7. EXISTING ALGORITHMS FOR CLOUD SECURITY

Many organizations and people store their important data on cloud and it is also accessed by many persons, so it is very important to secure the data from intruders. To provide secure communication over the network, encryption algorithm plays a vital role. It is the fundamental tool for protecting the data. Encryption algorithm converts the data or plaintext message into cipher text by using "the key" and only the user has the key to decrypt the data. In Symmetric key encryption, only one key is used to encrypt and decrypt the data. Another technique is using asymmetric key encryption where two keys- private and public keys are used. Public key is used for encryption and private key is used for decryption [12].

We are presenting some popular security algorithms used for data security in cloud computing.

RSA algorithm- The most common Public Key algorithm is RSA, named for its inventors Rivest, Shamir, and Adleman (RSA). RSA is basically an asymmetric encryption /decryption algorithm which involves both public and private key. The public key can be known to everyone and is used for encrypting messages which can only be decrypted using the private key. So, in our Cloud environment, Pubic-Key is known to all, whereas Private-Key is known only to the user who originally owns the data. Thus, encryption is done by the Cloud service provider and decryption is done by the Cloud user or consumer. Once the data is encrypted with the Public-Key, it can be decrypted with the corresponding Private-Key only.

DES algorithm- Data Encryption Standard (DES) is very commonly used symmetric key algorithm. It was the first encryption standard to be recommended by NIST (National Institute of Standards and Technology). It divides the whole message into blocks of 64 bits which encrypts and produces 64 bits of cipher text. The same algorithm and key are used for encryption and decryption. The key length of this algorithm is 56 bits; however, a 64 bits key is the actual input. The drawback of DES is that the key used in DES is very small and its security can be broken easily and DES works fast on hardware only and woks slowly on software.

AES algorithm - Advanced Encryption Standard (AES) is the new symmetric key encryption standard recommended by NIST to replace DES. Brute force attack is the only effective attack known against it, in which the attacker tries to test all the characters combinations to unlock the encryption. Both AES and DES are block ciphers. Each of these ciphers has 128-bits of block with key sizes of 128, 192 and 256 bits respectively. AES encryption is fast and flexible. It can be implemented on various platforms especially in small devices.

8. STEPS TO ENSURE OUR CLOUD IS SECURED

- Use certificates and encrypt all sensitive information.
- Deploy strong authentication for all remote users and do not use vendor supplied defaults passwords and other security parameters.
- Ensure isolation by using private IP address spaces and (virtual) networks.
- Provide location independence through virtual machines and networks that can be physically allocated in any data center.
- Use anti-virus software on every device.
- Install and maintain a firewall configuration and use firewall technology at every point and block unused services, ports and protocols [3].
- Teach all users "safe Internet skills."

9. CONCLUSIONS

With the rapid increase in the adoption of cloud computing by many organizations, security issues arise. One of the biggest security worries with the cloud computing model is the sharing of resources and data security. In this paper, we have discussed in details the different security and privacy issues and research challenges in cloud computing. The paper also included suggestions to mitigate these issues. The paper provided general cloud security recommendations as well.

REFERENCES

[1] Buyya R., Broberg J., Goscinski A. (2010). *Cloud Computing: Principles and Paradigms*, John Wiley & Sons, Vol. 87.

[2] Mohammed M. (2014). Alani: securing the cloud: threats, attacks and mitigation techniques, *Journal of Advanced Computer Science and Technology*, Vol. 3, No. 2, pp. 202-213.

[3] Buecker A., Lodewijkx K., Moss H., Skapinetz K., Waidne M. (2009). Cloud security guidance, *IBM Red Paper 2009*, p. 12.

[4] Padhy R.P., Patra M.R., Satapathy S.C. (2011). Cloud computing: security issues and research challenges, *IRACST- International Journal of Computer Science and Information Technology & Security(IJCSITS)*, Vol. 11.

[5] Tiwari P.K., Mishra B. Cloud computing security issues, challenges and solution, *International Journal of Emerging Technology and Advanced Engineering*. Vol. 2.

[6] Prince Jain: security issues and their solution in cloud computing, *International Journal of Computing & Business Research*.

[7] Anantwar R.G., Chatur P.N., Anantwar S.G. (2012). Cloud computing and security model: a survey, *International Journal of Engineering Science and Innovative Technology (IJESIT)*, Vol. 1.

[8] Tim M., Subra K., Shahed L. (2009). Cloud security and privacy: an enterprise perspective on risks and compliance, *O' Reilly Media*, USA.

[9] Barrie S. (2011). *Cloud Computing Bible*, Wiley Publishing Inc.

[10] Pearson S., Azzedine B. (2010). Privacy, security and trust issues arising from cloud computing, *2010 IEEE Second International Conference Cloud Computing Technology and Science (CloudCom)*, pp. 693-702.

[11] Hamouda S.K., Glauert J. *Security, Privacy and Trust Management Issues for Cloud Computing*, Taylor & Francis Group.

[12] Shakeeba S.K., Tuteja R.R. (year). Security in cloud computin using cryptographic algorithms, *International Journal of Innovative Research in Computer and Communication Engineering*, Vol. 3.