1	(EP2[b2] XOR c2]*c1	(Ep2[b3] XOR c3)*c1
2	(EP3[b0] XOR c0)*c2	(EP3[b1] XOR c1]*c2	(EP3[b2] XOR c2]*c2	(Ep3[b3] XOR c3)*c2
3	(EP4[b0] XOR c0)*c3	(EP4[b1] XOR c1)*c3	(EP4[b2] XOR c2)*c3	(Ep4[b3] XOR c3)*c3

Table A.1: Encryption Parameters

iii.Calculate b0,b1,b2,b3 parameter:

In order to compute b0, b1, b2, and b3 values, encryption parameters EP1,EP2, EP3 and EP4 are required which are computed using Table A.2:

	EP1 parameters	EP2 parameters	EP3 parameters	EP4 parameters
0	a0 XOR a1	EP1+15	a2 XOR a3	EP3+55
1	a0 XOR a2	EP1+25	a1 XOR a3	EP3+65
2	a0 XOR a3	EP1+35	a1 XOR a2	EP3+75
3	a2 XOR a3	EP1+45	a1 XOR a3	EP3+85

Table A.2: Encryption Parameters

b0= EP1[0]+EP2[0]+EP3[0]+EP4[0] (1)

b1= EP1[1]+EP2[1]+EP3[1]+EP4[1] (2)

b2= EP1[2]+EP2[2]+EP3[2]+EP4[2] (3)

b3= EP1[3]+EP2[3]+EP3[3]+EP4[3] (4)

iv. Calculate c0,c1,c2 and c3 parameters:

- c0=((EP1[b2] XOR EP2[b2])*a0)+b2 (5)
- c1=((EP1[b1] XOR EP3[b1])*a1)+b1 (6)
- c2=((EP1[b0] XOR EP4[b0])*a2)+b0 (7)
- c3=((EP2[b3] XOR EP3[b3])*a3)+b3 (8)

v. Calculate Subsitution box(S-box) values using Table A.3:

	0	1	2	3
0	(EP1[b0] XOR c0) * c0	(EP1[b1] XOR c1) * c0	(EP1[b2] XOR c2) * c0	(EP1[b3] XOR c3) * c0
1	(EP2[b0] XOR c0) * c1	(EP2[b1] XOR c1) * c1	(EP2[b2] XOR c2) * c1	(EP2[b3] XOR c3) * c1
2	(EP3[b0] XOR c0) * c2	(EP3[b1] XOR c1) * c2	(EP3[b2] XOR c2) * c2	(EP3[b3] XOR c3) * c2
3	(EP4[b0] XOR c0) * c3	(EP4[b1] XOR c1) * c3	(EP4[b2] XOR c2) * c3	(EP4[b3] XOR c3) * c3

Table A.3: S-box values

vi. Calculate Message parameter:

Message Parameter= Passkey Numeral (obtained in step i.)+ Randomly generated key between 1024 and 9999+ Average of a0,a1,a2 and a3 parameters(obtained in step ii.)+ Average of b0,b1,b2 and b3 parameters(obtained in step iii.)+ Average of c0,c1,c2 and c3 parameters(obtained in step iv.).

vii. Message Encryption:

- Reverse the plaintext to be encrypted to obtain Partial Message Encryption 1(PME1).
- Perform PME1 XOR S-box [index] operation to obtain Partial Message Encryption 2(PME2).
- Perform PME2 XOR Message parameter operation to compute Partial Message Encryption 3(PM3).
- Reverse hex encoded value of PME3 to compute Partial Message Encryption 4(PME4) which is the resultant encrypted text.

ISSN: 2278 – 7798

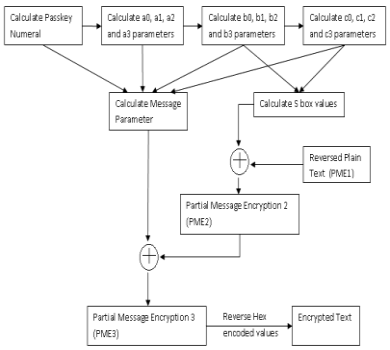

Figure 1: Encryption Process

Advantages of Proposed Encryption Algorithm for Reactive Cloud Security

The encryption algorithm has a faster processing time of 104 ms for plain text of 1024 bytes.

- Being a stream cipher; it works on only a few bits at a time, thus consuming less memory.
- Bytes are individually encrypted without association with other chunks of data, thus are less susceptible to transmission noise because in case of erroneous modification of one part of data, rest of data is still recoverable.
- This algorithm provides easy integration with cloud applications without performance impact.

Limitations of Proposed Encryption Algorithm

- Larger S-box matrix impacts performance when integrated with mobile simulator.
- This algorithm being a stream cipher can only work in forward direction unlike block ciphers which can work in both directions.

REFRENCES:

[1] G. Ateniese, R. Burns, R. Curtmola, J. Herring, L. Kissner, Z. Peterson, and D. Song, "Provable data possession at untrusted stores," in Proceedings of the 14th ACM Conference on Computer and Communications Security, ser. CCS '07, 2007, pp. 598–609.

[2]Z. Hao, S. Zhong, and N. Yu, "A privacy-preserving remote data integrity checking protocol with data dynamics and public verifiability," IEEE Transactions on Knowledge and Data Engineering, vol. 99, no. PrePrints, 2011.

[3] F. Seb´e, J. Domingo-Ferrer, A. Martinez-Balleste, Y. Deswarte, and J.-J.Quisquater, "Efficient remote data possession checking in critical information infrastructures," IEEE Trans. on Knowl. And Data Eng, vol. 20, no. 8, 2008.

[4] G. Ateniese, R. D. Pietro, L. V. Mancini, and G. Tsudik, "Scalable and efficient provable data possession," in Proceedings of the 4th International Conference on Security and Privacy in Communication Netowrks, 2008, pp. 1–10.

[5] C. Erway, A. K¨upc¸ ¨ u, C. Papamanthou, and R. Tamassia, "Dynamic provable data possession," in Proceedings of the 16th ACM Conference on Computer and Communications Security, 2009, pp. 213–222.

[6] Q. Wang, C. Wang, J. Li, K. Ren, and W. Lou, "Enabling public verifiability and data dynamics for storage security in cloud computing," in Proceedings of the 14th European Conference on Research in Computer Security, 2009, pp. 355–370.

[7] A. F. Barsoum and M. A. Hasan, "Provable possession and replication of data over cloud servers," Centre For Applied Cryptographic Research, Report 2010/32, 2010. uwaterloo.ca/techreports/2010/cacr2010-32.pdf.

[8]Ayad Barsoum, Anwar Hasan, "Enabling Dynamic Data and Indirect Mutual Trust for Cloud Computing Storage Systems," IEEE Transactions on Parallel and Distributed Systems, vol. 24, no. 12, pp. 2375-2385, Dec. 2013.

ISSN: 2278 – 7798

[9] R. Curtmola, O. Khan, R. Burns, and G. Ateniese, "MR-PDP: multiple-replica provable data possession," in 28th IEEE ICDCS, 2008, pp. 411–420.

[10] A. F. Barsoum and M. A. Hasan, "On verifying dynamic multiple data copies over cloud servers," Cryptology ePrint Archive, Report 2011/447, 2011, 2011.

[11] K. D. Bowers, A. Juels, and A. Oprea, "HAIL: a high-availability and integrity layer for cloud storage," in CCS '09: Proceedings of the 16th ACM conference on Computer and communications security. New York, NY, USA: ACM, 2009, pp. 187–198.

[12] Y. Dodis, S. Vadhan, and D. Wichs, "Proofs of Retrievability via hardness amplification," in Proceedings of the 6th Theory of Cryptography Conference on Theory of Cryptography, 2009.

[13] A. Juels and B. S. Kaliski, "PORs: Proofs of Retrievability for large files," in CCS'07: Proceedings of the 14th ACM conference on Computer and communications security. ACM, 2007, pp. 584–597.

[14] H. Shacham and B. Waters, "Compact proofs of retrievability", in ASIACRYPT '08, 2008, pp. 90–107.

[15] S. D. C. di Vimercati, S. Foresti, S. Jajodia, S. Paraboschi, and P. Samarati, "Over-encryption: Management of access control evolution on outsourced data," in Proceedings of the 33rd International Conference on Very Large Data Bases. ACM, 2007, pp. 123–134.

[16] E. Mykletun, M. Narasimha, and G. Tsudik, "Authentication and integrity in outsourced databases,"Trans. Storage, vol. 2,no. 2, 2006.

[17] G. Ateniese, K. Fu, M. Green, and S. Hohenberger, "Improved proxy re-encryption schemes with applications to secure distributed storage," in NDSS, 2005.

[18] A.K.M NAZMUS SAKIB, "Security Enhancement and solution for WAP2 (wi-Fi Protected Access 2)", in IRACST-International Journal of Computer Networks and Wireless Communication(IJCNWC), vol.1, No.1, December 2011.

[19] Arleen Kaur, Monika Aggarwal, " Analysis of various security issues in cloud computing using WLAN protocols", in International Journal of Reviews, Surveys and Research(IJRSR) volume 2, issue 1, January 2013, International Manuscript ID: ISSN23194618-V211M4-012013.

[20]A.K.M NAZMUS Sakib, " Security Improvement of WAP2(Wi-Fi Protected Access 2)", in IJEST, vol.3, No.1 Jan 2011, ISSN: 0975-5462.

[21] Ezedin Barka, Mohammed Boulmalf, " On the impact of security on the performance of WLANs", in Journal of Communications, vol.2, No.4, June 2007.

[22] Kashif Munir, Prof. Dr. Sellapan Palaniappan, "Secure Cloud Architecture", in Advanced Computing: An International Journal(ACIJ), vol.4, No.1, January 2013.

[23] Monjur Ahmed, Mohammad Ashraf Hossain, " Cloud Computing and Security issues in the Cloud", in International Journal of Network security & Its Applications(IJNSA), vol.6, No.1, January 2014.

ISSN: 2278 – 7798

[24] Dimitris Geneiatakis et.al., "Security and Privacy in mobile cloud under a citizen's perspective", Institute for the Protection and security of the citizen, Joint Research Centre(JRC), CCIS 182, PP.16-27,2013.

[25] Pardeep, Puspendra kumar Peteriya, " A Programmatic study on different stream ciphers and on different flavours of RC4 stream cipher", in (IJCSNS)International Journal of Computer Science and Network Security, vol.12, No. 3,March 2012.

[26] Paul Arana, "Benefits and Vulnerabilites of Wi-Fi Prtoected Access2(WPA2)", in INFS 612-Fall 2006.

[27] Amos Olagunju, Timothy Seedorf, "Requirements for Secure Wireless Networks: An Analysis of the WEP and WPA with Aircracking suite", in St. Cloud State university.

[28] Vishal Kumar et.al., "Vulnerabilities of wireless security protocols(WEP and WPA2)", in International journal of Advanced Research in Computer Engineering and Technology", volume1, Issue2, April 2012.

[29] Prof. Swarnalata Bolla Varapu, Bharat gupta, "Data Security in Cloud Computing", in International Journal Advanced Research in Computer Science and Software Engineering , volume 4, Issue 3, March 2014, ISSN: 2277 128X.

ISSN: 2278 – 7798