Copyright ⓒ 2021 KSII

An IPSO-KELM based malicious behaviour detection and SHA256-RSA based secure data transmission in the cloud paradigm

N. P. Ponnuviji[1*], and M. Vigilson Prem[2]
[1] Research Scholar, Department of Computer Science and Engineering, R.M.D. Engineering College, Kavaraipettai, INDIA
[Email: ponnuviji@gmail.com]
[2] Professor, Department of Computer Science and Engineering, R.M.D. Engineering College, Kavaraipettai, INDIA
[Email: vigiprem@gmail.com]
[*]Corresponding author: N. P. Ponnuviji

Received Janaury 13, 2021; revised July 13, 2021; accepted July 26, 2021; published November 30, 2021

Abstract

Cloud Computing has emerged as an extensively used technology not only in the IT sector but almost in all sectors. As the nature of the cloud is distributed and dynamic, the jeopardies present in the current implementations of virtualization, numerous security threats and attacks have been reported. Considering the potent architecture and the system complexity, it is indispensable to adopt fundamentals. This paper proposes a secure authentication and data sharing scheme for providing security to the cloud data. An efficient IPSO-KELM is proposed for detecting the malicious behaviour of the user. Initially, the proposed method starts with the authentication phase of the data sender. After authentication, the sender sends the data to the cloud, and the IPSO-KELM identifies if the received data from the sender is an attacked one or normal data i.e. the algorithm identifies if the data is received from a malicious sender or authenticated sender. If the data received from the sender is identified to be normal data, then the data is securely shared with the data receiver using SHA256-RSA algorithm. The upshot of the proposed method are scrutinized by identifying the dissimilarities with the other existing techniques to confirm that the proposed IPSO-KELM and SHA256-RSA works well for malicious user detection and secure data sharing in the cloud.

Keywords: Cloud computing, Data security, Attack detection, Malicious user detection, Secure authentication, SHA256 hashing, Rivest Shamir Adleman (RSA) encryption, Kernel Extreme Learning Machine (KELM).

1. Introduciton

While the Cloud Computing (CC) [1, 2] is not entirely new, it continues to gain the attention among organizations and individual users. The CC has allowed users to migrate their data and applications to the cloud [3]. With huge groups of users using the CC services get attracted to the exclusive services offered by the cloud service providers (CSPs) [4] coupled with the flexible usage and cost-savings [5]. However, the migration of the data to the cloud environment is cumbersome, due to excess operational and security challenges [6]. Cyber-attacks [7] and ongoing security threats are creating mess by penetrating into secure model. These immobilizing are created for cyber threats [8]. By storing huge volumes of data in the cloud makes better model [25]. Trials utilize the accompanying strategies. Initially, the boundary sets of IPSO calculation are decided by fixing the quantity of cycles, with huge number of particles, assess exhibitions of those five calculations by using the normal article related to the emphasis. Finally, the greatest cycle number is set with diverse objective correctness of the capacities' achievement rate along with the normal assembly emphasis number for analysis.

Intrusion Detection System (IDS) is the primary security functions in CC involving diversified client networks. The objective is to identify then monitor malicious network performance. Most of the current IDS is classified into two main categories. They are signature-based and anomaly-based IDS [9, 10]. The rule-based intrusion detection is presented in [25, 11] and the frequent rules are updated [12]. The general security architecture is presented in [23, 24].

Several encryption algorithms are developed to provide data security. Existing approaches secure the data by sending data in the form of ciphertext. But these approaches failed to provide confidentiality and privacy for data owners and users [14]. The voluminous information may cause security issues and network computation overhead [15] & cloud storage system is created in [16]. User authentication approaches have made certain significant contributions to mobile communication and advanced information technologies. This research contributes to improve the security and communication with better classification analysis. On comparing with GA, the PSO is simpler to effectuate and it has few parameters to fine-tune. Nonetheless, the initial PSO version was ineffective in the optimization problem. With the help of SHA256-RSA and IPSO-KELM, the routing issues, energy and security issues of key generation issues are overcome. These days' individuals all throughout the planet are keen on dividing data between themselves, however they are stressed over the security angle while sharing any data. For the present circumstance, cryptography has been an aid to mankind which is expected to get transmission of information. The target of this paper is to provide security to the information we send and getting the key that we are scrambling the information. The crowdNet structure is modeled with large scale malicious attacks and the kernel structure is designed for android services, which increases the availability but it has low security [23]. Intrusion detection in cloud environment is presented in [24]. The cloud based paradigm of intrusion detection and classification is done with feature analysis [25]. Android device application based malware attack detection is done with LSTM-CNN [26]. Path discovery is presented in [27]. Problem is to get the secure transmission in cloud environment also the large data handling may cause malicious behavior. Major objective of this approach is to perform secure data transmission system in cloud paradigm. To improve the classification performances like accuracy, precision and f-score value the proposed IPSO-KELM is performed. To detect the malicious

behavior for increasing the security of the system the proposed approach is created. Therefore, this research contributes to improve the security of cloud paradigm and to detect the malicious behavior, which improves the reliability of cloud environment in various applications.

This work is pre-arranged as: Section 2 presents the review papers centered on the proposed work; Section 3 illustrates the proposed approach; Section 4 renders the performance analyses and the outcomes of the proposed system and at last, Section 5 renders the conclusion.

2. Literature Survey

Gopal Singh Kushwah and Virender Ranga [17] presented DDoS attacks detection model in the cloud. This built with the Voting Extreme Learning Machine. From the model conducted with NSL-KDD dataset and ISCX dataset, the system has detected attacks with 99.18% and 92.11% accuracy respectively. S. Velliangiri and Hari Mohan Pandey [18] presented Fuzzy and Taylor-Elephant Herd Optimization inspired by Deep Belief Network classifier. The performance was compared against the state-of-the-art methods considering metrics.

Ihsan H Abdulqadder et al. [19] presented Multi-Layered Intrusion Detection and Prevention in an SDN/NFV-enabled cloud of 5G networks. Mohamed Yassin et al. [20] presented an Inter-Tenant Attack Detection and Prevention (ITADP) framework based on SQL syntactic analysis for multi-tenant SaaS. This framework was integrated into Amazon Web Services (AWS) public cloud. Mahesh Babu and Mary Saira Bhanu [21] presented a privilege management mechanism. This system was able to figure out the malicious behaviour of the users and unauthorized requests [13].

Hicham Toumi et al. [22] presented based on a Hybrid Intrusion Detection System. This permitted to detect both inside and outside attacks with high detection accuracy in the cloud environment.

3. Proposed Methodology

The proposed model providing the security of the cloud data and another mechanism called Improved Particle Swarm Optimization-Kernel Extreme Learning Machine (IPSO-KELM). At the data retrieval time, the data user requests permission from a Trusted Cloud Centre to access the data, which is stored in the cloud. The proposed method performs the authentication of the data user also. The TCC grants permission for the data users to access the cloud file (encrypted one) only if they are the authenticated ones. The data user finally downloads the encrypted file and decrypts it by utilizing the sender's private key and access the data. The architecture diagram of the IPSO KELM is shown in **Fig. 1**.

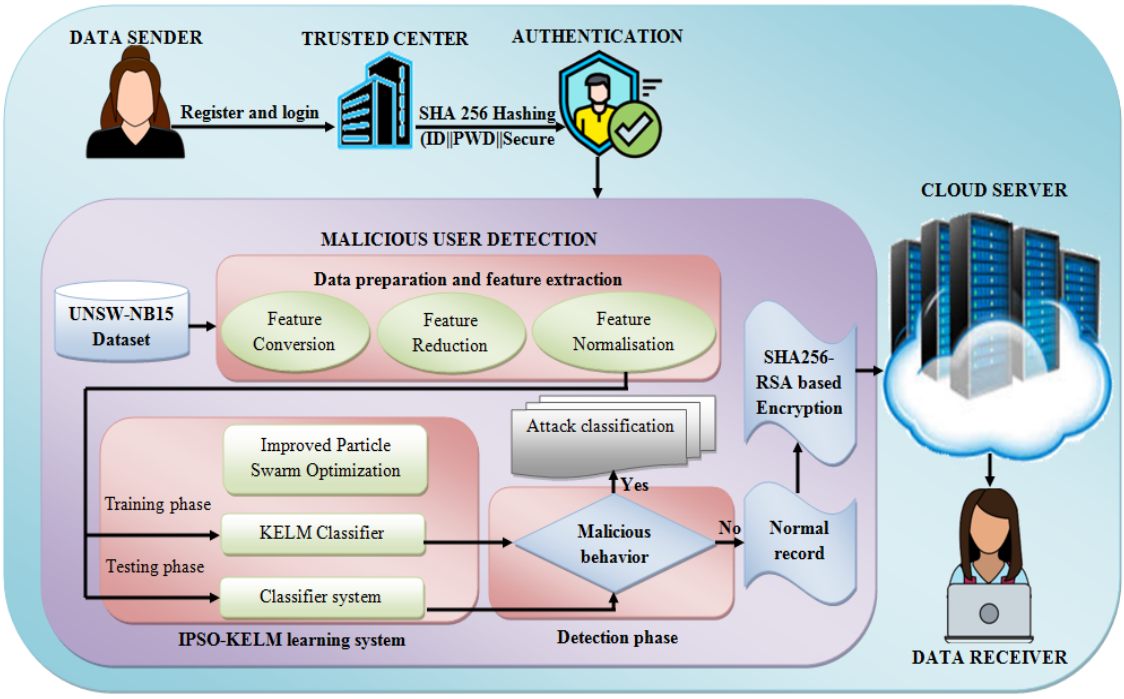


Fig. 1. Architecture diagram of IPSO-KELM

The work is comprised of four entities called Trusted Cloud Centre (TCC), Data Sender (DS), Data Receiver (DR), and Cloud Server (CS). There are four strategies: (i) sender authentication (ii) data sharing (iii) malicious user detection and iv) data retrieval. Each strategy is described in detail in the following subsections.

3. 1 Data Sender Authentication

Registration: In this phase, the DS registration is done. The DS registers the details such as, User ID, Password, and Secure ID to the TCC. Next, the user ID and password of the registered DS are combined and applied using the SHA256 hashing technique to obtain the hashed data of the DS. The generated hash value of the DS is stored in the database for performing authentication.

Login: DS logins to CS, this provides relevant data.

Verification: At the time of login, the given information of the DS's User ID and Password is hashed and compared with the hash value stored in a database. If both hash values are equal, then the data sender is identified as an authenticated DS, and data uploading permission for the DS is granted by the TCC, otherwise, the DS is identified as a fake or malicious user and their permission to upload the data to the cloud is denied. The working of SHA 256 is explained as follows:

3.1.1 SHA 256 Hashing Algorithm

The SHA 256 hashing algorithm is currently one of the most widely used hashing algorithms as it is yet to be cracked and the hashes are calculated quickly in comparison to the other secure hashes like the SHA 512.

$$H_i = H_{i-1} \oplus C_{M_i}\left(H_{i-1}\right), \text{ where } i = 1,2,...N \quad (1)$$

where, C denotes the SHA 256 compression function, $\oplus$ denotes the s word-wise mod 232 addition, and H denotes the hash of M . Here M denotes the message (user id and password). This generated hash function has been stored in the database as part of the authentication of the DS. This generated hash function is saved in the database for the authentication of DS. RSA commonly alludes to a public-key cryptosystem which is broadly utilized for secure information transmission. It utilizes combined keys where one is utilized to scramble messages and the other to unscramble them. SHA256 with RSA mark is a productive lopsided encryption technique utilized in many secure APIs. This initially ascertains a better has of the information utilizing SHA256 calculation. Hence, that point figures the biggest normal divisor between sets of keys, breaking a key at whatever point it imparted a great factor to some other key.

3.2 Malicious User Detection

After authentication of DS is performed, the DS uploads the data or file into the cloud. There is a possibility to attack or hack the data at the time of uploading the data to the cloud. So, it is necessary to check whether the data is received from the authenticated DS or it is received from a malicious user. For this purpose, the proposed method uses IPSO-KELM to identify the malicious behaviour of the DS. It is necessary to perform a training model using IPSO-KELM. For training, the proposed method uses the dataset of UNSW-NB15. The data values from the UNSW-NB15 dataset are trained first. The data received from the DS is tested by comparing the result of the training model. To train the system, initially, the data values from the dataset undergoes some processes like preprocessing, feature extraction, feature reduction, and recognition. The process of each of these steps are as follows:

3.2.1 Preprocessing

The dataset contains enormous quantities of unwanted duplicated values. Preprocessing purifies the data by removing unwanted data.

3.2.2 Feature Extraction

After preprocessing, the features, such as flow, basic, content, time, generated and additional ones are extracted from the pre-processed data. These features are established using both transactional flow identifiers (i.e., source and destination IP addresses) and transactional connection times (e.g., 10 or 100 connections per second). These features help to extract the characteristics of DS's behaviours. **Table 1** shows the UNSW-NB15 database.

Table 1. Features of UNSW-NB15 database

Feature Type	Features	Total
Nominal	1,3,5,6,14	5
Float	7,15,16,27,28,31,32,33,34,35	10
Integer	2,4,8,9,10,11,12,13,17,18,19,20,21,22,23,24,25,26,37,38,40,41,42,43,44, 45,46,47	28
Binary	36, 39	2
Timestamp	29, 30	2

The UNSW-NB15 dataset was made by the IXIA Perfect Storm apparatus in the Cyber Range Lab of UNSW Canberra for creating a mixture of genuine present day typical exercises and engineered contemporary assault practices. The tcp device grabbed 100GB of the crude traffic. Here the evaluation created to produce absolutely 49 features with the class name.

3.2.3 Feature Reduction

The unimportant and noisy features are removed from the extracted features by applying a feature reduction technique. The network packets containing prior information may be used to identify suspicious behaviours. In this paper, Linear Discriminant Analysis (LDA) is used for dimensionality reduction. LDA is a technique for multi-class classification that can be used to automatically perform dimensionality reduction.

3.2.4 Feature Representation and Normalization

Features in dataset measured with quantitative and qualitative form. Here the recognition model is shown in a unified format. **Fig. 2** shows the representation of three symbolic features getting mapped in the UNSW-NB15 dataset.

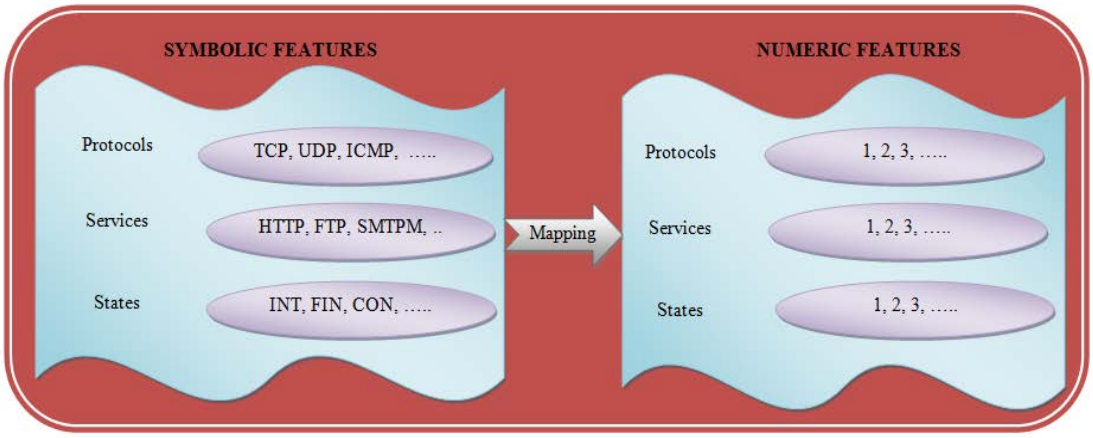


Fig. 2. Representation of feature conversion using the UNSW-NB15 dataset

The dataset contains some significant and repetitive features, which is immaterial. Feature selection assumes a significant part in accomplishing more precision in interruption discovery. The benchmark network dataset accessible in UNSW-NB15 dataset was made in 2015. The top critical features are proposed as feature determination for dimensionality decrease to acquire more exactness in attack recognition and to diminish False Alarm Rate. After the numeric data representation, the data are normalized using min-max normalization. The min-max applied on the reduced feature data is expressed as follows:

$$d_{Norm} = \frac{(d - min(d))}{(max(d) - min(d))} \tag{2}$$

3.2.5 The Recognition state

After feature normalization, the recognition of user behaviour is done. The proposed system performs training. For training, the proposed model uses the Improved Particle Swarm

Optimization-Kernel Extreme Learning Machine (IPSO-KELM) that predicts user behaviour by classifying the reduced features into a normal pattern and malicious pattern. A detailed explanation of IPSO-KELM is given in the below sections.

3.2.5.1 IPSO-KELM Approach

Kernel ELM, a kernel function is applied to the basic ELM. KELM has less adjustable parameters, faster convergence speed, and better generalization performance. So it is necessary to optimize the parameters of KELM. The proposed method uses IPSO for the optimization of KELM. So, the proposed method is named IPSO-KELM.

$$f(d) = h(d)\chi = H\chi \tag{3}$$

While χ is the weight between the hidden layer and the output layer. In ELM, the weight χ can be calculated using equation (4), in which Y is the coefficient.

$$\chi = \boldsymbol{H}^{T}\left(\frac{\boldsymbol{1}}{\boldsymbol{Y}} + \boldsymbol{H}\boldsymbol{H}^{T}\right) \tag{4}$$

$$f(d) = h(d)\chi = h(d)H^{T}\left(\frac{1}{Y} + HH^{T}\right)^{-1} T \tag{5}$$

$$f(d) = h(d)H^{T}\left(\frac{1}{Y} + HH^{T}\right)^{-1} T = \begin{bmatrix} K(d,d_1) \\ . \\ . \\ K(d,d_N) \end{bmatrix}\left(\frac{1}{Y} + \Delta_{KELM}\right) \tag{6}$$

The kernel matrix Δ_{KELM} can be defined as follows:

$$\left\{\begin{matrix} \Delta_{KELM} = HH^{T} \\ \Delta_{KELM\,i,j} = h(d_i).h(d_j) = K(d_i,d_j) \end{matrix}\right\} \tag{7}$$

$$K(p,q) = \exp\left(-\gamma p - q^{2}\right) \tag{8}$$

The performance of the KELM depends greatly on the kernel parameters (γ, Y). In the present approach, these kernel parameters are optimized using IPSO, which is explained in the below section.

3.2.5.2 Improved PSO

A stochastic optimization technique based on population is the PSO. In this technique, the particles act as potential solutions that fly through the problem space by following the current optimum particles. However, the initial version of PSO was not very effective in the optimization problem. So, the PSO for the proposed KELM optimization is known as Improved PSO (IPSO). The steps are as follows:

Step 1: Initialization of population and its position & velocity value with random identity.

Step 2: Estimate the fitness functions of the randomly generated particles.

Step 3: Compare the estimated fitness value with the particles.

Step 4: Compare the estimated fitness with the overall best previous values and if the fitness is better than G_{best} then that fitness is considered as G_{best} for the current particles array index.

Step 5: Fitness evaluation. The position and velocity of particles are expressed as follows:

$$s_i(t+1) = s_i(t) + v_i(t+1)) \tag{9}$$

Step 6: The velocity updates by,

$$v_i(t+1) = r_2 * fn(r_3) * v_i(t) + (1-r_2) * c_1 * r_1 * (p_i(t) - s_i(t)) + (1-r_2) * c_2 * (1-r_1) * (p_g(t) - s_i(t)) \tag{10}$$

where, t is current number of iterations, $v_i(t)$ is velocity of the i^{th} particle at instant t, $s_i(t)$ is the position of i^{th} particle at a time t, $p_i(t)$ is the former position of i^{th} particle, $p_g(t)$ is the best former position of population.

$$fn(r_3) = -1 \text{ where } r_3 \le 0.05 \tag{11}$$

and

$$fn(r_3) = 1 \text{ where } r_3 > 0.05 \tag{12}$$

Step 7: The movement of i^{th} particle is attracted to another more striking (brighter) j^{th} particle and is resolute with velocity by,

$$s_i = s_i + (s_j - s_i) + \left(rand - \frac{1}{2} \right) + v_i(t+1) \tag{13}$$

Step 8: The process is repeated until the solution with better fitness value is obtained. The pseudocode of the proposed IPSO is shown in **Fig. 3**.

Algorithm – Improved PSO based KELM optimization

Input: Kernel Parameters

Output: Optimized Kernel Parameters

Begin
initialize the particles in the population
for i=1 to i_max
for each particle $s_i(t)$ in the population do
$fs_i(t) = f(s_i(t+1))$
if $fs_i(t)$ is greater than $f(P_{best})$ then
$P_{best} = s_i(t)$
end for
if $P_{best} > G_{best}$ then
$G_{best} = Best(s_i(t))$ in population
else
renew the position and velocity of other particles by

$$v_i(t+1) = r_2 * fn(r_3) * v_i(t) + (1-r_2) * c_1 * r_1 * (p_i(t) - s_i(t)) + (1-r_2) * c_2 * (1-r_1) * (p_g(t) - s_i(t))$$

end if
update the best position using

$$s_i = s_i + (s_j - s_i) + \left(rand - \frac{1}{2}\right) + v_i(t+1)$$

end for
end for
End

Fig. 3. Pseudocode for IPSO

3.3 Data Encryption

After finding the behaviour of DS, the data is encrypted and stored in the cloud for providing security to the data. If the data is received from the authorized DS, it will be encrypted using the encryption algorithm and stored in the cloud for further access. This encrypted file is sent to the DR, once the DR requests the TCC for data access. If the DR is an authorized one, the TCC allows the DR to access the encrypted data file in the cloud.

3.3.1 SHA256-RSA

RSA algorithm is an asymmetric cryptography algorithm. Asymmetric actually means that it works on two different keys i.e. Public Key and Private Key. The public key can be shared with everyone, whereas the private key must be kept secret. The public key is used to encrypt messages. The messages that are encrypted using the public key can only be decrypted with the private key. The security level will be low, only if these factors can be found by the intruder through several kinds of attacks. The objective of using the SHA 256

hash function is to make the key-value of the RSA complex. So, it is difficult for the attacker to find the key value and decrypt the data. It automatically enhances the security level of the cloud data with complex key size. This kind of SHA 256 based RSA encryption is named SHA256-RSA. Generate four random prime numbers $p,q,r,and\ s$.

$$g = p \times q \times r \times s \tag{14}$$

$$\beta = (p-1)(q-1)(r-1)(s-1) \tag{15}$$

Multiply z with the third and fourth prime number.

$$x = z \times r \times s \tag{16}$$

$$w \equiv x^{-1}(mod\ \beta) \tag{17}$$

or

$$x \times w \equiv 1(mod\ \varphi), where\ 1 < w < \varphi \tag{18}$$

Generate the public and private keys using the below equations.

$$P_{uk} = SHA256\{x \,||\, g\} \tag{19}$$

$$P_{ruk} = SHA256\{w \,||\, g\} \tag{20}$$

Where P_{uk} denotes the public key and P_{ruk} denotes the private key and the values of w, p,q,r,s and β are maintained as secret.

$$E_c \equiv D^x(mod\ g) \tag{21}$$

$$D \equiv E_c{}^w(mod\ g) \tag{22}$$

3.4 Data Retrieval

After the data is encrypted, the encrypted data is stored in the cloud. If the receiver requests for data access in the cloud, the TCC verifies the DR by performing the processes performed in DS which is registration, login, and authentication. If the receiver is an authenticated one, the receiver is allowed by the TCC to access the encrypted data in the cloud. After getting the data, the receiver performs decryption and gets the original data sent by the data sender.

4. Results And Discussion

In this paper, a secure authentication and data sharing mechanism is proposed using SHA256-RSA and a malicious user detection approach is proposed using IPSO-KELM. The proposed method is successfully implemented in the working platform of Java. In this section, the results obtained by the proposed methods are compared with the existing techniques regarding some performance measures. Based on the comparative analysis of the

techniques, the performance of the techniques is analyzed. The dataset used for the proposed IPSO-KELM based malicious user detection is explained as follows:

4.1 Dataset used

The proposed method uses the dataset of UNSW-NB15. To train the model (IPSO-KELM), the proposed model uses a dataset having 3000 samples containing 1500 normal and 1500 malicious samples. For testing, 3000 patterns (1500 malicious and 1500 normal) are taken.

4.2 Performance Analysis of SHA256-RSA

Firstly, the proposed methods compared the result of the SHA256-RSA with the existing RSA, and the Triple-DES algorithm in terms of encryption time, decryption time, and information loss. The information loss metric denotes the quality of the data. So, here, the information loss of the proposed system is plotted against the existing techniques, which is shown in **Fig. 4**.

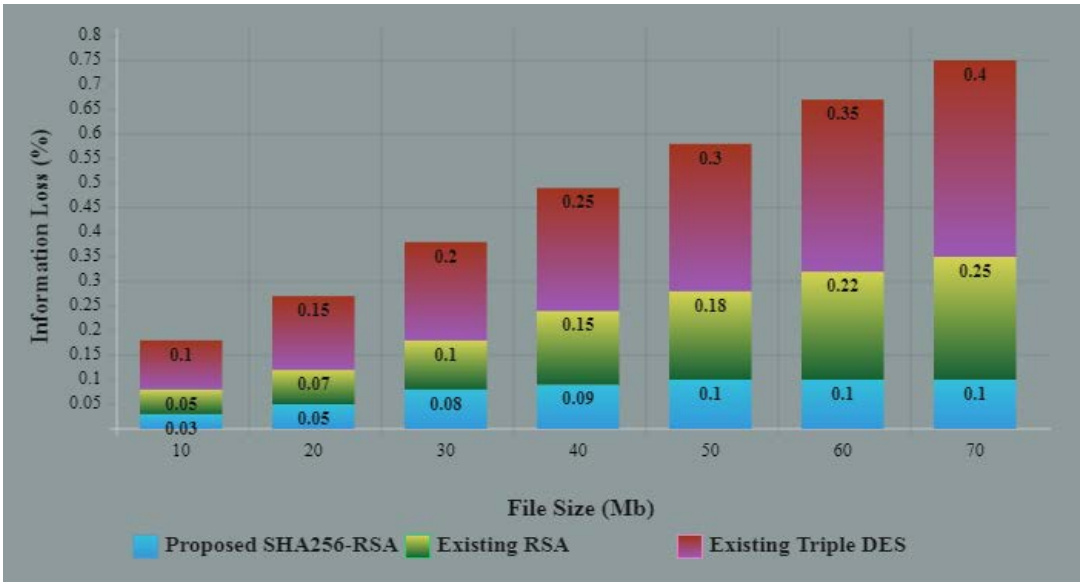
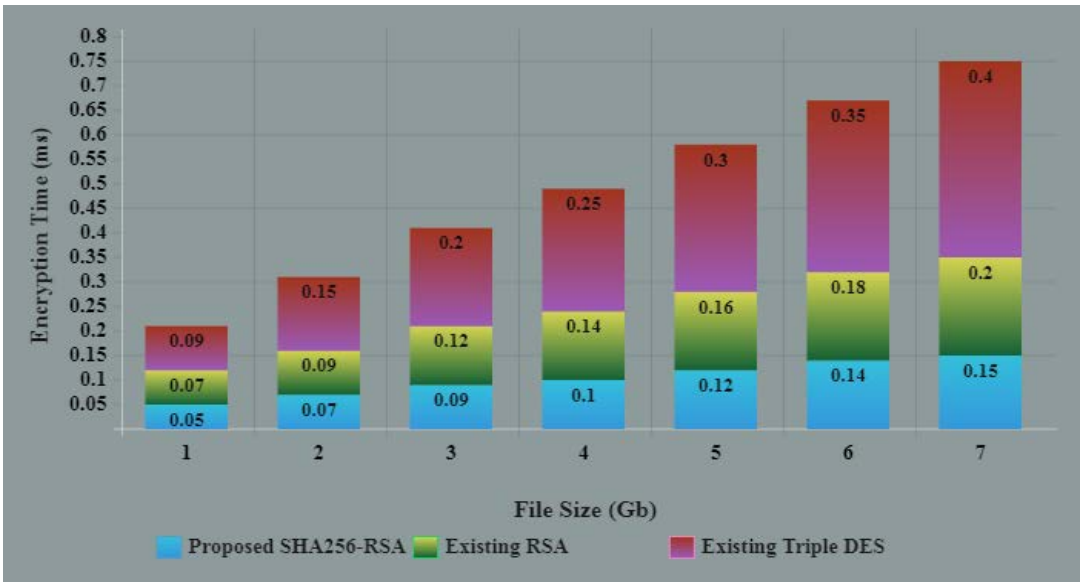
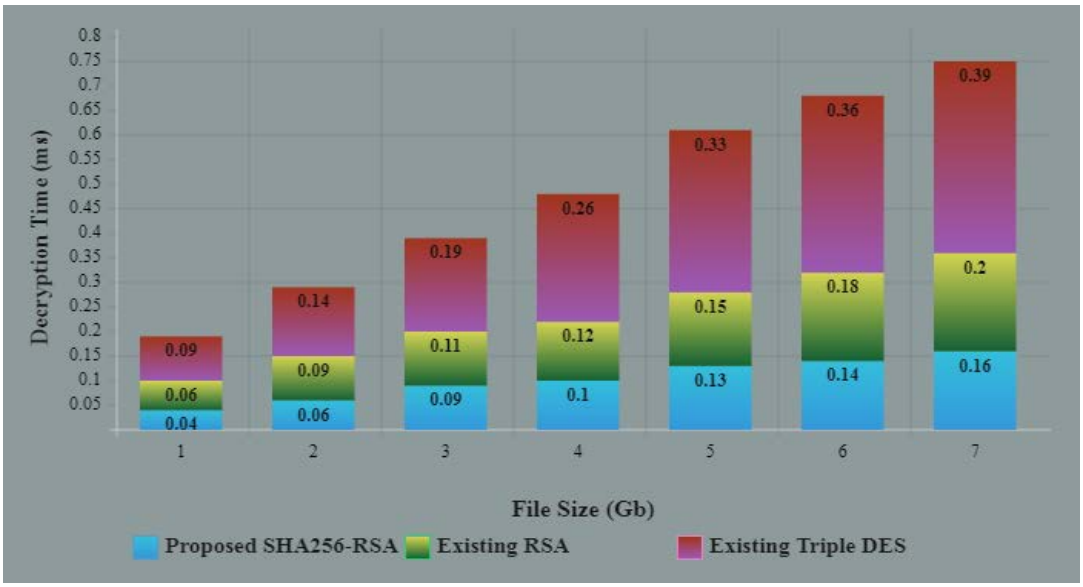


Fig. 4. Information Loss of the techniques

The information loss of the technique is plotted by varying the number of file sizes from (10Mb to 70Mb). For the 10Mb file size, the existing RSA and Triple DES obtain the information loss of 0.05 and 0.1 whereas the proposed SHA256-RSA gives the information loss of 0.03%, which is lower than the existing techniques. When the number of file size increases, the information loss of the techniques also increases, but the proposed SHA256-RSA gives better results than the existing approaches. The results of the other metrics, such as encryption and decryption time of the techniques are shown in **Fig. 5**.



(a)



(b)

Fig. 5. Encryption and Decryption time of the techniques

Fig. 5(a) shows the results of techniques in terms of encryption time. The result is plotted by varying the number of file sizes from 1 Gb to 7 Gb. When the file size is 1 Gb, the proposed SHA256-RSA obtains the encryption time of 0.05 ms, which is lower than the existing RSA (0.07 ms) and Triple DES (0.09 ms). The proposed method uses SHA256-RSA based key for performing both encryption and decryption. **Fig. 5(b)** shows the decryption time of the techniques.

4.3 Performance Analysis of IPSO-KELM

Totally 9 different kinds of attacks are identified such as Analysis, Backdoors, Denial-of-Service (DoS), Exploits, Fuzzers, Generic, Reconnaissance, Shellcode, and Worms. The performance metrics for the detection of malicious data sender using proposed IPSO-KELM presented in **Table 2**, shows that the classification results are promising. The technique obtains 96.5 for TPR and 3.5 for FPR.

Table 2. Performance of detection

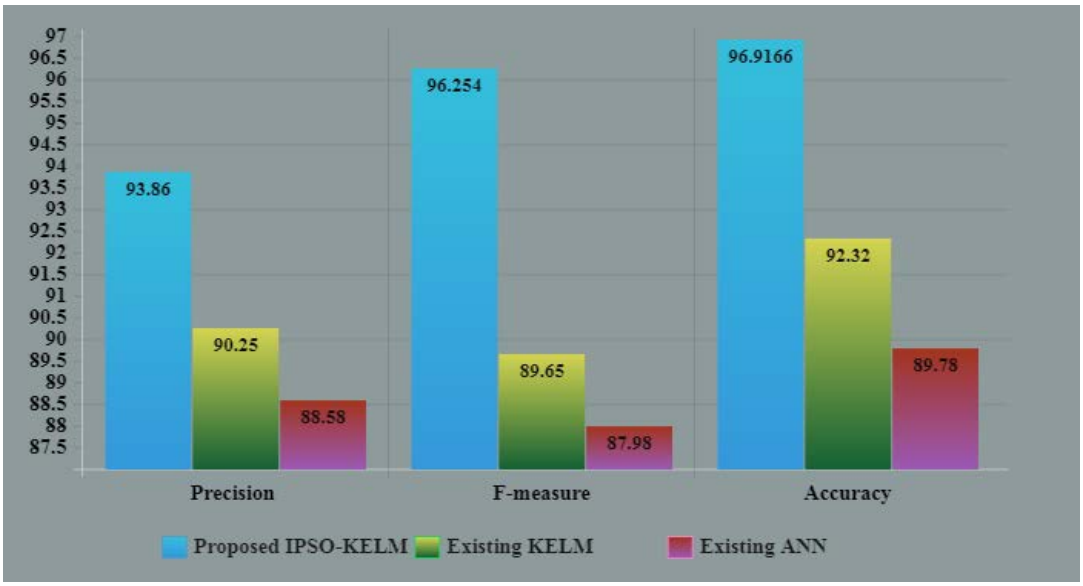
Metrics (%)	Normal behaviour	Malicious behaviour	Total
TPR	98	95	96.5
FPR	2	5	3.5

To evaluate recognition, the normal samples are excluded and only the malicious patterns are affected. **Table 3** shows the obtained performance metrics of all 9 attacks recognized via IPSO-KELM.

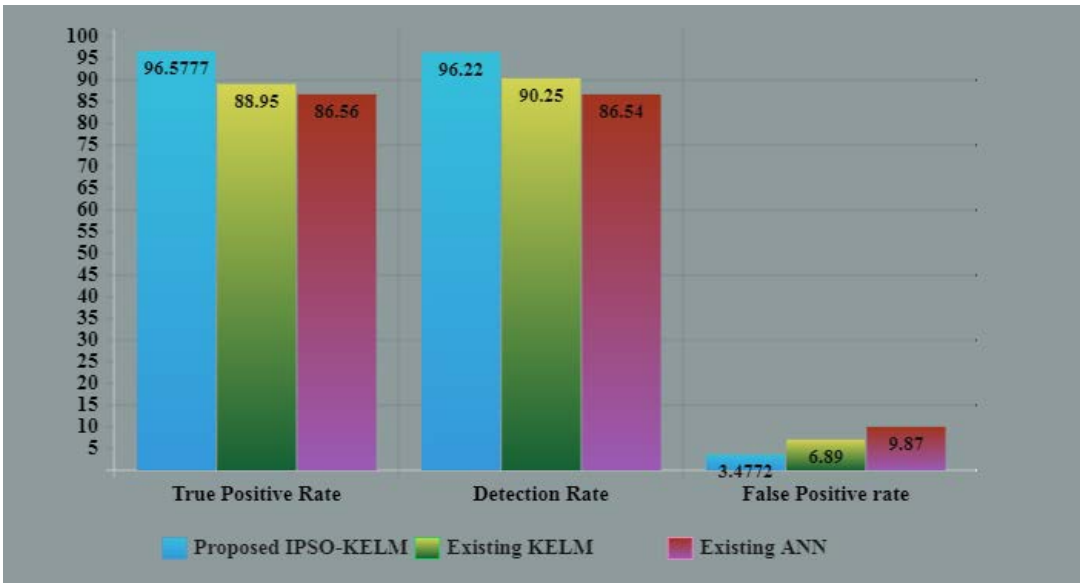
Table 3. Performance measurements for recognition

Metrics (%)	Analysis	Backdoor	Dos	Exploits	Fuzzers	Generic	Reconn	Shellcode	Worms
TPR	98	85	95	98	100	98	98	99	98.2
FPR	12	1	2	4	2	3	1.25	3	1
Precision	87	96	93	98	92	93.58	94.7	92.52	98
F-measure	93	90	98	98.2	96.35	97.85	99	97.89	96
Accuracy	94	97	98.5	94.23	95.87	96.78	98.77	99.65	97.45

All the values, the proposed one obtains the highest level of performance when recognizing all 9 kinds of attacks. Next, the comparison of the IPSO-KELM with other techniques is performed, which is shown in **Fig. 6**.



(a)



(b)

Fig. 6. Classification techniques comparison

In **Fig. 6(a)**, the precision, f-measure, and accuracy of the classification techniques are plotted, and in **Fig. 6(b)**, the TPR, detection rate, and FPR of the classification techniques are plotted. The proposed method obtains the highest accuracy of 96.9166% and lowest error rate (FPR) of 3.4772% when compared to ANN and KELM.

5. CONCLUSION

In this paper, an efficient SHA-256 based secure authentication is provided for both sender and receiver and SHA256-RSA based encryption algorithm is proposed to securely send the data to the receiver. In between data communication, if attacks are thrown by the malicious user that will be found by using the IPSO-KELM. The experiments are conducted to analyze the performance of the proposed method. Comparison of precision, f-measure, accuracy, TPR, detection rate, and FPR are obtained. The proposed algorithm gives better results than the existing algorithms in terms of every compared performance metrics. Likewise, the result of the proposed SHA256-RSA based encryption methodology is compared with the existing RSA and Triple DES algorithms. The proposed SHA256-RSA takes the lowest time for performing both encryption and decryption. The information loss of the proposed method is also low. So, comparing the results and analyzing the performance of the techniques, it is concluded that the proposed IPSO-KELM effectively identifies the malicious behaviour of the data sender, and it finds different kinds of attacks with a single classifier. The proposed technique implements secure authentication and data communication between the sender and the receiver. In the future, the proposed approach will be extended in deep learning techniques.

References

[1] Amandeep Singh Sohal, Rajinder Sandhu, Sandeep K. Sood, and Victor Chang, "A cybersecurity framework to identify malicious edge device in fog computing and cloud-of-things environments," *Computers & Security*, vol. 74, pp. 340-354, 2018. Article (CrossRef Link).

[2] Aviad Cohen, and Nir Nissim, "Trusted detection of ransomware in a private cloud using machine learning methods leveraging meta-features from volatile memory," *Expert Sys with App*, vol. 102, pp. 158-178, 2018. Article (CrossRef Link).

[3] Asimi Ahmed, and Tbatou Zakariae, "IaaS cloud model security issues on behalf cloud provider and user security behaviors," *Procedia computer sci*, vol. 134, pp. 328-333, 2018. Article (CrossRef Link).

[4] Gayatri Pandi S, Saurabh Shah, and K. H. Wandra, "Exploration of vulnerabilities, threats and forensic issues and its impact on the distributed environment of cloud and its mitigation," *Procedia Computer Sci*, vol. 167, pp. 163-173, 2020. Article (CrossRef Link).

[5] MGM Mehedi Hasan, and Mohammad Ashiqur Rahman, "A signaling game approach to mitigate co-resident attacks in an IaaS cloud environment," *J. Info. Security and App*, vol. 50, pp. 102397, 2020. Article (CrossRef Link).

[6] Salman Iqbal, Miss Laiha Mat Kiah, Babak Dhaghighi, Muzammil Hussain, Suleman Khan, Muhammad Khurram Khan, and Kim-Kwang Raymond Choo, "On cloud security attacks: A taxonomy and intrusion detection and prevention as a service," *J. Network and Computer App*, vol. 74, pp. 98-120, 2016. Article (CrossRef Link).

[7] Aviad Cohen, Nir Nissim, and Yuval Elovici, "Novel set of general descriptive features for enhanced detection of malicious emails using machine learning methods," *Expert Sys with App*, vol. 110, pp. 143-169, 2018. Article (CrossRef Link).

[8] Mahdi Rabbani, Yong Li Wang, Reza Khoshkangini, Hamed Jelodar, Ruxin Zhao, and Peng Hu, "A hybrid machine learning approach for malicious behaviour detection and recognition in cloud computing," *J. Network and Computer App*, vol. 151, pp. 102507, 2020. Article (CrossRef Link).

[9] Kanimozhi, V., and Prem Jacob T, "Artificial intelligence based network intrusion detection with hyper-parameter optimization tuning on the realistic cyber dataset CSE-CIC-IDS2018 using cloud computing," in *Proc. of Int. conf. Communication and Signal Processing (ICCSP)*, IEEE, pp. 0033-0036, 2019. Article (CrossRef Link).

[10] Neelakandan, S., Paulraj, D., "An automated exploring and learning model for data prediction using balanced CA-SVM," *J Ambient Intell Human Computer*, vol. 12, pp. 4979-7990, 2021. Article (CrossRef Link).

[11] Saurabh Dey, Qiang Ye, and Srinivas Sampalli, "A machine learning based intrusion detection scheme for data fusion in mobile clouds involving heterogeneous client networks," *Info. Fusion*, vol. 49, pp. 205-215, 2019. Article (CrossRef Link).

[12] Madhan, E. S., Neelakandan, S., Annamalai, R., "A Novel Approach for Vehicle Type Classification and Speed Prediction Using Deep Learning," *J. Computational and Theoretical Nanoscience*, American Scientific Publishers, Vol 17, N0 5, pp. 2237-2242, May 2020. Article (CrossRef Link).

[13] Xiong Li, Yongping Xiong, Jian Ma, and Wendong Wang, "An efficient and security dynamic identity based authentication protocol for multi-server architecture using smart cards," *J. Network and Computer App*, vol. 35, no. 2, pp. 763-769, 2012.

[14] Deebak, B. D, Fadi Al-Turjman, and Leonardo Mostarda, "Seamless secure anonymous authentication for cloud-based mobile edge computing," *Computers & Electrical Eng*, vol. 87, pp. 106782, 2020. Article (CrossRef Link).

[15] Uma Narayanan, Varghese Paul, and Shelbi Joseph, "A novel system architecture for secure authentication and data sharing in cloud enabled Big Data Environment," *J. King Saud University-Computer and Info Sci.*, 2020. Article (CrossRef Link).

[16] Gopal Singh Kushwah, and Virender Ranga, "Voting extreme learning machine based distributed denial of service attack detection in cloud computing," *J. Info Security and App*, vol. 53, pp. 102532, 2020. Article (CrossRef Link).

[17] Velliangiri, S, and Hari Mohan Pandey, "Fuzzy-Taylor-elephant herd optimization inspired Deep Belief Network for DDoS attack detection and comparison with state-of-the-arts algorithms," *Future Generation Computer Systems*, vol. 110, pp. 80-90, 2020. Article (CrossRef Link).

[18] Ihsan Abdulqadder H, Shijie Zhou, Deqing Zou, Israa T. Aziz, and Syed Muhammad Abrar Akber, "Multi-layered intrusion detection and prevention in the sdn/nfv enabled cloud of 5G networks using AI-based defense mechanisms," *Computer Networks*, vol. 179, pp. 107364, 2020. Article (CrossRef Link).

[19] Mohamed Yassin, Chamseddine Talhi, and Hanifa Boucheneb, "ITADP: an inter-tenant attack detection and prevention framework for multi-tenant SaaS," *J. Info. Security and App*, vol. 49, pp. 102395, 2019. Article (CrossRef Link).

[20] Mahesh Babu, B and Mary Saira Bhanu, "Prevention of insider attacks by integrating behavior analysis with risk based access control model to protect cloud," *Procedia Computer Science*, vol. 54, pp. 157-166, 2015. Article (CrossRef Link).

[21] Hicham Toumi, Fatima Zahra Fagroud, Amiyne Zakouni, and Mohamed Talea, "Implementing Hy-IDS, mobiles agents and virtual firewall to enhance the security in IaaS Cloud," *Procedia Computer Science*, vol. 160, pp. 819-824, 2019. Article (CrossRef Link).

[22] Madhan, E.S., "Pharmacovigilance predictive analysis using NLP-based cloud," *Int. J. Biomed. Eng and Tech.*, 26, 316, 2018. Article (CrossRef Link).

[23] Dina Moloja, and Noluntu Mpekoa, "Towards a cloud intrusion detection and prevention system for m-voting in south africa," in *Proc. of Int. Conf. Info Society (i-Society)*, IEEE, pp. 34-39, 2017. Article (CrossRef Link).

[24] S. Neelakandan, Muthukumaran, S., "Transformation-based Optimizations Framework (ToF) for Workflows and its Security issues in the Cloud Computing," *Int. J. Eng and Computer Sci.*, 4(08), 2015. Article (CrossRef Link).

[25] Firoz Kabir, M, and Sven Hartmann, "Cyber security challenges: An efficient intrusion detection system design," in *Proc. of Int. Young Engineers Forum (YEF-ECE)*, IEEE, pp. 19-24, 2018. Article (CrossRef Link).

N. P. Ponnuviji is a Research Scholar in RMD Engineering College in the Department of Computer Science and Engineering. She holds her M.Tech., in Computer Science and Engineering from SRM University, Chennai and is currently pursuing her research in Anna University, Chennai. She has 14 years of Academic experience and 5 years of Research experience. She has published her work in National and International journals. She owns a life-term ISTE membership.

M. Vigilson Prem works as a Professor in the Department of Computer Science and Engineering in RMD Engineering College. He holds his Ph.D., from Anna University, Chennai. He has over 25 years of experience in Academic and Research. He has published his work in various National and International Journals. He holds a life-term ISTE membership. He has conducted various workshops and seminars in Image Processing and Cloud Computing. He has chaired many National and International Conferences.