ISSN:0975-9646

Cloud Security with Encryption using Hybrid Algorithm and Secured Endpoints

Sunita Rani, Ambrish Gangal
Computer Science, lovely professional University,Phagwara ,India

Abstract— Cloud providers generally states that they are not responsible for the security that means leakage of the subscribed data or unauthorized modification of the data To make secure key for the purpose of securing cloud for transactions. It would have a private cloud for highly secure transactions and it would use a public cloud for upper layer of it's application.[1] To enhance security in the cloud is a very important task.

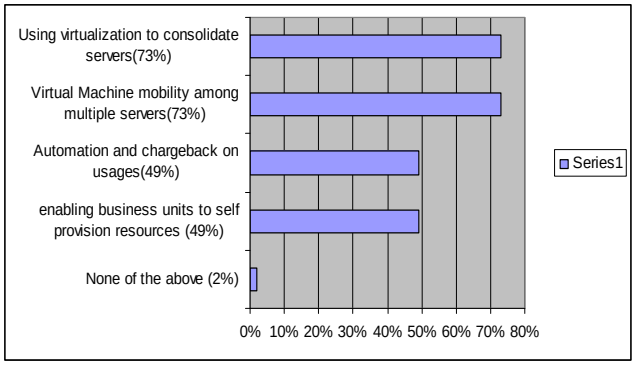
In this paper, we have proposed an encryption technique called hybrid algorithm in order to provide privacy in the cloud.

Keywords—Cloud Security, Hybrid Algorithm, Encryption.

I. INTRODUCTION

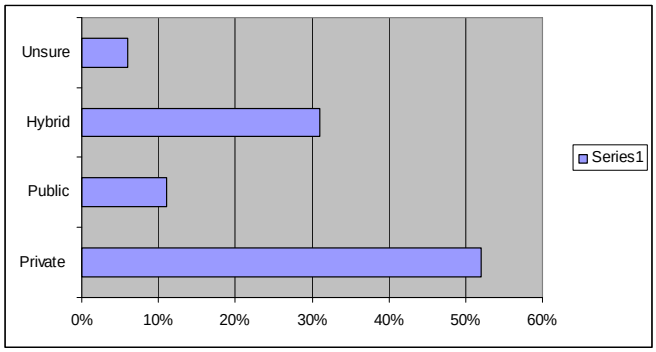
Cloud computing is a network-based environment that focuses on sharing computations or resources. Actually, clouds are Internet-based and it tries to disguise complexity for clients. [2]. During the past few years, cloud computing has grown from being a promising. business idea to one of the fastest growing parts of the IT industry. IT organizations have expresses concern about critical issues (such as security) that exist with the widespread implementation of cloud computing. These types of concerns originate from the fact that data is stored remotely from the customer's location; in fact, it can be stored at any location.[2,6]

Developers had asked IT professionals to tell what technologies they were currently deploying that support a current or planned cloud environment. Nearly three in four are currently using virtualization to consolidate servers and enabling virtual machine (VM) mobility across multiple servers (73 percent) in order to support a cloud.



[Percentage of cloud environment]

Nearly half offer automation and metering and chargeback based on usage and enable business units to self-provision resources.



[Preferred cloud development Model]

A private cloud is the leading deployment model for 52 percent of those surveyed—no matter what phase of implementation. It's most common among those already offering cloud computing (63 percent), those in the implementation phase (51 percent), and those still evaluating (49 percent). In setting up a Cloud framework that specifically addresses, organizations' information security, senior professionals and management may look to adapt and incorporate current data protection, trust and privacy policies in formulating a comprehensive set of Cloud computing guidelines. These guidelines may include:

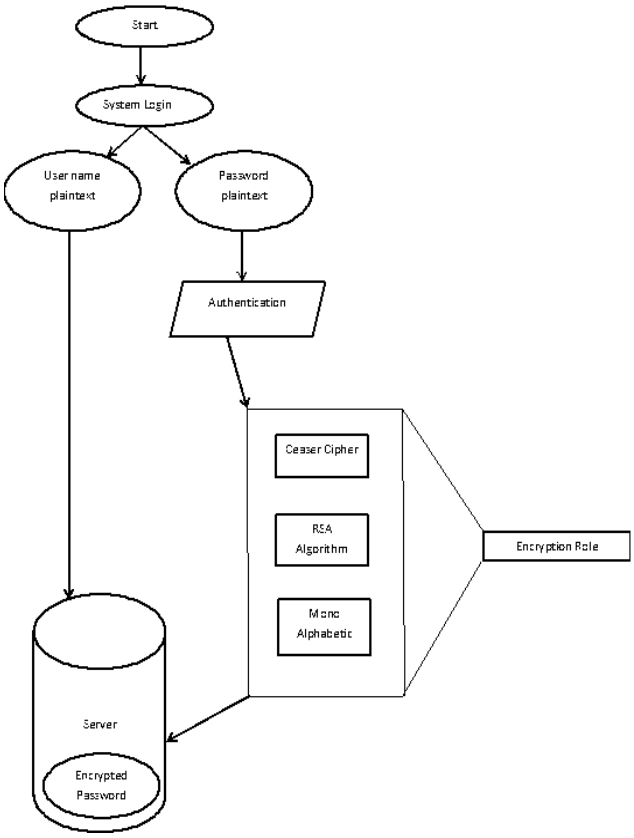
- Establishing an overall business Cloud computing policy that highlights the organizations stance on information protection.
- Govern the installation and communication of Cloud computing when IT decisions are made.
- Leverage of current IT audit and TAX processes with the in embedding cloud security disclosure and Cloud audit practices. [3,7]

II. PROPOSED ENCRYPTION TECHNIQUE

Protecting privacy in cloud providers is a technical challenge. In cloud environment, this challenge is complicated by distributed nature of clouds and lack of subscriber knowledge over where the data is stored i.e. about data center and accessibility of the users.

Suppose a user wants to login to a secured cloud system. To login into a system we must provide a correct combination of user name and password and it should be matched with the combination stored in the database whether in plaintext form or in encrypted form. For a secured login user provide login credentials and then to authenticate the user system encrypts the provided password up to the number of times defined to the system. "In the flowchart below i.e. our proposed methodology in that "Hybrid Algorithm" is used to encrypt the message by which firstly the password will be encrypted by the Ceaser cipher then the encrypted result will again be encrypted by using RSA substitution algorithm and finally the result will

again be encrypted by the mono alphabetic substation method". Then the password will be sent to the server with the plaintext user name and if it matches only then the user get access to the system. To define this problem more effectively the flowchart is given below:

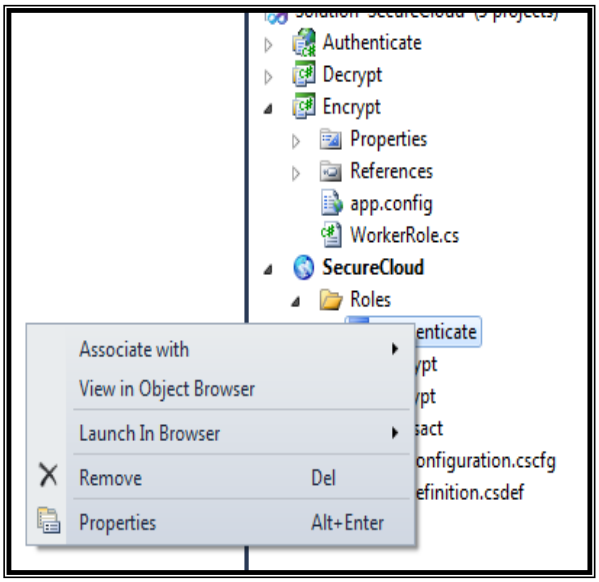


IT security pertains to protecting the confidentiality of information that is used by subscribers. Subscribers should use the strong encryption for web session whenever one application require to interact with another application or data transfer.

III. Result and Discussion

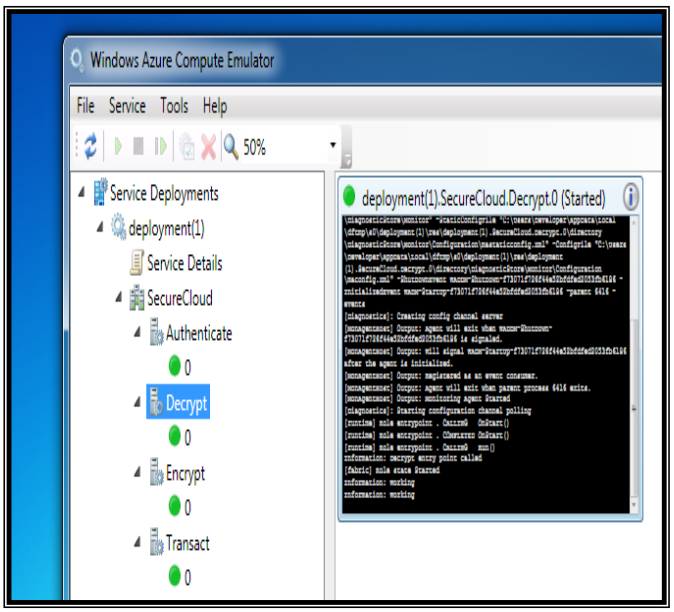
In this Research work, we have taken some results on the bases of algorithms which we have combined (i.e. Hybrid Algorithm) throughout our Research work in order to provide security by using PaaS (Platform as a sevice). For generation of encryption key best encryption method by combing algorithms is used.

By taking window Azure platform, I have shown the results of secure cloud.



For Authentication we have taken results as given below:

In this way privacy to the secured cloud is provided by which transactions can take place. Because technique behind user name and password by combining three algorithms that are RSA, Monotonic and ceaser cipher by which security is provided. Firstly Password is encrypted by the Ceaser cipher then the encrypted result is again be encrypted by using RSA substitution algorithm and finally the result is again be encrypted by the mono alphabetic substation method. Developers can benefit from this technique in order to provide security.



IV. Conclusion & Future Scope

We have proposed a best technique for securing cloud by mixture of algorithms i.e. Hybrid Algorithm. In this analysis fully delivers on the promise of merging the best aspects of dynamic and static testing into a tightly interwoven approach for rapidly resolving security vulnerabilities in software. It enables greater coverage and a far higher degree of accuracy, including first generation hybrid technology or dynamic and static testing conducted in isolation. Organizations can take advantage of this method for their transactions. Additionally, this technique can makes it possible to speed the remediation of critical issues, gain better insight into vulnerability root causes, and simplify software security assurance processes with unified reporting that organizes results by severity, correlation, common causes, and precise code location.

Finally, in Future more secure techniques can be developed in order to secure cloud. Banking application can also take also advantage by expanding their transactions on public cloud rather than private cloud. But for that appropriate techniques should be developed.

REFERENCES

[1] Sunita Rani and Ambrish Gangal "Security issues of banking adopting the application of cloud computing" International Journal of Information Technology and Knowledge Management July-December 2012, Volume 5, No. 2, pp. 243-246.

[2] Daniel Benton and Walid Negm, "Banking on cloud", 2010.

[3] Ramgovind S, Eloff MM, Smith E ,"The Management of Security in Cloud Computing", School of Computing, University of South Africa, Pretoria, South Africa ©2010 IEEE.

[4] Alok Tripathi, Abhinav Mishra," Cloud Computing Security Considerations", IT Division, DOEACC Society, Gorakhpur CentreGorakhpur, India, 2010, IEEE.

[5] Cong Wang, Qian Wang, and Kui Ren," Towards Secure and Effective Utilization over Encrypted Cloud Data", 2011 31st International Conference on Distributed Computing Systems Workshops, 2011 IEEE.

[6] I-Hsun Chuang, Syuan-Hao Li, Kuan-Chieh Huang, Yau-Hwang Kuo," An Effective privacy protection scheme for cloud computing",IEEE 2011.

[7] Jianfeng Yang and Zhibin Chen ," Cloud Computing Research and Security Issues", IEEE 2010.