Applied Mathematics & Information Sciences
An International Journal

http://dx.doi.org/10.18576/amis/160411

Intrusion Detection System in Cloud Security using Deep Convolutional Network

P. Varun [*] *and K. Ashokkumar*

Sathyabama Institute of Science and Technology, Department of Computer Science and Engineering, Chennai, India

Received: 2 Mar. 2022, Revised: 12 May 2022, Accepted: 17 Jun. 2022
Published online: 1 Jul. 2022

Abstract: When it comes to data processing, sharing, and storage, cloud computing is the industry standard. Due to the frequent attacks, it faced a number of security issues. The existence of diverse attack environments makes these security concerns worse. Intrusion Detection System is one of the traditional security measures used in cloud computing (IDS). But for the IDS system to improve cloud security, an effective security model is needed. a Deep Neural Network with Game Theory for Cloud Security is proposed in this paper (GT-CSDNN). The suggested model covers both attacker and defender methods while using the game theory approach.Additionally, the DNN network uses the proposed game theory model to classify attack and regular data. With the use of the CICIDS - 2017 dataset, the suggested GT-performance CSDNN's is assessed. The gathered data is normalised, and the improved whale algorithm is used to evaluate the best points regarding the normal and attack data (IWA). The networking layer of the model includes the proposed GT-CSDNN. According to the simulation findings, the suggested GT-CSDNN performs better than the current method in terms of accuracy, precision, F-Score, AUC, FPR, and detection rate.

Keywords: Optimization, CICIDS - 2017 dataset, Cloud Computing, game theory, Deep Neural Network

1 Introduction

Cloud computing provides a vast range of services for digital business evolution. It provides significant speed, elasticity, scalability, robustness, cost-effective for both users and enterprises [1]. The cloud exhibits significant advantages rather than educational institutions, medical fields, industries, banking sectors, Internet of Things (IoT), Fog-as-a-services, etc. The cloud efficiently manages the burst and heterogeneous data [2]. The cloud acts effectively between middle-ware of devices and end-users within IoT architecture. In the cloud, security is a major concern this incorporates consumption of power, product-life, and overall efficiency [3]. Some of the cloud devices which can be accessed and vulnerable to public places are CCTV cameras, social media, and so on. The cloud application comprises the number of devices due to weak authentication scheme with a Brute Force attack.

The cloud device is vulnerable to several attacks due to continuous data transmission and reception. This leads to a higher threat to cloud servers and resources. In cloud network IDS is incorporated for traffic monitoring and detection of malicious activities [4]. The conventional IDS system incorporates a signature-based anomaly detection scheme. To block malicious data in the network attacker tries to get access to false data. To achieve efficient defense mechanism intelligent systems are incorporated for regulating network traffic [5] [6]. To achieve efficient IDS game theory concept is observed as an intelligent monitor for network traffic. For the prediction of malicious nodes, game theory estimates the defender strategies with updated probability values. Finally, the in-game theory is delineated efficiently through the incorporation of the Nash equilibrium [7] [8].

Usually, attackers of a network focused on the processing layer in which cloud operation is comprised and processed. If the attacker effectively invades security in the cloud, the cloud service provider does not provide appropriate services to the end-user [9]. The top security concern in the cloud is data breaches, account hijacking, injection of malware, insider threat, data loss, and Application Programming Interface (APIs) [10]. In day by day manner bot, army for cloud security is increasing day by day. The malware injected within the cloud is transmitted within the cloud server and existing data is corrupted by this process. This leads to the demand for the development of a robust and secure framework for

[*] Corresponding author e-mail: varunprabhakaran@gmail.com

cloud security. Hence, cloud security is considered as a major performance indicator for reliable data transmission [11].

Here, to improve the security in the cloud IDS system developed a framework stated as GT-CSDNN. The proposed model incorporates an attacker and a defender mechanism for attack and normal data processing. The developed game theory is implemented in the DNN model with IWA for the identification of optimal solutions. The estimation is based on the identification of minimal and maximal optimal points in the dataset. The proposed GT-CSDNN model is evaluated for CICIDS -2017 dataset. The performance of the proposed GT-CSDNN is evaluated with the existing technique is performed. The simulation analysis exhibited that the proposed GT-CSDNN exhibits improved performance in terms of accuracy, detection rate, precision, F-Score, AUC, and FPR.

The paper is organized as follows: in section, II presented existing related works related to cloud security. In section III presented about game theory model for the cloud security network. In section IV illustrated about normalization approach designed with an optimization model. Finally, in section V presented results and comparative analysis of the proposed approach with existing techniques and followed by a conclusion in section VI.

2 Related Works

This section presented about cloud security applications developed are presented as follows:

In [12], the adopted Markov chain model with game theory is designed for malware detection and offloading in the cloud environment. Also, the post-learning scheme is incorporated for improving the learning mechanism of the system. [13] presented a review of the security mechanism in a multi-agent system based on applications. Through analysis of the review, it is delineated that cross-layer optimization is considered as an effective mechanism with a context-aware mechanism. In [14], developed a security mechanism based on the evaluation of the trust factor with a self-learning scheme. Also, a game-theoretical based approach is adopted for effective defense strategy in the cloud application. In this, the game model act as Petri-nets to examine the behavior of attacker and defender for stochastic applications. To identify possible attack paths enforcement algorithm is evolved based on the examined path of the attacker.

In [15]] presented a GT-QoSec optimization model with gradient boosting for a heterogeneous network environment. The proposed model incorporates game theory for load balancing and security in the cloud. The cloud metrics are evaluated based on the estimation of Nash Equilibrium (NE) with consideration of the expected number of steps in the cloud. Also, [16] developed a differential game model for cloud computing with consideration of IDS optimal strategies. The proposed model is based on the theoretical formulation of game theory in the IDS cloud system. In [17], constructed an authentication framework based on game theory for sensor -cloud communication. This incorporates trust value for further authentication and security improvement in the cloud network. The analysis of results expressed that the proposed scheme exhibits improved security in-network and devices. In [18] presented a Particle Swarm - Support Vector Machine (PSO -SVM) framework for a secure identity-based aggregation scheme for secret key management. The analysis of results expressed that the proposed scheme offers a feasible and efficient solution for cloud security. To achieve cyber system attacks, [19] developed a commutative prospect theory based on the Particle Swarm Optimization game theory model for attack detection with the adoption of a Q-learning strategy. The author [20] suggested the fuzzy c-means game model effectively increases the malicious activity detection rate. The game model increased the detection rate of 92% and a latency value of 25% with reduced power consumption and a false-positive rate. To examine the data center vulnerability in [21] proposed a cuckoo optimization, game-theoretical model. The analysis of results expressed that the proposed IDS increases cloud security. The developed model increases the defender scheme for attacker scenario. Through a review of literature, it is observed that most of the works concentrated on single defender mechanism

3 The proposed attacker - defender GT-CSDNN framework for cloud security

This research proposed a Game Theory - Cloud Security Deep Neural Network (GT-CSDNN) model for security improvement in the cloud. The proposed model is constructed based on the consideration of different attacks in the cloud. The attack model considered for analysis are presented in figure 1.

The deployment architecture model for cloud security for proposed GT-CSDNN is based on the consideration of the attacker scenario. The model for incorporated for security enhancement in the cloud is based on the architecture presented in figure 2.

The proposed GT-CSDNN architecture components are placed as per figure 2 illustrated. Within the constructed architecture, the proposed GT-CSDNN performance is estimated based on the type of players. The proposed model is involved in the classification of players as cooperative and non-cooperative games. In the case of cooperative games, players on both sides have similar goals and strategies for achieving security in the cloud. In the case of non-cooperative games, the goal of one player is different and opposite to other player strategies for achieving a maximal gain. The proposed

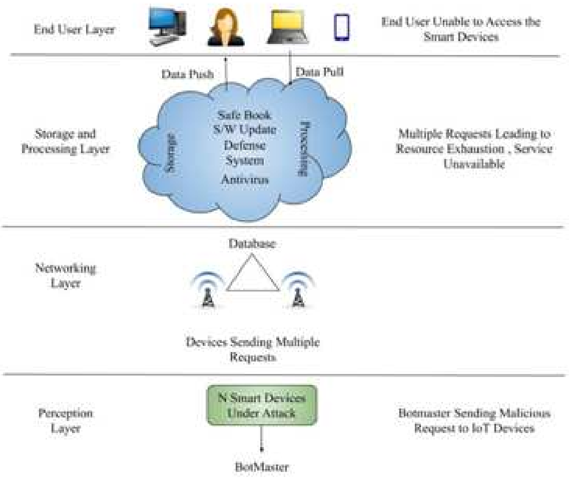
End User Layer
End User Unable to Access the Smart Devices
Data Push
Data Pull
Safe Book
S/W Update
Defense System
Antivirus
Storage
Processing
Storage and Processing Layer
Multiple Requests Leading to Resource Exhaustion , Service Unavailable
Database
Networking Layer
Devices Sending Multiple Requests
N Smart Devices Under Attack
Perception Layer
Botmaster Sending Malicious Request to IoT Devices
BotMaster

Fig. 1: Attack Scenario in Cloud

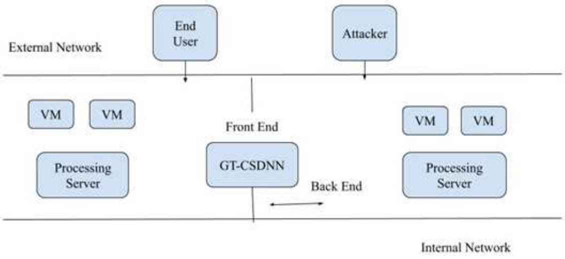

Fig. 2: Position of GT-CSDNN Cloud Network

GT-SCDNN main components re Defender (D) and Attacker (A). To state the problem, non-cooperative game attackers and defenders complete each other. The non-cooperative game model (G) is mathematically stated using the following equation (1) presented as follows:

$$G = \{(D,A)(S_D,S_A)(U_D,U_A)\} \tag{1}$$

In the above equation, the strategies of defender and attacker are represented as *SD* and *SA*. The defender and attacker payoff function is represented as U_D and *UA* respectively. The estimation of the player strategy developed model is incorporated in the Deep Neural Network (DNN) with an optimization algorithm. The entire designed model is incorporated into two modules of IDS such as Signature Detection (*SD*) and Anomaly Detection (*AD*) module.

The strategies of the defender and corresponding attacks are stored in the database for processing. The *SD* evaluates the database and provides efficient and fast results for securing data. On other hand, *AD* estimates the unknown and sophisticated attacks. The attacks in *AD* evaluate the deviation in incoming traffic or packet behavior with the provision of positive signal value for the attack. The attacker trap the network resides on the network with the estimation of dummy data. After the detection system, traffic is legitimate within the secure cloud. The attacker and defender strategies are represented as $SD = \{SD1, SD2, SD3\}$. In table 1 strategies of defender are presented.

Table 1: Defender Strategies

Representation	Strategy
SD1	MonitorIDS Signature
SD2	MonitorIDS anomaly
SD3	Monitor IDS signature

The maximum payoff attacker attacks are denoted as $SA = \{SA1, SA2, SA3\}$. In table 2 representation and strategies of attacks are presented.

Table 2: Attacker Strategies

Representation	Strategy
SA1	Cloud server with attacks
SA2	Waiting time period (t)
SA3	Cloud with new sophisticated attacks

4 Framework of O Proposed GT-CSDNN with optimization

This section presented about framework designed for analysis of security attacks in the cloud with proposed GT-CSDNN. In section 3 presented about game theory model for cloud security. The developed model is implemented in DNN with optimization for the prevention of attacks in the cloud. In figure 3 overall processing architecture of the proposed model framework is presented.

The analysis of collected data is based on the examination of the CICIDS-2017 dataset. The proposed GT-CSDNN optimizes the data through an improved whale optimization Algorithm (IWA). Through the optimization approach the points involved in the identification of optimal values of parameters to construct in IDS for normal operation. In figure 4, the defined framework for optimization of the CICIDS - 2019 data set is presented.

The proposed GT-CSDNN estimate the features in intrusion detection modules with the incorporation of a selection of features. This involved in the selection of 70 relevant features forms the 80 features in CICIDS - 2017 dataset. The data preprocessing model includes two operations such as data conversion and normalization. The CICIDS features and attributes are estimated based

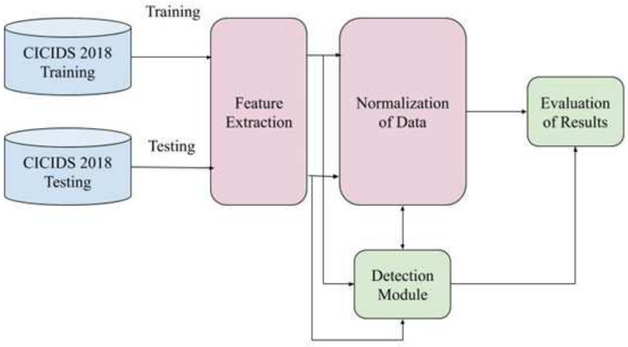

Fig. 3: Overall Function of Proposed GT-CSDNN

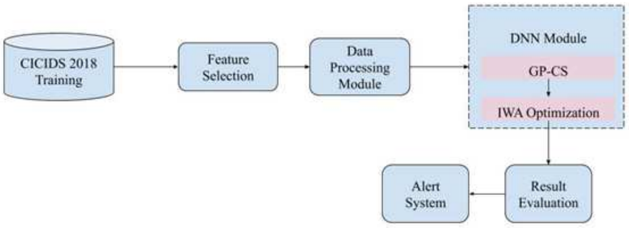

Fig. 4: GT-CSDNN Framework Architecture

on the assigned numeric values for reducing complexity in processing. To retain effective and detection processes with appropriate scaling and feature values Normalization are performed for calculation of numerical difficulties. The data processing involved in the normalization of min-max values through statistical normalization of data values.

The attack detection module with DNN includes optimization model IWA for the identification of near-optimal values in the IDS system of the cloud. The process performed for optimization is defined as the "optimization stage" for concluding the IWA process. The optimal values in the IDS-based DNN are estimated based on the estimation of optimal values. Through IDS based DNN optimization phases and optimal parameters are estimated using the proposed GT-CSDNN operates in normal mode. To predict the attack class CICIDS 2017 estimate the normal and attacks packet in the network. Finally, the alert system determines the optimized values and detect the attack in the cloud administrator. The algorithm defined for proposed for GT-CSDNN model is presented as follows:

Algorithm 1: GT-CSDNN Algorithm

```
Estimate the attacker and defender mechanism
Initialize the whales population $X_i$ ($i = 1, 2, ..., n$)
Calculate the fitness of each search agent
$X^*$=the best search agent
while ($t <$ maximum number of iterations)
    for each search agent
    Update a, A, C, l, and p
        if1 ($p<0.5$)
        if2 ($|A| < 1$)
            Update the position of the current search agent
        else if2 ($|A|>1$)
            Select a random search agent (Xrand)
            Update the position of the current search agent
    end if2
  else if1 (p 0.5)
        Update the position of the current search
end if1
end for
    Check if any search agent goes beyond the
search space and amend it
  Calculate the fitness of each search agent
  Update $X^*$ if there is a better solution
$t=t+1$
end while
return $X^*$
```

5 Results and discussion

To verify and validate the proposed GT-CSDNN model simulation is conducted in MATLAB. The proposed GT-CSDNN is estimated based on the consideration of payoff function and strategies. The defender detection rate is in the range of 0 - 0.99 also, the defender gain is stet as -5,0 and 5. The payer either win or loss is considered as -5 or win, else the player retain 5 or remain at rest state it receives 0 without gain. Otherwise, the defender does not have any points to achieve data in CICIDS - 2017 dataset. The simulation is conducted for 120 seconds with consideration of both players compete with each other. The simulation metrics considered for analysis of proposed GT-CSDNN is presented as follows:

The performance of the proposed GT-CSDNN is evaluated based on metrics, such as accuracy, precision, F-score, Detection rate, FPR and AUC.

Accuracy: Accuracy determines the closeness of the detection made by the classifier as represented in equation (2).

$$Accuracy = \frac{TP+TN}{TP+FP+FN+TN} \tag{2}$$

where, TP signifies true positive, TN refers to true negative, FN states the false negative, and FP refers to false positive

Precision: It measures the positive samples identified correctly by the proposed GT-CSDNN represented in equation (3).

$$Precision = \frac{TP}{TP+FP} \tag{3}$$

FPR: It measures the negative samples correctly rejected by the proposed GT-CSDNN stated in equation (4).

$$FPR = \frac{FP}{FP+TN} \tag{4}$$

F-Score: It provides the average score value measured for precision and recall value and it is defined in equation (5) as follows:

$$F-Score = \frac{2 \times Recall \times Precision}{Recall + Precision} \tag{5}$$

Detection Rate (DR): It provides the positive data that is classified effectively for the total positive and negative values as stated in equation (6)

$$DR = \frac{TP}{TP+FN} \tag{6}$$

AUC: The AUC value of proposed GT-CSDNN is computed using the equation (7) as follows:

$$AUC = 0.5 \times \left(\frac{TP}{TP+FN} + \frac{TN}{TN+FP}\right) \tag{7}$$

The parameters estimated for classification of attacks in the cloud system is calculated based on the confusion matrix. In table 3 configuration parameters defined for proposed GT-CSDNN is stated.

The proposed GT-CSDNN exhibits effective defense scheme for attacker. The defender payoff is effective with improved performance which prevent attack in the network. In figure 5 without defender scheme of optimization payoff of attacker is high. In figure 6 illustrated the attacker and defender scheme for GT-CSDNN is presented.

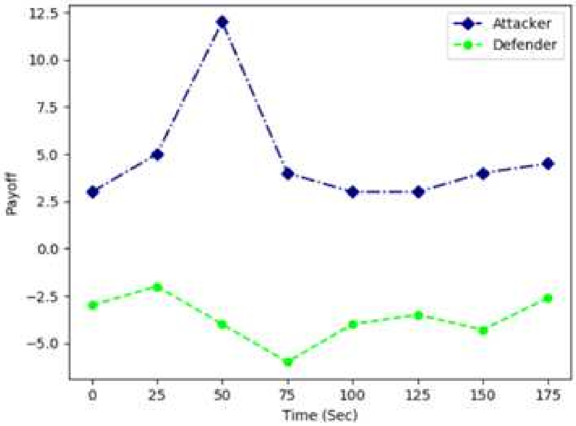

Fig. 5: Payoff of attacker and defender without GT-CSDNN

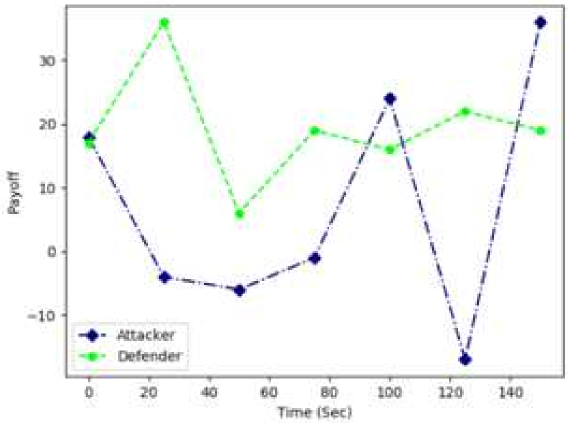

Fig. 6: Payoff of attacker and defender with GT-CSDNN

The analysis of Figures 5 and 6 demonstrated that the implemented GT_CSDNN mechanism improves the defender payoff with a reduction of attacker payoff. In the absence of the GT-CSDNN mechanism payoff of the attacker. In presence of the proposed GT-CSDNN payoff of the defender is higher than the attacker payoff. The comparative analysis of performance metrics of proposed

Table 3: Configuration of GT-CSDNN

Parameter Configuration	Values	Performance Metrics
Input Layer	70	Accuracy
Hidden Layer - 1	53	Precision
Hidden Layer - 2	27	Detection Rate (DR)
Output Layer	1	False Negative Rate (FNR)
Activation Function	Sigmoid	False Positive Rate (FPR)
Data Normalization	Min-Max	True Negative Rate (TNR)
Learning Rate	8.412874497406361E-7	F-score
Momentum term	1.264876945375064E-4	AUC - Ability to avoid misclassifications

Table 4: Distribution of CICIDS - 2017 dataset

	Data Distribution	Count
Training Set	Normal activity	67,343
	Anomaly	58,630
	DoS	45,927
	Probe Attack	11,656
	U2R (User to Root) Attack	52
	R2L (Root to Local)	995
Testing Set	Normal activity	9,710
	Anomaly	12,834
	DoS	7,458
	Probe Attack	2,422
	U2R (User to Root) Attack	67
	R2L (Root to Local)	2,887

GT-CSDNN with existing techniques are presented in Table 5.

In figure 7 detection rate measurement for proposed GT-CSDNN with existing technique is presented. The comparative analysis exhibited that proposed framework exhibits improved performance compared with existing technique.

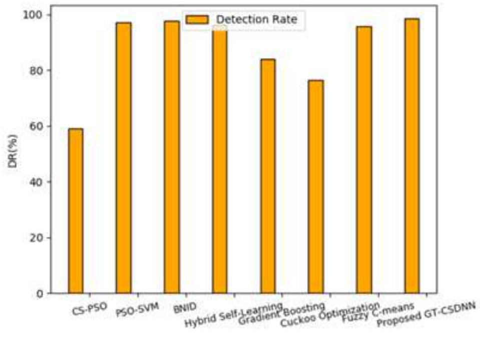

Fig. 7: Comparison of Detection Rate

The detection rate of proposed GT-CSDNN is significantly higher than the existing technique, this implies that proposed technique exhibits improved performance. In figure 8 accuracy measurement of proposed GT-CSDNN with exiting technique is presented.

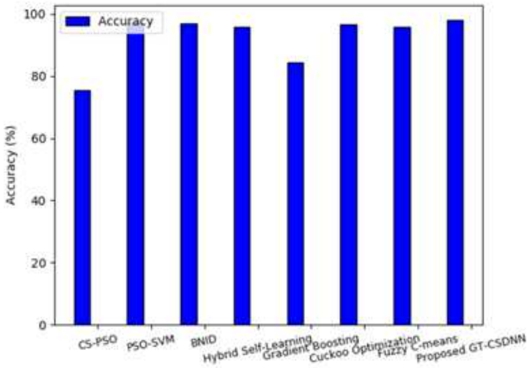

Fig. 8: Comparison of Accuracy

6 Conclusion

To adopt secure cloud communication with consideration of cloud security, this paper presented as the GT-CSDNN framework. The analysis is based on the estimation of defender and attacker strategies. The analysis is conducted for the CICIDS-2017 dataset with an estimation of features in the data. The proposed GT-CSDNN performs optimization of the CICIDS - 2017 dataset for accurate classification of normal and attack data. The proposed GT-CSDNN model is implemented using MATLAB simulation software. The simulation analysis exhibited that the proposed GT-CSDNN framework exhibits higher accuracy, detection rate, precision, and AUC. In the future, the proposed model can be implemented in real-time application scenario.

Table 5: Comparison of Metrics

Method	**Precision**	**FPR**	**Accuracy**	**Detection Rate (DR)**	**F-Score**	**AUC**
CS-PSO [19]	94.46	2.87	75.51	59.16	0.73	78.14
PSO-SVM [18]	97.83	0.87	97.10	97.08	0.97	97.10
BNID [16]	-	1.517	96.78	97.73	-	96.32
Hybrid Self-Learning [14]	96.45	1.02	95.67	96.23	-	-
Gradient Boosting [15]	87.116	-	84.253	83.87	0.83	-
Cuckoo Optimization [21]	95.23	0.56	96.53	76.50	0.8484	87.97
Fuzzy C-means [20]	97.34	1.67	95.68	95.67	-	-
Proposed GT-CSDNN	98.65	0.06	97.96	98.47	0.99	98.67

Conflict of Interest

The authors declare that they have no conflict of interest.

References

[1] Z. Wang, N. Wang, X. Su and S. Ge, An empirical study on business analytics affordances enhancing the management of cloud computing data security, *International Journal of Information Management*, **50**, 387-394, (2020).

[2] V. Prabhakaran and A. Kulandasamy, Integration of recurrent convolutional neural network and optimal encryption scheme for intrusion detection with secure data storage in the cloud, *Wiley, Computational Intelligence*, **37**, 344-370, (2021).

[3] L. Rajabion, A.A. Shaltooki, M. Taghikhah, A. Ghasemi and A. Badfar, Healthcare big data processing mechanisms: the role of cloud computing, *International Journal of Information Management*, **49**, 271-289, (2019).

[4] V. Prabhakaran and A. Kulandasamy, Hybrid sementic deep learning architecture and optimal advanced encryption standard key management scheme for secure cloud storage and intrusion detection, *Springer, NeuralComputing and Applications*, **33**, 14459-14479, (2021).

[5] N. Manikandan, S. Devayani and M. Divya, Domain-Specific Allocation & Load Balancing in Cloud Computing Using Virtual Machines, *4^{th} International Conference on Trends in Electronics and Informatics (ICOEI)(48184)*, 467-472, (2020).

[6] Z. Wang, N. Wang, X. Su and S. Ge, An empirical study on business analytics affordances enhancing the management of cloud computing data security, *International Journal of Information Management*, **50**, 387-394, (2020).

[7] S. Hosseini and R. Vakili, Game theory approach for detecting vulnerable data centers in cloud computing network, *International Journal of Communication Systems*, **32**(8), (2019).

[8] S. Kumar and G.K. Saha, Cloud Computing Security Threats and Attack Detection Issues, *International Journal of Applied Research on Information Technology and Computing*, **10**(1), 38-42, (2019).

[9] O.J. Nisha and S.M.S. Bhanu, Detection of malware applications using social spider algorithm in mobile cloud computing environment, *International Journal of Ad Hoc and Ubiquitous Computing*, **34**(3), 154-169, (2020).

[10] V. Patel, S. Choe and T. Halabi, Predicting Future Malware Attacks on Cloud Systems using Machine Learning, *IEEE 6^{th} Intl Conference on Big Data Security on Cloud (BigDataSecurity), IEEE Intl Conference on High Performance and Smart Computing,(HPSC) and IEEE Intl Conference on Intelligent Data and Security (IDS)*, 151-156, (2020).

[11] N. C. Xiao, H. Zhan and K. Yuan, A new reliability method for small failure probability problems by combining the adaptive importance sampling and surrogate models, *Computer Methods in Applied Mechanics and Engineering*, 113-336, (2020).

[12] K. S. Gill, S. Saxena and A. Sharma, GTM-CSec: Game theoretic model for cloud security based on IDS and honeypot, *Computers & Security*, **92**, 101-732, (2020).

[13] Y. Fan, X. Lin, G. Tan, Y. Zhang, W. Dong and J. Lei, One secure data integrity verification scheme for cloud storage, *Future Generation Computer Systems*, **96**, 376-385, (2019).

[14] B. Mao, Y. Kawamoto and N. Kato, AI-based joint optimization of QoS and security for 6G energy harvesting internet of things, *IEEE Internet of Things Journal*, (2020).

[15] K. Jiang, R. Merrill, D. You, P. Pan and Z. Li, Optimal control for transboundary pollution under ecological compensation: A stochastic differential game approach, *Journal of Cleaner Production*, **241**, 118-391, (2019).

[16] A.A. Khan, V. Kumar and M. Ahmad, An elliptic curve cryptography based mutual authentication scheme for smart grid communications using biometric approach, *Journal of King Saud University-Computer and Information Sciences*, (2019).

[17] M.A. Khan, I. Ullah, S. Nisar, F. Noor, I.M. Qureshi, F. Khanzada and M.A. Aziz, Multiaccess Edge Computing Empowered Flying Ad Hoc Networks with Secure Deployment Using Identity-Based Generalized Signcryption, *Mobile Information Systems*, (2020).

[18] Y. Li, F. Li, S. Yang, H. Chen, Q. Zhang, Y. Wu and Y. Wang, PTASIM: Incentivizing Crowdsensing With POI-Tagging Cooperation Over Edge Clouds, *IEEE Transactions on Industrial Informatics*, **16**(7), 4823-4831, (2019).

[19] A. Hammoud, A. Mourad, H. Otrok, O.A. Wahab and H. Harmanani, Cloud federation formation using genetic and

evolutionary game theoretical models, *Future Generation Computer Systems*, **104**, 92-104, (2020).

[20] Y. Chen, L. Duan and W. Zhang, Effect of User Involvement in Supply Chain Cloud Innovation: A Game Theoretical Model and Analysis, *Journal of Global Information Management (JGIM)*, **28**(1), 23-38, (2020).

Prabhakaran Varun obtained his Bachelor's degree in Information Technology from EVP Engineering College, Anna University, Chennai, Tamilnadu, India in 2002. Then he obtained his Master's degree in Information Technology in Sathyabama University Chennai, Tamilnadu, India in 2012 and pursuing Ph.D in the field of Cloud Computing Security in Sathyabama Institute of Science and Technology. Currently, he is an Assistant Professor in Department of Computer Science and Engineering at St.Joseph's College of Engineering. His spe-cializations include Networking, Software Engineering. His current research interests in Cloud Security.

Kulandasamy Ashokumar received his Masters's Degree in Computer Technology -Applied Science and Engineering from KSR college of Technology, Thiruchengode, Namakkal, Tamilnadu, India in 2002 and Master's Degree in Computer Science and Engineering from Sathyabama University, Chennai, Tamilnadu, India in 2005 and Ph.D from Sathyabama University, Chennai, Tamilnadu, India in 2016. He is currently an Associate Professor in the Department of Computer Science & Engineering in Sathyabama Institute of Science & Technology. His research interests are in Grid Computing, Cloud Computing, Data Analytics and Web Services. Dr. K.Ashokkumar is an editor in NCABC 2019 for special Issue and Reviewer in Computers and Electronics in Agriculture(Elsevier), Journal of Computer Science, Journal Of Agricultural Science and Technology. He is a Life member of Indian Society for Tech-nical Education.He has published more than 60+ research papers in reputed journals and conference proceedings. He is presently teaching a wide variety of courses at both under-graduate and postgraduate levels and has 16 years of teaching experience. He has guided more than 25 Undergraduate and Postgraduate students' projects and 5 Ph.D research scholars till date.