RESEARCH ARTICLE OPEN ACCESS

Enhancing Data Security in Cloud Computing Growth Security

[1]M.Subhashini, [2]Dr.P.Srivaramangai

[1] Ph. D.Research scholar Dept of Computer Science, Maruthu pandiyar college of Arts & Science, Thanjavur
[2]Assisitant Professor of Computer Science, Maruthu pandiyar college of Arts & Science , Thanjavur.

--************************----------------------------------

Abstract:

In this paper performed Cloud computing is an Internet-based computing and next stage in evolution of the internet. It has received significant attention in recent years but security issue is one of the major inhibitor in decreasing the growth of cloud computing. One of the most important and leading is security issue that needs to be addressed. Data Security concerns arising because both user data and program are located in provider premises. The architecture of cloud poses such a threat to the security of the existing technologies when deployed in a cloud environment. Cloud service users need to be vigilant in understanding the risks of data breaches in this new environment. we propose a two-factor data security protection mechanism with factor revocability for cloud storage system. Our system allows a sender to send an encrypted message to a receiver through a cloud storage server. The sender only needs to know the identity of the receiver but no other information (such as its public key or its certificate). A recent survey by Cloud Security Alliance (CSA) & IEEE indicates that enterprises across sectors are eager to adopt cloud computing but that security are needed both to accelerate cloud adoption on a wide scale and to respond to regulatory drivers. It also details that cloud computing is shaping the future of IT but the absence of a compliance environment is having dramatic impact on cloud computing growth.

Keywords — **Cloud, security**

--************************----------------------------------

1. INTRODUCTION

Cloud computing is an emerging technology which recently has drawn significant attention from both industry and academia. It provides services over the internet, by using cloud computing user can utilize the online services of different software instead of purchasing or installing them on their own computers. Cloud computing utilizes three delivery models by which different types of services are delivered to the end user. The three delivery models are the SaaS, PaaS and IaaS which provide infrastructure resources, application platform and software as services to the consumer. Data security is a major concern for users who want to use cloud computing. This technology needs proper security principles and mechanisms to eliminate users concerns.

Data security is another important research topic in cloud computing. Since service providers typically do not have access to the physical security system of data centres, they must rely on the infrastructure provider to achieve full data security. Even for a virtual private cloud, the service provider can only specify the security setting remotely, without knowing whether it is fully implemented. The infrastructure provider, in this context, must achieve the following objectives: (1) *confidentiality*, for secure data access and transfer, and (2) *audit ability*, for attesting whether security setting of applications has been tampered or not. Confidentiality is usually achieved using cryptographic protocols, whereas audit ability can be achieved using remote attestation techniques.

Most of the cloud services users have concerns about their private data that it may be used for other purposes or sent to other cloud service providers [6]. The user data that need to be protected includes four parts which are: (i) usage data; information collected from computer devices (ii) sensitive information; information on health, bank account etc. (iii) Personally identifiable information; information that could be used to identify the individual (iv) Unique device identities; information that might be uniquely traceable e.g. IP addresses, unique hardware identities etc. In cloud computing, data confidentiality and user authentication are correlated. Protecting a user's account from misuse is an important part of the larger problem of controlling access to cloud-based resources (such as objects, memory, devices, and soft MARCH/ APRI L 201 5 IEEE CLOUD COMPUTING 31ware). Cryptographic authentication solutions can help facilitate secure resource utilization. However, depending on the cloud deployment model, key management (assignment, distribution, and revocation)must be efficient and manageable at a large scale.

cipher techniques were merged with structural aspects of Simplified Data Encryption Standard (SDES) and Data Encryption Standard (DES). In which 64 bit block size of plain text is taken which is fixed and this 64 bit plain text is divided into two halves by using the "black box" the right half have 2 bits whereas left half has 6 bits, then these 6 bits are feed into "superior function" block where these 6 bits are further separated in two halves where first two bits represent the rows and last four bits represent the column by identifying the rows and column the corresponding value can be selected. Then this function is applied to all 8 octets of the output of vigenere block the resultant of black box is again of 64 bits then these bits are further divided into 4 new octants similarly right 4 bits are unified to formulate right halves. Finally left and right halves are XOR-ed to obtain left half of this arrangement. This process is repeated three times.

The results show that most common approach was encryption (45%) to assure the data security in cloud. In [27] a digital signature with RSA algorithm scheme is proposed to ensure the data security in cloud. In which software used to crunch down the data documents into few lines by using "hashing algorithm". These lines are called message digest then software encrypts the message digest with his private key to produce the digital signature. Digital signature will be decrypted into message digest by the software with own private key and public key of sender.

There are two widely used methods to retrieve the cipher text. First, there is a safety index-based approach which establishes a secure cipher text key words indexed by checking the existence of key words [13]. Second, there is a cipher text scanning-based approach which confirms the existence of key words by matching each word in cipher text [14]. ranked data confidentiality and audit-in gat number three in the list of top ten obstacles impeding widespread cloud adoption. The cloud service pro-viderscan access the data without. authorization from the user[2, 10] and other machines in cloud can also access the data .

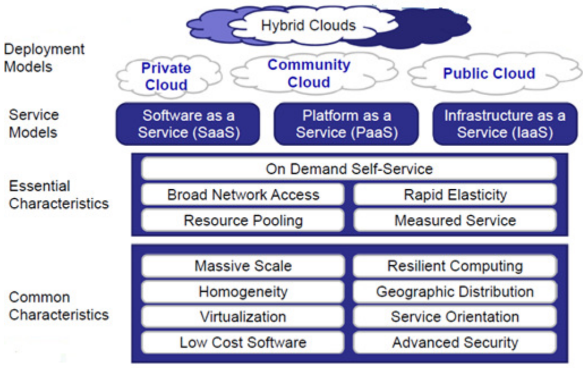
Cryptographic keys need to be stored and pro-tected. Compromise or failure of a key storage facility may lead to the loss of data. Therefore, cryptographic keys must be stored in a robust manner and a single point of failure should not affect the availability of data[10].The security concerns of outsourcing data to public clouds, serves as our motivation to work for the Development of data security technique. We aim for a tech-niquecapable of addressing the aforementioned. The main attributes of cloud computing are Multi-tenancy, massive scalability, elasticity, pay as you go and self-provisioning of resources

The services model of cloud computing is divided into three categories (1) IaaS (infrastructure as a service) provides the use of virtual computer infrastructure environment, online storage, hardware, servers and networking components; (2) PaaS (plat form as a service) provides platform for developing applications by using different programming languages; (3) SaaS (software as a service) enables the user to access online applications and software that are hosted by the service providers. The deployment model of cloud computing include (1) public cloud, that owned by service provider and its resources are rented or sold to the public (2) private cloud, that is owned or rented by an organization (3) community cloud, that is similar to private cloud but cloud resources is shared among number of closed community (4) hybrid cloud, exhibits the property of two or more deployment models [19]. Figure 1 shows the NIST definition framework for cloud computing. The cyber infrastructure enables the collection analysis of data from millions of various distributed end points such as smart meters, phasor measurement units, and circuit breakers, etc.

2.Resarch Methodology

In this research work we focused on the data security issue in cloud computing environment. Public cloud deployment model mostly suffers from the risk of data security. On the other hand, in SaaS delivery model client is dependent on service provider for proper security measures. The provider must implement some strict security measures to keep multiple users from seeing each other's data and gain the trust of users. Recent reviews on security issues in cloud computing are presented in [21, 22, 23] but these reviews are limited and not focused on detail study of data security issue. Neither of them adopts a proper literature review process. In our study we focused in details study on data security issue by adopting a proper systematic literature review process.

Empirical studies are now being undertaken more frequently, as a means of examining a broad range of phenomenon in computer field. A systematic literature review presented in [24] is followed in this research work to conduct the review. The review process is shown in figure 3. A systematic literature review endeavour to provide a comprehensive review of current literature relevant to a specified research questions. Many researchers contribute their efforts in the field of software engineering/computer science by adopting [24] systematic literature review process such as in [25, 26] systematic literature review process is adopted for the review of aspect oriented implementation of software product lines components and software component reusability assessment



3.Conclusion

Some of the benefits are using the cloud computing are cost efficiency, quick deployment, improved accessibility etc. There are many practical problems to be solved. One is data confidentiality. So many resarchers are contributed their efforts to minimised the data security. The data security is focused the different solutions. A survey of the work in the cloud computing data security. The security is based on the techinques for using encryption is the majority experimentation to validate.This result is focused only the encryption techniques for data concealment n cloud computing. We must implementated for more authorised in the protection of the data security is very authenticated.

Although our review of my work is trust and confidence of cloud computing by using the enchancesment of data security. A literature review of the works in the area of cloud computing data security is conducted and the results of review are presented in this paper. The results show that the majority of approaches are based on encryption (45%) out of which 71% encryption techniques results are validated. 67% of encryption techniques used experimentation to validate the results. These results point towards the fact that most of researchers show their interest in encryption technique to enhance the security of data in cloud computing environment. The results also reveals the fact of lack of validation in proposed approaches as 42% of the studies provide no validation of the results out of which 67% are guidelines. We must be design the structure frame of the data security in cloud computing.

BIBLIOGRAPHY

2. M. Bellare, S. Keelveedhi, and T. Ristenpart,“Message-Locked Encryption and Secure Deduplication,”*Advances in Cryptology* (EUROCRYPT13), LNCS 7881, 2013, pp. 296–312.

3. J. Li et al., “A Hybrid Cloud Approach for SecureAuthorized Deduplication,” *IEEE Trans. ParallelDistributed Systems*, vol. 26, no. 5, 2015, pp.1206–1216.

[1] NIST SP 800-145, “A NIST definition of cloud computing”, [online] 2012, http://csrc.nist.gov/publications/drafts/800-145/Draft-SP- 800-145_cloud-definition.pdf (Accessed: 23 December 2013).

[2] Gartner,”What you need to know about cloud computing security and compliance”(Heiser J), [online] 2009, https://www.gartner.com/doc/1071415/need-know-cloud- computing- Security (Accessed 23 December 2013).

[3] IDG Cloud Computing Survey: “Security, Integration Challenge Growth”, [online] http://www.forbes.com/sites/louiscolumbus/2013/08/13/idg- cloud-computing-survey- (Accessed: 28 December 2013).

[4] Ricadela, “Cloud security is looking overcast”[online] http://www.businessweek.com/magazine/cloud-security- is-lookin g-overcast-09012011.html. (Accessd: 29December 2013).

[5] S. Kamara and K. Lauter, “Cryptographic cloud storage,” *Financial Cryptography and Data Security,*Springer Berlin Heidelberg, 2010, pp. 136-149. [12] S. Kamara and K. Lauter, “Cryptographic cloud storage,” *Financial Cryptography and Data Security,*Springer Berlin Heidelberg, 2010, pp. 136-149. [12] S. Kamara and K. Lauter, “Cryptographic cloud storage,” *Financial Cryptography and Data Security,*Springer Berlin Heidelberg, 2010, pp. 136-149.

[6]M. Kaufman,”Data security in the world of cloud compu-ting,”*IEEE Security andPrivacy*,Vol. 7, No. 4, 2009, pp. 61-64.

[7] Cloud Security Alliance, “Security Guidance for Critical Areas of Focus in Cloud Computing”[online] https://cloudsecurityalliance.org/csaguide.pdf (Accessed 26 December2013)

[8] J. Archer et al., “Top Threats to Cloud Computing,” in *Cloud Security Alliance* [online] https://cloudsecurityalliance.org/topthreats/csathreats.v1.0.pdf (Accessed: 26 December 2013).

[9] Crampton, J., Martin, K., & Wild, P. (2006, 0-0 0). *On key assignment for hierarchical access control.* Paper presented at the Computer Security Foundations Workshop, 2006. 19th IEEE.

[10] D.Feng, et al. "Study on cloud computing security." *Journal of Software* 22.1 (2011): pp.71-83.

[11] R. Chow*, et al.*, "Controlling data in the cloud: Outsourcing computation without outsourcing control," presented at the Proceedings of the 2009 ACM workshop on Cloud computing security, Chicago, Illinois, USA, 2009.

[12] S. Dawn Xiaoding*, et al.*, "Practical techniques for searches on encrypted data," in *Security and Privacy, 2000. S&P 2000. Proceedings. 2000 IEEE Symposium on*, 2000, pp. 44-55.

[13] Michael Annbrust etc.,Above the Clouds: A Berkeley View of Cloud Computing, http: //eecs.berkeley.edu/Pubs/TechRpts/2009 /EECS 2009-28.pdf:2009.2 .

[14] Deyan, C., & Hong, Z. (2012, 23-25 March 2012). *Data Security and Privacy Protection Issues in Cloud Computing.* Paper presented at the Computer Science and Electronics Engineering (ICCSEE), 2012 International Conference on.

[15] Seccombe, A., Hutton, A., Meisel, A., Windel, A., Mohammed, A., & Licciardi, A. (2009). Security guidance for critical areas of focus in cloud computing, v2. 1. *Cloud Security Alliance*.

[16] T. Mather and S. Latif, “Cloud Security and Privacy,[online] 2009, http://www.slideshare.net/USFstudent1980 /cloud- computing security-concerns (Accessed: 4 September 2013)

[17] IBM, “what is cloud computing” [online] http://www.ibm.com/cloud-computing/in/en/what- is-cloud-computing.html (Accessed: 14 December 2013)

[18] Mell Peter and Grance Tim, “Effectively and securely using the cloud computing paradigm” [online] 2011, http://csrc.nist.gov/groups/SNS/cloud computing/cloudcomputing-v26.ppt (Accessed 18 August 2013).
International Journal of Computer Applications (0975 – 8887) Volume 94 – No 5, May 2014