Soft Computing
https://doi.org/10.1007/s00500-020-04892-x

METHODOLOGIES AND APPLICATION

Performance improvement of cloud security with parallel anarchies society optimization algorithm for virtual machine selection in cloud computing

B. Lanitha[1] · S. Karthik[2]

Abstract
Cloud computing (CC) is a future promising computing technology and has proven tremendous exceptional attainable in managing the hardware and software program sources placed at third-party provider vendors. However, security and virtual machines (VMs) selection to a process a request characterize a large venture. The major problem in the usage of the technology is the security concerns which increase the demand for a robust security mechanism to protect the data on the cloud. Hence in order to resolve this issue, an approach was designed for the purpose of enhancing the cloud security as well as the time of execution known as weighted mean-based convolutional neural network with advanced encryption standard (WMCNN-AES). By employing the method of pseudorandom number generators (PRNGs), random keys are generated and the finest keys are produced by using the WMCNN method. In the WMCNN approach, randomly generated keys are taken as input and the approximation concerning the secret key of the input is produced by the hidden layers. For the purpose of encrypting the data, the finest secret keys are generated by the output layer. By employing the advanced encryption standard (AES) algorithm, encryption is executed. Storage of the files concerning the encrypted data is done in the cloud storage system. Optimal selection of VMs performs a significant enhancement of the performance through reducing the execution time of requests (tasks) coming from stakeholders and maximizing utilization of cloud resources. For the purpose of optimizing the virtual machines' or VMs' selection, parallel anarchies society optimization (PASO) is employed in the cloud environment to increase the performance and resource utilization. When comparing the experimental results of the proposed system with the existing system, it is observed that the proposed system accomplished an enhanced performance with respect to resource utilization, cost, throughput, service latency as well as execution time.

Keywords Cloud computing · Convolutional neural network · Advanced encryption standard · Parallel anarchies society optimization

1 Introduction

Cloud computing is considered as the promising technology which has been creating a rising impact on private sectors as well as public sectors. It symbolizes a service model that is on demand for the purpose of providing resources such as data access and storage, through processing as well as software provisioning. Classic categories concerning cloud computing comprise of Infrastructure as a Service or IaaS, Platform as a Service or PaaS, in addition to Software as a Service or SaaS as well as Security as a Service or SECaaS. Infrastructures which are virtualized are offered as a service (computing, storage, server, network, etc.) in the IaaS category (Maggiani 2009; Voorsluys et al. 2011; Dikaiakos et al. 2009). Different types of services in IaaS are available in the cloud like Amazon EBS, Amazon EC2 and Amazon S3 (simple storage service). The PaaS category provides environment for the purpose of program development, execution, testing as well as software deployment like a service in the cloud (e.g., Google

Communicated by V. Loia.

✉ B. Lanitha
lanithanandakumar@gmail.com

S. Karthik
profskarthik@gmail.com

[1] KGISL Institute of Technology, Coimbatore, India

[2] SNS College of Technology, Coimbatore, India

Published online: 04 April 2020

App Engine, Microsoft Azure). The SaaS category offers various software which are cloud based on demand as a service on user's computer in order to eradicate the necessities for the installation as well as the maintenance of the software (e.g., Google Docs) (Garg et al. 2013). The fundamental benefits of employing cloud computing comprise of cost reduction, scalability, reliability, data availability as well as resilience.

Owing to the quick development of technologies like cloud computing, there is speedy amplification of cloud services that have become very remarkable. Important concern in cloud computing is to offer data protection to the end user in order to safeguard the files or data from users who are unauthorized (Singla and Singh 2013; Yu and Wen 2010). For any technology, security is considered as the main objective in which unauthorized users will not have the ability to access your files or even data present in the cloud (Padhy et al. 2011). There exist many problems concerning security in cloud computing like data storage security, confidentiality, third-party data access, data loss or data theft, transmission of data. Cloud computing introduces the variety of vital problems concerning privacy. One of the risks comprises of the third-party access to confidential or delicate information. It may cause a considerable threat toward guaranteeing intellectual property protection as well as personal details. In addition, issues relating to privacy remain in the cloud domain for a long time to come, and several laws have been published so far to protect the privacy of individual data and business confidentiality information. However, these laws and acts expired and are invalid for today's domains. Therefore, the problems concerning privacy problems are becoming more dangerous. The privacy problems comprise of malicious insiders, misuse of cloud computing in addition to many more.

Optimizations associated with the management of virtual machines have gathered significant attention in the most recent years due to its effect on costs, performance as well as emission of carbon. A major part of the past research works is included in the two types which are VM placement and VM selection. The objective of the virtual machine placement category deals with the determination of linking of VMs to physical machines with the aim of reducing the consumption of energy at the same time as obeying constraints concerning performance and also maintaining a small number of VM migrations (Wu et al. 2010). Conversely, VM selection deals with the allocation of computational tasks for the virtual machines (Mann 2015). The partition that exists between the problem of virtual machine placement and virtual machine selection is fixed in the fact that different types of factors perform the two categories of optimization. The cloud providers execute virtual machine placement, while the cloud users carry out VM selection (Schmidt et al. 2010). Virtual machine placement deals with resources, power as well as migration, while virtual machine selection classically relates to lease costs as well as application-level performance metrics.

Typically, a cloud provider would use virtual machines (VMs) and a hypervisor to separate customers. Technologies are currently available that can provide significant security improvements for VMs and virtual network separation. In addition, the trusted platform module (TPM) can provide hardware-based verification of hypervisor and VM integrity and thereby ensure strong network separation and security. Currently, technologies are accessible which can offer significant enhancements concerning security for virtual machines.

2 Related work

Kamara and Lauter (2010) launched a storage service which is a virtual private cryptographic for the purpose of providing to the user data, confidentiality along with integrity contained by the cloud. In the presented methodology, the client application consists of three components: (1) data processor, (2) data verifier as well as (3) token generator. A master key is produced by the client application that has been employed for succeeding operations. Encryption of the file is done by the data processor with the generated keys from the master key, and it is uploaded in the cloud. The data is downloaded with the help of token generator which produces a token, and the token comprises of files concerning identity which require a download. The data verifier tests the data integrity as soon as the data is downloaded from the cloud. Attribute-based encryption or ABE is employed for the purpose of encryption.

Lin and Tzeng (2012) set up a threshold proxy re-encryption scheme and combine it with a decentralized erasure code in order to devise a stable distributed storage system. The system employs servers with threshold key for the purpose of storing a user's key that has been produced by a system supervisor. Encryption of data is done by the user that has been split into data blocks, and each block is stored on different servers that have been arbitrarily chosen. The system moreover offers the forwarding functionality by permitting any users in order to advance the data to other users by not downloading. The authors employed the method of proxy re-encryption in order to forward the data that has been encrypted.

Juels and Opera (2013) proposed a method for the purpose of securing the cloud data which offers numerous services like integrity, availability as well as freshness. The authors utilized a gateway in the endeavor for the purpose

of handling the data's integrity as well as freshness checks. The Iris file system is created for the purpose of migration of the internal file system of the organizations to the cloud. Furthermore, a Merkle tree is employed by gateway that guarantees data's freshness along with integrity by the insertion of file blocks, MAC as well as file version numbers at diverse tree levels. The cryptographic keys concerning confidentiality requirements are also handled by the gateway application.

Shan Sung LIEW (Kumar 2019) proposed a CNN optimized architecture with gender classification for real time based on face images which produces minimum complexity when compared with CNN pattern recognition methods. Through fusing the convolutionary and subsampling layers, the number of processing layers within the CNN is reduced to just four. Unlike traditional CNNs, the authors substituted cross-correlation for the convolution operation, thereby reducing the computational load. The network is equipped using a second-order learning algorithm for back propagation with annealed global levels of learning.

Kiran et al. (2017) proposed a model that would identify the data according to their security parameters using machine learning and hybrid cryptographic technique. The authors employed modified ensemble learning technique to enhance the existing k-nearest neighbors (KNN) technique. Ensemble learning method comprises a set of different models being grouped together to improve each model's prediction and stability power. To focus on highly confidential data, HMAC function is added with the already available Rivest–Shamir–Adleman (RSA) algorithm.

Sarkar and Kumar (2016) proposed a new framework which hides the plaintext which can be stored in cloud by creating a secret key of small size which is appropriate for information-centric applications. The authors provided a security architecture for cloud storage based on the "modified cuckoo algorithm," a metaheuristic method for server discovery, three-stage authentication, confidentiality with elliptic curve cryptography (ECC) and cipher text optimization with covariance matrix adaptation evolution strategies (CMA-ES).

Amanpreetkaur and Singh (2018) presented different aspects of cloud for management of cloud resources in an energy-efficient, reliable and sustainable manner. The authors discussed the research challenges and possible future research directions.

Han and Chan (2017) proposed an allocation coverage called previously chosen servers first which goals to reduce the possibility of co-location by minimizing the user's requested VMs. An updated VM allocation strategy is used to reduce the probability that attackers would co-locate targets.

Elsedimy (2017), presented a novel approach to improve virtual machine placement efficiency, enhance virtual machine performance, minimize the power consumption of servers and to keep the use of multidimensional resources in an optimal utilization level. Virtual machine placement problem is optimized by a new version of particle swarm optimization (PSO) method.

Fang et al. (2016) proposed framework in order to find the optimal VMs placement in the cloud environment using ant colony optimization (ACO). This effort attempts to identify the placements of VMs in the data center to increase the VMs' quality, reduce energy cost as well as for energy saving. ACO Joined with Order Exchange and Migration (OEM) technique which is a local search is referred to as an OEMACS (ant colony systems). This algorithm efficiently reduces the number of servers employed for the allocation of virtual machines or VMs from a perspective of optimization by means of a new method for the purpose of pheromone deposition that directs the ants in the direction of promising solutions which can group VMs collectively. The OEMACS algorithm is executed for a range of issues concerning VMP with differing sizes of VM in the cloud environments comprising of homogenous as well as heterogeneous servers.

A new mechanism was designed by Li et al. (2018) for the purpose of optimizing the VM selection as well as allocation by employing similarities between memory content similarities for the purpose of combining the server in the cloud. By utilizing similarity between contents, we can redefine the above stated two issues like: 1) concluding which of the VMs ought to be shifted from the hosts that are overloaded (selection of VM problem) as well as 2) how to place the VMs to the target hosts (placement of VM problem) into a single problem for the purpose of reducing the transferred data in the VM migration. When a placed host is given overloaded threshold, solution for approximation is developed for the purpose of resolving the issues that contain a single overloaded host in addition to a single destination host.

An alternative multiobjective optimization approach is proposed in Alresheedi et al. (2019) by Shayem Saleh Alresheedi which combines the salp swarm and sine–cosine algorithms to determine a suitable solution for virtual machine placement.

3 Proposed methodology

This section explains the cloud computing model's architecture that has been suggested. It comprises of four components which include devices of stakeholders, requests of stakeholders (tasks), cloud broker and administrator that are illustrated in Fig. 1. The services concerning the devices which are communicating are

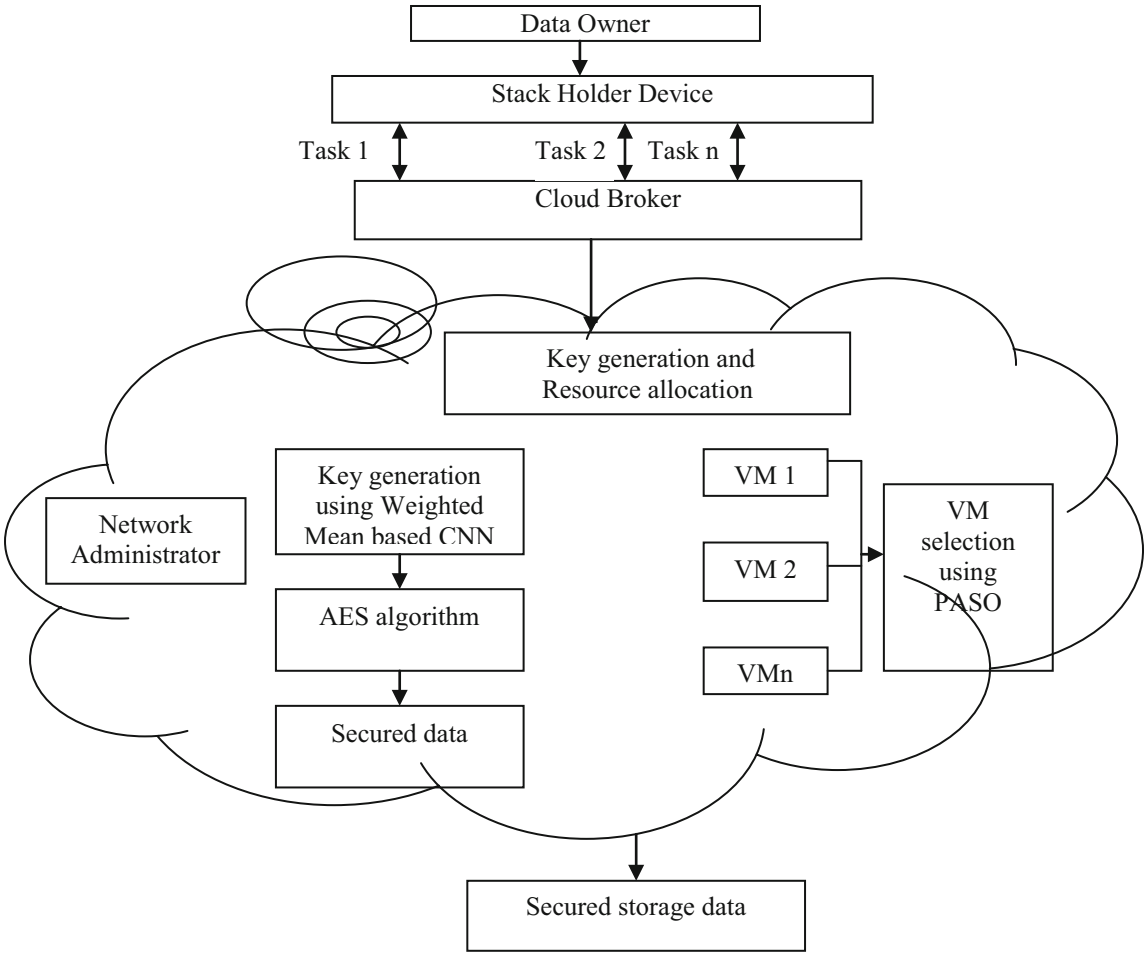

Fig. 1 Flow diagram of the proposed system

accountable for executing diverse communication management of network amid stakeholders as well as the cloud.

In this particular work, we commence with the data availability; the work presented a weighted mean-based convolutional neural network or WMCNN on the basis of data confidentiality, the loss of data recovery in addition to recovery of data. Additionally, this facilitates a novel model for the cloud environment by employing parallel anarchies society optimization or PASO for the purpose of optimizing VM selection.

The stakeholders employ a range of devices (laptop, PC, smartphone, digital sensors, tablet, etc.) in order to effortlessly send requests (tasks) by means of cloud computing in order to get diverse services. The cloud broker is in charge of receiving and sending requests (tasks) from cloud service. The cloud broker ensures secure data transfer between multiple cloud service providers and cloud consumer. Every network might possess numerous application hosts = {Host-1, Host-2… and Host-N} offering SaaS be assigned to carry out the requests of the cloud users. Every host possesses a group of resources = {R-1, R-2 … and R-N} which can be allocated for the requests of the stakeholder. Every network possesses a network administrator which is in charge for coordinating the intercommunication among hosts within the network as well as between the network and additional networks in the cloud. With the purpose of enhancing the data's confidentiality as well as data recovery, the key generation is executed with the assistance of weighted mean-based CNN; furthermore, the encryption of the files is done with the key that was generated, and it is stored in the cloud storage system by means of resource (VM) allocation using PASO.

3.1 Key generation using weighted mean-based CNN

Owing to the escalation of different issues concerning privacy, sensitive data has to be encrypted previous to cloud outsourcing. Considering cryptography, pseudorandom number generators or PRNGs were employed for the generation of secret keys amid two communicating parties. These naturally commence with a "seed" quantity along

with employing numeric or logical operations for the production of a series of values. A characteristic technique of pseudorandom number generation is referred to as a linear congruence pseudorandom number generator. The real-world secure systems employ these mechanisms for the purpose of generating cryptographic keys, initialization vectors as well as other values presumed to be arbitrary. Here, the secret key that is generated is arbitrary. However, here there exist certain probable attacks against PRNGs (Kelsey et al. 1998).

Convolution neural network or CNN is a type of network which is feed forward. Many characteristics are present like simple structure, less training parameters as well as adaptability. The network consists of an input layer that takes the key generated arbitrarily as the input and output layer from which the trained output is obtained in addition to the intermediate layers known as hidden layers. As mentioned previously, the network possesses a sequence of convolutional as well as sub-sampling layers; simultaneously, the layers generate an approximation of the input secret key (Fig. 2).

In the algorithm of convolutional neural networks, every sparse filter is simulated throughout the visual field. These units subsequently develop into attribute maps that share weight vector as well as bias. The gradient concerning the shared weights represents the sum of the gradients pertaining to the factors being shared. CNN also utilizes the notion of max pooling that is a type of non-linear down-sampling. In this particular method, partitioning of the key into non-overlapping rectangles is done. The result of every sub-part is considered to be the highest value.

3.2 Convolution layer

In the CNN network, the convolution layer is considered to be the first layer. The layer's structure is demonstrated in Fig. 3. It comprises of a mask, bias in addition to a function expression. In the convolution layer, the preceding layer's attribute maps are convoluted with kernels and subjected to a function in order to create the output attribute map. Every output map might merge convolutions along with various input maps. Generally, we know that

$$X_j^l = f\left(\sum_{i \in M_j} X_i^{l-1} * K_{ij}^l + b_j^l\right) \tag{1}$$

where X indicates the output, M_j indicates input map selection, X_i^{l-1} indicates the value of input, K_{ij}^l indicates weight connecting input to the output and b indicates bias value. Every output map is provided with a bias b which is additive; nevertheless, for a specific output map, convolution of the input maps with distinct kernels will be done. The resultant output is a 28 × 28 matrix. Then, bias is added and sigmoid function is applied on the matrix.

The above figure depicts a 5 × 5 mask that performs convolution of a 32 × 32 input attribute map. The resultant output is a 28 × 28 matrix. Then, bias is added and sigmoid function is applied on the matrix.

3.3 Sub-sampling layer

The layer of sub-sampling comes after the convolutional layer. It has planes with the same number as the convolutional layer. The objective of this layer is to minimize the size of the attribute map. It splits the image into blocks of 2 × 2 and carries out averaging. Sub-sampling layer maintains the relative records between attributes.

A sub-sampling layer generates down-sampled variations of the input maps. For N input maps, it produces N output maps

$$X_j^l = f(\beta_j^l \text{down}\ (X_j^{l-1}) + b_j^l) \tag{2}$$

where down (·) describes a sub-sampling function. This function is used to add each well-defined n x n blocks of the input image and produces output image which is n

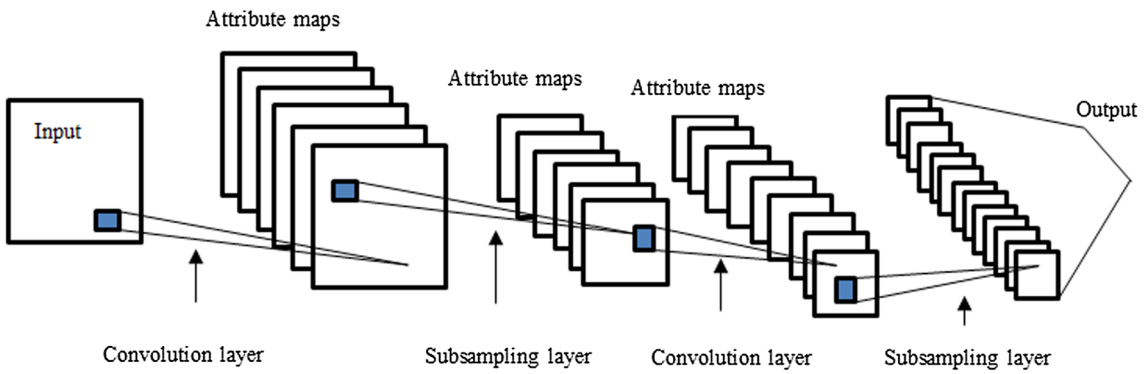

Fig. 2 Graphical flow of layers

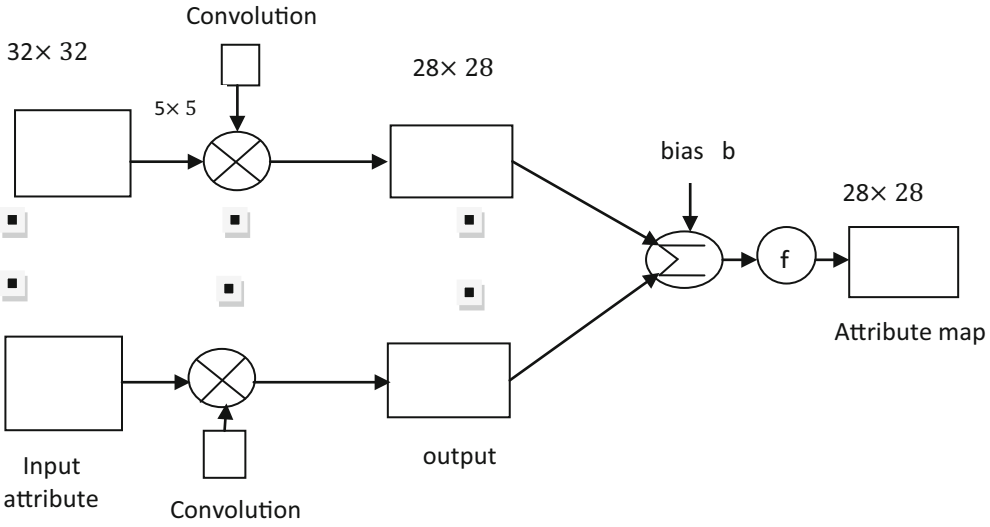

Fig. 3 Convolution layer working

times smaller across both dimensions. Every output map is given with its own multiplicative bias β and an additive bias b. Figure 4 represents the sub-sampling layer functions.

In this work, optimal value of the β and b is updated based on the overall mean value of weight of the attribute map. The weighted mean is defined as the sum of weight values of all the attributes divided by the total number of attributes.

$$\text{Weighted mean} = \frac{\sum_{i=1}^{N} wx_i}{N} \tag{3}$$

The bias mean is defined as the sum of bias values of all the attributes divided by the total number of bias value of attributes

$$Bias\ mean = \frac{\sum_{i=1}^{N} bias_i}{N} \tag{4}$$

where

N – Total number of attributes

w—weight value of the attribute

x_i—number of attributes.

The secret key from the output layer is used to encrypt the cloud data. It improves the confidentiality of data, the loss of data recovery and data recovery.

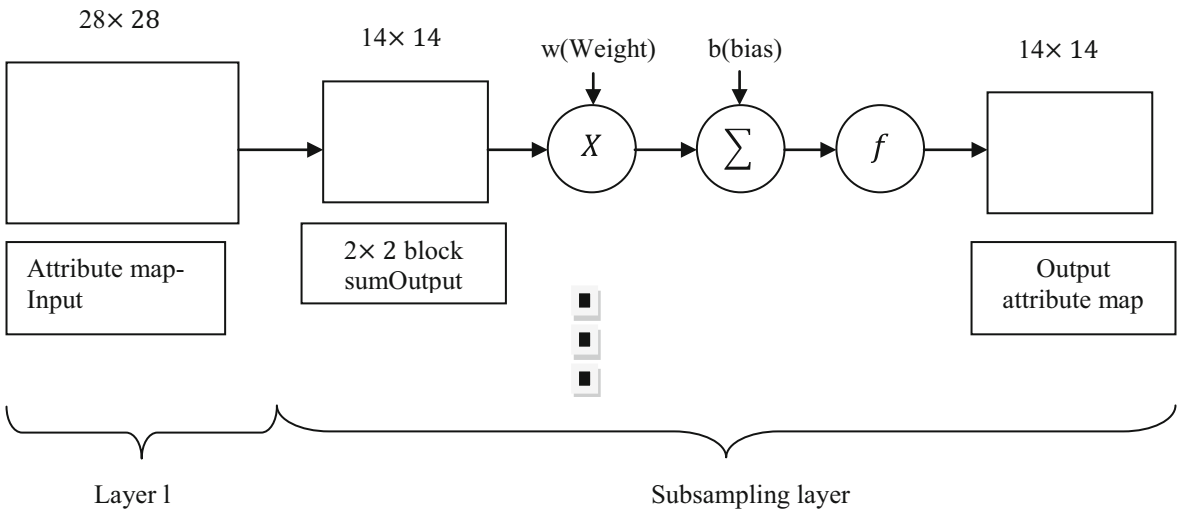

Fig. 4 Sub-sampling layer working

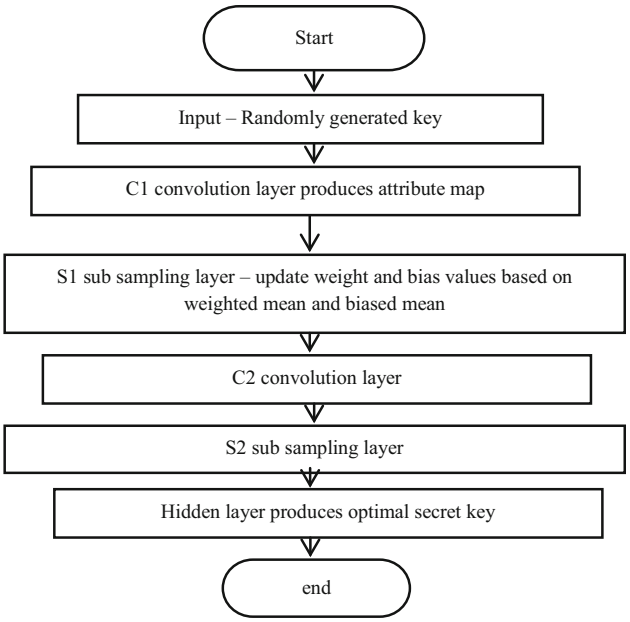

Fig. 5 Flowchart for proposed weighted mean-based CNN

Algorithm 1: Training procedure of CNN

1. Initializing Weight(CNN);
2. While not in convergence range do
3. Calculate Learning Rate(Samples);
4. Rearrange(Samples);
5. For every sample do
6. Output = Forward-Pass-CNN(sample);
7. Loss = Calculate-Error-rate(Output);
8. Error = Backward-Pass-CNN(Loss);
9. Weight-Update(error);
10. end for
11. end while

In Initializing Weight() method, random values are initialized to weights and random values are produced by initializing different parameter values with different initialization methods. In Calculate Learning Rate SDLM() method, learning rate is updated for individual weight or bias. Forward-Pass-CNN() refers to calculation process, and Backward-Pass-CNN() refers to process of counting changes in weights. In Calculate Errorrate()method, network error is identified. In Weight-Update() method, kernel weights are updated.

This section introduces weighted mean convolution neural network algorithm. Figure 5 depicts the flowchart, and the algorithm is as follows.

Algorithm 2: Weighted mean based CNN

Step 1: Initialize the randomly generated key as the input

Step 2: Perform the operation of convolution- layer C1 which uses 6 convolution kernels of size is 5×5, can produce six attribute maps.

Step 3: The six attribute maps are passed to the S1 sub sampling layer for sub sampling.

Step 4: Each attribute maps contains a weights and bias, S1 layer is used train 12 parameters.

Step 5: Update weight and bias values based on the weighted mean and bias mean.

Step 6: Perform same C1 process in C2 convolution layer and S1 process in S2 sub sampling layer

Step 7: Sub sampling layer output is given to hidden layer H

Step 8: Output attribute map(optimal secret key)

3.4 Advanced encryption standard (AES)-based encryption

Advanced encryption standard (AES) is one of the most common and reliable encryption algorithms. In this

Table 1 Parameters to reach the optimal selection of VM

S. No.	Criterion	Description	Formula
1	Utilization of CPU (UT)	The total amount of computer's CPU time of processing	UT = 100% (% idle time)
2	Turnaround time (TT)	Total time by a process, i.e., time difference between process completion time and process arrival time	TT = CT-AT
3	Waiting time (WT)	Time of task spent in ready queue, i.e., difference between turnaround time and burst time	WT = TT-BT

Table 2 Simulation parameters (virtual machine)

S. No.	Parameter	Values
1.	Total number of VMs	100
2.	VM memory (MB)	512–2048
3.	Type of manager	Time shared

Table 3 Simulation parameters (task)

S. No.	Parameter	Values
1.	Total number of tasks	0–90
2.	Length of tasks	5000–20,000
3.	Type of manager	Space shared

proposed work, AES algorithm is used to encrypt the data and stored in cloud storage system for providing security so that only the concerned user can be considered as private key. AES algorithm is not only for security but also for great speed. This algorithm has a specific form for encrypting and decrypting subtle data and is used in all software and hardware. Encrypts data blocks of 128 bits in 10, 12 and 14 round depending on key size. Since there are various rounds in this algorithm, the plaintext is encrypted several times, which allows the data to be secure. It is extremely difficult for hackers to get the actual data. AES is not vulnerable to attacks and makes a fine choice for cloud information security.

3.5 VMs optimizing model using parallel anarchies society optimization (PASO) algorithm

A new approach among swarm intelligence method is anarchic society optimization (ASO). ASO is motivated by a human society whose participants conduct themselves anarchically and adventurously in order to find much better circumstances. ASO can be applied in a straightforward manner to any problem and is capable of accurately checking the solution space and avoiding dropping into optimum local solutions. In this ASO algorithm, virtual machines are chosen randomly within the solution space. Every VM in the cloud is viewed as a member which is a solution (VM) that can be allotted for performing the various subtasks of the stakeholders. The proposed PASO algorithm attempts to discover optimal selection of VMs with reduced execution time and maximum resource utilization and to increase system efficiency. In PASO, the parallel processing targets to produce the end result using more than one processor concurrently which is used to limit the running time. Then, the fitness of every member (VM) is determined. Fitness function (optimal selection of VMs) is computed by using utilization, turnaround time and weight time. The algorithm coherence is maintained with the help of barrier synchronization which is used to stop the algorithm from move to the next step until the fitness function (optimal selection of VMs) has been reported. Complete the procedure of fitness evaluation for all of the members (VMs). Based on the determined fitness value, a comparison is made with $X^*(\mathrm{k})$, P_i^{best} and G^{best} and the current position of the VM will be determined along with the movement policy, where $X^*(\mathrm{k})$ is the best position in the kth iteration, P_i^{best} is the best position reached by ith member in kth iteration and G^{best} is the best position experienced by all members in the first k iterations(Bozong-Haddad et al. 2017). One of the members (VM) will attain the optimal position after a sufficient number of iterations. Optimal position indicates that the virtual machine selected will meet the best fitness values which consist of minimum turnaround time and minimum waiting time. As we are allocating the number of tasks and the number of VMs, we achieved better resource allocation. The resource allocation is done with the optimal selection of virtual machine. If the number of tasks is increased, with the help of parallel processing, we achieve better performance when compared with the existing system.

Algorithm 3: PASO Algorithm
Input: N members
Output: Optimal VMs with Optimal Execution Time
1. Initialize the N members, member position and set of iterations counter I=0
2. Users Tasks = X ,
3. Assign number of VMs and for each VM
4. Generate M initial solutions and evaluate their fitness values (UT, TT and WT)
5. While (termination criteria are not satisfied)
6. Determining the values of X^*(k), P_i^{best} and , G^{best}
7. For i=1 to M
8. Computing FI_i(k)
9. If FI_i (k) is less than threshold X_i (k) , then X_i (k) moves towards X^*(k)
10. Else X_i (k) moves towards a random member
11. End if
12. End for
13. For i=1 to M
12. Computing EI_i(k)
13. If EI_i (k) is less than threshold X_i (k) , then X_i (k) moves towards G^{best}
14. Else X_i (k) moves towards a random member
15. Endif
16. Endfor
17. For i=1 to M
18. Computing II_i(k)
19. If II_i (k) is less than threshold X_i (k) , then X_i (k) moves towards P_i^{best}
20. Else X_i (k) moves towards a random member
21. End if
22. End for
23. For i=1 to M
24. Updating the position by combining the movement policies
25. Calculating the fitness values (UT,TT and WT) for the members
26. End for
27. End while
28. Output the best optimal solution
29. End

where

1. $FI_i(k)$—member's fickleness index for i in kth iteration which measures the satisfaction of the current position.

$$FI_i(k) = 1 - \propto_i \frac{f(X^*(k))}{f(X_i(k))} - (1 - \propto_i)\frac{f(P_i(k))}{f(X_i(k))}$$

where $\propto_i$ is either 0 or 1. So, the fickleness index is also number in the range of [0, 1]. Depending on the values of fickleness index, the ith member would select next position. The ith member has the best position among all members if $F\ I_i$ (k) is smallest.

2. E I_i (k)—irregularity external index for the ith member in the kth iteration based on other members positions.

$$EI_i(k) = 1 - \mathrm{e}^{-\theta_i[f(X_i(k)) - f(G(k))]}$$

in which θ_i is a positive number and the above equation defines the distance of community member i from G^{best}. If the community member is close to G^{best}, it will have a more logic behavior.

1. II_i (k)—irregularity internal index for the ith member in the kth iteration based on previous positions.

$$II_i(k) = 1 - \mathrm{e}^{-\beta_i[f(X_i(k)) - f(P_i(k))]}$$

where β_i is a positive number. The members will act more logically, as the threshold converges to one.

3.6 Objective function

The execution time of stakeholders' requests is calculated with the help of fitness function which consist of turn-around time, CPU utilization and waiting time. The following parameters are used to calculate these criteria.

Arrival Time (AT): Entry time of the task in the ready queue.

Burst Time (BT): CPU execution time for the task.

Burst time is computed as follows:

$$BT = \text{BurstClock Time} \div \text{Burst\_Ratio} \quad (5)$$

where

$$Burst\_\text{ratio} = \text{Threshold of Burst} \div \text{Limit of Burst} \quad (6)$$

Completion time (CT): total time required for task execution which includes arrival time, burst time and interrupt time.

The following Table 1 describes the formulas for calculating the criteria using the parameters to attain the optimal selection of virtual machine.

4 Experimental work and results

This segment discusses the experimental results of our proposed model. The version is implemented using Java. Ahmadi Javid proved that the ASO algorithm (Smys and Josemin Bala2012) is a more general state of the PSO algorithm. The existing parallel particle swarm optimization (PPSO) (Abdelaziz et al. 2018) and proposed parallel anarchies society optimization (PASO) are compared in terms of resource utilization, cost, throughput and execution time. The simulation parameters are represented in Tables 2 and 3.

1. Resource utilization

With the use of a multi-tenant model, resources are pooled to serve more than one clients according to client demand with physical and virtual resources dynamically assigned and reassigned.

The performance of the existing PPSO and proposed PASO schemes is compared in terms of resource utilization; the number of tasks is taken in x-axis, and useful resource utilization is taken in y-axis. Resource utilization is calculated by using the ratio of busy time with available time. The experimental effect shows that the planned system achieves better resource utilization compared with the existing model (Fig. 6).

2. Execution time

The performance of the current PPSO and proposed PASO schemes is compared in terms of execution or runtime. The computational time of the various iterations with

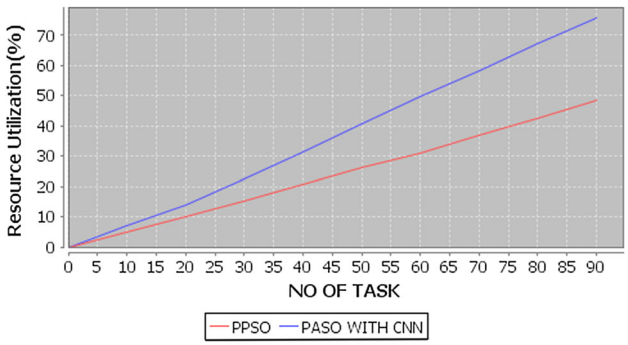

Fig. 6 Resource utilization comparison

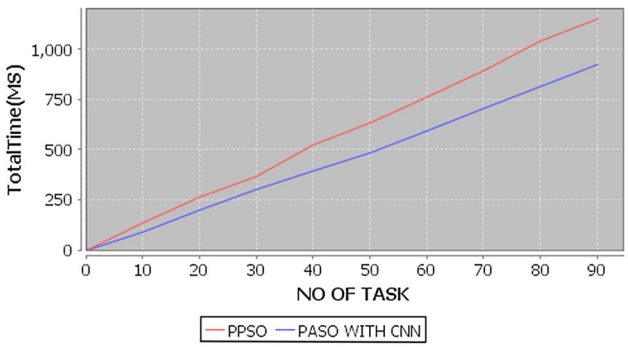

Fig. 7 Execution time comparison

varying number of virtual machine and task allocation is low when compared with the PPSO algorithm. The proposed system achieves lower execution time to allocate all tasks when compared with the existing system (Fig. 7).

3. Cost

The cloud service provider cost mostly depends on CPU utilization of the active (leased) resource. The performance of the current PPSO and proposed PASO schemes is in contrast in phrases of cost. The total cost for virtual machine selection and the task allocation is established and compared with the existing model. The experimental effects show that the proposed model achieves minimal value when compared with the existing model (Fig. 8).

4. Throughput

Throughput of a system is calculated by the rely of task in the maximum average execution time of a set of tasks. Figure 5 compares the throughput performance of the proposed PASO and existing PPSO approaches. The trial result shows that the planned model achieves higher throughput compared with the present model (Fig. 9).

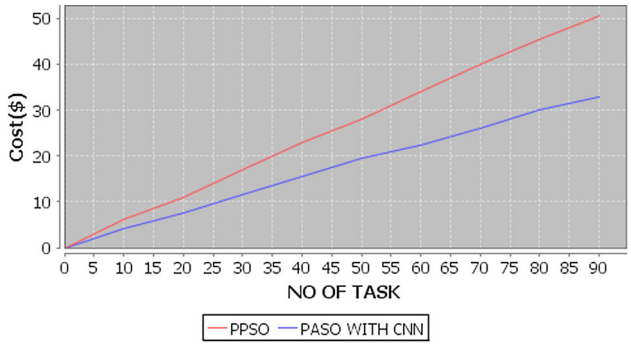

Fig. 8 Cost comparison

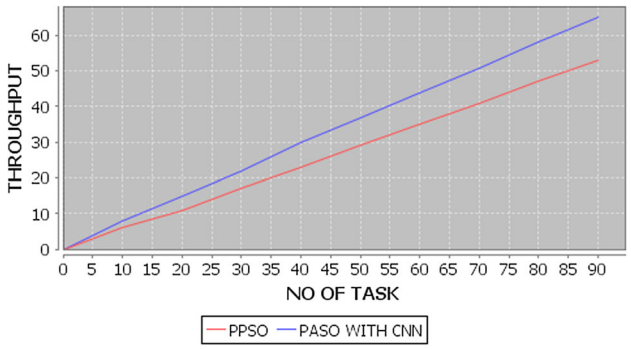

Fig. 9 Throughput comparison

5 Conclusion

The proposed system improves cloud security and execution time when compared with other existing systems. In this work, weighted mean-based CNN model is used for key generation. The encryption is performed by using AES algorithm. Then, encrypted data files are stored in cloud storage which improves the data security. In addition, optimal selection of VM is performed by using PASO algorithm which reduces the execution time. The experimental results show that the proposed system achieves better performance when compared with the existing system in terms of resource utilization, cost, throughput, service latency and execution time. Future work will focus on applying the proposed model in different healthcare Systems. Different kinds of data will be used to evaluate the consistency of our system.

Compliance with ethical standards

Conflict of interest All authors state that there is no conflict of interest. We used our own data.

References

Abdelaziz A, Elhoseny M, Salama AS, Riad AM (2018) A machine learning model for improving healthcare services in cloud computing. Elsevier, Amsterdam

Alresheedi SS, Lu S, Ahmed MA, Ewees A (2019) Improved multi objective salp swarm optimization for virtual machine placement in cloud computing 2019

Amanpreetaur K, Singh VP (2018) The future of cloud computing: opportunities challenges and research trends. In: IEEE explore

Bozong-Haddad O, Latifi M, Bozorgi A (2017) Development and application of the anarchic society algorithm(ASO) to the optimal operation of water distribution networks. IWA publishing 2017

Dikaiakos MD, Katsaros D, Mehra P, Pallis G, Vakali A (2009) Cloud computing: istributed internet computing for IT and scientific research. IEEE Internet Computing 13:10–13

Elsedimy E, Rasad MZ, Darwish MG (2017) Multi objective optimization approach for virtual machine placement based on particle swarm optimization in cloud data centers. J Comput Theory Nanosci 79:5145–5150

Fang Z, Hui J, Deng D, Li Y, Gu T, Zhang J (2016) An Energy Efficient Ant Colony System for Virtual Machine Placement in Cloud Computing". Computational Intelligence Society, IEEE 22:1–15

Garg SK, Versteeg S, Buyya R (2013) A framework for ranking of cloud computing services. Fut Gener Comput Syst 29(4):1012–1023

Han Y, Chan T, Alpcan C (2017) Leckie Using virtual machine allocation policies against co-resident attacks in cloud computing, IEEE Trans Dependable Secure Comput 95–108

Juels A, Opera A (2013) New approaches to security and availability for cloud data. Commun ACM 56(2):64–73

Kamara S, Lauter K (2010) Cryptographic cloud storage. Financial cryptography and data security. Springer, Berlin, pp 136–149

Kelsey J, Schneier B, Wagner D, Hall C (1998) Cryptanalytic attacks on pseudorandom number generators. In: International workshop on fast software encryption, pp 168–188. Springer, Berlin, Heidelberg

Kiran SS (2017) Enhance data security in cloud computing using machine learning and hybrid cryptography techniques. In: International journal of advanced research in computer science, 2017

Kumar D (2019) Review on task scheduling n ubiquitous clouds. J ISMAC 1(01):72–80

Li H, Li W, Wang H, Wang J (2018) An optimization of virtual machine selection and placement by using memory content similarity for server consolidation in cloud. Fut Gener Comput Syst 84:98–107

Lin H, Tzeng W (2012) A secure erasure code-based cloud storage system with secure data forwarding. IEEE Trans Parallel Distrib Syst 23(6):995–1003

Maggiani R (2009) Cloud computing is changing how we communicate. In: Professional communication conference, 2009. IPCC 2009. IEEE

Mann ZA (2015) A taxonomy for the virtual machine allocation problem. Int J Math Models Methods Appl Sci 9:269–276

Sarkar MK, Kumar S (2016) A framework to ensure data storage security in cloud computing, IEEE, 2016

Padhy RP, Patra MR, Satapathy SC (2011) Cloud computing: security issues and research challenges. Int J Comput Sci Inf Technol Secur (IJCSITS) 1(2):136–146

Schmidt M, Fallenbeck N, Smith M, Freisleben B (2010) Efficient distribution of virtual machines for cloud computing. In:

Parallel, distributed and network-based processing (PDP), 2010 18th Euromicro International Conference on pp 567–574. IEEE
Singla S, Singh J (2013) Cloud data security using authentication and encryption technique. Int J Adv Res Comput Eng Technol (IJARCET)2(7)
Smys S, Josemin Bala G (2012) Performance analysis of virtual clusters in personal communication networks. Clust Comput 15(3):211–222
Voorsluys William, Broberg James, Buyya Rajkumar (2011) Introduction to cloud computing. Cloud computing. Principles and Paradigms. Springer, Berlin, pp 1–41
Wu H, Ding Y, Winer C, Yao L (2010) Network security for virtual machine in cloud computing". In: 2010 5th international conference on computer sciences and convergence information technology (iccit), pp 18–21. IEEE
Yu X, Wen Q (2010) A view about cloud data security from data life cycle". In: 2010 international conference on computational intelligence and software engineering (CiSE), pp 1–4. IEEE