Efficiency and Effectiveness in Privacy and Security of Data Sharing on Multi Cloud Architectures

G. Katyayani*1, P. Srinivasulu*2

M.Tech Scholar, Dept of CSE, QISCET, ONGOLE, Dist: Prakasam, AP, India.
Professor & HOD, Department of CSE, QISCET, ONGOLE, Dist: Prakasam, AP, India

ABSTRACT:

Cloud Computing and its features of seamless performance is really an achievement for the Information technology industry or we can call is one if the milestone we reached to adhere the changing world. If we consider the global world which is looking forward the best of the technological approach; hence were present in the paper the multi cloud and its security architectures. When the concept of the multi cloud comes in to picture the lay stone which keeps in is the parallel distributed environment where we have given emphasis on the Security and its robustness of the design multi cloud which may involve the hybrid cloud. In the current context of the cloud Security is the measure for which many high end application fear to implement. We achieve the Security thought he multitier based security by partitioning the data and level of impotence with acknowledgement to the object maintain an interrelated session among the nodes of the cluster based approach where map and key with parent node map is the crucial one.

KEYWORDS: Cloud, security, privacy, multi cloud, application partitioning, tier partitioning, data partitioning, multiparty computation.

I. INTRODUCTION

Informally one could say that the input is kept private by “mixing” it with random values, until the information that is sent to the other player’s looks completely random. A more formal explanation is that each player uses a function. This function takes the information that is going to be sent to the other players and some random information as input. The output of the function is a set of shares where each player gets one share. The output should be such that each share is either completely random or a value statistically indistinguishable from a random value, so that each player might not learn anything about the original input. In secret sharing, each share is a different value and only certain sets of players can reconstruct the original information, while in homomorphism cryptography all shares are the same value and only the player(s) who know the private key can reconstruct the original information. When information is shared using functions that are not information theoretically secure the players do not have unlimited computational power. For example when information is shared using holomorphic cryptography, the assumption is that the players cannot decrypt the encrypted information.
The input domains $X_i$ and output range $Y$ have been represented using bits. The model will now shift from focusing on individual bits and will instead focus on variables. This leads to the following definition: Using a cryptosystem as a basis for multiparty computation makes it possible to do multiparty computations between only two players. These two players will have different roles. One role will be called the evaluator, and the other role will be called the multiplication oracle. The evaluator will receive the encrypted input values and will perform the addition operation. This role must not have access to the decryption key. The multiplication oracle will perform a multiplication protocol with the evaluator. The multiplication oracle must also be able to decrypt the output value(s), therefore this role must have access to the decryption key. The roles are split to ensure that the players handling the encrypted information have no way of decrypting it, and the player that has the decryption key does not have access to any of the information.

II. RELATED WORK

When recombining shares, the player that is going to reveal the value receives all the shares connected to that value. The player does not know the random values in the original polynomial; therefore the player has to compute an interpolation polynomial.
the encrypted values become too large, making the scheme impossible work with.

III.PROPOSED METHODOLOGY

Multiparty computation consists of only two basic operations. The secret shared values can be added or multiplied with other secret shared values or values known to all players. Although addition and multiplication do not seem like much, these two basic operations can be used together with sharing and revealing to form more complicated operations. First we examine the concept of adversaries. Then we examine the additive secret sharing scheme, Shamir’s secret sharing scheme and the cryptosystem, and show how addition and multiplication can be accomplished in these secret sharing schemes. It also includes an introduction into a fully holomorphic encryption scheme. Fully hemimorphic encryption schemes are schemes where both addition and multiplication can be done without interaction. It was long thought that this was not possible, but results by Craig Gentry have shown this is possible.

In the Above fig.3.1 concludes with some optimizations for Shamir’s secret sharing scheme, these optimizations might be applicable to other secret sharing schemes as well. When this cryptosystem is expanded to more than two players, the roles will have to be distributed among the players. The only restriction when distributing the roles is that any player handling encrypted information should not have full knowledge of the decryption key. The decryption key in a crypto system might be shared among multiple parties, as was first proposed by, when the decryption key is shared between a set of players, then they function as a multiplication oracle. Since none of them have full knowledge of the decryption key, it also implies that the same players might also function in the evaluator role. The communication between the players will then have to be structured so that the two roles do not overlap. Protocols for decryption and verifying the decryption in the cryptosystem with a distributed key can be found in. Essentially the decryption key is shared using Shamir’s secret sharing scheme and the parties compute a distributed exponentiation.

IV.EVALUATION AND ANALYSIS

If the messages are not labeled, or the messages are not sent and received in the correct sequence, then the four secret shared variables might be shared in the wrong order, the multiplications might be done in the wrong order, or the values might be revealed in the wrong order. If a message or operation labeling is not done, then all operations have to be carried out in a strict
order across the computer system, and a
corner will likely spend a significant
amount of time waiting for input from the
other computers. Labeling, on the other
hand, increases the efficiency because the
players can work asynchronously, by
continuing the computation as soon as the
necessary input is available. On the other
hand, each message will have to be labeled
uniquely. Creating an algorithm that
enforces unique labels on all messages is a
challenge in and of it, and is a topic that is
not discussed in the multiparty computation
literature.

V. CONCLUSION AND FUTURE WORK

Two security weaknesses were found, both
of which relate to the way a random number
is used to secure a revealed answer. Both
weaknesses could possibly reveal the private
key to any of the players. The first weakness
relates to the distributed trial division step;
whereas the second weakness is regarding
the alternative step in the biprimarily test.
Test several candidates in parallel by testing
several values for p and q simultaneously.
The nature of multiparty is not very
efficient, given that the players are waiting
at several synchronization points to receive
shares from each other. By testing several
candidates in parallel, each player normally
has some calculations that can be done for at
least one of the candidates, which decreases
the idle time for each player, and thus
improving the efficiency of the protocol.

VI. REFERENCES


AUTHORS PROFILE:

Name: G. Katyayani, M.Tech Scholar, Dept of CSE, QISCET, ONGOLE, Dist: Prakasam, AP, India.

Name: Dr. P. Srinivasulu, Professor & HoD, Department of CSE, QISCET, ONGOLE, Dist: Prakasam, AP, India.