A Novel Framework to Prevent Privacy Breach in Cloud Data Storage Area Service

Chandramohan.D, Student Member, IEEE, Vengattaraman.T,
Rajaguru.D, Baskaran.R, and Dhavachelvan.P
Department of Computer Science, Pondicherry University, Pondicherry
Dept.of Inf.Technology, Perunthalaivar Kamarajar Inst.of Eng. & Technology, Karaikal
Department of Computer Science and Engineering, Anna University, Chennai, India
{pdchandramohan, vengat.mailbox, raja.guru42, dhavachelvan}@gmail.com, baaski@cs.annauniv.edu

***Abstract*— The present paper focuses on user data privacy invasion and it is more important in cloud data storage. Numerous approaches and techniques have proposed so for, to preserve the cloud user privacy. This paper introduces a layered framework for preserving secrecy of cloud user and preventing digital data loss, using onion privacy layer, garlic privacy layer. This layered framework prevents the confidential information by multiple encryption of onion and garlic privacy preserving layered approach.**

Keywords*— Privacy Preserving, Cloud Computing, Onion Privacy Layer, Garlic Privacy Layer, Load Balancing, Digital Data.

I. INTRODUCTION

This paper focuses on cloud digital data loss and its privacy preserving by proposing a novel framework approach to mitigate the risk and protect the data from attackers. The high digital data storage center, user privacy maintenance is a wearisome chore for end-user and service provider. Unceremonious seclusion contracted with habitual user personal information, the main reason to develop and propose this novel framework for maneuver in sequence data progression and maturity. The current information dispensation conceded slightest relationship and input circumstances. Radical usages of cloud data irrespective of consign and contrivance may direct to violate user's privacy and their needs. [1-5] et al expresses the dominant usage of critical data and its preserving techniques are handled in an earlier data protection method. Virtual swarm is ensuing cohesion with provider and user. More informational confidentiality has personage precincts for user acquiescence and admittance to data exodus in storage area. This paper focuses the general privacy issue and its preserving methodologies adopted so for are not meeting the requirement of cloud user. The limitation of data attackers generally overcomes to preserve better utilization of authorized user data.[5], [7], [13] author et al uses a cookie based monitoring the user behavior, an identity based data storage and retrieval and a frame work to establish enough trust among user on providers. To illustrate the scientific structure for normal systems are not adequate more over a perfunctory approach for preserving confidential data. It is noted to be less cost effective process for implementing in many field where-ever privacy is necessity. [6-9], The general behavior proposed in this approach experiments a better data utility option with improved privacy preserving technique. Once all information readily available online one can easily get into others storage without any risk and makes the data into risk and there is no information privacy in it. [18], [21], [26], and [28] a secure and efficient data retrieval by data using attribute based encryption, theoretical analysis of authentication and an novel architecture to preserve user privacy and authentication. If and only if no one else knows even something regarding your personal data, it may climb to be information privacy. Why the social networking providers need of user personal information, literally they are utilizing it for business and making confidential data into profit. [1-4] author et al proposed a privacy preserving approach for mitigating the security for user data using encryption and decryption technique, a Petri-net based framework approach to preserve user information, and an evolutionary model for protecting digital data. [6], [29-31] cloud service privacy representation to ensure the trust in cloud providers. An intelligent model based hybrid approach to preserve user digital content, pervasive and ubiquitous computing environment privacy preservation carried out, and a generic approach to molt the assurance of secrecy in maintain cloud digital data. [8-12], [22, 23, 25] author et al proposes a multi agent system to accommodate the software process and a framework to mitigate the issue. [10], author et al a SVIP based mechanism for SIP dependent system and its security measures are handled. [14-17], [19-20], author et al proposed a global replica management by ensuring and enhancing the QOS parameters, and an efficient service cache management for mobile peer to peer network. [24], [27] a testbed and an evaluation criteria for a distributed web service environment for the service suitability.

II. PROPOSED APPROACH

Cloud computing researches have few scratches with serious issue of data privacy invasion. There are several approaches, techniques, algorithms, protocols, and framework to prevent the user privacy in cloud environment. this paper shows its importance in proposing a novel privacy preserving framework to prevent digital data loss happening in current cloud data storage. Privacy breach directly propositional to the cloud technologies as the technology grows one way, its data privacy breach happening in many ways. There is no end to technological advancement and also privacy breach. This paper focused on privacy issue and proposed a framework to mitigate the privacy preserving in the cloud digital storage area, with a novel onion and garlic privacy preserving cohesive approach to

Major Project Scheme, UGC, India, Reference No: F. No. 40-258/2011 (SR), dated 29 June 2011.

prevent the data loss. Onion and garlic privacy preserving approach-OGPPA have a right to prevent the privacy of communication happening in cloud systems. Keeping users data online are not guaranteed to be protected from attackers. Unknown observers are watching it and holding the stuffs easily without the knowledge of data owners. It should be possible for every individual to hide their data and communication details as a log file. Onion and garlic privacy preserving approach can be launched on the top of the cloud layer. The basic idea of onion routing proposed by [D.Chawan].

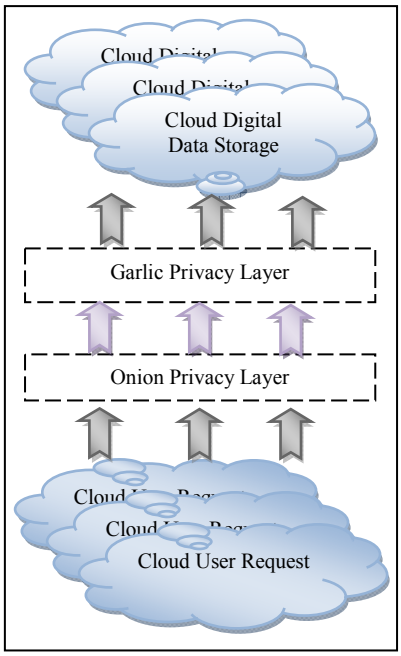

Fig.1 Onion Garlic Privacy Preserving Approach (OGPPA)-Framework

a) Onion privacy preserving approach layer
b) Garlic privacy preserving approach layer
c) Virtualization management

1) Onion privacy preserving approach layer-OPPA

Large number of mixed nodes to serve as the simple layer of accepting user request and encrypting the details with public key and decrypting it and then sending them to next layer of onion privacy preserving approach-OGPPA. Fig.1 Each layer of OGPPA would also perform certain time variation of the request and send to next layer. It provides both side encryption and decryption for users and service providers and enables them to communicate anonymously. It also transfers the user data only to original users against all attacks and hackings. This complicates the cloud intermediates to get through the process.

d) Anonymous communication over a computer networks
e) Messages are repeatedly encrypted and then sent through several network nodes called onion routing
f) By unpeeling an onion, each onion router removes a layer of encryption to check the routing intrusions.

An onion privacy preserving approach is a multiple encryption layered structured approach with information about the users kept inside the cloud. Whenever a user request for any information from the cloud digital storage, the OPPA decrypts it and contains the next hop of the onion layer, this process will continue until the user identification matches the requested and log maintained of current system. The decryption packet is identical to the user data that was produced by the user application beginning of the process. Onion privacy relies on using the public key cryptography, which allows it to encrypt the data using OPPA such that it intended the recipients of each layer can decrypt it with their private keys.

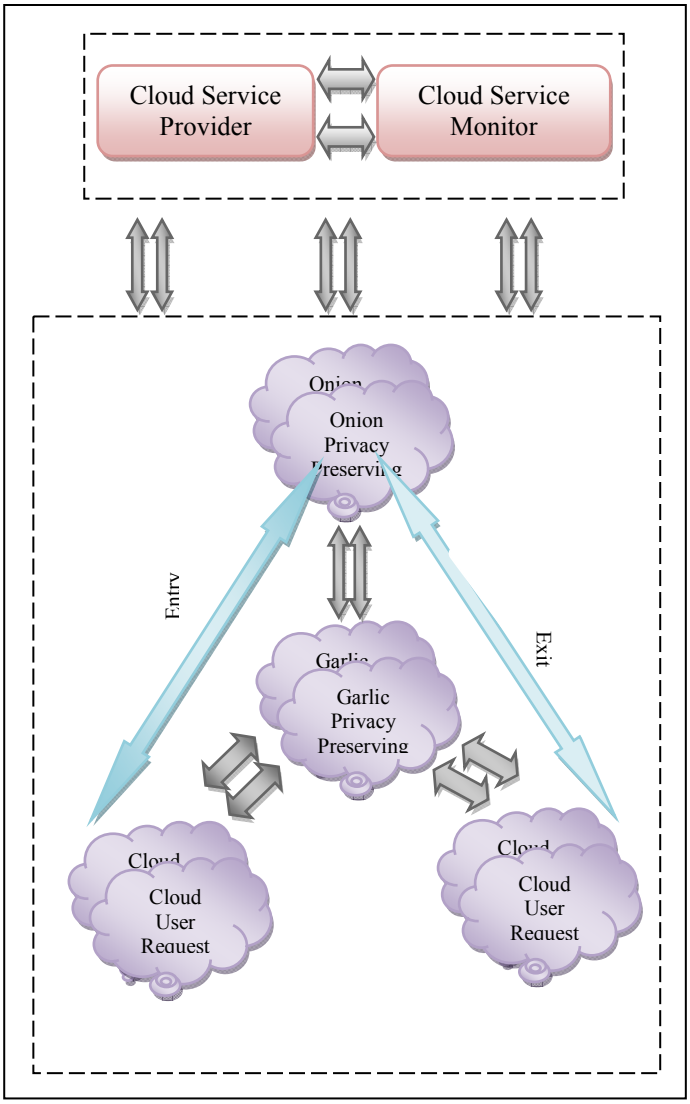

Fig.2 OGPPA- Privacy Preserving Process for Cloud

2) Garlic privacy preserving approach layer-GPPA

The current research focuses on cloud computing worldwide growth through communication systems and internet, the privacy and security breach of concerns of cloud users have increased. Either side of coin user suffers from privacy issue of their data and the other side the vast utilization and enjoying the benefits of cloud in their door steps. Fig.1, This work intends to mitigate these conflicting issues by proposing a novel onion privacy preserving approach. Government and private sector are concerned about the anonymous user access to confidential data by unknown hackers. It presents a nominal solution for revocable user access to cloud data and monitors the behavior and attempts on others data.

a) It encrypts multiple messages together to make it more difficult for attackers to interrupt.

Garlic privacy preserving approach is a variant onion privacy that encrypts multiple messages together to make it more difficult for attacks to perform users request analysis and preserve their data. Garlic privacy is one of the key factors that distinguish cloud user and providers. Distributing data storage area uses the current GPPA.

3) Virtualization management

a) Load balancing
b) Storage
c) Connecting storage to a virtual host
d) Allocating storage properly
e) Network knowledge to configure hosts properly.

III. CONCLUSION

Cloud computing is taking forward the technological advancement at smart phone door steps and holding hands with other cloud supporting devices. Enormous development in the cloud increases the risk factor simultaneously for user information stored in it. The proposed system converts the user data by onion encryption technique and stored in cloud environment. Onion and garlic privacy preserving framework gives a strong back up with encryption and decryption techniques to handle the privacy breach happens during critical attacks by unknown users. Future research focuses on three factor encryption in cloud layer to boost up and mitigate the privacy prevention in cloud storage service.

ACKNOWLEDGEMENT

This work is a part of the Research Project sponsored under the Major Project Scheme, UGC, India, Reference No: F. No. 40-258/2011 (SR), dated 29 June 2011. The authors would like to express their thanks for the financial support offered by the Sponsored Agency.

REFERENCES

[1] D.Chandramohan, T.Vengattaraman, M.S.S.Basha and P.Dhavachelvan, "MSRCC–Mitigation of Security Risks in Cloud Computing", Springer Book Series-AISC-2012, Vol.176, pp.525-532.

[2] Chandramohan.D, Vengattaraman.T, Dhavachelvan, P, "HPPC-Hierarchical Petri-Net based Privacy nominal model approach for Cloud", India Conference (INDICON), 2012 Annual IEEE-DOI:10.1109/INDCON.2012.6420771, ISBN:978-1-4673-2270-6, pp.1047-1052.

[3] Chandramohan.D, Student Member, IEEE, Vengattaraman.T, Rajaguru.D, Baskaran.R and Dhavachelvan.P, "A Privacy Breach Preventing and Mitigation Methodology For Cloud Service Data Storage", IEEE-IACC Proceedings, ISBN: 978-1-4673-4528-6/2013.

[4] Chandramohan.D, Student Member, IEEE, Vengattaraman.T, Rajaguru.D, Baskaran.R and Dhavachelvan.P, "EMPPC-An Evolutionary Model Based Privacy Preserving Technique for Cloud Digital Data Storage Service", IEEE-IACC Proceedings, ISBN: 978-1-4673-4528-6/2013.

[5] Laura McCarthy, Dave Yates, "The use of cookies in Federal agency web sites: Privacy and recordkeeping issues", Elsevier-Government Information Quarterly 27 (2010) pp.231– 237

[6] Chandramohan.D, Vengattaraman.T, Rajaguru.D, Baskaran.R and Dhavachelvan.P, "A Privacy Preserving Representation for Web Service Communicators' in the Cloud", 9th International Conference on Heterogeneous Networking for Quality, Reliability, Security and Robustness, QSHINE-Proceeding Springer ISBN: 978-1-936968-71-8. Vol.115 (LNICST)-2013.

[7] Jinguang Han, WillySusilo, YiMu, "Identity-based data storage in cloud computing", Elsevier-Future Generation Computer Systems, pp.673-681.

[8] T. Vengattaraman, S. Abiramy, P. Dhavachelvan and R. Baskaran, "An Application Perspective Evaluation of Multi-Agent System in Versatile Environments", International Journal on Expert Systems with Applications, Vol. 38, No. 3, pp. 1405-1416.

[9] S. Venkatesan, P. Dhavachelvan and C. Chellapan, "Performance analysis of mobile agent failure recovery in e-service applications", International Journal of Computer Standards and Interfaces, Vol-2, No.1-2, pp. 38 43. ISSN:0920-5489.

[10] D. Chandramohan, D. Veeraiah, M. Shanmugam, N. Balaji and G. Sambasivam ,"SVIP-Enhanced Security Mechanism for SIP Based VoIP Systems and Its Issues", Springer Book series-Advances in Intelligent Systems and Computing, 1, Volume 176, Pages 81-86-2012.

[11] T. Vengattaraman and P. Dhavachelvan, "An Agent-Based Personalized E-Learning Environment: Effort Prediction Perspective", IEEE-IAMA-2009.

[12] P. Dhavachelvan, G.V. Uma and V.S.K.Venkatachalapathy, "A New Approach in Development of Distributed Framework for Automated Software Testing Using Agents", International Journal on Knowledge Based Systems, Vol. 19, No. 4, pp. 235-247, August 2006.

[13] Imad M. Abbadi, Muntaha Alawneh, "A framework for establishing trust in the Cloud", Elsevier-Computers and Electrical Engineering 38 (2012) PP.1073–1087

[14] P. Victer Paul, N. Saravanan, S.K.V. Jayakumar, P. Dhavachelvan, R. Baskaran, "QoS Enhancements for Global Replication Management in Peer to Peer networks", Future Generation Computer Systems (2011), Elsevier, Volume 28, Issue 3, March 2012, Page No. 573-582.

[15] R. Baskaran, P. Victer Paul and P. Dhavachelvan, "Analytical Inspection for Replica Management in WANET using Distributed Spanning Tree", IEEE International Conference on Recent Trends in Information Technology (ICRTIT), May 2012, Chennai, pp. 297 - 301. ISBN: 978-1-4673-1599-9.

[16] R. Baskaran, P. Victer Paul and P. Dhavachelvan, "Algorithm and Direction for Analysis of Global Replica Management in P2P Network", IEEE International Conference on Recent Trends in Information Technology (ICRTIT), May 2012, Chennai, pp. 211 - 216. ISBN: 978-1-4673-1599-9.

[17] R. Baskaran, P. Victer Paul and P. Dhavachelvan, "Ant Colony Optimization for Data Cache Technique in MANET", International Conference on Advances in Computing (ICADC), 2012, Advances in Intelligent and Soft Computing" series, Springer, India. pp.873-878.

[18] Dongyoung Koo, Junbeom Hur, Hyunsoo Yoon, "Secure and efficient data retrieval over encrypted data using attribute-based encryption in cloud storage", Elsevier-Computers and Electrical Engineering (2012)

[19] P. Victer Paul, D. Rajaguru, N. Saravanan, R. Baskaran, P. Dhavachelvan, "Efficient service cache management in mobile P2P networks", In Press, Accepted Manuscript, Future Generation Computer Systems, Elsevier, Available online 22 December 2012, ISSN 0167-739X, 10.1016/j.future.2012.12.001.

[20] P. Victer Paul, T. Vengattaraman, P. Dhavachelvan, "Improving efficiency of Peer Network Applications by formulating Distributed Spanning Tree", Third International Conference on Emerging Trends in Engineering & Technology (ICETET-2010), IEEE, India, May 2010. pp. 813-818.

[21] Ye Wang, Shantanu Rane, Stark C. Draper, Prakash Ishwar, A Theoretical Analysis of Authentication, Privacy, and Reusability Across Secure Biometric Systems", IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY, VOL. 7, NO.6, pp.1825-1840, 2012

[22] P. Dhavachelvan and G.V.Uma, "Reliability Enhancement in Software Testing: An Agent-Based Approach for Complex Systems", 7th ICIT 2004, Springer Verlag - Lecture Notes in Computer Science (LNCS), Vol. 3356, pp. 282-291. ISSN: 0302 9743.

[23] P. Dhavachelvan and G.V.Uma, "Multi-agent Framework Construction for Intra Class Testing of Object-Oriented Software", 18th ISCIS 2003, Springer Verlag - Lecture Notes in Computer Science (LNCS), Vol. 2869, pp. 992-999. ISSN: 0302-9743.

[24] M. S. Saleem Basha and P. Dhavachelvan, "Web Service Based Secure E-Learning Management System- EWeMS", International Journal of Convergence Information Technology, Vol. 5, No. 7, pp. 57-69.ISSN: 1975 9320.

[25] P. Dhavachelvan and G.V.Uma, "Complexity Measures For Software Systems: Towards Multi-Agent Based Software Testing Proceedings, ICISIP'05 2005, pp.359-364.

[26] Sree Hari Krishnan Parthasarathi, Hervé Bourlard, Daniel Gatica-Perez, "Wordless Sounds: Robust Speaker Diarization Using Privacy-Preserving Audio Representations", IEEE TRANSACTIONS ON AUDIO, SPEECH, AND LANGUAGE PROCESSING, VOL.21, NO.1, PP.83-96, 2013.

[27] D.Chandramohan, S.K.V.Jayakumar, Shailesh Khapre, M.S.Nanda Kishore, "DWSE-Simulator For Distributed Web Service Environment", IEEE-ICRTIT-2011, pp.1203-1208.

[28] Anmin Fu, Shaohua Lan, Bo Huang, Zhenchao Zhu, Yuqing Zhang, "A Novel Group-Based Handover Authentication Scheme with Privacy Preservation for Mobile WiMAX Networks", IEEE COMMUNICATIONS LETTERS, VOL. 16, NO. 11, pp.1744-1747, 2012

[29] Chandramohan.D, Vengattaraman.T, Dhavachelvan.P and Baskaran.R, "IMBPC- An Intelligent Model Based Hybrid Authentication Technique to Preserve User Privacy and Secrecy for Cloud Users", Springer LNICST-2013.

[30] Chandramohan.D, Vengattaraman.T, Dhavachelvan.P and Baskaran.R, "An Approach to Provide Privacy Preservation for User Data in Pervasive & Ubiquitous Environment", Springer LNICST-2013.

[31] Chandramohan.D, Vengattaraman.T, Rajaguru.D, Baskaran.R, and Dhavachelvan.P,"A Generic Privacy Preserving Approach for Cloud Providers and Users, Springer LNICST-2013.