INVESTIGATION ON THE SECURITY ASPECTS OF THE CLOUD COMPUTING USING SYMMETRIC AND ASYMMETRIC ALGORITHMS

Dr. K. SAI MANOJ, Ms. K. Mrudula, Mrs G. Maanasa, Prof. K. Phani Srinivas

1 CEO, Innogeecks Technologies and Amrita Sai Institute of Science and Technology/Reviewer, Vijayawada, AP, India
2 Director, Innogeecks technologies, Vijayawada, AP, India
3 Research Scholars, Acharya Nagarjuna University, Guntur Dist, AP, India
4 Editor and Reviewer, Director R&D, Innogeecks Technologies and Amrita Sai Institute of Science and Technology, Vijayawada, AP, India

ABSTRACT:

Many Developers are concentrating on the security aspect of the cloud computing. Still there is need to concentrate on the investigation of the new type of security algorithms. In this research paper we had done an investigation on the comparison of symmetric and asymmetric algorithms. Data security is one of the very important issue in the cloud computing. In this article we investigated on the comparative study on one important technique related to the symmetric and asymmetric algorithm that enhanced Data Security in cloud computing system. We Pointed AES for symmetric encryption algorithm and Elliptic curve for asymmetric encryption algorithm.

Keywords: Data Security, cloud computing, symmetric algorithm, Asymmetric algorithm, AES, Elliptic curve.
[1] INTRODUCTION

Cloud computing emerged in the last few decades to handle systems with large-scale services sharing between huge numbers of users. It provides enormous storage for data and computing power to users over the Internet. There are many issues with the high growth of data.

Information security has grown to be an enormous factor, especially with modern communication networks, leaving ambiguity that could be expecting to the extremely impressive effects. This article presents a discussion on two popular encryption schemes that can be used to tighten communication security in Symmetric and Asymmetric Encryption. In principle, the best way to commence this discussion is to start from the basics first.

[2] ALGORITHMS:

An algorithm is basically a procedure or a formula for solving a data snooping problem. An encryption algorithm is a set of mathematical procedure for performing encryption on data. Through the use of such an algorithm, information is made in the cipher text and requires the use of a key to transforming the data into its original form. This brings us to the concept of cryptography that has long been used in information security in communication systems.

[3] MAIN CONCEPTS IN THIS RESEARCH ARTICLE:

Difference between Symmetric and Asymmetric Encryption
1) Symmetric encryption uses a single key that needs to be shared among the people who need to receive the message while asymmetrical encryption uses a pair of public key and a private key to encrypt and decrypt messages when communicating.
2) Symmetric encryption is an old technique while asymmetric encryption is relatively new.
3) Asymmetric encryption was introduced to complement the inherent problem of the need to share the key in symmetrical encryption model, eliminating the need to share the key by using a pair of public-private keys.
4) Asymmetric encryption takes relatively more time than the symmetric encryption.

[4] INVESTIGATION:

About AES:
Advantage of symmetric algorithm AES:
It implies Advanced Encryption algorithm. One of the Symmetric key algorithms such as AES performs each and every case well in both hardware and software environments in a wide range to protect voice, data, video etc from attacks. These include 8-bit, 64-bit, 128 bit etc Digital signal Processors. Its inherent performance describes the efficient use of processor capacity which results excellent software performance. This algorithm has speedy key setup time and good key ability to think and understand quickly. It requires less memory for implementation, making it suitable for restricted-space environments. The structure has good potential for benefiting from instruction-level parallelism way. There are no very serious weak keys in AES. It supports any block sizes and key sizes that are multiples of 32 (greater than 128-bits). Statistical analysis of the cipher text
has not been possible even after using huge number of test cases. No differential attacks have been yet proved on AES.

**Disadvantage of Symmetric algorithm AES:**
1) It uses very simple algebraic structure
2) Each and Every Block is encrypted in the same manner.
3) Software implementation is very much difficult
4) There exists problem in this algorithm pointing to Data Security.

**Benefits of the Asymmetric Key algorithm such as Elliptic Curve:**
Key size: The key of an elliptic curve based crypto system takes significantly less memory. The ratio increases rapidly with the increase of security levels. For instance, RSA crypto system with the key length of 1024 bits is equivalent to an elliptic curve crypto system with the key length of 163 bits.

**Disadvantages of the Asymmetric key Elliptic Curve:**
1) Vey much complex in mathematical background point of view
2) Large group of weak Elliptic curves exists
3) Still there is improvement in the further research regarding this technique is required.

**[5] CONCLUSION**

After Clear conceptual oriented investigation on the comparison of symmetric and asymmetric algorithm our conclusion is that asymmetric algorithm technique such as Elliptic curve has some advantages for securing the data in the cloud than symmetric algorithm technique AES.

**REFERENCES:**
5) INVESTIGATION ON THE DATA SECURITY IN CLOUD COMPUTING USING BIOMETRICS Dr.Sai Manoj.K International Journal of Current Advanced Research Volume 7; Issue 12(B), December 2018; Page No: 16473-16475.