Homomorphic Encryption Scheme Using PSO Algorithm in Cloud Computing

[1]Ruchika Aggarwal, [2]Er. Yogesh Kumar

[1]Research Scholar, [2]Assistant Professor
BGIET Sangrur

***Abstract*: The cloud computing is the decentralized type of architecture which is vulnerable to various type of security attacks. The homomorphic encryption is the encryption scheme to encrypt objects which are used to access data from the cloud server. The homomorphic encryption scheme has major disadvantage of key management and key sharing which reduce its efficiency. In this research work, technique of Particle swarm optimization is applied which generate key for the encryption. The nature-inspired meta-heuristic algorithms that are population dependent are known as Particle swarm optimization algorithms (PSO) in which the social behavior of birds and fishes is used as an inspiration to build up a scientific approach. The Particle swarm optimization based homomorphic algorithm is implemented in MATLAB and simulation results shows that it performs well in terms of execution time, resource utilization. The execution time and resource utilization of Particle swarm optimization (PSO) based homomorphic algorithm is less as compared to homomorphic algorithm. The result is optimized upto 10 percent approx in the improved algorithm as compared to existing algorithm.**

***Keywords*: PSO, Encryption, Homomorphic Encryption**

Introduction

Cloud computing is the computational model in which large pools of systems are interconnected with public as well as private networks and provides scalable infrastructure for various applications, data and file storage. Cloud computing have certain features that is the computational cost, hosting applications, storage of content and reduced delivery. It is the practical approach which experience cost benefits and having a capability of transforming data center from a capital-intensive set up to a variable priced environment. It is based on the very simple principle of reusability of IT capabilities [1]. The advancement cloud computing provides in traditional concepts of grid computing, distributed computing, utility computing, or autonomic computing and broaden the horizons across organizational boundaries. It is the pool of abstracted, highly scalable, and managed compute infrastructure capable of hosting end customer applications and billed by consumption. Therefore, cloud computing refers to the model computing technology in which machines having large data centers can animatedly provisioned configured, controlled and reconfigured to deliver services in a scalable manner. It is a novel IS (Information System) architecture; which visualizes what may be the future of computing [2]. It delivers computing as a service rather than as a product; in which share resources, application software and information to provide computers or other electronic devices as a utility over the Internet in real time. Enterprises can choose to deploy applications on Public, Private or Hybrid clouds. Cloud Integrators can play a vital part in determining the right cloud path for each organization. Public clouds are those clouds which are owned and operated by third parties. The superior economies of scale to customers are delivered by public clouds, as the cost of infrastructure are spread is very low, provides attractively low cost to each and every client. The customer shares the same infrastructure pool within the limited configuration, security protection and available [3] variances. These infrastructures are managed and supported by the cloud provider. The advantage of using public cloud is that, they may be large in size than the enterprises cloud and provides the ability to scale the cloud on public demand. There are two variations to a private cloud; it is constructed mainly for the single enterprises. The main aim of private cloud is to show concern on data security and have good control on the data, which lacks in public cloud computing. Hybrid clouds are the combination of both, public as well as private cloud models [4]. The providers have the option to use 3rd party cloud provider in a complete or partial manner which in turn increases the flexibility of the computing. These models have the ability to provide on-demand externally provisioned scale. This model has the capacity to expand private cloud along with the resources of public clouds and used to handle workloads. There are some common challenges despites of its growing advancement cloud computing has certain challenges. Data security is the most important requirement of any network. The enterprises are not able to purchase the business data security from the vendors, because they have the fear of losing data confidentiality and data security. The actual storage location was not disclosed which also adds the security [5] concerns of the enterprises. The firewall across data centers protects and secures the confidential information. Maintenance of data security is the responsibility of the service provider and thus the enterprises depends on them. In production environments, operational teams support service level agreements are present in the business applications and are strictly followed. Operational team plays a very important part in the maintenance of service level agreements and runtime supremacy of the applications [6]. Due to the presence of multiple cloud providers, the maintenance of platform and infrastructure is very immature. There are certain characteristics like Auto scaling is very essential requirement of various enterprises. There is need to improve the scalability and load balancing features. Many countries do not share the personal information and other confidential information of the customers living outside the state or country. In order to have access, the cloud providers need to have a setup or a storage site within the country and obey the regulations. Planting such a huge infrastructure is may not be possible and one of the biggest issue of concern. Encryption schemes are designed to maintain confidentiality [7]. The security of encryption schemes should not rely on the obfuscation of their codes, but it should only be based on the secrecy of the key used in the encryption process. PSO stands for Particle Swarm Optimization is computational method which optimizes the problems by improving the candidate solutions regarding to the given measure of quality. It solves the problems by considering the number of candidate solutions, particles are dubbed, moved around the search-space according to a simple [8] mathematical formula applied over the particle's position and velocity. In order to solve the practical problems, the numbers of particles are selected in between 10 and 50. It is a novel population-based stochastic search algorithm which provides alternate solutions to the complex non-linear optimization problems.

Literature Review

K.Shankar et.al (2018) proposed [9] an innovative technique to encrypt data and query points. This techniques works in accordance to the K-nearest neighbor computational approach and preserves the data privacy and query privacy. The hypothetical and test results exhibit the adequate plan of security and its performance. In order to make this happen, the researcher have introduced another method which takes care of the keys sharing problems. The researchers concluded that the by using proposed approach the data can be safeguard even in the case of dishonest query clients releases their data towards adversary nodes.

Mikhail Babenko et.al (2018) considers [10] cryptosystems for homomorphic encryption techniques based on the Residue Number System (RNS) and secret sharing schemes. One of the major disadvantages of this proposed approach is that they are directly related to the redundant data and due to which the size of the node is increased. In order to overcome this disadvantage the homomorphic encryption is applied by combining it with the arithmetic coding approach called Chinese remainder theorem. In this paper, another approach of cryptanalysis had been proposed based on the properties of RNS and theory of number approach. Therefore, the researcher concluded from the work that the proposed approach used factorization algorithm which was very complex and hence increases the size.

Debasis Das et.al (2018) proposed [11] a scheme which integrates the multi-party computation by using homomorphic encryption and calculates the encryption data without decrypting them. The cloud model used cryptographic technique and the overheads are compared with the help of homomorphic encryption and multi-party computation. The proposed approach of homomorphic encryption is employed on the encrypted data without decrypting the data. These techniques designed and modeled to have a secure homomorphic encryption and multi-party computational techniques are tailored to specify the private semi-trusted cloud settings. The researchers concluded that the setting allows developers to create the private cloud along with the cryptographic techniques and it is very important to protect the data.

Ahmed EL-Yahyaoui et.al (2018) presented [12] an innovative technique of fully homomorphic encryption scheme. This scheme is highly recommended for the data security measures in cloud computing. This proposed can be used to secure the data present in the cloud computing. In this paper, large integer rings are used as clear text space and one key is required for encryption-decryption, it is symmetric type of encryption technique. Therefore, researchers concluded that the proposed approach of homomorphic encryption is noise free and probabilistic scheme and it is effectively used to protect the data within the cloud computing. The security measures are based on the problems of factorization of large numbers.

Xidan Song et.al (2017) developed [13] a hybrid cloud computing scheme which works in accordance to the Pailler algorithm also known as homomorphic and RSA encryption technique. The request of customer calculation request is described as the combination of simple add and multiplication and the operands. The cloud present in the public performs calculation without having exact idea of the data present in the cloud. Various simulations were performed which analyzed that the proposed scheme is practical and efficient. This approach proves the practicability of the system when the size of the key is smaller than the 4096 bits.

Ahmed EL-YAHYAOUI et.al (2017) presented [14] a verifiable fully homomorphic encryption technique. The proposed technique is noise free and probabilistic cryptosystem and cipher text space is non commutative ring based. This technique is categorized as the smart category type of encryption technique which allows the working with the data even in its encrypted format. The main objective of this paper is to introduce an efficient and effective FHE based new mathematical structure which is free from all the noises. This technique is quite effective in terms of the smart computation performed on the encrypted data and can be implementing on the big data security. The researcher concludes that the proposed scheme is efficient and practical approach, its security relies on the problem solving over-defined system of quadratic multivariate polynomial equations.

Research Methodology

This study is mainly focused on to develop modal for fully homomorphism disk encryption schemes. The new scheme will provide reliable key storage and key management services. This will enhance the reliability and security of the existing fully homomorphism encryption scheme. In this new modal, secure channel establishment algorithm will used for key management and key sharing. The secure channel establishment algorithms are Diffie- Helman and RSA. The Diffie- Helman algorithm is most secure and reliable algorithm. In the Diffie-Hellman algorithm if two parties, say, Master and Slave wishes to exchange data. Before starting the communication, secure channel is established. Both parties select their own random number. On the basis of the selected random numbers, secure channel and shared key is established.

We have embedded the Diffie Hellman key exchange algorithm for authentication procedure. In cloud network, it defines the source node and destination node. To establish secure channel between communicating parties, each party select a random prime number g and n, selected numbers become public keys of both parties. The source node become master and destination node become slave, master and slave select their private keys 'a', 'b' respectively. The master calculates new value "M" from their selected public and private numbers.

$$M= g^{a} \bmod n$$

The Slave calculates new value "S" from their selected public and private numbers

$$S= g^{b} \bmod n$$

The Master and slave exchange their calculated "M" and "S" values through intermediate nodes. When Slave receives "M" and Master receives "S" both parties will calculate mode inverse value. When master receive value "S" from slave and calculate new value "K1" from the received "S" value.

$$K1=S^a \bmod n$$

Slave receives value "M" from master and calculates new value"K2" from the received "M"

$$K2=M^b \bmod n$$

After calculating "K1" and "K2", both parties establish secure channel, by calculated new key "K". If both communicating parties have same "K1" and "K2" values, secure channel is made between Master and Slave.

$$K=K1+K2$$

Communication starts between both parties when secure channel is made between master and slave. The communication between Master and Slave is encrypted with public keys. Each parties use their own private keys to decrypt the communication.

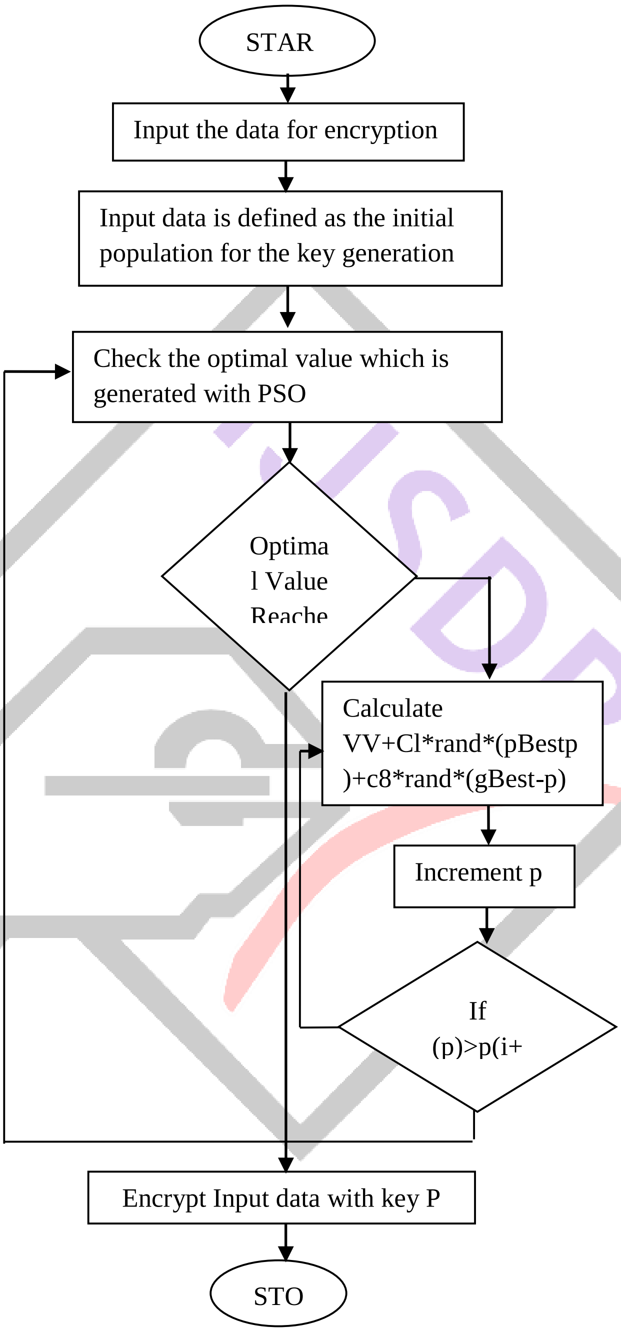
STAR
Input the data for encryption
Input data is defined as the initial population for the key generation
Check the optimal value which is generated with PSO
Optima l Value Reache
Calculate VV+Cl*rand*(pBestp)+c8*rand*(gBest-p)
Increment p
If (p)>p(i+
Encrypt Input data with key P
STO

Figure 1: Proposed Flowchart

Experimental Results

The proposed research is implemented in MATLAB and the results are evaluated by comparing existing and proposed techniques in terms of different performance parameters.

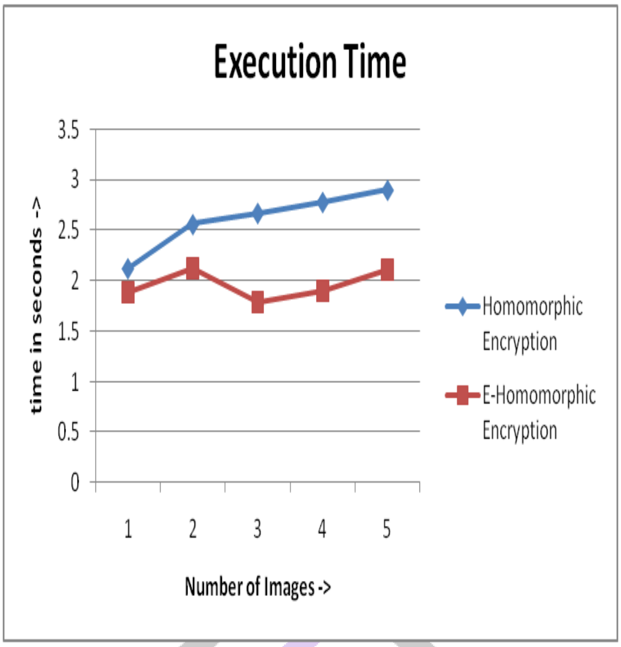

Fig. 2: Execution Time

As shown in figure 2, the execution time of the enhanced homomorphic algorithm is compared with the existing algorithm. The proposed algorithm is the homomorphic encryption schema and proposed algorithm is enhanced homomorphic encryption scheme. The enhanced homomorphic algorithm take less time because the keys are generated using the PSO value. The keys which are generated with PSO is more optimized for the generation of encrypted data.

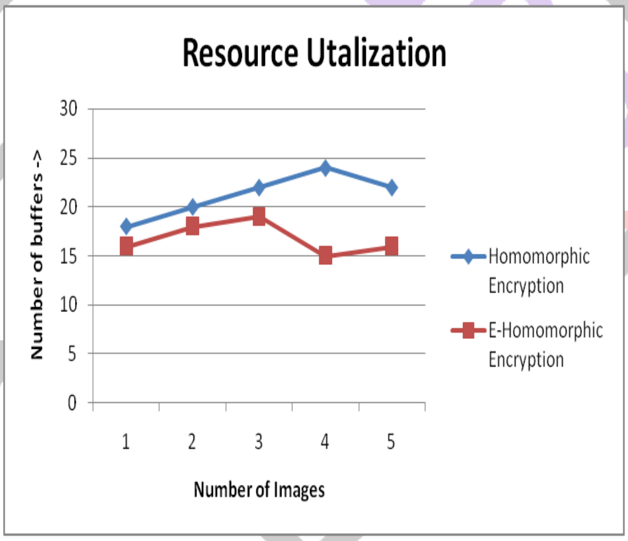

Fig. 3: Resource Utilization

As shown in figure 3, the resources utilization of proposed algorithm which is enhanced homomorphic encryption scheme is compared with the homomorphic encryption scheme. It is analyzed that resource utilization of enhanced homomorphic encryption technique is less as compared to existing technique. In the enhanced homomorphic algorithm, the keys for the generation of encrypted data is generated using PSO algorithm which are much optimized as compared to manual selection of the keys.

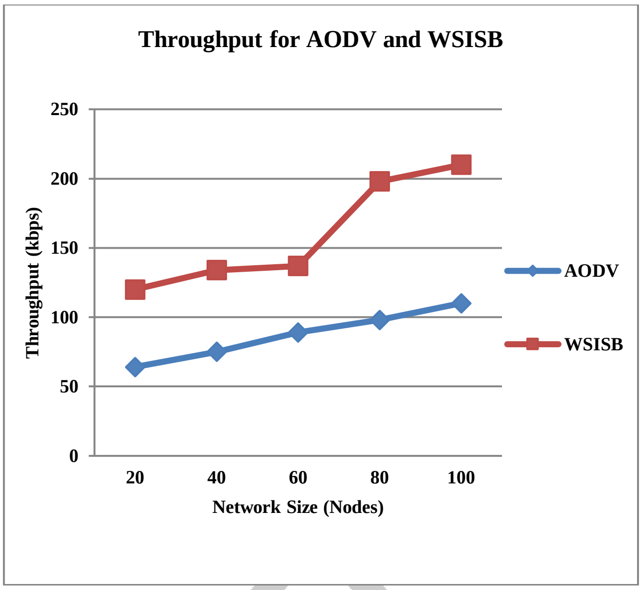

Fig. 4: Throughput comparison between AODV and WSISB

Fig. 4 represents the effect of number of nodes in throughput and compare the results of conventional AODV with proposed approach. Throughput defines total number of packets successfully delivered between source to destination in given simulation time period. In case of AODV, the performance is decreasing because of presence of selfish nodes which drops the packets those are received by other nodes within simulation. But WSISB identifies these type of node using some confidence factor therefore nodes are successfully delivered packet from source to destination that will enhance the performance of network.

Conclusion

There are several cryptographic techniques utilized by various security mechanisms. To ensure security within the cloud, cryptographic techniques are important to be applied. Thus, the confidentiality and integrity of data can be protected here. The data that is being shared in the cloud is provided security and is also ensured to be stored securely due to these approaches. The technology that designs ciphers is referred to as cryptography. In this work, it is concluded that homomorphic encryption is the scheme which encrypt cloud data. The homomorphic encryption scheme has major disadvantage of key management and key sharing. The generated key is given as input to the homomorphic encryption scheme to generate encrypted data. The Enhanced homomorphic algorithm is implemented in MATLAB and results are analyzed in terms of execution time, resource utilization. The Enhanced homomorphic algorithm has less execution time and resource utilization as compared to existing homomorphic encryption scheme.

References

[1] Shafi. Goldwasser, Silvio. Micali, “Probabilistic encryption”, J. Comput. Syst. Sci. 28(2), 270–299 (1984)
[2] S. Sobitha Ahila, Dr.K.L.Shunmuganathan, “State Of Art in Homomorphic Encryption Schemes”, 2014 Int. Journal of Engineering Research and Applications
[3] Tatsuaki Okamoto, Shingenori Uchiyama, “A new public-key cryptosystem as secure as factoring”, in Proceedings of Advances in Cryptology, EUROCRYPT’98, 1998, pp. 308–318
[4] Pascal. Paillier, “Public key cryptosystems based on composite degree residue classes”, Proceedings of Advances in Cryptology, EUROCRYPT’99, 1999, pp. 223–238
[5] Pascal. Paillier, D. Pointcheval, “Efficient public-key cryptosystems provably secure against active adversaries”, in Proceedings of Advances in Cryptology, ASIACRYPT’99, 1999, pp. 165–179
[6] V.Selvi and R.Umarani, "Comparative Analysis of Ant Colony and Particle Swarm Optimization techniques," International Journal of Computer Applications, , vol. 5, no. 4, pp. 1-6, 2010.
[7] Kwang Y. Lee and Jong-Bae Park, "Application of Particle Swarm Optimization to Economic Dispatch Problem: Advantages and Disadvantages," IEEE, 2010.
[8] Stehle, D. & Steinfeld, R. “Faster Fully Homomorphic Encryption”, 2010, Advances in Cryptology – Proceedings of ASIACRYPT’10, Lecture Notes in Computer Science (LNCS), Vol 6477, Springer-Verlag, pp. 377-394
[9] S. M. Mikki and Ahmed A. Kishk, "Hybrid Periodic Boundary Condition for Particle Swarm Optimization," IEEE Transactions on Antennas and Propagation, vol. 55, no. 11, pp. 3251-3256, NOVEMBER 2007.
[10] James Kennedy and Tim Blackwell Riccardo Poli, "Particle swarm optimization An overview," Swarm Intelligence, vol. 1, no. 1, pp. 33–57, 2007.
[11] A. P. Engelbrecht F. van den Bergh, "A New Locally Convergent Particle Swarm Optimiser," IEEE Conference onSystems, Man and Cybernetics, Tunisia, 2002.
[12] K.Shankar and M. Ilayaraja, “Secure Optimal k-NN on Encrypted Cloud Data using Homomorphic Encryption with Query Users,” 2018 International Conference on Computer Communication and Informatics (ICCCI -2018), Jan. 04 – 06, 2018

[13] Mikhail Babenko, Nikolay Chervyakov, Andrei Tchernykh, Nikolay Kucherov, Maxim Deryabin, Gleb Radchenko, Philippe OA Navaux and Viktor Svyatkin, "Security Analysis of Homomorphic Encryption Scheme for Cloud Computing: Known-Plaintext Attack," 2018, IEEE

[14] Debasis Das, "Secure Cloud Computing Algorithm Using Homomorphic Encryption And Multi-Party Computation," 2018, IEEE