ISSN 2349-0292
Impact Factor 3.802

GLOBAL JOURNAL OF ADVANCED ENGINEERING TECHNOLOGIES AND SCIENCES

FRAMEWORK FOR CLOUD COMPUTING SECURITY

Mr. Sanket Gupta[1], Mr. Arpit Solanki [2]
[1]Student, Dr. A.P.J. Abdul Kalam University, Indore, M.P., India
[2]Assistant Professor, Dr. A.P.J. Abdul Kalam University, Indore, M.P., India
*

ABSTRACT

A full recognition of the security issues is that studies have found in recent years that the cloud may serve as a deterrent to the uptake of cloud computing. An organization loses control over its business-critical data and computations when it outsources them to the cloud on a large scale because of the authority that goes along with the data loss. offered via the cloud. How can the company identify which security measures to implement to safeguard its computations and data, which have distinct security needs from a Cloud Service Provider (CSP) with an unknown or undefined degree of corruption? The answer to this question can be found on the organization's perception about the CSP's reliability and the trustworthiness and the security requirements of its data of an organization. This paper proposes a decentralized, dynamic and evolving policy-based security framework that helps any of an organization to derive such perceptions to provide the proper authority from knowledgeable and trusted employee responsibilities and their functionality are based on that, the choice of the most relevant security policy postulating the confidential measures is very much necessary for outsourcing data and computations to the cloud. The organizational opinion is developed completely direct user participation with that particular organization and is allowed to advance with respect to the time and requirement of an organization.

KEYWORDS: Cloud, Cloud organization, Data privacy, Cloud service provider (CSP), Information Dispersal Algorithms (IDA), Security framework, Cloud security policy.

INTRODUCTION

The current situation has seen a growth in cloud computing. Customers are extremely hesitant to move their businesses to the cloud from every single firm. However, in our opinion, one of the most significant and significant issues that creates a poor impression, shrinks the enormous market for cloud computing, and causes challenges with the confidentiality of the data [2]. This problem also affects data protection and privacy. As is well known, an organization contains a number of sensitive data that needs to be kept secret from outside parties. These data can be the very much confidential data like customer data, his private business details, and his family details and so on. Such kind of data would be kept confidential from the third party while exchanging the data [1]. There may be various situations where the data have to flow but they doesn't have permission to change it, for an example employee of the organization needs to access the data of different field respective of his work because of his role in an organization so that would be not to be restricted but any other individual like ordinary employee, supplier and any customer want to access the data then he can only view the data but cannot make any change in it [3]. However, while using cloud computing, we frequently wonder if we should outsource the data and its calculations to a public cloud or not. The idea of security, the reliability of the cloud service provider, data confidentiality, data availability, and other elements will all be destroyed, along with the loss of control over the data. A few significant Legal and cross-border concerns, data privacy, and data placement are all aspects in this case.

As a result of these issues, several researchers have attempted to address them and offered solutions. They have contributed to the effort to find cloud security, and their strategy has also come close to success. An company was able to outsource its sensitive data with security needs because to their methods. When a company is By outsourcing its data, it maintains a certain level of confidence in the cloud service provider. The cloud service provider is in charge of safeguarding the data against external, internal, and third-party assaults [5]. As is well known, a service level agreement (SLA) will be struck between the company and the cloud service provider.

We attempted to develop a dynamic, decentralized approach for extremely secure cloud outsourcing as a solution to this issue. Here, we can comprehend what decentralized means because it can be defined as the accomplishment of two goals using two accounts. For instance, the CEO of the firm will advise us on how to handle his company's important financial data. In this paper we will suggest the best possible method of the organizational implementation by our acknowledgement studies.

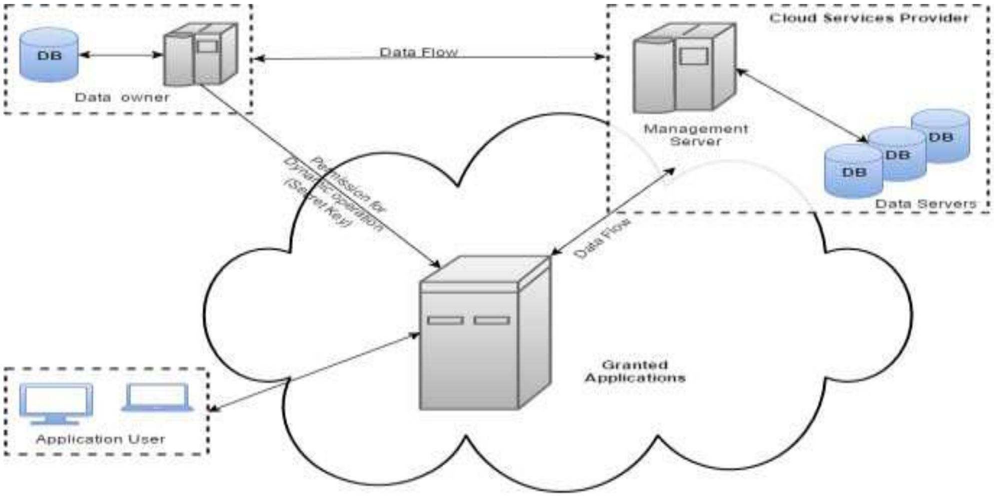

Figure 1.1 Audit System Architecture for cloud computing

The organization's cloud computing infrastructure is depicted in the above image. The data owner's data flows to the cloud service provider's data server and management server. Users of the application must authorize authorization to access the organization's data. Before granting the application user access, the verification process will be completed.

RELATED STUDY

Previous research on computing and storage in the secured cloud has carefully taken into account several adversarial models. These models take into account a Byzantine opponent, also known as the challenger, who can act randomly and compromise a limited number of servers. Three different kinds of attacks can be launched by the corrupted clouds throughout this process:
1) Storage cheats on compromised servers might alter stored data arbitrarily or remove seldom accessed files—that is, material that users cannot utilize frequently—in order to save storage costs.
2) Computation: This kind of cheating occurs when servers either produce erroneous computation results or use alternate inputs for ongoing calculations in an effort to save computational costs.
3) Privacy: This type of cheating involves a compromised cloud server that allows users' private information to be disclosed to third parties. It indicates that user data may be moved from one account to another, making it completely unpredictable.

Here, we can think about how the untrusted cloud can fail in a Byzantine [4] manner, meaning that user data stored there may be erased, altered, or leaked to third parties. This can lead to arguments and the most general fault model, which takes into consideration both malicious attacks on CSPs and unintentional data corruption. A collection of situations with varying degrees of trust attributed to It has recognized the cloud. They define a trustworthy cloud as one that has no malevolent insiders and serves users accurately in line with SLA when there are no unforeseen failures. Our security system is based on three fundamental trust relationships: organization vs user, user versus CSP, and organization versus CSP.[3] Not all users are equally trusted by the company; for example, those in higher positions are trusted more than others. Users are reliable. provides just the information and calculations related to the role that the user has been allocated. The Enterprise Data Access Policy (EDAP) matrix, which specifies the types of accesses and privileges allowed for each user and data element combination, serves as a guide for the organization's relationship with user trust. A super-user is a user who has the ability to select a security policy for the data components to which he has access.

Access control matrices specify access rights on objects. An object is the abstraction of resources controlled by a computer system. Role based access control (RBAC) [4] policies regulate a user's access to objects in a system based on the activities he performs on these. We present the EDAP matrix as an intermediate access control matrix derived from role-based access control policies used in the organization. It specifies user's data access rights from which one can validate the computation permitted for each role in the organization. We note that computations require different data elements as inputs and produce new data elements and / or modify existing data elements as output. Therefore, a user can perform a computation only when he has the necessary access rights to relevant input and output data elements [5].

PROPOSED SYSTEM

We Propose a system with several owners and applications. Institute private files and data are handled by several directors for any one institution. Data security and authentication are difficult tasks under such circumstances. We are suggesting a system with several owners, each of whom would have a unique password and access key to the organization's data and files.

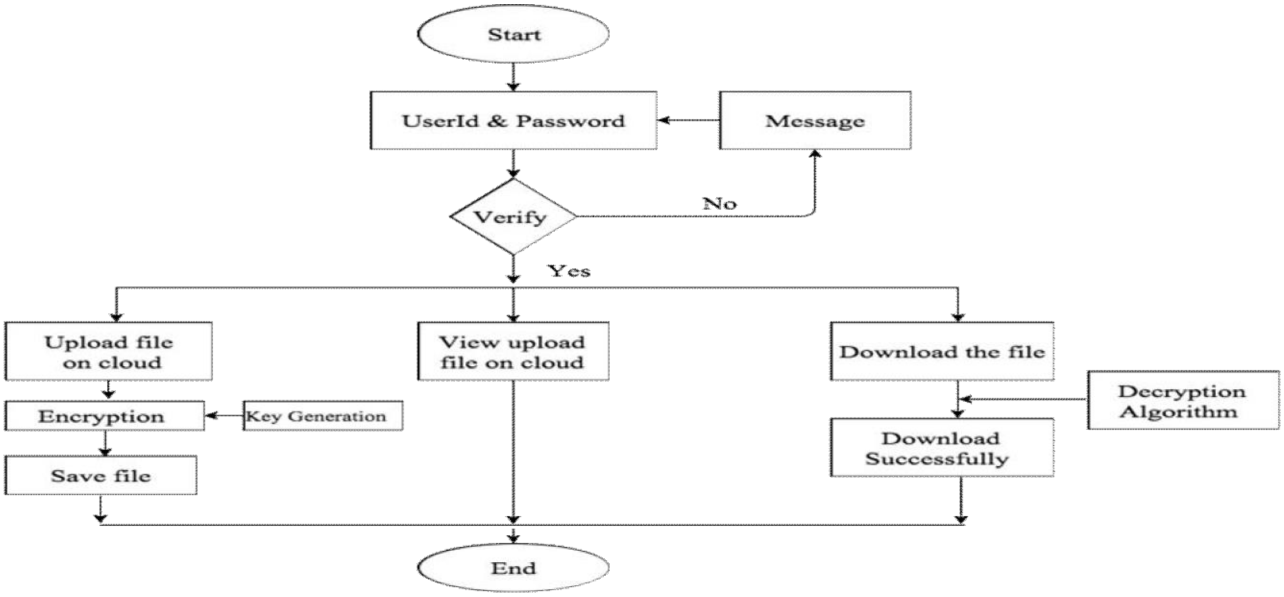

Figure 1.2 Proposed System Flow Chart

CONCLUSION

In this paper we discussed our current research on a semantic approach to our policy-based security framework for business management procedures in this article. We are aware of every security requirement that arises in daily life, and these needs are divided into two categories: task level and process level. The security framework's architecture is designed to control and execution of maintenance runtime policies. Ontology serves as the foundation for security policies, which enhance the depiction of security issues and allow for the rationale of conflicts between policy debates and detection.

REFERENCES

[1] Acquisti, and J. Grossklags, ―Privacy and Rationality in Individual Decision Making‖, IEEE Security and Privacy Vol. 3 No. 1,IEEE, 2005, pp. 26-33.

[2] M. A. AlZain, and E. Pardede, ―Using Multi Shares for Ensuring Privacy in Database-as-a-Service‖, 44th Hawaii International Conference on System Sciences, IEEE, 2011.

[3] M. A. AlZain, E. Pardede, B. Soh, and J. A. Thom, ―Cloud Computing Security: From Single to Multi-Clouds‖, 45thHawaii International Conference on System Sciences, IEEE, 2012.

[4] A. Bessani, M. Correia, B. Quaresma, F. Andre, and P. Sousa, ―DEPSKY: Dependable and Secure Storage in a Cloud-of-Clouds‖, Proceedings of the 6 th conference on computer systems EuroSys'11, ACM, New

York USA, 2011, pp. 31-46.

[5] S. Bugiel, S. Nurnberger, A. Sadeghi, and T. Schneider, „Twin Clouds: An Architecture for Secure Cloud Computing—,Workshop on Cryptography and Security in Clouds, 2011.

[6] S. Chaves, C. B. Westphall, and F. R. Lamin, —SLA Perspective in Security Management for Cloud Computing‖, 6thInternational Conference on Networking and Services, IEEE, 2010.

[7] Y. Chen, and R. Sion, —On Securing Untrusted Clouds with Cryptography‖, Proceedings of the 9th annual ACM Workshop on Privacy in Electronic Society WPES'10, ACM, New York USA, 2010, pp. 109-114.

[8] N. Christin, S. Egelman, T. Vidas, and J. Grossklags, „ It's All About the Benjamins: An empirical study on incentivizing users to ignore security advice‖, Financial Cryptography and Data Security, Springer Berlin Heidelberg, 2012, pp. 16-30.

[9] S. De, S. Saha, and A. K. Pal, —Achieving Energy Efficiency and Security in Mobile Cloud Computing‖, Proceedings of the 3 rd International Conference on Cloud Computing and Services Sciences CLOSER 2013, SciTePress, 8-10 May 2013, Aachen, Germany.