Journal of Autonomous Intelligence (2024) Volume 7 Issue 3
doi: 10.32629/jai.v7i3.654

ORIGINAL RESEARCH ARTICLE

A coherent salp swarm optimization based deep reinforced neuralnet work algorithm for securing the mobile cloud systems

Osamah Ibrahim Khalaf[1,*], D. Anand[2], Ghaida Muttashar Abdulsahib[3], G. Rajesh Chandra[4]

[1] *Department of Solar, Al-Nahrain Research Center for Renewable Energy, Al-Nahrain University, Jadriya, Baghdad 10072, Iraq*

[2] *Department of Computer Science and Engineering, Koneru Lakshmaiah Education Foundation, Green Fileds, Vaddeswaram, Andhra Pradesh 522302, India*

[3] *Department of Computer Engineering, University of Technology, Baghdad 10066, Iraq*

[4] *Department of Computer Science and Engineering, KKR & KSR Institute of Technology & Sciences, Vinjanampadu, Guntur 522017, India*

*** Corresponding author:** Osamah Ibrahim Khalaf, usama81818@nahrainuniv.edu.iq

ABSTRACT

Protecting the mobile cloud computing system from the cyber-threats is the most crucial and demanding problems in recent days. Due to the rapid growth of internet technology, it is more essential to ensure secure the mobile cloud systems against the network intrusions. In the existing works, various intrusion detection system (IDS) frameworks have been developed for mobile cloud security, which are mainly focusing on utilizing the optimization and classification algorithms for designing the security frameworks. Still, some of the challenges associated to the existing works are complex to understand the system model, educed convergence rate, inability to handle complex datasets, and high time cost. Therefore, this research work motivates to design and develop a computationally efficient IDS framework for improving the mobile cloud systems security. Here, an intrinsic collateral normalization (InCoN) algorithm is implemented at first for generating the quality improved datasets. Consequently, the coherent salp swarm optimization (CSSO) technique is deployed for selecting the most relevant features used for intrusion prediction and categorization. Finally, the deep reinforced neural network (DRNN) mechanism is implemented for accurately detecting the type of intrusion by properly training and testing the optimal features. During validation, the findings of the CSSO-DRNN technique are assessed and verified by utilizing various QoS parameters.

Keywords: mobile cloud computing; security; intrusion detection system (IDS); intrinsic collateral normalization (InCoN); coherent salp swarm optimization (CSSO); deep reinforced neural network (DRNN)

ARTICLE INFO

Received: 23 May 2023
Accepted: 10 August 2023
Available online: 9 January 2024

1. Introduction

In present days, the utilization of smart devices like mobiles, watches, tablets, and etc are increasing rapidly[1,2]. Depending on to the current studies, it is analyzed that the internet traffic is account for 79% in 2022[3], due to the high usage of mobile networks and WiFi. Typically, the mobile network[4] can be accessed by the mobile devices for services, but it suffers with the major problems of increased energy utilization, lack of security, storage overhead, and high processing power. Therefore, the mobile cloud environment[5] is developed, which helps to enable a wireless communication using an external computing devices. In general, the mobile cloud computing is one of the most popular wireless technology[4] that provides an enormous services[6,7] to the customers according to their

requirements or demands. In this network, the mobile users[8,9] are interconnected with the base station, where the interaction among users is performed with the cloud through internet. Moreover, the cloud computing is one of the most efficient and convenient platform[3] that is executed by various remote servers[10,11] that are connected in the network. Also, it ensures the centralized data storage and online accessing operations, which helps to enable an efficient data communication. Typically, the cloud[12–16] is categorized into three types such as private, public, community and hybrid, in which the public cloud is extensively usipby many corporations like Google, Amazon, Microsoft. The typical architecture model of mobile cloud computing is shown in **Figure 1**.

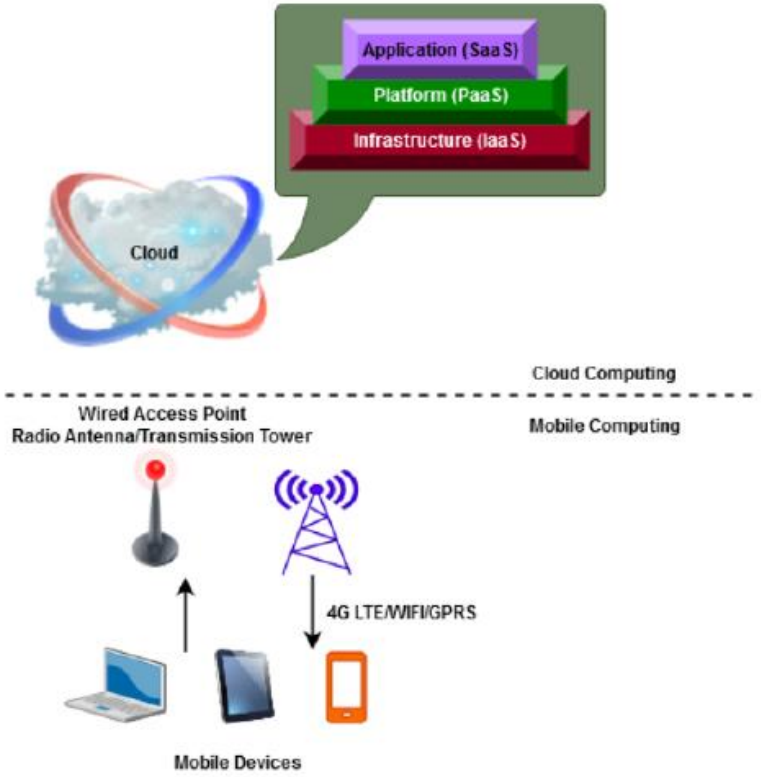

Figure 1. Flow of proposed system.

In the traditional algorithms[17,18], the various kinds of security approaches have been developed to increase the security of mobile cloud environment. However, it limits with the problems[19–21] of complex mathematical computations, high detection time, re used prediction rate, and low convergence rate. The current research aim is to suggest a novel classification framework for ensuring "mobile cloud computing security". The objectives of this paper are:

- To produce the quality improved datasets, an intrinsic collateral normalization (InCoN) mechanism is developed that normalizes the attributes by removing the unwanted fields and replacing the missing attributes.
- To select the specifications for identifying and categorizing the intrusions kinds from the normalized dataset, a coherent salp swarm optimization (CSSO) algorithm is utilized.
- To accurately predict the intrusions with proper training and testing operations using a deep reinforced neural network (DRNN) has used.
- To verify the findings of the current suggested CSSO-DRNN based security approach, an extensive validation has been conducted.

The rest of sections of this research are divided into the number of parts: part 2 investigates the traditional security approaches utilized for protecting the mobile "cloud" environment from the intrusions.

tiso, it examines the benefits and challenges of using those techniques. part 3 presents the working methodology of the propos: 1 system with overall flow and algorithms. part 4 checks the findings of traditional and suggested algorithms by utilizing different evaluation indicators. Finally, the whole research is summarized and its future works in section 5.

2. Related works

This section investigates the various kinds of security algorithm used for protecting a mobile cloud networks from various network intrusions. Moreover, it examines the merits and limitations of each algorithm according to its features and operating conditions.

Shamshirband et al.[22] presented a comprehensive survey on various computational intelligence mechanism used for increasing the security of "mobile cloud systems". The purpose of the current paper was to develop an effective intrusion detection system (IDS) framework for by using an intelligent techniques. Mugabo et al.[23] introduced an enhanced support vector machine (SVM) with information gain based intrusion detection method for protecting the mobile cloud systems. an efficient security algorithm tool for ensuring the properties of data integrity, confidentiality, and availability has designed. Moreover, the information gain was one of the most essential feature used for solving the data redundancy problem, which could be highly useful for increasing the performance of classification. The suggested framework includes essential modules of data preprocessing and intrusion detection, in which the data discretization and normalization processes were performed during preprocessing. Then, the training & testing, alert generation and reporting were performed during the detection phase. However, the suggested approach was not more capable for handling the large dimensional datasets, which degrades the efficacy and performance. Dey et al.[24] utilized a machine learning algorithm to design an IDS framework for heterogeneous mobile cloud networks. The aim of this paper was to model the multi-layered architecture for identifying the network traffic to categorize the type of intrusions. Also, the k-means integra' DBSCAN clustering mechanism was utilized to increase the attack detection accuracy. Yet, it has the major limitations of inefficient processing, high time consumption, and delay in process. Thilagam et al.[25] implemented a recurrent convolutional neural network (RCNN) technique incorporated with an ant lion optimization (ALO) algorithm for mobile cloud security. The primary objective of this paper was to use an intelligent optimization technique for preserving the security of mobile cloud systems with reduced error rate and increased accuracy. Still, the RCNN model could be difficult to understand, and it follows some complex operations for attack prediction and classification. Typically, the cloud is one of the popular and emerging platform highly used in various application systems[26]. According to the different types of services, the benefits and limitations[27] of using the cloud models are represented in **Table 1**.

Nguyen et al.[20] deployed an efficient cyber-attack detection framework for mobile cloud security by assuring the properties of privacy, confidentiality, and data integrity. This framework includes the major stages of data collection, preprocessing, attack detection, and request processing. Here, the feature analysis process was performed to analyze the attributes relevant to the attacks. The primary advantages of using this system were high stability, robustness, and reliability.

Alshahrani et al.[28] introduced a collaborative intrusion detection framework 43 securing the IoT networks, which is termed as CoLL-IoT. This architecture includes the main layers of IoT layer, fog layer, network layer, and perception layer. The purpose of this work was to ensure the security properties of privacy protection, multiple authentications, and confidentiality. Here, the data protection, key agreement and node authentication have been performed in the perception layer. The key benefits of this work were reduced detection rate and latency.

Table 1. Benefits and limitations of cloud models.

Type	Benefits	Limitations
Iaas	Minimal cost	Lack of performance outcomes
-	Efficient utilization of	Privacy Sr. security issues
-	Elasticity	Interoperability problems
Paas	Easy to deploy	Inflexibility
-	Simple to understand	Highly depends on the connection of internet
-	High scalability	Security breaches
-	Reduced cost	-
Saas	Reduced maintenance costs	Control loss
-	Easy to access	Connectivity problems
-	Dynamicity & scalability	Lack of privacy

Based on this survey, it is studied that the existing optimization + classification methodologies[9,29–32] object to develop an accurate IDS framework for "mobile cloud systems". However, it confines with the following difficulties:

- Difficult to understand the system model.
- High time cost.
- Reduced speed of processing.
- High error rate.
- Ability to handle the complex data.

3. System design

This part explains the clear description about the" intrusion detection". Methodology used for protecting the" mobile cloud systems". In the traditional algorithms, various kinds of security approaches have been developed to increase the security of mobile cloud environment. However, it minimizes with the restrictions of complex mathematical computations, high detection time, increased mis-prediction rate, and low convergence rate. So that, the current research objects to improve a novel coherent salp-swarm optimization (CSSO) integrated deep reinforced neural network (DRNN) mechanism for strengthening the security of "mobile cloud systems". This work aims to counter the security problems in the mobile cloud environment by providing an immediate countermeasure with the use of CSSO-DRNN mechanism. For implementing this system, the recent and popular 1135 data records have been used in this work (https://www.cso.ie/en/databases/)[31], and the performance is evaluate dosing various measures. The working flow of the proposed mobile cloud security framework is shown in **Figure 2**, which includes the following stages:

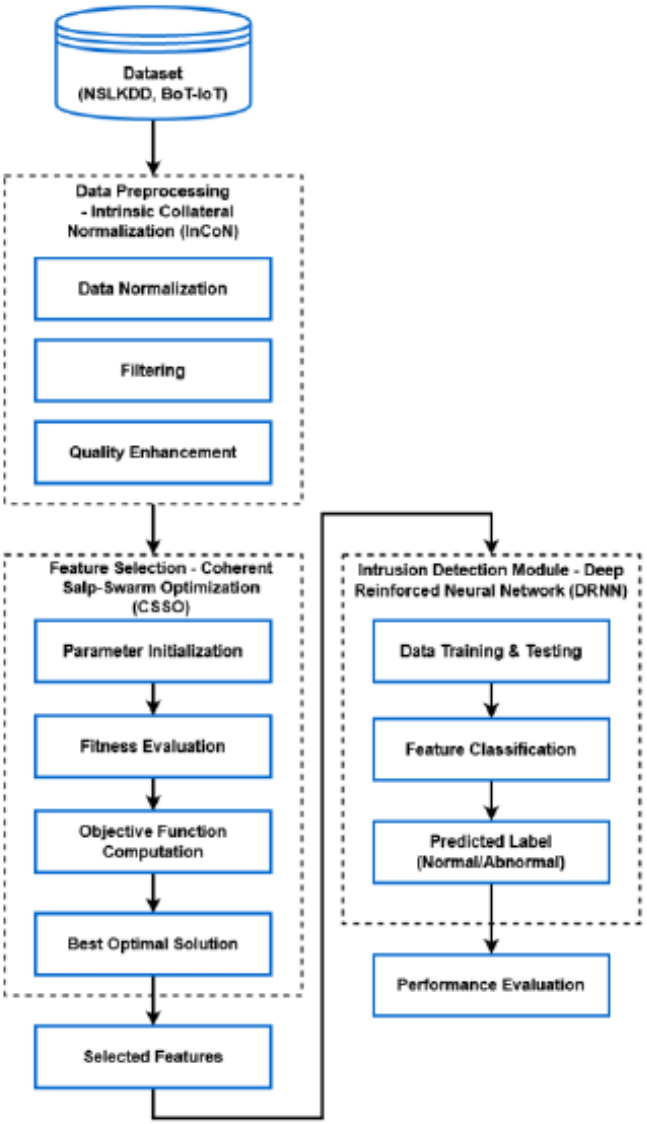

Figure 2. Flow of proposed system.

3.1. Preprocessing

Here, the data preprocessing is performed to normalize the datasets before attack detection and prediction operations. Typically, the data normalized is treated as the one of the most essential process in the security system, because the raw datasets have some missing attributes/fields, and unwanted information. Also, it may disrupt the detection process of classifier, so it must be appropriately normalized or preprocessed for generating the quality improved dataset. In this work, the normalization, filtering, and quality enhancement processes have been performed during preprocessing. For this purpose, an intrinsic collateral normalization (InCoN) mechanism is implemented, which is a highly efficient filtering algorithm used for preprocessing the dataset. When compared to the other filtering mechanisms, it has the following benefits: simple to understand, minimized operating complexity, and high quality of data. Here, the coefficient variance is estimated at first as shown in below:

$$Pv = \frac{\sigma}{\mu} \tag{1}$$

where, it is the mean value, a is the standard deviation, and pv represents the covariance, in which the values of t and o- are as follows:

$$\mu = 1/Y \sum_{D=1}^{Y} Q_D \quad (2)$$

$$\sigma = \sqrt{\frac{1}{y-1} \sum_{D=1}^{y} (QD = \beta v)} \quad (3)$$

$$S_D = QD - \mu_d/\sigma_d \quad (4)$$

where, QD is the data exist in the list, and AI denotes the average value. Consequently, the values of data are standardized in the range of 10 to 1, based on this, the normalized dataset is produced as the output. The obtained quality improved dataset can be used for further optimization and classification processes. Specifically, it is more helpful for attaining an increased accuracy, and reduced error rate during intrusion detection and classification.

3.2. Coherent salp swarm optimization

In this stage, the optimal set of parameters or features relevant to the different types of intrusions are extracted from the normalized dataset. Here, a coherent salp-swarm optimization (CSSO) technique is used to choose the relevant features for accurately predicting the intrusions in the mobile cloud systems. In the existing works, various nature inspired and bio-inspired optimization algorithms are used to select the features for classification. For instance[33], the particle swarm, ant colony, bee colony, firefly, BAT, and cuckoo search are the extensively used algorithms in the conventional intrusion detection frameworks. When compared to these approaches, the CSSO has the following benefits: increased convergence rate, fast processing capability, and simple understand/easy to deploy. Therefore, the proposed work motivates to use the CSSO algorithm for selecting the parameters from the normalized dataset. In this technique, the position of salps are initialized at first in N dimensional searching space, where N represents the count of variables. After that, the position of each salp is updated based on its food searching behavior, in which the

$$KJi = \begin{cases} FPJ + €1\big((UPbj - lbbj)€2 + lb\,bj\big)€3 > 0 \\ FPJ - 1\big((UPbj - lbbj)€2 + lb\,bj\big)€3 < 0 \end{cases} \quad (5)$$

where, KJi is the position of leader salp at dimension j, fee presents the position of food source, E1, E2, E3 are the random numbers, upb and Mb) are the maximum and minimum bounds respectively. Then, a position of only leader salp is further updated based on its food location. Best food during this process, the random coefficient El is treated as an important parameter, and best food fitness is calculated KJi position if the position value is greater than the E1 value and E2 value then the food is treated as a best food. The threshold vale of the best food is in between E1 and E2. But we taken this best food by its efficiently balances both exploration and exploitation stages as shown in below.

$$€_1 = 2e^{-(\frac{4c}{H})2} \quad (6)$$

where, c is the present iteration, and H represents the maximum number of iterations. After that, the followers' position are updated based on the following

$$K_j^i = 1/2\ xT^2 + So(T) \quad (7)$$

where, t is the time, so represents the initial speed. And the value of x is computed by using the following equation.

$$X = S_{final}/So \text{ and } S = k - k_0/T \quad (8)$$

Similar to that, the position of followers s also updated by using the following equation

$$K_j^i = ½(Kji + K\ J\ i\text{-}i) \quad (9)$$

where, I >= 2, and k_j^i is the position of follower at dimension j. As shown in **Figure 3**.

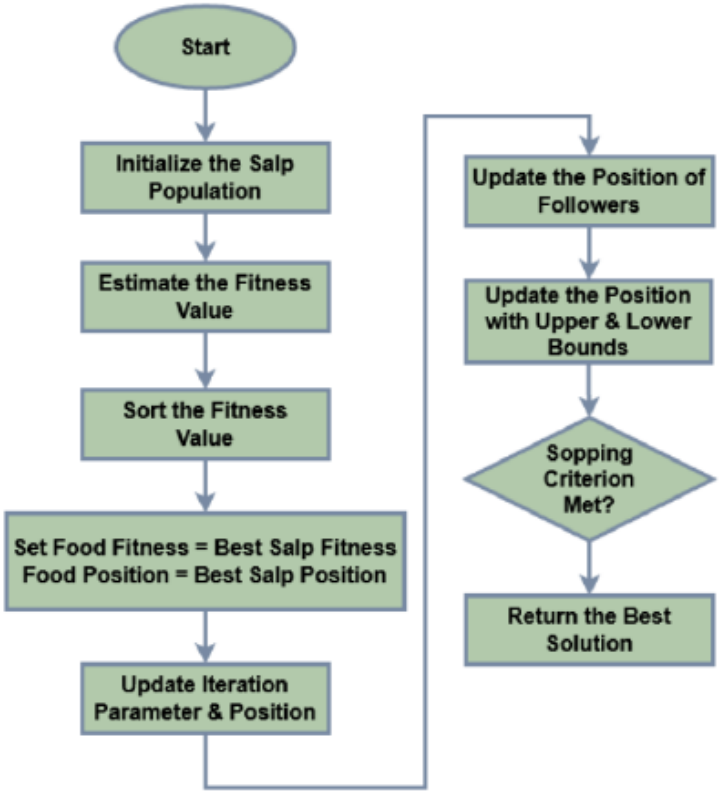

Figure 3. Flow of the CSSO algorithm.

3.3. Deep reinforced neural network (DRNN)

After feature optimization, the DRNN classification technique is deployed to predict the intrusion based on the optimized set of features. It integrfls the operations of two restricted Boltzmann machine and multi-layer perceptron models, which helps to obtain an increased detection accuracy with reduced computational time and complexity. In au existing works, various machine learning based classification techniques[34 - 40] are used for detecting and categorizing the types of intrusions in the mobile cloud networking. it limits with the disadvantages of reduced detection accuracy, high false positives, and error rate. lire fore, the current suggested paper used a new and intelligent deep learning mechanism for detecting and categorizing the intrusions from the "mobile cloud systems". In the current design the optimal features are passed to the input of classifier and its hidden layers are represented as shown in below:

$$H^1 = \{h^1_1, h^1_2 \ldots.\} \tag{10}$$

4. Conclusion

This paper presents a computational efficient CSSO-DRNN based IDS frame work for protecting the mobile cloud systems from the cyber-threats. The original contribution of this work is to omplement a simple and efficient algorithm for developing an IDS architecture for strengthening the security of mobile clou systems. For system implementation and validation. The most popular cyber-threat datasets are ytuuzed ub this work. At first, quality improved dataset is generated by using an InCon filtering technique, which normalizes the attributes of information to preprocess the dataset. After that, a CSSO algorithm is deployed to select the relevant features correlated to the different types of network intrusion. It also helps to simplify theprocess of intrusion prediction and categorization by providing the best optimal function. Moreover, the DRNN technique is testing the samples of data. Simple to design computationally efficient

increased converagence rate high accuracy reduced error rate. High accuracy, reduced error rte and minimal time cost. In addition to that, the results of the proposed security approach are evaluated and compared by using various parameters. Finally the estimated values re compared with the existing optimization and classificataion algorithms based on the different types of intrusions in the dataset. In future this work canbe extended by implementing a new machine learning techniques for increasing the security of integrated networking paradigms.

Author contributions

Conceptualization, OIK and DA; methodology, OIK and GMA; formal analysis, OIK; funding acquisition, software, validation, DA; writing—review & editing, investigation, GMA and GRC. All authors have read and agreed to the published version of the manuscript.

Conflict of interest

The authors declare no conflict of interest.

References

1. Anand D, Khalaf OI, Abdulsahib GM, et al. Identification of meningioma tumor using recurrent neural networks. Journal of Autonomous Intelligence. 2023, 7(2). doi: 10.32629/jai.v7i2.653
2. SatheeshKumar Palanisamy et al. Design of Artificial Magnetic Conductor based Stepped V-shaped Printed multiband antenna for Wireless Applications. Int. J. Advance Soft Compu. Appl, 15(3). doi: 10.15849/IJASCA.231130.07
3. Ghaida Muttashar Abdulsahib et al. A Modified Bandwidth Prediction Algorithm for Wireless Sensor Networks. Journal of Information Science and Engineering, 40(1): 177-188.
4. Al-Janabi S, Al-Shourbaji I, Shojafar M, Abdelhag M. Mobile cloud computing: Challenges and future research directions. In: Proceedings of the 10th International Conference on Developments in eSystems Engineering (DeSE); 14–16 June 2017; Paris, France. pp. 62–67.
5. Wiriaatmadja DT, Choi KW, Hossain E. Discovering mobile applications in cellular device-to-device communications: Hash function and bloom filter-based approach. IEEE Transactions on Mobile Computing 2016; 15(2): 336–349. doi: 10.1109/TMC.2015.2418767
6. Tsai JL, Lo NW. A privacy-aware authentication scheme for distributed mobile cloud computing services. IEEE Systems Journal 2015; 9(3): 805–815. doi: 10.1109/JSYST.2014.2322973
7. Chu CH, Wang P, Wang D, He D. Anonymous two-factor authentication of distributed systems: Attainments are beyond certain goals are beyond attainment. IEEE Transactions on Dependable and Secure Computing 2015; 12(4): 428–442. doi: 10.1109/TDSC.2014.2355850
8. Xingsi Xue et al. Soft computing approach on estimating the lateral confinement coefficient of CFRP veiled circular columns. Alexandria Engineering Journal, 81: 599-619. doi: 10.1016/j.aej.2023.09.053
9. Lei L, Sengupta S, Pattanaik T, Gao J. MCloudDB: A mobile cloud database service framework. In: Proceedings of the 3rd IEEE International Conference on Mobile Cloud Computing, Services, and Engineering; 30 March–3 April 2015; San Francisco, USA. pp. 6–15.
10. Alqahtani HS, Kouadri-Mostefaou G. Multi-clouds mobile computing for the secure storage of data. In: Proceedings of the 2014 IEEE/ACM 7th International Conference on Utility and Cloud Computing; 8–11 December 2014; London, United Kingdom. pp. 495–496.
11. Imgraben J, Engelbrecht A, Choo KKR. Always connected, but are smart mobile users getting more security savvy? A survey of smart mobile device users. Behaviour & Information Technology 2014; 33(12): 1347–1360. doi: 10.1080/0144929X.2014.934286
12. Almenares F, Sanchez R, Marin A, et al. Enhancing privacy and dynamic federation in IdM for consumer cloud computing. IEEE Transactions on Consumer Electronics 2012; 58(1): 95–103. doi: 10.1109/TCE.2012.6170060
13. Xiang Y, Chonka A, Huang X, et al. A generic framework for three-factor authentication: Preserving security and privacy in distributed systems. IEEE Transactions on Parallel and Distributed Systems 2011; 22(8): 1390–1397. doi: 10.1109/TPDS.2010.206
14. Hwang MS, Li LH, Lin LC. A remote password authentication scheme for multi-server architecture using neural networks. IEEE Transactions on Neural Network 2001; 12(6): 1498–1504. doi: 10.1109/72.963786
15. Li LH, Hwang MS. A new remote user authentication scheme using smart cards. IEEE Transactions on Consumer Electronics 2000; 46(1): 28–30.

16. Yang S, Kwon Y, Cho Y, et al. Fast dynamic execution offloading for efficient mobile cloud computing. In: Proceedings of the International Conference on Pervasive Computing and Communications (PerCom); 18–22 March 2013; San Diego, USA.
17. Jararweh Y, Doulat A, AlQudah O, et al. The future of mobile cloud computing: Integrating cloudlets and mobile edge computing. In: Proceedings of the 23rd International Conference on Telecommunications (ICT); 16–18 May 2016; Thessaloniki, Greece.
18. Xue X, Palanisamy S, et al. A Novel partial sequence technique based Chaotic biogeography optimization for PAPR reduction in eneralized frequency division multiplexing waveform. Heliyon 2023; 9(9). doi: 10.1016/j.heliyon.2023.e19451
19. Al-Hamami AH, AL-Juneidi JY. Secure mobile cloud computing based-on fingerprint. World of Computer Science and Information Technology Journal (WCSIT) 2015; 5(2): 23–27.
20. Jia W, Zhu H, Caoyx Z, et al. SDSM: A secure data service mechanism in mobile cloud computing. In: Proceedings of the IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS); 10–15 April 2011.
21. Kumar R, Rajalakshmi S. Mobile cloud computing: Standard approach to protecting and securing of mobile cloud ecosystems. In: Proceedings of the International Conference on Computer Sciences and Applications; 14–15 December 2013; Washington, USA.
22. Qureshi SS, Ahmad T, Rafique K, Islam S. Mobile cloud computing as future for mobile applications-implementation methods and challenging issues. In: Proceedings of the International Conference on Cloud Computing and Intelligence Systems; 15–17 September 2011; Beijing, China.
23. Armel ASR, Thavavel V. Ghost encryption: Mobile data security model encrypting data before moving it to the cloud service provider. In: Proceedings of the Fifth International Conference on Advanced Computing (ICoAC); 18–20 December 2013; Chennai, India.
24. Abolfazli S, Sanaei Z, Shiraz M, Gani A. MOMCC: Market-oriented architecture for Mobile Cloud Computing based on Service Oriented Architecture. In: Proceedings of the International Conference on Communications in China Workshops (ICCC); 15–17 August 2012; Beijing, China.
25. Anne VPK, Rao JV, Kurra RR. Enforcing the security within mobile devices using clouds and its infrastructure. In: Proceedings of the CSI Sixth International Conference on Software Engineering (CONSEG); 5–7 September 2012; Indore, India.
26. Oshamah Ibrahim Khalaf,Ashokkumar. S.R,S.Dhanasekaran,Ghaida Muttashar Abdulsahib and Premkumar. A DECISION SCIENCE APPROACH USING HYBRID EEG FEATURE EXTRACTION AND GAN-BASED EMOTION CLASSIFICATION. Advances in Decision Sciences, 2023,Vol 27.https://doi.org/10.47654/v27y2023i1p172-191. Pages 172-191 .
27. Ragini, Mehrotra P, Venkatesan S. An efficient model for privacy and security in mobile cloud computing. In: Proceedings of the International Conference on Recent Trends in Information Technology; 10–12 April 2014; Chennai, India.
28. Dai Q, Yang H, Yao Q, Chen Y. An improved security service scheme in mobile cloud environment. In: Proceedings of the 2nd International Conference on Cloud Computing and Intelligence Systems; 30 October–1 November 2012; Hangzhou, China.
29. S. Sadesh, O. I. Khalaf, M. Shorfuzzaman, et al. Automatic clustering of user behaviour profiles for web recommendation system. Intelligent Automation & Soft Computing 2023; 35(3): 3365–3384. doi: 10.32604/iasc.2023.030751
30. Cremene M, Borda M, Boudaoud K. Popa D. A security framework for mobile cloud applications. In: Proceedings of the 11th RoEduNet International Conference (RoEduNet);17–19 January 2013; Sinaia, Romania.
31. Sajid, M., Kumar Sagar, A., Singh, J., Khalaf, O.I., & Prasad, M. (Eds.). (2023). Intelligent Techniques for Cyber-Physical Systems (1st ed.). CRC Press; 2023. doi: 10.1201/9781003438588
32. Zhou G, Tian W, Buyya R. Deep reinforcement learning-based methods for resource scheduling in cloud computing: A review and future directions. Available online: https://arxiv.org/pdf/2105.04086.pdf (accessed on 21 August 2023).
33. Anand D, Arulselvi G, Balaji GN, Chandra GR. A deep convolutional extreme machine learning classification method to detect bone cancer from histopathological images. International Journal of Intelligent Systems and Applications in Engineering 2022; 10(4): 39–47.
34. Anand D, Arulselvi G, Balaji GN. Detection of tumor affected part from histopathological bone images using morphological classification and recurrent convoluted neural networks. Journal of Pharmaceutical Negative Results 2022; 13(9): 4992–5008. doi: 10.47750/pnr.2022.13.S09.617
35. Anand D, Arulselvi G, Balaji GN. An assessment on bone cancer detection using various techniques in image processing. In: Editor Deepak BBVL, Editor Parhi D, Editor Biswal B, et al. (editors). Applications of Computational Methods in Manufacturing and Product Design. Springer; 2022.
36. Xue X, Poonia M, Abdulsahib GM, et al. On cohesive fuzzy sets, operations and properties with applications in electromagnetic signals and solar activities. Symmetry 2023; 15(3): 595. doi: 10.3390/sym15030595

37. Dash S, Parida P, Sahu G, et al. Artificial intelligence models for blockchain-based intelligent networks systems: Concepts, methodologies, tools, and applications. In: Handbook of Research on Quantum Computing for Smart Environments. IGI Global; 2023.
38. Xue X, Marappan R, Raju SK, et al. Modelling and analysis of hybrid transformation for lossless big medical image compression. Bioengineering 2023; 10(3): 333. doi: 10.3390/bioengineering10030333
39. Xue X, Chinnaperumal S, Abdulsahib GM, et al. Design and analysis of a deep learning ensemble framework model for the detection of COVID-19 and pneumonia using large-scale CT scan and x-ray image datasets. Bioengineering 2023; 10(3): 363. doi: 10.3390/bioengineering10030363
40. Xue X, Shanmugam R, Palanisamy S, et al. A hybrid cross layer with harris-hawk-optimization-based efficient routing for wireless sensor networks. Symmetry 2023; 15(2): 438. doi: 10.3390/sym15020438