ABSTRACT

Cloud computing is a way to increase the capacity or add capabilities dynamically without investing in new infrastructure, training new personnel, or licensing new software. It extends Information Technology's (IT) existing capabilities. In the last few years, cloud computing has grown from being a promising business concept to one of the fast growing segments of the IT industry. But as more and more information on individuals and companies are placed in the cloud, concerns are beginning to grow about just how safe an environment it is. Despite of all the hype surrounding the cloud, enterprise customers are still reluctant to deploy their business in the cloud. Security is one of the major issues which reduces the growth of cloud computing and complications with data privacy and data protection continue to plague the market. The advent of an advanced model should not negotiate with the required functionalities and capabilities present in a current model. A new model targeting at improving features of an existing model must not risk or threaten other important features of the current model. 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.

Cloud computing is a flexible, cost-effective and proven delivery platform for providing business or consumer IT services over the Internet. Despite of all the hype surrounding the cloud, enterprise customers are still reluctant to deploy their business in the cloud. This research proposes a robust

security model comprising of two modules which together will make the cloud reliable and trustworthy.

A security framework that provides ‘Security as a Service’ for cloud applications and another framework that provides data storage security is proposed. The application security framework provides security as a single-tier or multi-tier based on the application’s demand. Moreover these tiers are enabled to change dynamically making the entire security system less predictable. The behavior of this framework is designed to be customizable based on the application’s importance and is localized. This design will help the cloud in adverse situations of threats, because the threats will also be localized and will not pose a threat to the entire cloud. In a cloud where there are heterogeneous asset systems, a single security system would be too costly for certain applications and if there is less security then the vulnerability factor of some applications like financial and military applications will shoot up. This consideration is incorporated within the framework, which enables security levels based on the importance of the assets of the services provided by the cloud and their respective clients. The framework was tested and the results prove the efficiency and performance of the proposed model.

The research also proposes methodologies for enabling coupling of private and dedicated security modules along with the cloud security environment. Such a feature will help the user to equip his applications with a trustworthy security even in the event of the user having a distraction away from the cloud. The flexibility in choosing security tiers will attract everyone right from individual users to conglomerates.

Enterprises are migrating to the Cloud environment at a faster pace. Security of information that is being processed by the applications and ultimately getting stored in the data centers are of big concerns of this newly evolving environment. The security of the data is a concern not only during transferring of data through the wires but also during its storage phase where data stays most of the time.

In order to keep the data secure during its storage phase, a preventive, robust security model is required. Instead of developing a robust security module to prevent hackers from intruding into data centers, a model which will prevent intruders from getting the required information even at the event of intrusion will be of utmost use. Conventional security models secure data by encryption or by fragmentation. A security model developed using a fragmentation technique that is based on the sensitivity, criticality and value of the data provides better security by means of disintegration of value of the data and also a good technique for prevention of information leaks. The proposed method also provides solutions to access the fragmented data. The proposed model provides a efficient security solution for data stored in cloud. When compared to conventional methods, the speed of data queries are less for small databases, but prove to be very efficient for huge databases. This model provides an efficient solution for data storage security in cloud environment. The proposed method classifies data at the schema level based on the criticality of each segment of data. Then the data is segregated based on importance and stored in a distributed environment. The segregated data are combined only during runtime and only during requirement. Once the

usage of data is completed, the value of the data is destroyed and stored. The research also proposes a data engine which will help in segregating data and then combining them during runtime. This engine will automatically create mapping tables and also does query composition. This technique coupled with standard encryption techniques will make this model more robust.

When the frameworks for the application and data storage security are coupled together and deployed in the cloud, the data is secured both at the transmission and storage phases. This coupled deployment will turn the cloud to a more secure, robust and trust worthy environment and users can reap the advantages of the cloud without any sacrifice to security and reliability.