ISSN (Print) : 2319-5940
ISSN (Online) : 2278-1021

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 2, Issue 3, March 2013

High level security in cloud for scalable data

P. Kiran Rao [1], V. Lakshmi Sailaja [2], Alfisha Khan [3], S. Mamatha[4]

Assistant Professor, Dept.of.IT, GPCET, Kurnool, India [1]

IV B.Tech - II SEM, Dept. of CSE, GPCET, Kurnool, India [2, 3, 4]

Abstract: Now-a-days data is more private over online, so securing the privacy of data is becoming more prominent. Providing protection to the cloud data helps the developers and users to secure the data. Adding a layer of security to the cloud at platform level by implementing various technologies makes the data secure. Data security and privacy plays a vital role for any organisation. Information stored in cloud makes organization vulnerable to external hack attacks, as all are aware that information or data over internet is not 100% secure ,but there is always lurking possibility of stealth(secrecy) of sensitive data. Cloud is great technology, which brings convenience of file sharing and using that some of us never dreamed before. Every user can lock on their files, but only needed thing is protection for the data that rests in cloud. Hence, creating a layer of security itself creates the data protection; hence this helps millions of cloud data users. By providing the protection to the data dramatically helps to reduce the per-application development effort.

Keywords: Stealth, security, vulnerable, data protection, lurking, per-application

I. INTRODUCTION

In general Cloud computing is a paradigm in which information is stored in servers on internet. Information stored in a cloud is permanent. The storage can be deployed in various configurations like public cloud, private cloud, and hybrid cloud. Cloud provides the ability to access the information or software's from internet that can be delivered on demand to the users. Users simply rent or access the software by paying for what they use only. Cloud computing promises greater flexibility, highly automated integration, cost efficient, ubiquitous network access, fast service, more storage capacity and quick deployment. Inspite of many advantages cloud computing has disadvantages too.

Privacy, security, transferability, downtime are some disadvantages. Among many issues, security is one of the major issues, providing security to the cloud users is one of the laborious tasks because user should know that they will be conceding their data to the reliable service provider and the information can't be hacked by the hackers. So that the data is confidential and would not be at any risk.

Data privacy and data security in cloud computing are appealing the consideration of users companies or organizations and cloud service providers alike. There are some security and acquiescence concerns confronting the users and providers. Hence, the users generally worry to maintain the data in cloud. Therefore, security and privacy are the challenging tasks for a user to maintain their respective data in cloud. User wants to augment their services by getting benefits. Building a secure layer provides the protection to the cloud data. By adding a security layer to the cloud data, provides the privacy and protection to the data. This solution makes the users to be tension free. Providing the protection by adding a security layer at platform level is a fine looking option, the platform level security helps to gain economies to a magnitude by providing the high level security to the scalable data for malicious applications.

Storing of information in cloud makes organizations data vulnerable to external threats and attacks, we propose a new paradigm i.e. protection to the data that provides services is the main axiom. These data protection solution at platform level enforces the data security and data privacy to the data owners, even in the case of many applications.

II. DATA SECURITY AND PRIVACY

Business trade information, online transactions, account information of banking, social networking, organization financial information, banking transactions etc, are some of the widely used applications in day-to-day life. Hence all the above applications need the privacy and security as they were used by many users. Information stored in cloud makes organization vulnerable to external hack attacks, as all are aware that information or data on internet is not 100% secure, but there is always lurking possibility of stealth (secrecy) of sensitive data.

- Building a layer of security provides the protection for the immensity data dispensation. This provides protection to the entire application.
- Developers can use this platform, as the security is provided at basic platform level which enforces the data security and privacy. The platform encompasses authentication of users, substantial communication with third party and base software environment.
- Providing security at platform level provides easy maintenance and hasty development of many applications. This ensures a high level security in cloud for scalable data by key management, access control and logging which

were added at platform level. User have their own identity management system to access control to information and other computing resources.

III. SERVICES OFFERED FOR DATA PRIVACY

Providing the services for data includes the provision of scalability and this defines a newly supplement, delivery and consumption model for IT services which are internet based. The services offered for data privacy helps to achieve the following:

- **Scalability**: The data in the cloud provides an imperative service i.e scalability. It is the aptitude of a system to increase total throughput when the resources are enlarged.
- **Easy accessibility**: Data can be accessed and retrived easily. Logs indicates and identifies the authorized users and unauthorized users.
- **Personnel security**: Service providers ensures that all the critical bulk data are masked and only authorized users can access the data.
- **Confidentiality of data**: Depending upon the third party the data is made confidential would not be at any risk.
- **Application security and integrity**: The applications in the cloud are secured by implementing the integrity, acceptance and testing procedures for outsourced application.
- **Easy development and maintenance**: Developers can develop and maintain the data easily because they can upgrade sofwares and can fix bugs easily in cloud. Service providers ensures that the data is adequately secure and it is restricted to authorized users. The third party auditor collects and produces all the information of the users activities.

IV. DATA PROTECTION FOR SECURITY AND PRIVACY

Now a days many developers and users choose up on sound agreements and unessential productive and reputational harm as a substitute constancy. Hence cloud platform helps to get a stout solution i.e by providing the protection and making the developers to develop and maintain their applications. Lost data comes into control with handing the data and information in cloud. Security and confidentiality of data and information is ensured depending on the third party. Hence, protection to the data is achieved. As security at platform level provides easy maintenance and hasty development of many applications.

Protection of data straightly addresses the issues of quick development and maintenance. Here maintenance of the cloud computing applications is easier, because they do not need to be installed on each users computer and can be accessed from different places. To provide the security at basic platform level, we add a secure layer by implementing the various technologies like encryption, key management, logging and access control. After crossing the layer of security (i.e key management, logging) only the third party and user can access the data. For encryption different algorithms are implemented in the architecture. The algorithms implemented for the data security and privacy are FDE and FHE. Hence, encryption plays an prominent role in providing the security to the cloud data users as well as to the developers.

ENCRYPTION

Encryption is a technique which is used to convert the data in to unreadable format i.e cipher text. The use of encryption is generally fast and straightforward. The implementation of encryption algorithms technically depends upon the IT infrastructure and software environment, so that this helps to verify the scalability and its integrity of the source data.

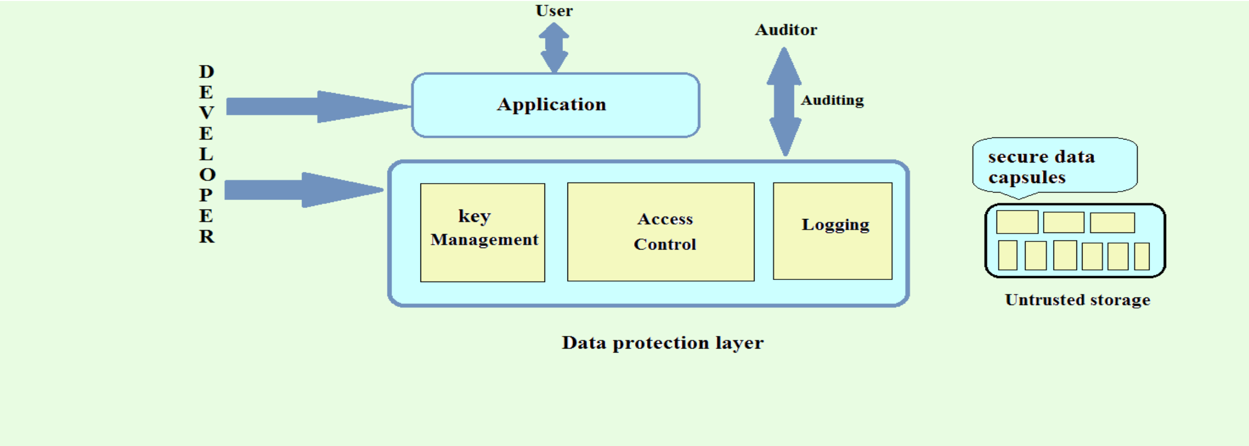

Fig 1 :Architecture for security and privacy

FDE

FDE is disk encryption technology which is used to protect the information of the data by converting the data into an unreadable code.The unreadable code cannot deciphered easily by the unauthorized users.This disk encryption encrypts the every bit of data that is present in the disk and also prevents unauthorized users to access the data and storage of data. Disk encryption does not substitutes in all situations.FDE uses the same key for the encryption and decryption of data.If an attacker gains to access the information from the system at runtime,then he can access all files.Conventional file and encryption folder then allows different keys for different portions of disk.Hence the hacker cannot extract information and data from encrypted folders and files,because in fde multiple keys are used for encrypting different partitions.

Whole disk encryption indicates that every bit present in disk gets encrypted including the programs that encrypts the bootable operating system partitions.FileVault 2 encrypts the operating systems startup volume totally.Authorized users information is uploaded from an separate non encrypted boot volume.By using master boot record in systems,then that part of disk relics non encrypted.Based upon the full disk encryption some systems encrypts the total disk including the master boot record.

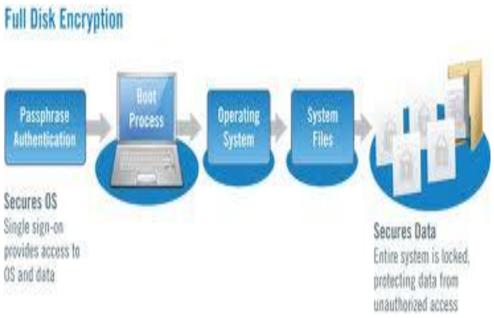
Full Disk Encryption
Passphrase Authentication
Boot Process
Operating System
System Files
Secures OS
Single sign-on provides access to OS and data
Secures Data
Entire system is locked, protecting data from unauthorized access

Fig 2 : Full disk encryption

FHE

Fully homomorphic encryption is a form a encryption,FHE allows specific types of computations to be done on ciphertext and obtains the encrypted result which is the ciphertext of the result of operations performed on plaintext. Homomorphic encryption uses hash functions,private information retrieval schemas and helps to enables widespread use of cloud computing by ensuring the privacy and security of processed data.There are several efficient homomorphic cryptosystems.If the homomorphism is treated carefully then it performs computations securely.

Creating a layer of security itself creates the data protection, hence this helps millions of cloud data users.By providing the protection to the data dramatically helps to reduce the per-application development effort.Encryption,logging,key management and access controls acts like barriers for secure storage of data.For the implementation of architecture offers evidence of privacy to the data owners,even in the presence of malicious applications.

The modules for the implementation of the architecture includes: admin, auditor i.e third party and the user. Admin is the one who deals up with all signup and registration details of the user, where as the auditor is the third party who deals with user authentication and views all user data details and verifies the data. Auditor views the user data with a key. Admin provides the permission to the auditor for viewing the data of the authenticated user.. User stores data after auditor views and verifies data. Encryption of the data is done at platform level. Platform acts correctly with respect to code loading, authorization and key management for security. Protection to the data guarantees the integrity of data via cryptography authentication of data in storage by auditing the source data at runtime. Authorization, access controls and auditing are milestones for developers.

V. CONCLUSION

The protection acts as a suite of security primitives offered. Such a layer includes encryption, logging, key management. This protection layer enforces delicate admission control policies on figures units through application confinement and information flow checking.This employs incomprehensible protections at rest and offers robust logging and auditing to provide accountability. Crucially,this application directly addresses the issues of rapid development and maintenance. As unsociable data moves online, the need to secure it properly becomes very essential.

The enjoyable details deviates the equivalent strengthening rapt data in enormous data centers will also aid in using collective security expertise more effectively. Appendix protections to a immaculate unfeeling platform rear immediately benfits hundreds of applications and by extention, hundreds of millions of users.Hence,this provides high level security in cloud for scalable data.This application can be enhanced by providing an online help line service to help the authorized users finding it difficult to work with the application or to help the new users who want to use the application.This can be further enhanced by allowing the users ,not only to upload the text files but also allowing the users to upload movies, music, videos, documents and even more.

REFERENCES

[1] C. Gentry. Fully Homomorphic Encryption Using Ideal Lattices. In STOC, pages 169–178, 2009.

[2] Greenberg. IBM’s Blindfolded Calculator. Forbes, June 2009. Appeared in the July 13, 2009 issue of Forbes magazine.

[3] S.McCamant and M. D. Ernst. Quantitative information flow as network flow capacity. In PLDI, pages 193–205, 2008.

[4] M. S. Miller. Towards a Unified Approach to Access Control and Concurrency Control. PhD thesis, Johns Hopkins University, Baltimore, Maryland, USA, May 2006.

[5] Sabelfeld and A. C. Myers. Language-Based Information-Flow Security. IEEE Journal on Selected Areas in Communications, 21(1):5–19, 2003.

[6] L. Whitney, “Microsoft Urges Laws to Boost Trust in the Cloud,” CNET News, 20 Jan. 2010.

[7] C. Dwork, “The Differential Privacy Frontier Extended Abstract,” Proc. 6th Theory of Cryptography Conf. (TCC 09), LNCS 5444, Springer, 2009, pp. 496-502.

[8] Hamlen, K. W., Morrisett, G., & Schneider, F. B. (2006). Certified In-lined Reference Monitoring on. NET. In Proceedings of the ACM SIGPLAN Workshop on Programming Languages and Analysis for Security (PLAS).

[9] L. Whitney, “Microsoft Urges Laws to Boost Trust in the Cloud,” CNET News, 20 Jan. 2010.

[10] E. Naone, “The Slow-Motion Internet,” Technology Rev.Mar./Apr. 2011; GoogleSpeed_charts.pdf.

[11] Devries, B. W., Gupta, G., Hamlen, K. W., Moore, S,& Sridhar, M. (2009). ActionScript Bytecode Verification with Co-Logic Programming. In Proceedings of the ACM SIGPLAN Workshop on Programming Languages and Analysis for Security (PLAS).

[12] P. Maniatis et al., “Do You Know Where Your Data Are? Secure Data Capsules for Deployable Data Protection,” Proc. 13th Usenix Conf. Hot Topics in Operating Systems (HotOS 11), Usenix, 2011; www.usenix.org/events/hotos11/ tech/final_files/ManiatisAkhawe.pdf.

[13] Q. Wang, K. Ren, W. Lou, and Y. Zhang, “Dependable and Secure Sensor Data Storage with Dynamic Integrity Assurance,” Proc. of IEEE INFOCOM, 2009.

[14] D. L. G. Filho and P. S. L. M. Barreto, “Demonstrating Data Possession and Uncheatable Data Transfer,” Cryptology ePrint Archive, Report 2006/150, 2006.

[15] G. Ateniese, R. D. Pietro, L. V. Mancini, and G. Tsudik, “Scalable and Efficient Provable Data Possession,” Proc. of SecureComm ’08, pp. 1–10, 2008.

BIOGRAPHY

P. Kiran Rao received the degree in B.Sc computer science engineering from the St. Joseph degree college, Kurnool, M.C.A degree from Sri Kottam Tulasi Reddy Memorial College of Engineering, JNTUH and the M.Tech degree in computer science from the JNTU College of Engineering, Anantapur. He is currently working as an Assistant Professor in Department of Computer Science in G. Pullaiah College of Engineering and Technology, Kurnool.

Lakshmi Sailaja pursuing her B.Tech Final Year in Computer Science and Engineering in G.Pullaiah College of Engineering and Technology, Kurnool and a Member of CSI.

Alfisha Khan pursuing her B.Tech Final Year in Computer Science and Engineering in G.Pullaiah College of Engineering and Technology, Kurnool and a Member of CSI.

S.Mamatha pursuing her B.Tech Final Year in Computer Science and Engineering in G.Pullaiah College of Engineering and Technology, Kurnool and a Member of CSI.