Annals of R.S.C.B., ISSN:1583-6258, Vol. 25, Issue 4, 2021, Pages. 71 - 75
Received 05 March 2021; Accepted 01 April 2021.

Cloud Data Protection using Data Protection as a Service

K. Chandra Aviniash[1], K. Hareesh[2], Jesudoss A[2]
[1*,1] UG Student, Department of Computer Science and Engineering,
Sathyabama Institute of Science and Technology, Chennai, India
[2]Associate Professor, Department of Computer Science and Engineering,
Sathyabama Institute of Science and Technology, Chennai, India
chandrakuchivada@gmail.com,
hareeshkondabolu@gmail.com,
jesudossas@gmail.com

Abstract. Offering strong data protection to cloud users while enabling rich applications is a challenging task. We explore a new cloud platform architecture called Data Protection as a Service, which dramatically reduces the per-application development effort required to offer data protection, while still allowing rapid development and maintenance.

Keywords: Cloud, Protection, Storage, Security.

1 Introduction

Cloud computing promises lower costs, rapid scaling, easier maintenance, and services that are available anywhere, anytime. A key challenge in moving to the cloud is to ensure and build confidence that user data is handled securely in the cloud. A recent Microsoft survey found that "...58% of the public and 86% of business leaders are excited about the possibilities of cloud computing. But, more than 90% of them are worried about security, availability, and privacy of their data as it rests in the cloud." There is tension between user data protection and rich computation in the cloud[21,22]. Users want to maintain control of their data, but also want to benefit from rich services provided by application developers using that data[19,20]. At present, there is little platform-level support and standardization for verifiable data protection in the cloud. On the other hand, user data protection while enabling rich computation is challenging[17,18]. It requires specialized expertise and a lot of resources to build, which may not be readily available to most application developers[15,16]. We argue that it is highly valuable to build in data protection solutions at the platform layer: The platform can be a great place to achieve economy of scale for security, by amortizing the cost ofmaintaining expertise and building sophisticated security solutions across different applications and their developers[13].

2 Literature Survey

Cloud computing is the provision of dynamically scalable and often virtualized resources as a services over the internet Users need not have knowledge of, expertise in, or control over the technology infrastructure in the "cloud" that supports them [1]. Cloud computing represents a major change in how we store information and run applications [2]. Instead of hosting apps and data on an individual desktop computer, everything is hosted in the "cloud an assemblage of computers and servers accessed via the Internet [3]. The data-protection-as-a-service cloud platform architecture dramatically reduces the per-application development effort required to offer data protection while still allowing rapid development and maintenance [4]. The Data is protected on the cloud using various encryption techniques and the keys are shared between parties through alternative channel for enhanced security [5]. Security is the core element of an application particularly for Healcare systems. Hence it is designed considering all possibile

Annals of R.S.C.B., ISSN:1583-6258, Vol. 25, Issue 4, 2021, Pages. 71 - 75
Received 05 March 2021; Accepted 01 April 2021.

vulnerabilities in the system [6,16,17]. Christy A et al (2015) cluster-based metrics are efficient in analyzing outliers than distance-based metrics [7]. G. M. Gandhi and Salvi proposes that each car should be connected to a shared public ledger where they can share their experience so that all the cars possessing that shared ledger can learn when to stop from the experience of one single car thereby eliminating the cumbersome task of training each car separately. This collective learning can be carried out using Block chain Technology [8]. Prayla et al.(2016) have made an attempt to mitigate the botnet attacks by detecting the same in early stage[14,18,19]. The real network is captured and they have used botminer algorithm with K means and C means clustering to detect the attacks. Their results have shown a remarkable result in the early detection[9]. Jesudoss et al proposed a security framework for healthcare information system which works based on password encryption scheme that authenticates every user in an innovative way [10]. Indhuja D et al (2016) proposed a auto precautionary program explains the different techniques that can be used to avoid accidents by identifying their cause and by offering facilities that stop the unfortunate from occurring [11,20]. M.S.Roobini et al (2019) proposed disease identifying framework using ANN, Naïve Bayes, KNN algorithms for classification of Diabetes Mellitus [12,13,14,15].

3 Motivation

Cloud computing promises lower costs, rapid scaling, easier maintenance, and service availability anywhere, anytime, a key challenge is how to ensure and build confidence that the cloud can handle user data securely. A recent Microsoft survey found that “58 percent of the public and 86 percent of business leaders are excited about the possibilities of cloud computing. But more than 90 percent of them are worried about security, availability, and privacy of their data as it rests in the cloud.”

4 Proposed Work

We propose a new cloud computing paradigm, data protection as a service (DPaaS) is a suite of security primitives offered by a cloud platform, which enforces data security and privacy and offers evidence of privacy to data owners, even in the presence of potentially compromised or malicious applications. Such as secure data using encryption, logging, key management. The figure 1 shows the architecture of Proposed System.
Cloud Computing Cloud computing is the provision of dynamically scalable and often virtualized resources as a services over the internet Users need not have knowledge of, expertise in, or control over the technology infrastructure in the "cloud" that supports them. Cloud computing represents a major change in how we store information and run applications. Instead of hosting apps and data on an individual desktop computer, everything is hosted in the "cloud"—an assemblage of computers and servers accessed via the Internet. Cloud computing exhibits the following key characteristics:

1. Agility improves with users' ability to re-provision technological infrastructure resources.

2. Multi tenancy enables sharing of resources and costs across a large pool of users thus allowing for:

3. Utilization and efficiency improvements for systems that are often only 10–20% utilized.

4. Reliability is improved if multiple redundant sites are used, which makes well designed cloud

Annals of R.S.C.B., ISSN:1583-6258, Vol. 25, Issue 4, 2021, Pages. 71 - 75
Received 05 March 2021; Accepted 01 April 2021.

computing suitable for business continuity and disaster recovery.

5. Performance is monitored and consistent and loosely coupled architectures are constructed using web services as the system interface.

6. Security could improve due to centralization of data, increased security focused resources, etc., but concerns can persist about loss of control over certain sensitive data, and the lack of security for stored kernels. Security is often as good as or better than other traditional systems, in part because providers are able to devote resources to solving security issues that many customers cannot afford. However, the complexity of security is greatly increased when data is distributed over a wider area or greater number of devices and in multi-tenant systems that are being shared by unrelated users. In addition, user access to security audit logs may be difficult or impossible. Private cloud installations are in part motivated by users' desire to retain control over the infrastructure and avoid losing control of information security.
7. Maintenance of cloud computing applications is easier, because they do not need to be installed on each user's computer and can be accessed from different places.

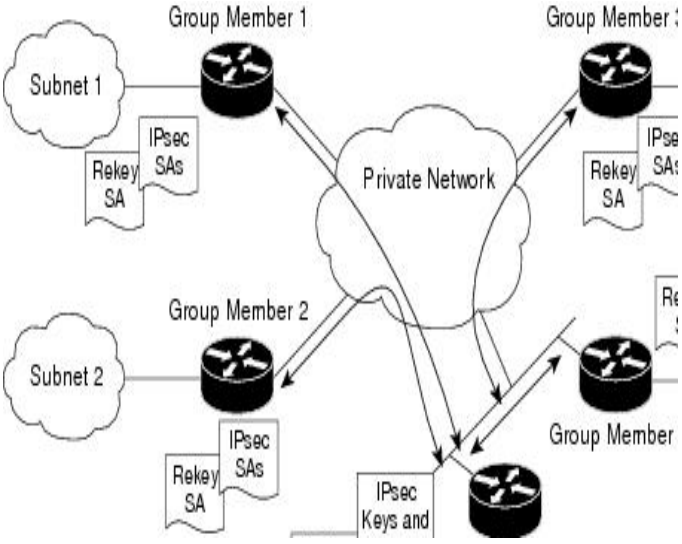

Fig. 1. Architecture of Proposed System

Trusted Platform Module Trusted Platform Module (TPM) is both the name of a published specification detailing a secure crypto processor that can store cryptographic keys that protect information, as well as the general name of implementations of that specification, often called the "TPM chip" or "TPM Security Device". The TPM specification is the work of the Trusted Computing Group. Disk encryption is a technology which protects information by converting it into unreadable code that cannot be deciphered easily by unauthorized people. Disk encryption uses disk encryption software or hardware to encrypt every bit of data that goes on a disk or disk volume. Disk encryption prevents unauthorized access to data storage. The term "full disk encryption" (or whole disk encryption) is often used to signify that everything on a disk is encrypted, including the programs that can encrypt bootable operating system partitions. But they must still leave the master boot record (MBR), and thus part of the disk, unencrypted. There are, however, hardware based full disk encryption systems that can truly encrypt the entire boot disk, including the MBR.

Third Party Auditor In this module, Auditor views the all user data and verifying data and also changed data. Auditor directly views all user data without key. Admin provided the permission to Auditor. After auditing data, store to the cloud.

User Module User store large amount of data to clouds and access data using secure key. Secure key provided admin after encrypting data. Encrypt the data using TPM. User store data after auditor, view and verifying data and also changed data. User again views data at that time admin provided the message to user only changes data.

5 Conclusion

In the first phase of our project we have developed two modules out of four modules. Our first module is User module with registration with his login session. In the second module we have implemented data storage with encryption and decryption. In the Second Phase of our project we have tried to develop the cloud Server and making it secure and one more thing is we are tried to develop an auditor module. In its future scope this can be done as Android application.

References

1. Smith TF, Waterman MS (1981) Identification of common molecular subsequences. J Mol Biol 147:195–197. doi:10.1016/0022-2836(81)90087-5
2. May P, Ehrlich H-C, Steinke T (2006) ZIB structure prediction pipeline: composing a complex biological workflow through web services. In: Nagel WE, Walter WV, Lehner W (eds) Euro-Par 2006. LNCS, vol 4128. Springer, Heidelberg, pp 1148–1158. doi:10.1007/11823285_121
3. Foster I, Kesselman C (1999) The grid: blueprint for a new computing infrastructure. Morgan Kaufmann, San Francisco
4. Czajkowski K, Fitzgerald S, Foster I, Kesselman C (2001) Grid information services for distributed resource sharing. In: 10th IEEE international symposium on high performance distributed computing. IEEE Press, New York, pp 181–184.
5. doi:10.1109/HPDC.2001.945188
6. Foster I, Kesselman C, Nick J, Tuecke S (2002) The physiology of the grid: an open grid services architecture for distributed systems integration. Technical report, Global Grid Forum
7. National Center for Biotechnology Information. http://www.ncbi.nlm.nih.gov
8. Christy A, Gandhi M.G and Vaithyasubramanian, S (2015),'Cluster based outlier detection algorithm for Health care data', Procedia Computer Science 50, Pp. 209-215
9. G. M. Gandhi and Salvi, "Artificial Intelligence Integrated Blockchain For Training Autonomous Cars," 2019 Fifth International Conference on Science Technology Engineering and Mathematics (ICONSTEM), Chennai, India, 2019, pp. 157-161.
10. S.Prayla shyry, Asha Deepika,R.Subhashini"Efficient identification of bots by K-means clustering " Proceedings of the International Conference on Soft Computing Systems (pp.307-318)",2016
11. Jesudoss A. and Subramaniam N.P., "EPBAS: Securing Cloud-Based Healthcare Information Systems using Enhanced Password-Based Authentication Scheme", Asian Journal of Information Technology, Vol. 15, Issue 14, 2016, pp. 2457-2463.
12. M.S.Roobini,DrM.Lakshmi,(2019),"Classification of Diabetes Mellitus using Soft Computing and Machine Learning Techniques", International Journal of Innovative Technology and Exploring Engineering,ISSN: 2278-3075, Volume-8, Issue- 6S4
13. Nagarajan, G., & Minu, R. I. (2015). Fuzzy Ontology based Multi-Modal semantic information retrieval. Procedia Computer Science, 48, 101-106.
14. Nagarajan, G., & Minu, R. I. (2018). Wireless soil monitoring sensor for sprinkler irrigation automation system. Wireless Personal Communications, 98(2), 1835-1851.
15. Nagarajan, G., Minu, R. I., & Devi, A. J. (2020). Optimal Nonparametric Bayesian

Model-Based Multimodal BoVW Creation Using Multilayer pLSA. Circuits, Systems, and Signal Processing, 39(2), 1123-1132.

16. Selvan, M. P., Gupta, A., & Mukherjee, A. (2019). Give Attention to Overlapping Network Detection in Networks for Multimedia. Journal of Computational and Theoretical Nanoscience, 16(8), 3173-3177.
17. Christy, A., & Thambidurai, P. (2008). Ctss: A tool for efficient information extraction with soft matching rules for text mining.
18. Gladence, L. M., & Ravi, T. (2016). Heart Disease Prediction and Treatment Suggestion. Research Journal of Pharmaceutical Biological and Chemical Sciences, 7(2), 1274-1279.
19. Preethi, C., & Prasad, K. M. (2019, April). Analysis of Vehicle Activities and Live Streaming using IOT. In 2019 International Conference on Communication and Signal Processing (ICCSP) (pp. 0754-0757). IEEE.
20. Paul, P., & Franklin, R. G. (2016). Fragmenting the Data in Cloud for Enhancing Security and Performance. RESEARCH JOURNAL OF PHARMACEUTICAL BIOLOGICAL AND CHEMICAL SCIENCES, 7(3), 349-355.
21. Nagarajan, G., and K. K. Thyagharajan. "Rule-based semantic content extraction in image using fuzzy ontology." Int Rev Comput Softw 9, no. 2 (2014): 266-277.