Original Article

IMPROVED HOMOMORPHIC ENCRYPTION FOR SECURITY IN CLOUD USING PARTICLE SWARM OPTIMIZATION

Mohammad Faiz[1], Nausheen Fatima[2], Ramandeep Sandhu[3], Mandeep Kaur[4], Vipul Narayan[5]

[1,2,3,4]Lovely Professional University, Phagwara, Punjab, India.
[5]School of Computer Science and Engineering, Galgotias University, Greater Noida, U.P, India.
faiz.28700@lpu.co.in, nausheen.28838@lpu.co.in, ramandeep.28362@lpu.co.in, mandeep.29212@lpu.co.in, vipulupsainian2470@gmail.com
DOI: 10.47750/pnr.2022.13.S10.577

Abstract

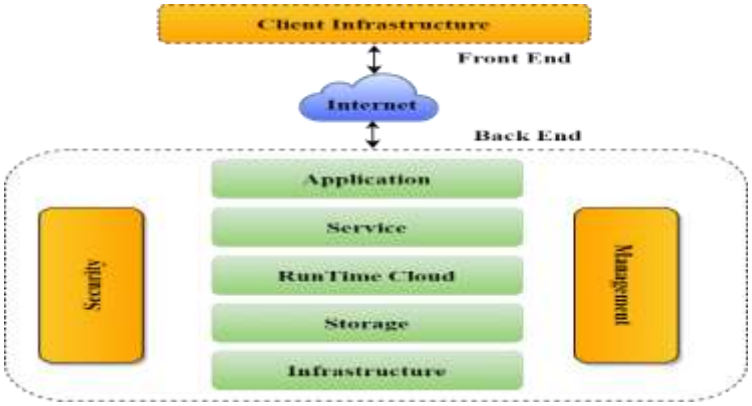
Cloud computing is vulnerable to several security risks because of its decentralised nature. Homomorphic encryption is an encryption technique used to encrypt data that are used to access from the cloud server. In the proposed work particle swarm optimization technique is used to improve the encryption key. Particle swarm optimization algorithms (PSO) gets their inspiration from the social behaviour of birds and are well known population-dependent meta-heuristic algorithms. Depending on the assessed quality, hybrid homomorphic encryption methods starts with a randomly distributed collection of particles to enhance the outcomes. The results of the simulation shows the improvement in encryption process by the proposed hybrid encryption technique compared to existing homomorphic encryption.

Keywords: Cloud, Security, Particle Swarm Optimization, Virtual Machines

1. INTRODUCTION

The term "cloud computing" describes a model that allows people for universal, reasonable, and on-demand network access for recurrently used configurable computer services and resources with the capability of quick provisioning and releasing the service provided by the services provider with minimum communication and overhead. Cost reductions, high storage capacity, a faster pace of computation, and scalability are the major benefits that cloud computing provides. The general people, governmental organisations, and business organisations are increasingly embracing cloud computing due to these benefits. The operational and financial advantages of cloud computing come with an elevated risk of internal security breaches. The identity and location of mediators and SPs are obscured by the cloud in such scenarios [1]. Figure 1.1 depicts the architecture of cloud computing.

Figure 1.1: Layered Architecture of Cloud Computing



The front end and the back end of a cloud system are split into two components as shown in the Figure 1.1 to help explain how it works. A network, typically the Internet, connects both of these points. The front end is the side that is used by the user or client . "The cloud" component of the system is represented by the back end. The device or computer network used by the user makes up the front end. Additionally, the application is essential for accessing the cloud system. All cloud computing platforms do not necessarily need to have the same user interface. The numerous computers, servers, and data storage systems that make up the cloud's back end [2].

1.1.1 Cloud Deployment Models

There are 4 cloud deployment models described by the NIST namely public clouds, private clouds, community clouds and hybrid clouds. These models provide the information regarding the implementation and consumption of technologies and can execute on the whole range of service models. The models are defined as [3]:

a. **Public Cloud:** This model is easily accessible for any subscriber using an internet connection and to the cloud space.

b. **Private cloud:** This kind of cloud is deployed for particular group or organization and it assists in bounding the access to just that specific group.

c. **Hybrid cloud:** This model has integrated two or more clouds which are stayed as unique entities. However, the standardized or proprietary technology has bound then together which facilitated the mobility to data and application.

d. **Community cloud:** A number of organizations share this framework and a particular community capable of sharing concerns is supported by this model. The organisations or a third party have been in charge of it, and it may be on or off site.

1.1.2 Cloud Service Models

There are 3 major service models of cloud environment. These models are known as IaaS, PaaS and SaaS.

- Infrastructure-as-a-Service (IaaS): The basic infrastructure services are given to the customers using this model. The physical machines, VMs, networking, storage or some mixture of these services is comprised in these services. The development of this model is facilitated at the time of requirement on the zeal of the managed infrastructure. These platforms are executed for replacing the data centres which are managed internally. The IaaS provides more viability organizations at alleviated expenses [15][16].

- Platform-as-a-Service (PaaS): A development platform an operating system and a database platform can be obtained from PaaS. These models facilitate the organizations for building the applications without any concern regarding the set up of infrastructure that is required for sustaining the development environment [17][18].

- Software-as-a-Service Software as a Service (SaaS): Applications, data services are obtained from this model. The service provider assists in offering data, applications and all the essential platforms. Software as a Service Software is considered as an original cloud service model. It has attained a lot of popularity among a huge number of provider options [19][20].

1.2 Security Issues in Cloud Computing

The three broad categories into which security risks in cloud computing can be divided are as follows:

i. Traditional security threats

ii. Threats related to system availability

iii. Third threats related to third-party data control

Additionally, certain additional security vulnerabilities in CC are also described, along with these groups of security-related concerns [21][22].

1.2.1.1 Traditional threats:

Any system with an Internet connection is prone to some vulnerabilities. These vulnerabilities varies based on the specification of the cloud. The abundance of cloud resources exacerbates the consequences of these risks, which have also had a significant impact on a wide number of users. Issues among cloud users are numerous and include difficulty in identifying the root cause of issues as well as ambiguous liability limits between customers and CSPs. These vulnerabilities are installed on the user's end in the website via internet. The user is in charge of safeguarding the system used to access the cloud and communicate with applications that are hosted in the cloud services offered by CSPs. In order to protect users, specific components of this infrastructure are kept outside of user's firewall and it makes the task more complicated [23][24].

1.2.1.2 Threats related to system availability: The availability of cloud services is also a key security concern. Due to system failure, power outages, and other catastrophic events, cloud services may be interrupted for an extended period of time. A data lock could prevent the business model of a large company that depends on these data for correct operation if such an unusual incident occurs. Phase transition events as well as other occurrences that are unique to complex systems can have an impact on clouds [4]. The fact that clients can't be assured that a cloud-hosted application offers accurate results is one of the serious availability concern [25][26].

1.2.1.3 Threats to third party control: Third-party control results in two issues: lack of transparency and only giving the user a limited amount of control. A service provider might allow the purchase of some assets from a low-trust third party. Sometimes subcontractors were unable to retain the user data. Other times, the third party was a hardware supplier rather than a subcontractor, and less effective storage methods resulted in data loss. It is unsafe to put sensitive data on the cloud because to the covert activities of cloud providers, which leads to serious hazards. Users are often responsible for data security according to the conditions of commercial agreements. For instance, users may not feel confident due to the AWS (Amazon Web Services) user agreement. Therefore, a cloud user would find it difficult to figure out that the service provider has removed the data from the cloud [27][28].

2. LITERATURE REVIEW

Aobing Sun, et.al (2018) suggested a quantifiable security evaluation system for diverse clouds whose accessing was done through the consistent API [7]. Various evaluation parameters concerning security, maintenance etc. in

correspondence with several fields had included in the suggested model. A three tuple had been allocated by every parameter on vulnerabilities, score and repair technique. One vote vetoed methodology was utilized in this system for one field so as its score was computed and its summary was added up as the total score. One security view was also made easier with the help of this method. On the G-Cloud platform, a quantitative evaluation was done for a number of cloud users. With the help of visual graphs, a dynamic security scanning based score was shown for one or more clouds, and users were shown how to change the configuration, improve the operation, and fix vulnerabilities, which made their cloud resources better.

Poorvika Singh Negi, et.al (2020) stated that the chance of compromising of security was maximized through the malicious users as the technology was growing rapidly [8]. The Honeypot was a technique utilized for redirecting the malicious traffic away from systems. It was a colossal strategy which assisted in enhancing the security of systems. The concept of Honeypot was put forward in a file-sharing application whose execution was done on the cloud server. The detection attacks in a cloud environment and the use of Honeypot to keep it secure had described and a novel method was recommended for this purpose. It was analyzed the presented technique had provided extra security and detection attribute. This security was further amplified in standard as the technology advances.

PanJun Sun, et.al (2020) recommended the detailed privacy security protection architecture and also described some risks of privacy security of CC first of all [9]. After that, the research progress of a number of techniques named access control, CP-ABE, KP-ABE, PRE, SE and revocation mechanism were described. Various technologies were integrated. This paper also presented the analysis and comparison of attributes and application scope of various techniques. At last, the existing challenges were defined and possible future research directions were also underlined.

Jacob AdeboyeAjala, et.al (2019) described that the application of stenography method was analyzed in cloud environment as an approach for improving the security of cloud data [10]. The data privacy and security were controlled using the presented technique that protected the data from fraudulent actions. Sometimes, data was stolen while transmitting the files. Though, the data was encrypted and a key was allocated using data proprietor in the cloud server in order to maintain the security of presented method. This resulted in securing the data under the transmission process with the help of mails. The secret communications despite of safety and privacy of data were supported in the stenography method. Consequently, its preference was enhanced for the cloud computing systems. An additional security layer and confidentiality for the encrypted data was obtained under the Steganography procedure while attaching the key embedding in the image. Thus, the presented technique in association with the cryptography proved as the most excellent method to secure the cloud data.

A R Suraj, et.al (2018) stated that a variety of network services were offered for the applications working on the Internet [11]. A top-notch security model was suggested along with the maximum-security approaches for preserving the data of user available on the cloud. This integrated security solution framework performed completely not only on the diverse delivery layers but on the system also. Thus, an inclusive security solution was obtained from this model for tackling the issues in Cloud Computing (CC).

Zina Balani, et.al (2020) discussed that the users who were not aware about the maximization of number of attacks and the emerging technology properly had more concerns regarding the data storage in clouds as the security was a major issue [12]. Some schemes and systems were offered for protecting the data in an online environment. These systems were less expensive and every user was capable to utilize them as a simple way for defending themselves against attackers. The security standards were inspected to provide security in CC environment.

Hicham Toumi, et.al (2019) introduced a novel intrusion detection contribution for securing the architecture of CC against inside threats [13]. Hy-IDD planned on the basis of flexible and interoperable mobile agents had implemented for recovering and analyzing the malicious data. The novel actions of responses were created and utilized in this system.The system became more fault tolerant with the interest-driven cooperating agents. Additionally, the autonomy provided to agents assisted in generating administration tasks of the security officer much easier.

Anagha Markandey, et.al (2018) emphasized on acquiring data security of cloud storage and integrating the equivalent cloud storage security strategies [14]. The security risks were taken in account to incorporate these

strategies with the outcomes of accessible data. These strategies were moved to the suitable security method that was planned on the basis of properties of cloud storage system. This paper had provided the information regarding security viewpoints for Data-in-Transit and Data-at-Rest [29][30].

3. PROPOSED METHODOLOGY

In order to offer effective security, several homomorphic encryption technique variations have been put forth. In contrast to exponential and scalar multiplication operations, pairing operations often have a significant computing cost. This provided inspiration for the creation of the enhanced homomorphic encryption certificate-less signing technique. In our proposed approach based on certificate-less signature scheme for improved homomorphic encryption contains the main offerings are as follows:

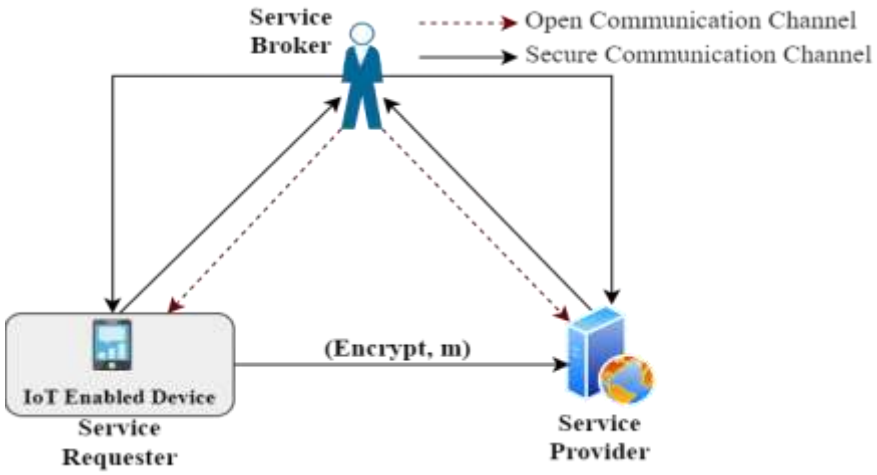
- Proposed approach offers high security with low cost of computations as it does not need any kind of bilinear computations.
- Proposed approach ensures vital security services such as, integrity, non-repudiation, and authentication.
- It is un-forgeable due to the stability property of discrete logarithm problem (DLP).

3.1 System Model

There are three main components of the model in the proposed scheme.

i. Service Requester
ii. Service Broker
iii. Service Provider

Figure 3.1: System model of the proposed encryption technique in Cloud



3.1.1 Service Broker: It functions similarly to a key generation center (KGC) and broadcasts system parameters to both service providers and service requesters. It produces a private key and transmits it through a secure communication channel to the appropriate service requester and service provider.

3.1.2 Service provider: It is effective in terms of capacity, storage, power backup, and computational power. It produces its own public key by using a hash function on the device identification after obtaining a system parameters from the broker. Finally, it utilizes a secure connection to obtain the private key from the broker of the service.

3.1.3 Service Requester: All IoT-enabled devices that desire access to system services are included. When the system parameter is received from the service broker, it applies a hash function on the device identity to establish its own public key. Finally, it uses a secure route to obtain the service broker's private key.

3.2 Encryption based on Particle Swarm Optimization

An efficient key management and sharing method is proposed using the enhanced homomorphic encryption technique and the particle swarm optimization algorithm, to present a successful key management solution. The cooperative behaviour of fish and birds serves as a paradigm for the creation of a scientific framework, and particle swarm optimization techniques are population-dependent meta-heuristic algorithms inspired by nature. Depending on the measure quality, the approaches enhance the solutions from a base of randomly dispersed particles. A variety of mathematical methods are used to improvise by shifting the particles about the search space. Only a very limited number of inter-particle exchanges make use of these simple and fundamental mathematical formulas. The optimum site for the swarm is chosen by recommending each particle's mobility in the direction of the spot with the most expertise. The definition of vibrant function is represented using equation (1). After each iteration its value changes.

$$s_i + 1 = s + c * rand * (k_{best} - x_i) + c * rand * (z_{best} - x_i) \qquad (1)$$

As denoted using above equation, velocity of particles is represented by Si, the maximum value among available options is denoted using k_{best} , and a random value is denoted by a rand variable. The ‘x’ value is utilized for the development of each characteristic of web application while ‘c’ value is applied for the description of whole features of web app. The value of z_{best} is the optimal value identified from all inhabitants and the optimal value identified from each iteration is denoted by z_{best}.

Once the quality negotiation and targeting function is finalized, the computed value is represented using the following equation (2) as:

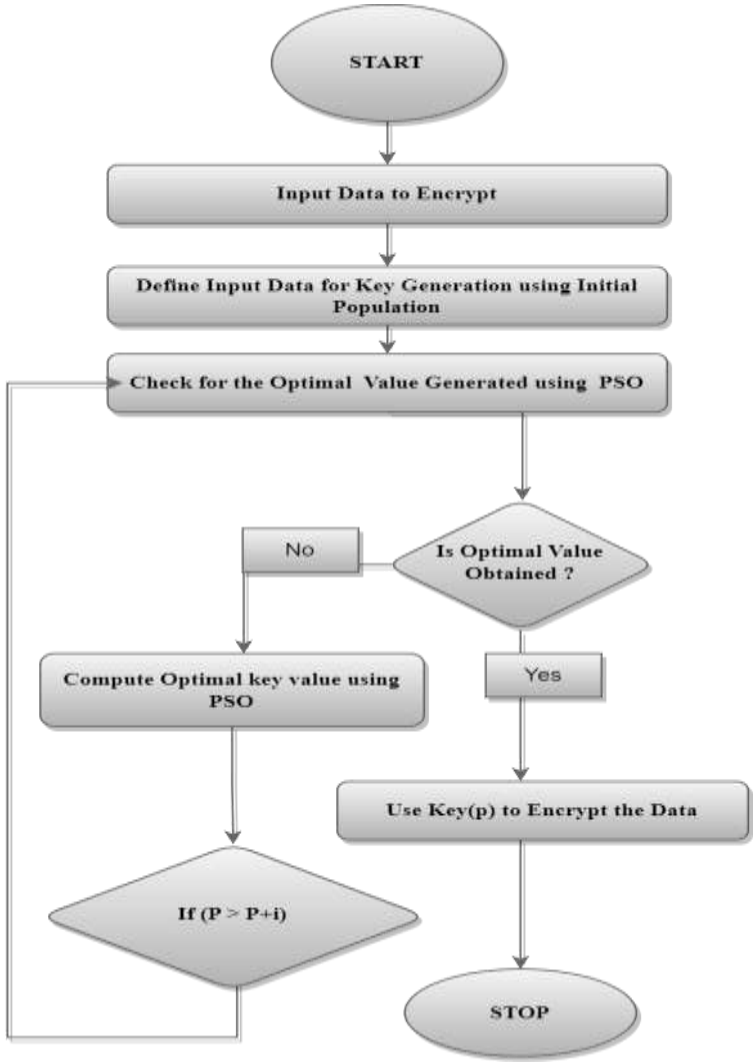
$$x_i + 1 = x_i + s_i + 1 \qquad (2)$$

Position vector is denoted by x_i+1. The PSO algorithm is applied for the exclusion of multi-aiming based optimization problems.

The arbitrary changes takes place are also included in this. There is no various versions that employ various updating rules, though, in this repository.

Figure 3.2 shows the flow chart of the proposed PSO based improved homomorphic encryption scheme.

Figure 3.2: Flow chart of the proposed PSO based encryption



Algorithm: Proposed Improved Homomorphic Encryption Steps

1: Input: Data_set for Data encryption
2: Output: Encrypted_Data set
3: ***Generation of Key()***
4: i = Input_Data set
5: For (i = 1 to Max_IP)
6: For each particle (p) available in Z
7: Do
8: *Fp = f(Z)*
9: If *fp* performs better compared to *f(k_Best)*
10: Assign *Z_Best = p;*
11: End
12: End
13: Z_Best = *fittest p in Z*
14: Do
15: $\mathbf{s_i + 1 = s + c * rand * (k_{best} - x_i) + c * rand * (z_{best} - x_i)}$

```
16:      Z ← p+s;
17:        End
18:        End
19:  Data encryption key ← Z
20:  If(User entered key =Z)
21:       Perform Decryption of data
22:  Else
23:  Display alert message as wrong credentials
24:  End
```

3.3 Result and Analysis

The proposed hybrid technique is simulated using MATLAB programming to encrypt data in a cloud computing system. The shape of an image is taken by applied input. Cloud data is encrypted and decrypted using a balanced homomorphic encoding technique. An improved key is obtained via the applied PSO technique. Using this obtained key and a homomorphic encoding technique, information is encoded. Two parameters are used to examine and demonstrate the prediction system: execution time and resource consumption. In table 1, the outcomes of the reproductive process are displayed. The operating system utilized on each fundamental process in the data sample is named Xnon. There are eight fundamental computers, each of which has 8 GB of RAM are used. There are 50 images in all, each measuring 256x256 pixels.

Table 3.1: Simulation Parameters

Parameter	**Values**
Number of virtual machines	8
Operating System	Xnon
Host Count	10
R.A.M	8 GB
Input Data	Image Data
Number of Images	50
Image size	256*256

Figure 3.3: Execution Time

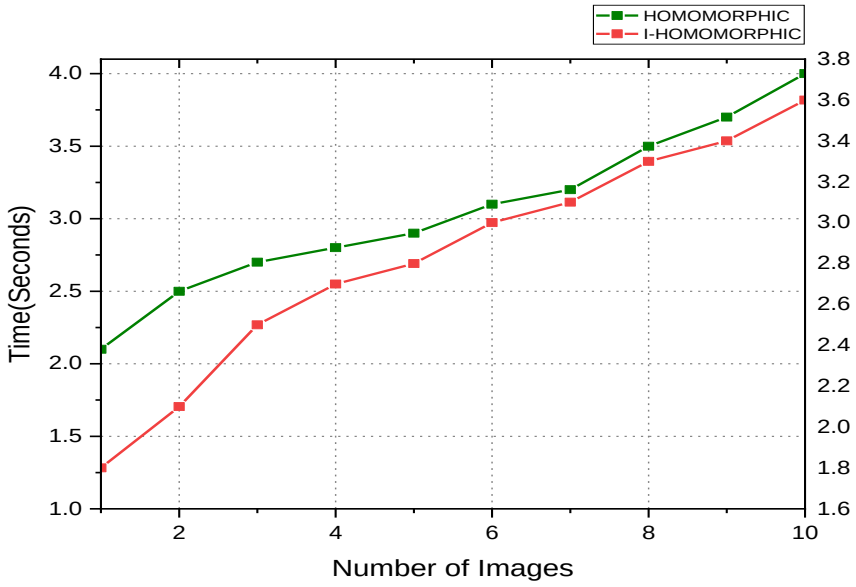
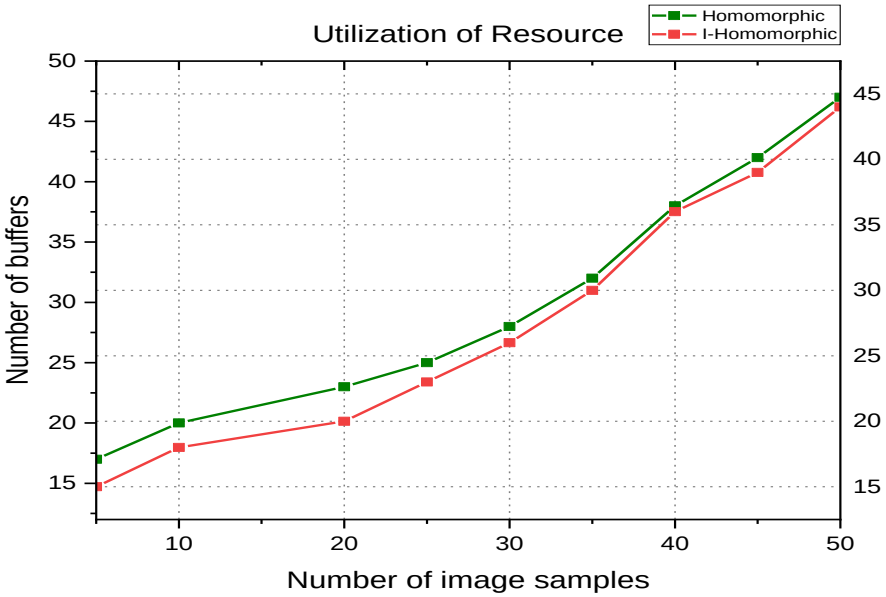


Figure 3.3 shows a comparison between proposed and existing algorithm. The proposed algorithm is a hybrid improved variant of homomorphic encoding technique.

Figure 3.4: Utilization of Resource



A comparison between proposed improved homomorphic encoding approach with existing homomorphic encoding approach and is performed to identify the utilization of resources shown in Figure 3.4. After exploration, it has been obtained and showed that the resource utilization is less using the proposed improved homomorphic encryption technique.

Table 3.2: Comparison of Techniques

Parameter	**Homomorphic Encryption**	**I-Homomorphic Encryption**
Resource Utilization	47 Buffers	44 Buffers
Execution Time	4 seconds	3.6 seconds

The Table 3.2 shows a comparison data obtained from the proposed improved homomorphic encoding approaches and existing homomorphic encoding and by means of resource utilization and execution time where the proposed approach showed improvements in the results. The comparative results shows that the I-homomorphic encoding based approach performed better on the selected parameters.

5. Conclusion

Numerous security methods use a large variety of different cryptographic approaches. Cryptographic methods need to be used to offer security in the cloud. A key must be used in this process in order for the data to be encrypted and decrypted. Data integrity and confidentiality may therefore be ensured in this situation. These techniques enable security for data storage and assure the security of data delivered to the cloud. The most effective method for encrypting cloud data used in the proposed work is homomorphic encryption. Key exchange and key maintenance are the homomorphic encryption technique's two primary drawbacks. The encryption algorithm in homomorphic encryption encrypts the data using the generated key. The PSO based homomorphic encryption algorithm is used to encrypt the data after receiving the produced key. When compared to the performance of standard homomorphic encryption, improved results are obtained with the proposed hybrid I-Homomorphic Encryption utilizing particle swarm optimization (PSO) to generate the encryption key.

REFERENCES

[1] Abdullah Abuhussein, HarkeeratBedi, Sajjan Shiva, “Towards a Stakeholder-Oriented Taxonomical Approach for Secure Cloud Computing”, 2013 IEEE Sixth International Conference on Cloud Computing

[2] Amit Hendre, Karuna Pande Joshi, “A Semantic Approach to Cloud Security and Compliance”, 2015, IEEE 8th International Conference on Cloud Computing

[3] MohemedAlmorsy, John Grundy, Amani S. Ibrahim, “Collaboration-Based Cloud Computing Security Management Framework”, 2011, IEEE 4th International Conference on Cloud Computing

[4] Faiz, M. and A.K. Daniel (2022) “Threats and Challenges for Security Measures on the Internet of Things”, Law, State and Telecommunications Review, 14(1), pp. 71–97. doi: 10.26512/lstr.v14i1.38843.

[5] Faiz, M., Daniel, A.K. A multi-criteria cloud selection model based on fuzzy logic technique for QoS. Int J Syst Assur Eng Manag (2022). https://doi.org/10.1007/s13198-022-01723-0

[6] Faiz, M., Daniel, A.K. (2022). Multi-criteria Based Cloud Service Selection Model Using Fuzzy Logic for QoS. In: Woungang, I., Dhurandher, S.K., Pattanaik, K.K., Verma, A., Verma, P. (eds) Advanced Network Technologies and Intelligent Computing. ANTIC 2021. Communications in Computer and Information Science, vol 1534. Springer, Cham. https://doi.org/10.1007/978-3-030-96040-7_12

[7] Aobing Sun, Guohong Gao, Tongkai Ji, Xuping Tu, “One Quantifiable Security Evaluation Model for Cloud Computing Platform”, 2018, Sixth International Conference on Advanced Cloud and Big Data (CBD)

[8] Poorvika Singh Negi, Aditya Garg, Roshan Lal, “Intrusion Detection and Prevention using Honeypot Network for Cloud Security”, 2020, 10th International Conference on Cloud Computing, Data Science & Engineering (Confluence)

[9] PanJun Sun, “Security and privacy protection in cloud computing: Discussions and challenges”, 2020, Journal of Network and Computer Applications

[10] Jacob AdeboyeAjala, Sanika Singh, Saurabh Mukherjee, Sudeshna Chakraborty, “Application of Steganography Technique in Cloud Computing”, 2019, International Conference on Computational Intelligence and Knowledge Economy (ICCIKE)

[11] A R Suraj, Sneha Janani Shekar, G S Mamatha, “A Robust Security Model for Cloud Computing Applications”, 2018, International Conference on Computation of Power, Energy, Information and Communication (ICCPEIC)

[12] Zina Balani, HacerVarol, “Cloud Computing Security Challenges and Threats”, 2020, 8th International Symposium on Digital Forensics and Security (ISDFS)

[13] Hicham Toumi, Fatima Zahra Fagroud, AmiyneZakouni, Mohamed Talea, “Implementing Hy-IDS, Mobiles Agents and Virtual Firewall to Enhance the Security in IaaS Cloud”, 2019, Procedia Computer Science

[14] AnaghaMarkandey, Prajakta Dhamdhere, Yogesh Gajmal, “Data Access Security in Cloud Computing: A Review”, 2018, International Conference on Computing, Power and Communication Technologies (GUCON)

[15] Narayan, Vipul, and A. K. Daniel. "Design consideration and issues in wireless sensor network deployment." (2020): 101-109.

[16] Choudhary, Shubham, et al. "Fuzzy approach-based stable energy-efficient AODV routing protocol in mobile ad hoc networks." Software Defined Networking for Ad Hoc Networks. Cham: Springer International Publishing, 2022. 125-139.

[17] Narayan, Vipul, and A. K. Daniel. "RBCHS: Region-based cluster head selection protocol in wireless sensor network." Proceedings of Integrated Intelligence Enable Networks and Computing: IIENC 2020. Springer Singapore, 2021.

[18] Narayan, Vipul, and A. K. Daniel. "CHOP: Maximum coverage optimization and resolve hole healing problem using sleep and wake-up technique for WSN." ADCAIJ: Advances in Distributed Computing and Artificial Intelligence Journal 11.2 (2022): 159-178.

[19] Narayan, Vipul, and A. K. Daniel. "CHHP: coverage optimization and hole healing protocol using sleep and wake-up concept for wireless sensor network." International Journal of System Assurance Engineering and Management 13.Suppl 1 (2022): 546-556.

[20] Narayan, Vipul, and A. K. Daniel. "IOT based sensor monitoring system for smart complex and shopping malls." Mobile Networks and Management: 11th EAI International Conference, MONAMI 2021, Virtual Event, October 27-29, 2021, Proceedings. Cham: Springer International Publishing, 2022.

[21] Narayan, Vipul, and A. K. Daniel. "Energy Efficient Protocol for Lifetime Prediction of Wireless Sensor Network using Multivariate Polynomial Regression Model." Journal of Scientific & Industrial Research 81.12 (2022): 1297-1309.

[22] Awasthi, Shashank, et al. "A Comparative Study of Various CAPTCHA Methods for Securing Web Pages." 2019 International Conference on Automation, Computational and Technology Management (ICACTM). IEEE, 2019.

[23] Narayan, Vipul, and A. K. Daniel. "FBCHS: Fuzzy Based Cluster Head Selection Protocol to Enhance Network Lifetime of WSN." ADCAIJ: Advances in Distributed Computing and Artificial Intelligence Journal 11.3 (2022): 285-307.

[24] Narayan, Vipul, et al. "E-Commerce recommendation method based on collaborative filtering technology." International Journal of Current Engineering and Technology 7.3 (2017): 974-982.

[25] Narayan, Vipul, et al. "To Implement a Web Page using Thread in Java." (2017).

[26] Srivastava, Swapnita, and P. K. Singh. "HCIP: Hybrid Short Long History Table-based Cache Instruction Prefetcher." International Journal of Next-Generation Computing 13.3 (2022).

[27] Srivastava, Swapnita, and P. K. Singh. "Proof of Optimality based on Greedy Algorithm for Offline Cache Replacement Algorithm." International Journal of Next-Generation Computing 13.3 (2022).

[28] Smiti, Puja, Swapnita Srivastava, and Nitin Rakesh. "Video and audio streaming issues in multimedia application." 2018 8th International Conference on Cloud Computing, Data Science & Engineering (Confluence). IEEE, 2018.

[29] Srivastava, Swapnita, and Shilpi Sharma. "Analysis of cyber related issues by implementing data mining Algorithm." 2019 9th International Conference on Cloud Computing, Data Science & Engineering (Confluence). IEEE, 2019.

[30] Narayan, Vipul, and A. K. Daniel. "Multi-tier cluster based smart farming using wireless sensor network." 2020 5th international conference on computing, communication and security (ICCCS). IEEE, 2020.