Bacterial Foraging Optimization For Enhancing The Security In Intrusion Detection System

S. KALAIVANI, GOPINATH GANAPATHY

Abstract: Most of the currently available Heterogeneous protocols operate on the basis of reliable and secured communication environment. These protocols are vulnerable to modern intruding techniques that include different types of raised attacks. Routing attacks are very tedious because of the dynamic nature of heterogeneous network. Routing as well as member nodes are with different Computational powers. Heterogeneous Network architectures plays a vital role in modern world communication that is virtually all communications and secret resource transactions are widely depending on the heterogeneous network architecture. However, the existing Intrusion detection systems have a number of barriers in system efficiency, flexibility and scalability. Therefore, Bacterial Foraging optimization (BFO) has been concerned to optimize the parameters in the dynamic nature of environment for update itself by its genitival processes. It can afford high security, without exchange of mean value. The BFO ensures high security against attacks and leads best Qos improvement. The Planned work is a new effort to improve the existing security of the heterogeneous network routing protocols, using Bacterial Foraging Optimization against different types of attacks and it can be most useful in secured Cloud computing.

Keywords: Cloud Computing, Intrusion detection system, Bacterial Foraging optimization, heterogeneous network, efficiency, scalability.

1 INTRODUCTION

In current scenario, data centric network services have developed effectively with the growth of intelligent data processing and network power computing [1]. Cloud computing is the emerging technique with enormous number of data centric network applications like medical information system [2-4], data storage [5], data sharing and big data management. Usually, cloud system depends on the architecture of service oriented computing that is proficient to provide identity-as-a-service, anything-as-a-service and database-as-a-service [6-8]. Cloud computing utilize the resources or data for achieving scale of economics and coherence, similar to public utility [9].The users are unable to move their valuable data from the cloud, once the user loses their direct control on data, especially in public cloud with multi-tendency and high consolidation [10]. The ordinary user's rarely accessed data may be neglect to keep or delete by Cloud Service Providers (CSPs) for saving more storage space, which is considered as most severe case [11]. This will leads to Intrusion detection system in cloud computing, where Intrusion detection methods are classified into two general classes such as signature-based detection (misuse detection) and anomaly-based detection. The cloud computing components could be classified to front-end and back-end, according to their locations [12]. The front-end is related to both external and internal network. Placing the network-based detection systems in the front-end of the cloud helps the detection of the attacks and intrusions from the external network. In this way, however, the system may not be able to detect internal intrusions [13-15].

- *S. KALAIVANI Dept. of Computer Science and Engineering, Bharathidasan University, Tiruchirappalli*
- *GOPINATH GANAPATHY Professor, Dept. of Computer Science and Engineering, Bharathidasan University, Tiruchirappalli*

If this attack is identified as a new attack, the new rule of blocking will add this attack to the blacklist of the blocking. The related architecture includes intrusion detection components, warning clustering, threshold check, intrusion response and blocking, and cooperation agents. The intrusion detection module initially removes the attacking packet and then sends the warning messages regarding the detected attack to the other cloud-based areas [16]. The warning clustering module collects the warnings generated by every area. Making decisions about warnings (whether it is generated true or false) is done after calculating the intensity of the collected warnings. In this proposed method, BFO is proposed to detect the attacks in intrusion detection techniques. This method is suitable to protect cloud-based systems against fault occurrence because of its distributed service denial attack mechanism. The Bacterial Foraging Optimization gained popularity in solving optimization problems. Bacterial Foraging Algorithm is based on a computational intelligence technique that is not largely affected by the size and non-problem and has converged to the optimal solution for many problems where the most analytical methods fail to converge and also has its advantages such as less computational burden, global convergence, less computational time requirement and can handle more number of objective function. The remaining paper consists of survey of recent techniques included in Intrusion detection techniques are reviewed in Section 2. The definition of intrusion detection system is represented in Section 3. The explanation of proposed technique is described in Section 4. The validation of proposed technique with other existing technique is presented in Section 5. Finally, the conclusion of the research work with future work is described in Section 6.

2 LITERATURE REVIEW

Numerous methodologies are developed by the researchers in cloud intrusion detection area. In this sub-section, a brief evaluation of a few essential contributions to the existing literature is presented. B. B. Gupta, and Omkar P. Badve., [17] built up a novel solution, where DDoS attack traffic was distinguished in a cloud by utilizing chaos hypothesis. To anticipate the system traffic state, nonlinear time series model [i.e., generalized autoregressive

conditional heteroscedasticity(GARCH) model] was utilized as it caught the Long-Range Dependence (LRD) and long-tail conveyance which was an imperative property of system traffic. The prediction error was determined by utilizing the prediction made by the GARCH model and real traffic design. Filtering was completed with the assistance of backpropagation Artificial Neural Network (ANN) on the traffic that exceeds the certain limit determined by some threshold. The calculation time of the GARCH strategy was extremely high because the technique considered only one group of packets for calculating entropy in the entire dataset. K. Bhushan and B. B. Gupta, [18] examined the constrained flow table-space issue which was an essential restriction of OpenFlow switches in Software Defined Network (SDN). Hence, this restriction was misused by performing flow table over-loading DDoS attacks on the SDN based cloud. Further, this method proposed a novel flow-table sharing approach to protect the SDN-based cloud from flow table over-loading DDoS attacks. This methodology used inactive flow-table of other OpenFlow switches in the system to protect the switch's flow-table from over-loading. This methodology expanded the resistance of the cloud framework against DDoS attacks with minimal contribution of the SDN controller. Therefore, the methodology had low communication overhead. Yet, the method attacked only one switch at a moment and expected that every other switch were not under attack. X. K. Du, et al., [19] examined security gadget organization issue in an SDN based multi-tenant cloud data center environment. The paper proposed a Load-adaptive Traffic Steering and packet sending Scheme called LTSS to rectify the issue. This plan combined the SDN controller with TagOper module to decide the traffic paths with the minimum burden for tenants and enabled them to get their desired security services in SDN-based datacenter systems. The technique additionally assembles a model framework for LTSS to confirm its functionality and evaluated the execution of LTSS structure. A few factors like switch load, security device area, and administration request impact affected the algorithm execution. And furthermore, the LTSS technique leads to poor execution in a larger dataset.T. Ha, et al., [20] proposed a Traffic Sampling (TS) system for SDN that completely used the inspection ability of malicious traffic while maintaining the total volume of the examined traffic below the inspection processing capacity of the Intrusion Detection System (IDS). The TS procedure planned an optimization issue to find an appropriate sampling rate for each switch and tested the traffic streams in the system depends on optimal sampling rates utilizing the SDN functionalities. The experimental outcomes showed that the TS approach essentially improved the inspection execution of malicious traffic in large-sized systems. The time elapses for the TS algorithm exceptionally relied upon the execution of the IDS and Open vSwitch (OVS) switches, and it was additionally decreased in business scale conditions. A. Chowdhary, et al., [21] The technique investigated a game theoretic system according to reward and punishment mechanism which was utilized effectively in game theoretic models. Utilizing a greedy calculation, the method tackled an optimization issue for rate constraining network, data transfer capacity as a punitive mechanism for mischievous players in a dynamic system game. The optimization algorithm utilized in this work, based on Nash Folk hypothesis, permitted to corrupt system transmission capacity gracefully, without applying a static hard limit on system traffic. The experimental work focused on DDoS attacks, specifically ICMP Flood, TCP SYN Flood, UDP Flood. The algorithm had the capacity to manage all attacks dependent on alerts received from the SDN controller. Confinement of this work was the quantity of host subprocess, that the technique can spawn utilizing the multi-processing thread, which was currently constrained to around 500.D. He, et al., [22] have looked into the capacities of SDN that was utilized to create effective traffic anomaly detection strategies, and examined recent advancement toward this direction. However, new difficulties were forced on the design of traffic anomaly techniques. To address these difficulties, this research work proposed refined unsupervised feature selection and density peak clustering calculations, for detecting anomaly of large scale and high-dimensional system information without labels. When a hierarchy of controllers was utilized, this proposed methodology was utilized to investigate traffic information locally in every controller. The intermediate information at that point converged to create the last outcome. This diminished the amount of traffic shuffled over the system. This research work leads to poor execution on real-time packet clustering to defend against interruptions auspicious. Interior clients are the primary causes of anomalous and suspicious behaviours in a communication network. Although conventional security middleboxes are available, interior attacks may lead the system to blackouts or to leakage of sensitive data. Martin Andreoni Lopez, Diogo Menezes FerrazaniMattos, and Otto Carlos MB Duarte, [23] proposed BroFlow, an Intrusion Detection and Prevention System dependent on Bro traffic analyzer and on the worldwide system perspective on the SDN which was given by the OpenFlow. The BroFlow primary contributions were dynamic and flexible resource provision of traffic investigating machines under demand, recognition of DoS attacks through basic calculations implemented in a policy language for system events. The other commitments of proposed were the immediate response to DoS attacks, dropping malicious flows close of their sources, and near-ideal solutions of sensors through a proposed heuristic for strategically positioning sensors in the system framework, which was shared by multi-tenants, with a maximum number of sensors. The research work built up a model of the proposed framework and assessed it in a virtual environment of the Future Internet Testbed with Security (FITS). An evaluation of the framework under attacks demonstrated that BroFlow ensured the forwarding of legitimate packets at the maximal connection rate, decreasing up to 90 % of the maximal system delay caused by the attack. BroFlow achieved 50 % of data transfer capacity gain when contrasted with traditional firewalls approaches, even when the attackers were real tenants acting in collusion. Moreover, the framework diminished the number of the sensor, while keeping full coverage of system flows.

3 INTRUSION DETECTION SYSTEM

Any set of actions that attempt to comprise the integrity, confidentiality or availability of a resource. Intrusion leads to violations of the security policies of a computer system,

such as unauthorized access to private information, malicious break-in into a computer system, or rendering a system unreliable or unusable.
A full-blown network security system should include the following subsystems:
1) Intrusion Detection Subsystem: Distinguishes a potential intrusion from a valid network operation.
2) Protection Subsystem: Protects the network and security system itself from being compromised by the network intrusions.
3) Reaction Subsystem: This part either traces down the origin of an intrusion or fights back the hackers.

There are a number of approaches in this field. Most of them fall into three primary categories: Anomaly Detection, Misuse Detection and Hybrid Schemes. The anomaly detection approach is based on a model of normal activities in the system. This model can either be predefined or established through techniques such as machine learning. Once there is a significant deviation from this model, an anomaly will be reported. By contrast, a misuse detection approach defines specific user actions that constitute a misuse and uses rules for encoding and detecting known intrusions. The hybrid detection approach uses a combination of anomaly and misuse detection techniques.
4) Denial of Service: The lifeblood of today's world is information. The denial-of-service intrusions attempt to prevent or delay access to the information or the information processing systems. The basic idea behind this type of intrusion is to tie up a service provider with bogus requests in order to render it unreliable or unusable.

4 PROPOSED METHODOLOGY

This has been evolving as a new and promising branch in Bio inspired Algorithms that can bridge the gap between microbiology and engineering. These classes of algorithms inherit the characteristics of bacterial foraging patterns such as chemo taxis, metabolism, reproduction and quorum sensing. The complex and organized activities exhibited in bacterial foraging patterns inspire a new approach to solve complex optimization problems. Passino discovered this new technique. It is technique of the nature inspired optimization algorithm. In this the bacteria search for nutrients in order to maximize the energy per unit time. When bacteria search for food, then the movement is done with the set of tensile flagella. Flagella are the threadlike structure that enables many bacteria to move from one place to another Flagella has two basic operations. When the flagella of the bacteria are revolved in the right-handed direction, each flagellum stretches the cell. Each flagella moves independently. This algorithm mainly consists of three principal mechanisms namely, chemo taxis, reproduction, and elimination dispersal. Foraging is a phenomenon of a bacterial colony rather than an individual behaviour.

A) Chemotaxis: This process imitates the movement of bacteria via swimming and tumbling. Sometimes, it can swim for a period of time in same direction or it may tumble. With counter clockwise direction, bacterium moves in the straight line. With clockwise, the flagellum moves in different direction. Swarming the cells when gets energetic with the high level of succinate release aspartate, which helps them to get aggregate into groups and density of the bacteria increases.

B) Reproduction: The bacteria with low level of nutrients, least healthy bacteria will die while the bacteria with the good health will split into two bacteria.

C) Elimination and Dispersal: Sometimes there is the sudden change in the environment due to various reasons like raise in temperature. This may kill the group of bacteria that are currently in that part which is rich in nutrients. Elimination and dispersal have the impact of destroying chemotactic progress. Figure 1 shows the basic diagram of BFO.

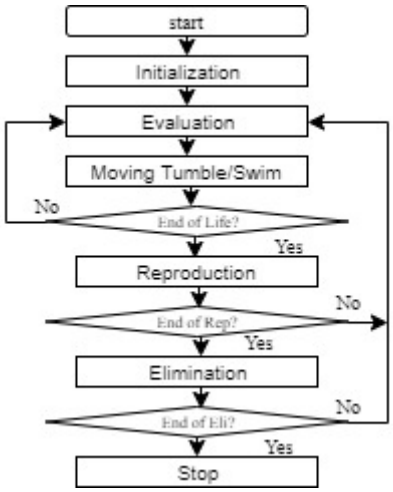

Fig 1: *Working procedure of BFO algorithm*

In next section, the validation of BFO is tested on Twitter data against other existing techniques are explained.

5 RESULTS AND DISCUSSION

In this section, the effectiveness of BFO method is validated by using several parameters such as accuracy, f-measure, precision and recall. The experiments are conducted on Twitter dataset called Sanders Twitter Corpus (STC) dataset which is shown in Table 1. STC datasets contains four different categories such as Apple, Google, Microsoft and Twitter, which can be downloaded from http://www.sananalytics.com/lab/twittersentiment/. This research work considered 5513 manually-classified positive, negative and neutral tweets, whose polarity are 0 forneutral, 1 for positive and -1 for negative tweets.

Table 1*: STC datasets for classification*

Category	*Sample query string*	*No. of tweets analysed*
Apple	*apple*	*1313*
Google	*google*	*1381*
Microsoft	*microsoft*	*1415*
Twitter	*twitter*	*1404*
Total		*5513*

The BFO is a domain-independent which is proven by this datasets to detect the implicit and explicit aspects to attain higher effective results. The parameter evaluation of

proposed BFO method and their validated results are given in below sections.

A Parameter Evaluation

The experiments are implemented using Python 3.7.3 on a computer with Intel Core i5 CPU 2.2 GHz with 8.00 GB RAM. The text classification community has traditionally used measurement precision (the portion of documents classified as positive that truly are positive), recall (the portion of positive documents that are classified as positive). For a given class c_i, the general formula for calculating the precision and recall is given in the equations (1) and (2).

$$Precision = \frac{|Documents\ correctly\ classified\ to\ the\ class\ c|}{|Total\ documents\ classified\ to\ class\ c|} \quad (1)$$

$$Recall = \frac{|Documentscorrectlyclassifiedtotheclas}{|Totaldocumentsinclassc|} \quad (2)$$

Accuracy is the measure of statistical variability and a description of random errors. The overall accuracy of text classification results for determining the intrusion is given in the equation (3).

$$Accuracy = \frac{|Totalcorrectlyclassifieddocumen}{|Totalnumberofdocuments|} \quad (3)$$

F-measure is the measure of accuracy test and it considers the both precision and recall of the test in order to calculate the score. The general formula for F-measure is given in the Equation (4).

$$F - Measure = \frac{2*Precision*Recall}{Precision+Recall} \quad (4)$$

In this experimental research, simulated twitter data is used for comparing the performance evaluation of existing methodologies and the proposed approach in terms of accuracy, F-measure, precision and recall. Two series of experiments under various experimental circumstances are conducted in STC datasets. The experiments primarily aim to determine the best supervised approach when compared with PSO, ACO, variations of Support Vector Machine (SVM), GWO approach, principal component analysis (PCA), and Random Forest (RF). In order to validate the results of sentiment analysis, Sanders topic based corpus is used which includes Apple, Microsoft, Google and Twitter. The BFO is calculated for each of the topic based text classified tweet of Sanders corpus. This classification helps the organization in focusing on tweets with highest impacts to detect any intrusion data. The discussion of BFO of Sanders defined topics in subsequent sections are represents below.

B Performance Analysis in terms of Precision, Recall and F-Measure

The overall performance of precision, recall and F-measure of BFO with existing techniques such as Binary SVM, PSO, GWO, ACO, PCA and term frequency-inverse document frequency-SVM (TFIDF-SVM) in Table 2.

Table 2: *Overall performance of Bi-LSTM in terms of precision, recall and F-Measure*

Methods	*Precision*	*Recall*	*F-Measure*
PSO	*57.23*	*36.49*	*47.01*
GWO	*59.47*	*40.12*	*43.82*
ACO	*60.25*	*45.85*	*49.07*
Binary SVM	*58.13*	*47.51*	*47.49*
TFIDF-SVM	*65.82*	*65.24*	*65.17*
SW-SVM	*81.16*	*80.85*	*80.83*
PCA	*74.74*	*74.20*	*74*
Proposed BFO	*89.20*	*93.58*	*91.17*

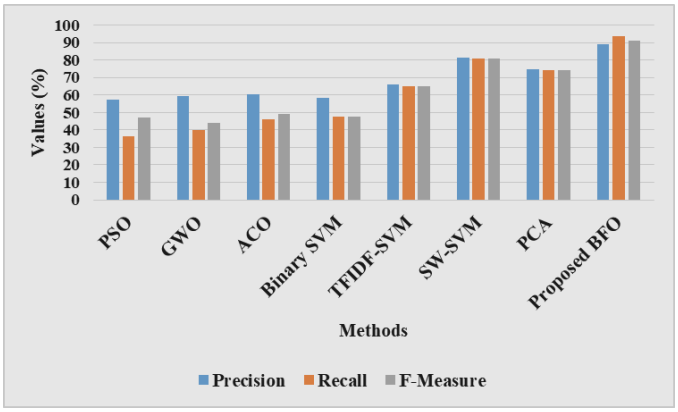

Fig 2: *Performance of BFO*

From the above table 2, it is clearly shows that the proposed BFO achieved higher values of precision, recall and F-Measure when compared with existing techniques. The Binary SVM achieved very low 58.13% precision, 47.51% recall and 47.49% F-Measure because the method didnot focus on pre-processing of tweets. But, the other variation of SVM (i.e. SW-SVM) achieved 81.16% precision, 80.85% recall and 80.83% F-Measure by using weighting approach. The precision values of TFIDF-SVM, PCA are 65.82% and 74.74%, whereas the recall values are 65.24% and 74.20%. The next section will describe the performance of BFO in terms of accuracy.

C Performance Analysis of BFO in terms of accuracy

In this section, the classification accuracy of proposed BFO are compared with existing techniques such as PCA with RF, GWO, PSO, ACO, SVM. Table 3 represents the accuracy values of proposed method with existing system.

Table 3: *Performance of Accuracy for proposed BFO*

Methods	*Accuracy*
PCA with RF	*74.24*
GWO	*84*
PSO	*87*
ACO	*67.4*
SVM	*75*
Proposed BFO	*90.04*

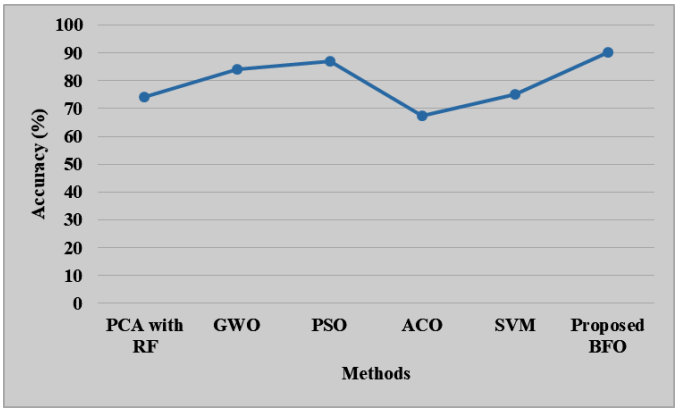

Fig 3: *Performance of BFO in terms of Accuracy*

From the experimental results, the proposed BFO achieved higher accuracy (i.e 90.04%) for twitter classification from STC datasets. The ACO achieved very low accuracy when compared with all other existing techniques. The PSO approach obtained 87% accuracy, but failed to focus on computation work amount. The testing results of the STC dataset is compared with the training results. The best performances of the BFO method are produced in STC dataset when compared with existing techniques such as PCA with RF, SVM and GWO. It could be seen that the number of samples in the testing and training datasets played a significant role in producing highly accurate results.

D Overall Performance of BFO

In this section, the overall performance of BFO is discussed in terms of four parameters which is shown in Table 4.

Table 4: *Overall performance of BFO*

Parameters	*Values of BFO*
Accuracy	*90.87*
Precision	*88.12*
Recall	*92.31*
F-Measure	*90.17*

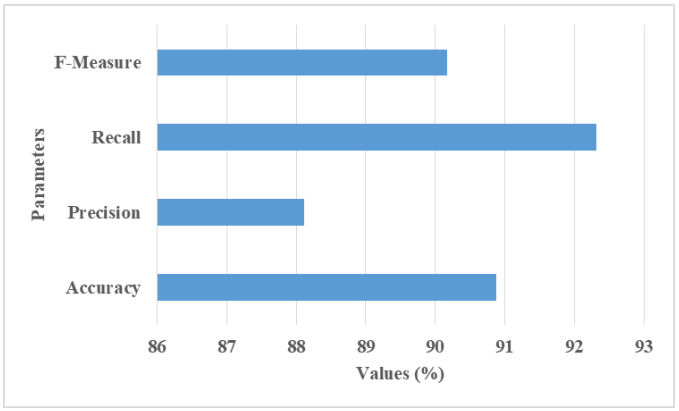

Fig 4: *Overall Performance of BFO*

The results indicate that the proposed BFO proves its capability to enhance the discriminating power of terms for tweet classification. The proposed method can aid in dimensionality reduction, sentiment analysis, spam detection, and many other applications that face different challenges of tweet. Therefore, the proposed scheme mitigates the effect of these challenges on the performance of the classification task.

6 CONCLUSION

Intrusion detection systems are a vital component for an effective defense-in-depth security strategy. IDS' provide the primary mechanism for notifying security practitioners if and when policy has been violated. Intrusion protection systems are emerging evolution of IDS technology that includes automated responses to perceived attacks. Cloud Security information management systems promised to provide better correlation and understanding of the large volume of information and alerts generated by IDS' and other security systems. A well designed IDS solution can reduce the loss. Then an Intrusion Detection System especially for DDos attacks is implemented using BFO Algorithm. By analyzing the simulation results, proposed method outperforms other methods in the contest by providing more throughput and security. It also reduces the negative QoS factors such as End-to-End Delay, Jitter, Latency and Power Consumption by analyzing the accuracy, precision, recall and f-measure. Providing higher security with lesser power consumption makes the BFO more suitable to use in heterogeneous network environments.

7 REFERENCES

[1] Z. Wu, L. Tian, P. Li, T. Wu, M. Jiang, and C. Wu, "Generating stable biometric keys for flexible cloud computing authentication using finger vein", Information Sciences, 2016.

[2] C.T. Li, D.H. Shih, and C.C. Wang, "Cloud-assisted mutual authentication and privacy preservation protocol for telecare medical information systems", Computer methods and programs in biomedicine, vol.157, pp.191-203, 2018.

[3] V. Kumar, S. Jangirala, and M. Ahmad, "An Efficient Mutual Authentication Framework for Healthcare System in Cloud Computing", Journal of medical systems, vol.42, no.8, pp.142, 2018.

[4] A. Mehmood, I. Natgunanathan, Y. Xiang, H. Poston, and Y. Zhang, "Anonymous Authentication Scheme for Smart Cloud Based Healthcare Applications", IEEE Access, 2018.

[5] S. Challa, A.K. Das, P. Gope, N. Kumar, F. Wu, and A.V. Vasilakos, "Design and analysis of authenticated key agreement scheme in cloud-assisted cyber–physical systems", Future Generation Computer Systems, 2018.

[6] I. Indu, P.R. Anand, and V. Bhaskar, "Encrypted Token based Authentication with Adapted Security Assertions Mark-up Language Technology for Cloud Web Services", Journal of Network and Computer Applications, 2017.

[7] D. Li, M. Li, and J. Liu, "A dynamic multiple-keys game-based industrial wireless sensor-cloud authentication scheme", The Journal of Supercomputing, pp.1-21, 2018.

[8] Q. Jiang, J. Ni, J. Ma, L. Yang, and X. Shen, "Integrated Authentication and Key Agreement Framework for Vehicular Cloud Computing", IEEE Network, vol.32, no.3, pp.28-35,2018.

[9] A. Lee, “Authentication scheme for smart learning system in the cloud computing environment”, Journal of Computer Virology and Hacking Techniques, vol.11, no.3, pp.149-155, 2015.
[10] Liu, C., Ranjan, R., Yang, C., Zhang, X., Wang, L. and Chen, J., 2015. MuR-DPA: Top-down levelled multi-replica merkle hash tree based secure public auditing for dynamic big data storage on cloud. IEEE Transactions on Computers, 64(9), pp.2609-2622.
[11] Thangavel, M. and Varalakshmi, P., 2018. Enhanced DNA and ElGamal cryptosystem for secure data storage and retrieval in cloud.Cluster Computing, 21(2), pp.1411-1437.
[12] Yu, J., Ren, K., Wang, C. and Varadharajan, V., 2015. Enabling cloud storage auditing with key-exposure resistance.IEEE Transactions on Information forensics and security, 10(6), pp.1167-1179.
[13] Shen, J., Shen, J., Chen, X., Huang, X. and Susilo, W., 2017. An efficient public auditing protocol with novel dynamic structure for cloud data.IEEE Transactions on Information Forensics and Security, 12(10), pp.2402-2415.
[14] Anbuchelian, S., Sowmya, C.M. and Ramesh, C., 2017. Efficient and secure auditing scheme for privacy preserving data storage in cloud.Cluster Computing, pp.1-9.
[15] Guo, C., Luo, N., Bhuiyan, M.Z.A., Jie, Y., Chen, Y., Feng, B. and Alam, M., 2018. Key-aggregate authentication cryptosystem for data sharing in dynamic cloud storage.Future Generation Computer Systems, 84, pp.190-199.
[16] Zhang, Y., Yu, J., Hao, R., Wang, C. and Ren, K., 2018. Enabling efficient user revocation in identity-based cloud storage auditing for shared big data.IEEE Transactions on Dependable and Secure Computing.
[17] B. B. Gupta, and Omkar P. Badve., "GARCH and ANN-based DDoS detection and filtering in the cloud computing environment." International Journal of Embedded Systems 9.5 (2017): 391-400.
[18] K. Bhushan, and B. B. Gupta. "Distributed denial of service (DDoS) attack mitigation in a software-defined network (SDN)-based cloud computing environment." Journal of Ambient Intelligence and Humanized Computing (2018): 1-13.
[19] X. K. Du, Lu, Z. H., Duan, Q., Wu, J., & Wu, C. R. (2017). “LTSS: Load-Adaptive Traffic Steering and Forwarding for Security Services in Multi-Tenant Cloud Datacenters”. Journal of Computer Science and Technology, 32(6), 1265-1278..
[20] T. Ha, S. Kim, N. An, J. Narantuya, C. Jeong, J. Kim, and H. Lim, “Suspicious traffic sampling for intrusion detection in software-defined networks”.Computer Networks, 109, 172-182, 2016.
[21] A. Chowdhary, S. Pisharody, A. Alshamrani, and D. Huang, "Dynamic game-based security framework in SDN-enabled cloud networking environments". In Proceedings of the ACM International Workshop on Security in Software Defined Networks & Network Function Virtualization (pp. 53-58). ACM, 2017.
[22] D. He, S. Chan, X. Ni, and M. Guizani, “Software-defined-networking-enabled traffic anomaly detection and mitigation”.IEEE Internet of Things Journal, vol. 4, no. 6, pp. 1890-1898, 2017.
[23] Martin Andreoni Lopez, Diogo Menezes FerrazaniMattos, and Otto Carlos MB Duarte."An elastic intrusion detection system for software networks."Annals of Telecommunications 71.11-12 (2016): 595-605.