INTERNATIONAL JOURNAL OF RESEARCH IN COMPUTER APPLICATIONS AND ROBOTICS
ISSN 2320-7345

DPaaS security suit for data protection in Cloud

[1]Varun Reddy K, [2]Jagadeeshwar Rao E
[1]*Dept. of Computer Science & School of IT, Jawaharlal Nehru Technological University, India.*
[2]*Dept. of Computer Science & School of IT, Jawaharlal Nehru Technological University, India*
varunr29@gmail.com

Abstract

Enabling rich applications and at the same time offering strong protection to data in the cloud easy is a challenging task. The cryptographic security solutions applied over internet cannot directly be applied to the environment of cloud. This paper presents available security solutions- homographic encryption and disk encryption methods and proposes a security suit which combines the benefits of both the techniques- Data protection as a service. The efforts to combine the benefits of both the techniques give rise to further more possibilities. The author hopes that all the security requirements are met by a single platform layer security suit and there would be scope for further development.

Keywords: Cloud computing Security, data protection, Homographic Encryption, Disk Encryption, data protection as a service- Security Suit

1. Introduction

Cloud computing provides lower prices, fast scaling, simpler maintenance, service and availability anytime, anywhere. A key challenge is how to ensure and build confidence that the cloud can handle user data securely. A recent survey by Microsoft found that "58 percent of the people and 86 percent of business personnel are excited about the probability of cloud computing. But more than 90 percent of them are unclear about security, availability, and privacy of their data as it rests in the cloud."

Major concerns in cloud computing is the massive concentration of risk:

- Expected loss from a single breach can be significantly larger. In case of a breach a huge amount of data in cloud is a risk. So, a cloud demands for a hack proof and explosion proof security.
- Concentration of "users" represents a concentration of threats. More number of users gives rise to lot of management issues.

"Ultimately, you can outsource responsibility but you can't outsource accountability." To guarantee a practical solution, we consider relating to data protection as well as ease of development and maintenance.

- *Integrity*: reliable storage of user's private data and give assurance that it shall not be corrupted.
- *Privacy*: Un-authorized personnel shall not have access to the user's private data.
- *Access transparency*: The logs containing the access information of data indicating who or what performed each access should be easily available.
- *Ease of verification*: Users should easily be able to verify on what platform or application the code is running. They may also wish to verify whether their privacy policies have been strictly enforced by the cloud or not.

- *Rich computation*: The platform should allow computations on sensitive user data, and should be able to run those computations efficiently.
- *Development and maintenance support*: Any developer probably faces a huge list of challenges: frequent software upgrades or patches, find bugs and fix, demand for high performance by the users and continuous change of usage patterns. A credible ad efficient data protection approach must deal with these matters, which are very often overlooked in the literature on the topic.

This paper initially introduces cloud computing. The encryption techniques applicable to cloud computing, which became popular. Limitations of these methods. Key management issues are discussed. And, finally a complete security suit framed by combining above techniques, so that the benefits of both the techniques are realized.

2. Literature Review

Literature survey is an important step in software development process. Before developing any tool it is required to determine the cost, time factor and strength of the company. Once these things are checked, next task is to determine which OS or language can be used to developing the tool. Once the programmers begin building the tool, they are going to need a lot of external assistance. This support can be obtained from websites or senior programmers.

Before building the system the below understanding are required for developing the proposed system.

3. Cloud Computing

Cloud computing is delivering of computing as a service instead as a product, thereby sharing resources, software, and information. Just like the electricity grid where in the user does not produce electricity, instead he pay for his usage.

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 enables sharing of resources and costs across a large pool of users thus allowing for effective usage of recourses. This improves normal hardware usage wherein often only 10–20% utilized.

Cloud computing improves multiple redundant sites, which makes well-designed cloud computing suitable for business continuity and disaster recovery. Cloud computing is very well monitored, consistent and loosely coupled architectures, which are constructed using web services as the system interface.

Cloud applications are easier to build and handle, because they do not need to be installed on each user's computer and can be accessed from different places.

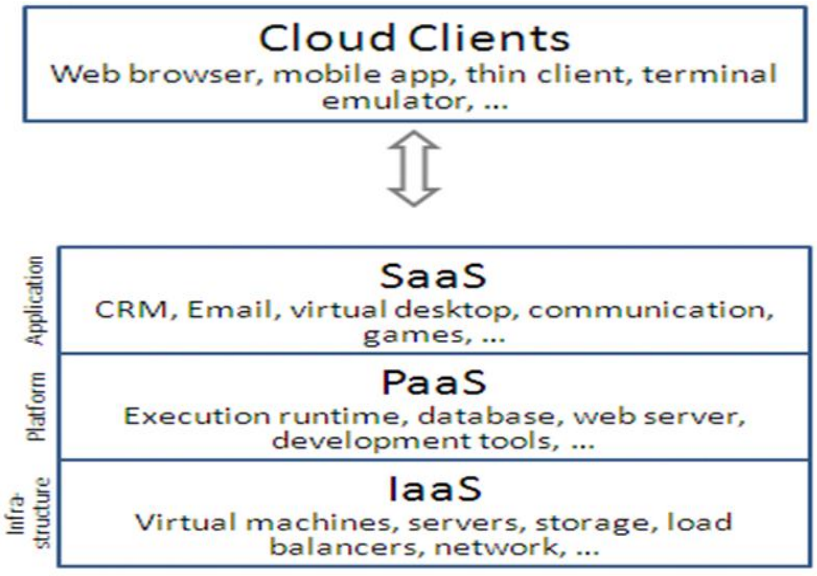

Figure. 1 Services offered to clients in cloud computing

3. Data Protection as a Service

Presently, users rely primarily on legal agreements or implied economic or reputational harm as a proxy for trustworthiness of application.

As an alternative, a platform of cloud could help achieve a robust solution by making it simple for developers to make maintainable codes that protect user data in the cloud, therefore providing the same economies of scale for security and privacy as for storage and computation, and enabling in-dependent verification for both the platform's operation and the runtime of applications on it, so that users can gain assurance that their data is being handled well.

An operating system provides isolation between tasks but allows freedom inside a process. Similarly, in cloud platforms could offer transparently verifiable partitions for programs that compute on data units, yet allowing broad commutating latitude within those partitions.

Data protection as a service enforces fine-grained access control policies on data units through application confinement and information flow checking. It employs cryptographic security and offers reliable logging and auditing to provide accountability. Data Protection as a service also directly addresses the issues of quick development and maintenance.

To support this vision, cloud platform would have to offer DPaaS in addition to their existing host environment; this would be especially useful for small firms or developers who don't have much security expertise, and helps them to build user confidence more quickly than in other way.

4. What About Encryption?

In cryptography, encryption is the process of converting one form of data to other form, usually referred to as cipher text, in such a way that only authorized parties can read it. In an encryption scheme, the message or information, usually referred as plaintext, is encrypted using an algorithm, generating cipher text that can only be read when decrypted.

The use of encryption/decryption is as old as the art of communication. At the time of war, a cipher, can be used to keep the enemy from accessing the contents of transmissions.

Full-disk encryption (FDE) computing on data have recently gained attention, but this technique have fell short in answering all the security and maintenance challenge. FDE encrypts complete physical disks with a symmetric key, for simplicity and speed. Although FDE is good at protecting private data in a few scenarios such as stolen pc's, laptops and backup tapes, it can't fulfill major data protection goals in the cloud, where physical theft is not the major problem.

On contrary, fully homomorphic encryption (FHE), offers general computation on cipher texts. The server does the actual work, but it does not know the data which it is computing. Basically, this property gives strong privacy while computing on private data, but the practicality for general cloud usage still remains a question.

5. FDE Vs FHE

Advancements are made in both fully homographic encryption and fully disk encryption security solutions. Yet, both of them have their own merits and demerits.

Data aggregation is nothing but performing various operations on data such as data mining. In fully disk encryption the encryption keys are present with the cloud itself, hence data aggregation is easy. Whereas in case of fully homographic encryption each data unit is encrypted with different keys, hence computation on data is not possible

Performance is the rate at which an operation is done. Fully disk encryption is a disk firmware and it uses symmetric encryption which allows it to run at disk's full bandwidth.

Fully homographic encryption has slower response. A goggle search would take a 1 trillion more time using fully homographic encryption.

Ease of development is more in case of fully disk encryption. Fully disk encryption is hidden behind an abstraction of physical disk and has no impact on application development.

Maintenance deals with activities such as debugging of bugs. Quickly debugging of bugs is top priority in cloud. To determine what went wrong would be difficult with fully homographic encryption. Privacy and

invisibility are very important aspects of security. Fully homographic encryption encrypts the data unit and not the disk and hence the security is always with the data. Moreover, the data itself remains invisible to the server.

6. Key management issues in cloud

Referring to the paper, "Cryptographic Key Management" by Dr Keith Martin, in which he discussed about key management issues and techniques. The security of the system mainly depends on the security of the keys. Irrespective of the algorithm used a security system without strong management procedures, there is no security.

In case of FDE, the disk is encrypted with data kept inside of it. The data itself is not encrypted. So, the keys are kept with the cloud itself. Data in the physical disk is safe until it is in the disk, but when it gets transported it is done in the clear form. Thus, there exists a threat of leakage. Moreover the user must trust the cloud completely with his data, while the cloud provider may hire a third party which might turn out to be risky.

Whereas if the keys are owned and managed by the user. It might be difficult for the cloud to perform any local user maintenance and management operations. And moreover, the safety and the reliability of the keys with the user are to be doubted. After all the main theme of cloud computing is to overcome user maintenance.

7. A Way Forward

Full-disk encryption (FDE) FDE is effective where physical theft is the main threat, such as stolen laptops and backup tapes. Disk is encrypted and not the data. But, it offers high performance.

In Fully homomorphic encryption (FHE) Security lies with the sharable data unit itself. Sever doesn't know the data it is computing. Low performance and high maintenance are drawbacks.

DPaaS approach is better suited for the target applications because it falls between the two. It keeps the "natural" granularity of FHE by keying on units of sharable data and maintains the performance of FDE by using symmetric encryption. It pushes key management and access control to a middle tier—the computing platform—to balance rapid development and easy maintenance with user-side verifiability.

DpaaS security suit performs keying on sharable data units thus implementing FHE. It uses symmetric encryption and thus implementing the advantages of FDE. Key management and access control is moved to a middle tier for easy maintenance and user side verifiability. In addition auditing of the user data is also implemented which further helps to bolster the user's confidence.

In DPaaS a TPM chip is used to provide trust.TPM can load or execute TC which provides dynamic root of trust by isolation, key management, access control and logging. TPM provide confinement by using SDC's and SEE's. A secure

Data capsule is a data unit packed with security policy, for example ACL capsule. A secure execution environment prevents leakage of user data through isolation. A SEE could be a pool of VM's or a more light weight approach is to use

OS process isolation. SDC's can be imported or exported to outside websites using policies. Additionally DPaaS can log all the instances where the data is exported. To confine the data the platform decrypts the SDC's data only in SEE in compliance with the policies. The platform also enforces ACL modifications, un-sharing or sharing and the creator of the data units can add or revoke other authorized users. DPaaS uses AES which requires more performance but once the data is loaded into SEE's it need not encrypt or decrypt again.

Auditing is done using logs. There are four basic types of logs- online data access logs, access control modification by authorized user logs, logs of offline data requests and logs relating to maintenance operations. DPaaS gives the flexibility of even using third party auditing. Ordinary user access is governed using ACL's whereas the administrator's access is governed using administrative policies.

DPaaS offers platform verifiability. This is done by logging and auditing at platform level so that all the applications running on it can share its benefits. When in offline mode the auditor verifies the working of protection features of platform. At runtime the platform provides user with trusted computing to at least for software or an application running on it.

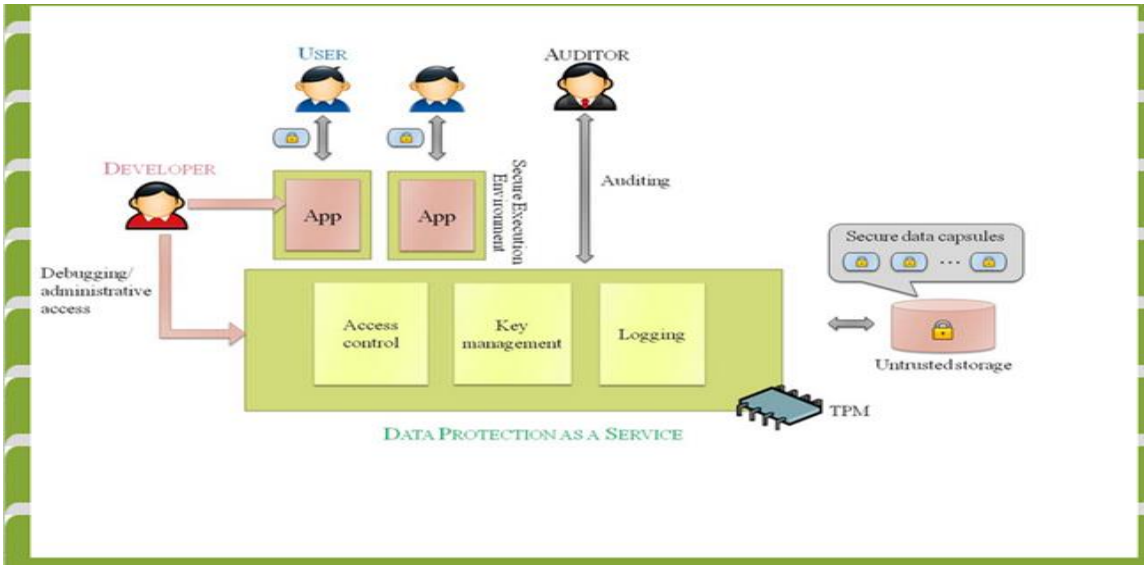

Figure. 1 DPaaS Architectural design

We can be implemented this in four modules- Cloud computing module, trusted platform module, third party auditor module and user module. Cloud computing module consists of remote cloud and storage. In trusted platform module maintains the details of all the logins and data manipulation statistics. Third party auditor is used to provide assurance to the user. It keeps the track of all kinds of modifications on data. Finally, the user module is actually a user interface. It allows the user to login with his account and perform several user related operations such as- uploading files into the cloud, checking the file status, viewing his own data. In DPaaS the security lies with the data also i.e. the data is secure inside and outside the cloud.

8. Experiments

The application is built using JSP and the database is loaded into the cloud. AES encryption techniques are used to secure the data. The data is uploaded by the user using a user interface. All the users are managed by an administrator. The uploaded data can be modified or viewed by auditor and user. The admin can also view the data. Every data requires a unique data key. The paper is successfully implemented by implementing security but not effecting performance.

9. Conclusion

Cloud computing offers utility based computing that is, pay per usage without any maintenance overhead. It saves a lot of time as it offer services anytime, anywhere and with any device. Not just time but space and cost of equipment are also saved. Cloud computing in future aims at implementing 'Internet of Things.' IOT aims at establishing network with all the objects in the world. This makes the cloud accessible from anywhere. These entire features make cloud computing most preferred for business and personal usage. Yet many people are finding it difficult to accept it, due to security concern.

FDE offers excellent performance, it does little to protect privacy at the required granularity.FHE, on the other hand, gives greater privacy in so doing, and it incurs significant performance and development costs. DPaaS approach is one which falls between the two. Still many barriers are yet to be overcome, one challenge for cloud security is that the software keeps updating with patches. One way would be to log the update history.

Auditing is a great way to bolsters the confidence of the users. The users are always kept aware of their data and operation performed on it, such as modifications, additions, permissions, sharing etc.
Other challenge is that Software verification is expensive due to large number of users, so auditors are required to use certifications to verify them.

Acknowledgement

This work is supported and made under the esteemed guidance of E. Jagadeeshwar rao garu, who is a lecturer in software engineering department at School of IT, Jawaharlal Nehru Technological University, Hyderabad.

REFERENCES

[1] C. Wang, Q. Wang, K. Ren, and W. Lou, "Privacy-Preserving public auditing for storage security in cloud computing," in Proc.of IEEE INFOCOM'10, March 2010.
[2] Maha TEBAA, Saïd EL HAJJI, Abdellatif EL GHAZI, "Homomorphic Encryption Applied to the Cloud Computing Security." In proc. Of the World Congresson Engineering 2012 Vol I WCE 2012, July 4 - 6, 2012, London, U.K.
[3] Dr Keith Martin, "Cryptographic Key Management," in2006 Information Security conference, Royal Holloway,University of London, United Kingdom.
[4] Tilo Müller, Tobias Latzo, and Felix C. Freiling, "Self-Encrypting Disks pose Self-Decrypting Risks." InAnnual Computer Security Applications Conference (ACSAC), Orlando, Florida USA, Dec. 2011. University of Illinois at Urbana-Champaign, ACM.
[5] Shivlal Mewada, Umesh Kumar Singh and Pradeep Sharma, "Security Enhancement in Cloud Computing (CC)", ISROSET-International Journal of Scientific Research in Computer Science and Engineering, Volume-01, Issue-01, Page No (31-37), Jan -Feb 2013
[6] C. Gentry, "Fully Homomorphic Encryption Using Ideal Lattices," Proc. 41st Ann. ACM Symp. Theory Computing (STOC 09), ACM, 2009, pp. 169-178.
[7] B. Bosen. "FDE Performance Comparison: Hardware Versus Software Full Drive Encryption. "In Trusted Strategies LLC, Jan. 2010.
[8] Dawn Song, Elaine Shi, and Ian Fischer, "Cloud Data Protection for the Masses." Published by the IEEE Computer Society, 0018-9162/12/$31.00 © 2012 IEEE.
[9] Shaheen Ayyub1, Devshree Roy, "Cloud Computing Characteristics and Security Issues." In International Journal of Computer Sciences and Engineering, Vol.- 1(4), pp (18-22) Dec 2013.
[10] S. McCamant and M.D. Ernst, "Quantitative Information Flow as Network Flow Capacity," Proc. 2008 ACM SIGPLAN Conf. Programming Language Design and Implementation (PLDI 08), ACM, 2008, pp. 193-205.

A Brief Author Biography

K. Varun Reddy – Pursuing master's in "Computer networks and Information technology," at school of IT, JNTU university, Hyderabad. Areas of interest include cloud computing, programming, Unix. Mail- Varunr29@gmail.com.

E. Jagadeeshwar Rao – Lecturer for School of IT, JNTU university, Hyderabad. Provided guidelines in successfully completing the project. Areas of interest include software engineering, image processing, cloud computing.