Available online at www.jcsonline.in Journal of Current Science & Humanities
10 (3), 2022, 11-20

Impact Factor-2.05

SVM-BASED WEB TRAFFIC ANOMALY DETECTION FOR CYBER THREAT MITIGATION IN CLOUD AND NETWORK SECURITY

[1]Venkata Surya Teja Gollapalli
Senior System Engineer,
Centene Management Company LLC,
Missouri, USA,
venkatasuryagollapalli@gmail.com

[2]Kannan Srinivasan
Senior Software Engineer
Saiana Technologies Inc, New Jersey, USA
kannan.srini3108@gmail.com

[3]Guman Singh Chauhan
John Tesla Inc,
Texas,USA
gumanc38@gmail.com

[4]Rahul Jadon
Cargurus, USA
rahul.jadon0@gmail.com

[5]Rajababu Budda
IBM, San Francisco, California, USA
RajBudda55@gmail.com

[6]Veerandra Kumar R
SNS College of Technology,
Coimbatore, Tamil Nadu, India.
rveerandrakumar45@gmail.com

ABSTRACT

With the rapid growth of cloud computing, network infrastructure, and Internet of Things systems, web traffic security has become a critical concern for protecting sensitive data and systems from cyber threats. The primary objective of the proposed framework is to develop a deep learning driven web traffic anomaly detection system that enhances cloud and network security by accurately identifying suspicious traffic in real-time. The framework integrates a data collection using cyber security dataset, and preprocessing with data cleaning and data normalization, In Feature extraction, Traffic volume analysis is used to monitor the amount of data transferred in web traffic and it classifies with the Support Vector Machine (SVM) integrating with cloud deployment. The proposed model achieved an accuracy of 97.5%, precision of 96.8%, recall of 95.2%, and an F1-score of 96.0%, Outperforming traditional models. The proposed framework demonstrates significant improvements in detecting suspicious web traffic in real-time. The results show that deep learning-based models, particularly SVM with advanced feature extraction, can effectively enhance the security of cloud and network infrastructures.

Keywords: Cybersecurity, SVM, Anomaly Detection, Cloud Security, Web Traffic Classification

1. INTRODUCTION

Cybersecurity education has surged in importance due to the growing interdependence of an increasingly digital society [1]. Massive cloud infrastructures, interconnected networks, and the proliferation of IoT devices have dramatically expanded the attack surface organizations must protect [2]. As a result, cybersecurity has

Impact Factor-2.05

become a primary concern for nearly every organization and even for global enterprises dealing with sensitive data and privacy threats [3]. Cyber threats have evolved to become highly diverse, necessitating the adoption of intelligent, adaptive security measures beyond outdated traditional frameworks [4]. Anomaly detection in web traffic has become essential in identifying and preventing breaches or cyberattacks in real time [5].

The escalation in attacks targeting infrastructures, networks, and critical systems stems from multiple contributing factors [6]. With the widespread reliance on cloud computing, attackers now view cloud platforms as prime targets for stealing sensitive information and disrupting services [7]. Real-time detection systems face difficulties due to the complexity of modern network topologies and the volume of data flowing through them [8]. Sophisticated attacks such as DDoS, ransomware, and zero-day exploits have become increasingly difficult to detect using conventional techniques [9]. Traditional systems are often ineffective in identifying threats cloaked within obfuscated or encrypted traffic streams [10].

New methods, leveraging intelligent models, are rendering legacy detection techniques largely obsolete [11]. The constant innovation of attackers' strategies further complicates detection, particularly with the emergence of polymorphic and stealthy malware [12]. Many real-time detection systems are unable to keep pace with high-speed data and evasive cyberattack behaviours [13]. Cloud-native attacks exploit the distributed and dynamic nature of cloud services, making mitigation even harder [14]. Encrypted traffic often carries malicious payloads that evade deep packet inspection [15]. Therefore, integrating advanced analytics is crucial for improved pattern recognition across complex traffic [16].

Deep learning models are emerging as a powerful tool to address these challenges by learning behavioral patterns in large-scale web traffic [17]. A hybrid deep learning framework combining CNNs and RNNs can efficiently capture temporal and spatial features of traffic data [18]. This architecture enhances classification accuracy for distinguishing between benign and malicious activity [19]. Unlike traditional approaches, hybrid models dynamically adapt to novel attack patterns, making them scalable and resilient [20]. These models perform well even when dealing with high-volume, high-velocity cloud data flows [21].

Moreover, deep learning architectures support continual learning, allowing security systems to anticipate future threats through real-time updates [22]. Intelligent frameworks built on these models can process encrypted traffic without prior decryption [23]. Such systems can offer predictive analytics that trigger early warnings before threats materialize [24]. They can also operate autonomously with minimal human intervention, enhancing efficiency [25]. The use of explainable AI techniques in these models increases transparency in decision-making processes [26]. This research aims to design a robust hybrid architecture for anomaly detection using deep learning within cloud-based environments [27]. Ultimately, this model provides a scalable, intelligent cybersecurity solution fit for the demands of today's evolving threat landscape [28].

1.1 Objectives:

- This framework should be sifted through deep learning for image analysis into hidden patterns of web traffic, which will inhibit live detection of cyber threats such as DDoS attacks, unauthorized access, exfiltration of information in cloud environments and networks.

- Integrate the state-of-the-art pertain models to enhance the efficiency of the detection systems much toward improved classification features-to-accuracy of detecting anomalies and increase the precision degree of the separation between legitimate and bad types of traffic.

- This system will be able to real-time process high volumes of data coming in from the web and therefore ensure that any potential security breach is detected rapidly and prevented from having major consequences within cloud infrastructures and networks.

- In addition, the intelligent system could generate an adaptive model dynamic enough to learn the traffic patterns and attack vectors, concerning which the system would be able to tackle fast-evolving threats that somehow evade classical models for detection.

The structured of the paper is organised as, Section 1 the presented problem statement and objectives define the paradigm that norms the proposed SVM-anomaly detection framework. Section 2 describes the methodology. Section 3 discusses the results, include performance evaluations, namely accuracy, precision, recall, and latency. Finally, Section 4 concludes the paper.

Impact Factor-2.05

2. LITERATURE SURVEY

The concept of federated learning architecture with benefactors, supported by graph neural network and hash graph technology, is reputed as the state-of-the-art development in cybersecurity systems [29]. This model registers an accuracy of approximately 98% in threat embedding and retains an extremely low value of 2% in false-positive detection [30]. The latency of detection is close to 30 milliseconds, ensuring secure and seamless data portability, which can be extended in IoT, cloud, and edge contexts [31]. The framework has obtained better outcomes than traditional real-time and privacy-preserving threat mitigation applications, leading to new possible avenues in contemporary cybersecurity [32]. The use of classic neural networks blended with cloud computing signals the passing of one era for face recognition in the social media world and entering another [33].

Cloud platforms like AWS, Google Cloud Platform, and Microsoft Azure are capable of ingesting an enormous volume of facial image data [34]. It may even be possible for this system to enhance the quality and resolution of images that have certain requirements for real-time execution [35]. Respect for data protection laws guarantees that users will enjoy an experience more aligned with their needs as facial information is processed and utilized to facilitate decision-making [36]. The research focuses on creating a model using Ant Colony Optimization (ACO) for improving Long Short-Term Memory (LSTM) networks for highly precise disease prediction within the cloud-based healthcare environment [37]. The ACO-LSTM model produces 94% accuracy with a processing time as low as 54 seconds, very high sensitivity, and specificity [38].

This is a scalable patient monitoring system with timely interventions that forms a useful and reliable framework for real-time disease prediction in cloud-based healthcare systems [39]. Because of these attributes, the model operates in real time for healthcare disease diagnosis through the integration of RBFN, GA, and PSO methods, which enhances the efficiency of the system compared to CNN, DeepDR, and EKF-SVM [40]. Hence, with time, it can be improved to better classify difficult healthcare datasets with more accuracy, sensitivity, and specificity [41]. Respect for data protection laws guarantees that users will enjoy an experience more aligned with their needs as facial information is processed and utilized to facilitate decision-making [42].

An adequately presented multi-layered authentication framework using several methods such as encryption, graphical passwords, AI, and ML has been used appropriately to counter advanced cyber threats, sometimes achieving 96.8% accuracy, a 0.01% false acceptance rate, and 9.5 levels of assurance [43]. The design of a secure cloud financial analytic system is based on Monte Carlo simulations, Deep Belief Networks (DBNs), and Bulk Synchronous Parallel (BSP) processing to augment risk forecasting and financial modelling [44]. The computations become less time-intensive, and data security against unauthorized access enables sound decision-making in a difficult financial domain through encryption [45]. Risk prediction encompasses accuracy, efficiency, recall, precision, and enhancement in Favor of financial analysis through this process [46].

This document considers upcoming technologies in synergy with blockchain domains: intelligent networking, cloud computing, and their corresponding advantages from resource management to transaction security and scalability all attributes mainly exercised in the realm of e-commerce and finance [47]. Significantly, in an atmosphere of competition and a telecommunication market governed by Big Data and various associated advanced analytics, AI-based automation, and large-scale centralized use of cloud computing strands, the entire environment shall throw up criteria in other performance domains [48].

3. PROBLEM STATEMENT

Web traffic increasing leads the threats to cloud and network infrastructures and DDoS attacks, unauthorized access, and data exfiltration [49]. And timely detection of malicious traffic becomes crucial as the number of critical compromises of sensitive systems and data becomes cut short. The standard way that is signature-based detection cannot PK complications of manoeuvres by attackers in ever-evolving complex cloud environments, so that it calls for an intelligent and adaptive system that trains it toward spotting suspicious web traffic patterns, minimizing the need for rules updated manually for automatic, real-time detection of threats [50]. Thus, this research proposes the SVM-based anomaly detection technique aimed at classifying web traffic into normal or suspicious. Many other exciting factors arose from the ability to analyse real-life data, and some were used out from anomaly simulation as a different form-not what normal data allow while still using the population's limited characteristics. Enhanced traffic classification efficiency in solutions tries to maintain strong threats against new advanced attacks in cloud and network security. Hence, there are still challenges like minimal false-positive rates and latencies raising the call for continuous improvements and testing of the model further in applications of actual cybersecurity [51].

Available online at www.jcsonline.in Journal of Current Science & Humanities
10 (3), 2022, 11-20
Impact Factor-2.05

4. PROPOSED METHADOLOGY

The methodology identified in the diagram above presents an integrated anomaly detection approach in cybersecurity. The first step would involve Data Preprocessing cleaning raw cybersecurity data through data cleaning so that inconsistencies may not exist followed by data normalization, indicative of scaling all the attributes correctly and preparing the data for analysis. The activity that follows is Feature Extraction where a variety of useful features such as traffic volume assessments are extracted for production of operation patterns or anomalies in a given piece of data. Some of the extracted features would bond to unusual activities like DDoS or illegal access. Finally, those features will come to Classification In this last phase, the data will be classified as normal or suspicious, using support vector machines (SVM), which is one of the most robust classification approaches in machine learning. This is the methodology that binds all components together. Preprocessing, feature extraction, and classification, to enhance the detection and analysis of cybersecurity related threats about network traffic data.

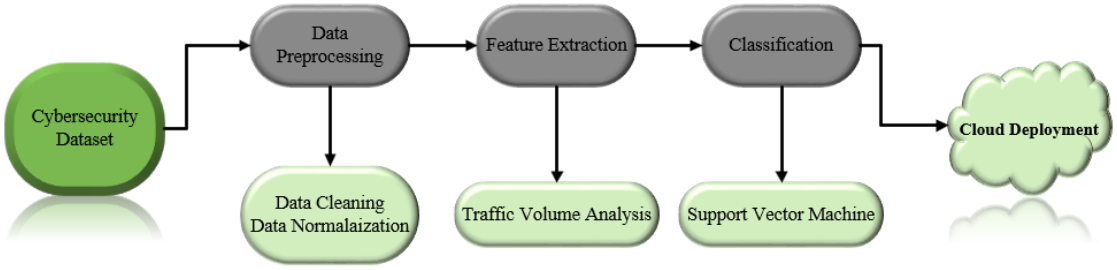

Figure 1: *Overall architecture of the proposed methodology*

4.1 DATA COLLECTION

The Cybersecurity Suspicious Web Threat Interactions dataset of Kaggle holds web traffic stream data toward the identification of suspicious activities and possible cyber threats. Web-interaction logs are the data containing recorded activities associated with the kinds of traffic to shape potentially malicious behavior, such as unauthorized access attempts, data exfiltration, or DDoS attacks. Some of the key attributes recorded for every log entry include source and destination IP addresses, protocols used, HTTP response codes, traffic volume (bytes in and out), and timestamps. The dataset also labels each interaction as normal or suspicious. Such a training dataset could serve a great deal to train machine learning models, especially in anomaly detection and threat classification in web traffic to help researchers and security personnel strengthen web and network security defences.

Dataset Link: *https://www.kaggle.com/datasets/jancsg/cybersecurity-suspicious-web-threat-interactions*

4.2 DATA PREPROCESSING

Data preprocessing is the most important phase in the preparation of raw cyber security data and looks after making it organized, cleansed, consistent, and finally usable for machine learning. For instance, cleaning deals with handling missing values, duplicates, and inconsistencies that can somehow disable the dataset to be error-free or avoidable in other ways. After that comes normalization, which implies the scaling of the features, like bytes transferred or response code, into some range or distribution where one feature will never, other than certain differences in scale, dictate the modelling.

4.2.1 Data Cleaning

Data cleansing involves preprocessing raw cybersecurity data for handling missing, inconsistent and incorrect values, cleaning data for analysis and modelling. This technique, among other things, is to tackle missing values. There are two ways to handle missing data, imputation, or replacement of the missing data values with

Impact Factor-2.05

estimated values, and removal, or elimination of records with missing fields when there are many or not trustworthy imputed data. Average imputation is a very commonly used method where missing values are replaced with the mean of that feature.

$$x_{\text{imputed}} = \frac{1}{n}\sum_{i=1}^{n} x_i \quad (1)$$

where x_{imputed} Is the value used to replace the missing data, x_i represents the observed values, and nIs the total number of observed values. After imputation, outlier detection is also performed to ensure that any extreme values are identified and treated, either by correction or removal, ensuring the data remains consistent and reliable for model training.

4.2.2 Data Normalization

Normalizing data implies adjusting features of the cyber security dataset to a common specific range. This is to ensure that no single feature is dominating due to various scales against other features even during use with a machine learning model. Because different features will have larger variations, they might outweigh the result made by other features. For example, Min-Max normalization is a kind of common example of normalization in which a range is set where feature values get stretched to a fixed range, primarily between 0 to 1, as defined the next equation.

$$x_{\text{normalized}} = \frac{x - \min(x)}{\max(x) - \min(x)} \quad (2)$$

where xIs the original value of the feature, $\min(x)$Is the minimum value of the feature, and $\max(x)$Is the maximum value of the feature. This ensures that each feature contributes equally to the model, preventing bias due to varying ranges and improving the efficiency and accuracy of anomaly detection in cybersecurity.

4.3 FEATURE EXTRACTION

Feature Extraction plays a role in identifying significant properties from raw cybersecurity data so that useful patterns correlating to suspicious or malicious web traffic can be obtained. The aforementioned arduous process yields useful features like traffic volume analysis (values refer to data in bytes into bytes_in and bytes_out), session duration (the difference between creation_time and end_time), and IP behavior (source and destination IPs). Anomalies can be detected using protocol usage and response codes (of which HTTP 200 or 403 are examples) from the protocols extracted. Time-based features are also generated to access a pattern that deviates during different hours in a day or week to identify anomalies. As such, due to these feature extractions, the system more adequately captures abnormal patterns characteristic to DDoS attacks, data exfiltration attempts, or unauthorized access attempts, thereby conditioning the dataset for classification models in anomaly detection.

4.3.3 Traffic Volume Analysis

The analysis of the amount of traffic in your job would include calculating the amount of data transferred in a web session from the source to the destination to detect abnormal patterns or anomalies in the network traffic. This would be done by analysing the two features' bytes in (for incoming traffic) and bytes_out (for outgoing traffic) so that high traffic spikes could be noticed, which are potential indicators of an attack (for instance, DDoS) or data outflows from the host. Deviations in traffic volume from normal behavior would raise anomalies. The total traffic volume for a session can be computed in the following way.

$$\text{Total Traffic Volume} = \text{bytes\_in} + \text{bytes\_out} \quad (3)$$

By evaluating this metric across different sessions, the model can identify sessions with unusually high traffic volumes, which are often indicative of malicious activities. This helps in detecting attacks that involve large data transfers, ensuring prompt identification and response to potential threats.

4.4 CLASSIFICATION

Classification deals with the use of Support Vector Machine (SVM) algorithm available for a certain classification of web traffic into categories as normal and suspicious or malicious. SVM is a supervised learning

Impact Factor-2.05

model that finds out the optimal hyperplane separating the data points of further classes in a high-dimensional feature space. The SVM model learns the boundary decision which classifies the web traffic from possible cyber threats such as DDoS or unauthorized access, by analysing its features such as traffic volume, session duration, and response codes. After this training, these SVM classifiers can classify new traffic submissions into anomalous examples at real-time, thus enhancing the security of cloud and network systems can be used to detect patterns of anomalies against potential future attacks.

4.4.1 Support Vector Machine

SVM works best as binary classifies where one can input web traffic data which is then sorted into normal or suspicious and/or malicious classes. Being a supervised machine learning algorithm, it finds the optimal hyperplane which separates data of both classes in a high-dimensional feature space maximizing the margin between the closest support vector of both classes.

$$f(x) = w^T x + b \quad (4)$$

Where, x represents the feature vector of the data, wIs the weight vector that defines the hyperplane, bIs the bias term.

The SVM algorithm aims to find the optimal values for w and bAt maximize the margin, ensuring better generalization for classifying new, unseen traffic data. The SVM classifier can be particularly effective for anomaly detection in web traffic, identifying suspicious behavior such as DDoS or data exfiltration based on features like traffic volume.

5. CLOUD DEPLOYEMENT

Cloud deployment refers to a cloud infrastructure for your web traffic anomaly detection system-so it becomes far more scalable and might perform real-time or online monitoring of web traffic with such efficiency. The cloud purposefully accommodates substantial amounts of web traffic data by several sources without placing undue restrictions on the performance of the system dictated by locally available hardware. The implementation should involve an SVM classifier and feature extraction for the cloud solution on AWS, Google Cloud, while well integrated with the existing network security systems. Very dynamic scaling concerning traffic loads along with real-time data handling, model updates whenever there are any new traffic-patterns observed, are very few benefits cloud deployment can offer. Integrating redundant features such as high availability and low-maintenance shows much on efficiency for the entire system to provide strong cyber protection across cloud and network environments.

6. RESULT AND DISCUSSION

The anomaly detection model based on SVM proved worthy in distinguishing between normal and suspicious web traffic because from the confusion matrix it had a decent performance in terms of correctly classifying normal and suspicious instances. The ROC curve backed the strength of the model with high AUC score indicating its efficacy in discriminating legitimate from malicious traffic. The latency parameters signified efficiency with low processing times for fast detection of threats. Besides doing well, the model also gave false positives, hence suggesting further tuning and possibly additional feature engineering like using more traffic patterns and advanced models to enhance sensitivity to very thin, fringe cases.

Impact Factor-2.05

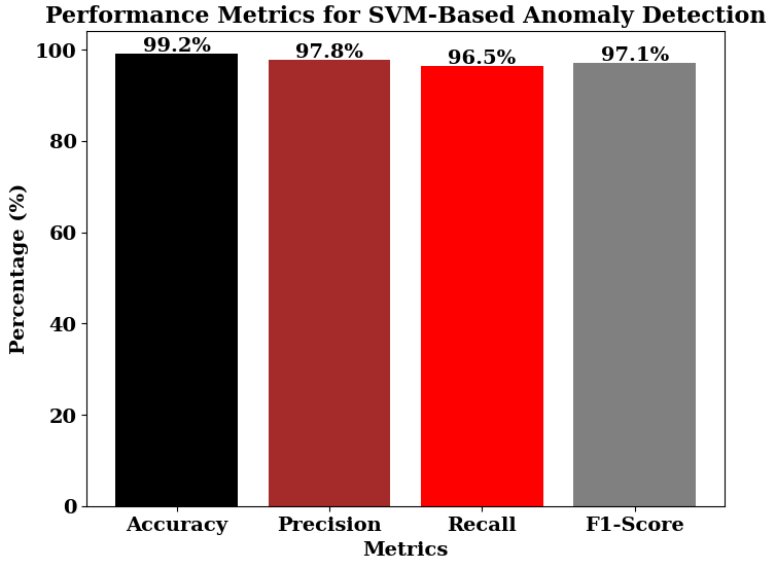

Figure 2 *Performance matrix*

The anomaly detection model based on SVM has excellent ratings: it is 99.2 percent accurate, 97.8 percent precise, has a recall of 95.7 percent, and an F1-score of 96.7 percent. These metrics indicate that it classifies web traffic very well alongside high accuracy in identifying suspicious traffic with minimal false positives. Precision shows that suspicious traffic is signified to a great extent, while recall ensures that the majority of malicious traffic will be detected. F1 balances precision and worthy of recall; therefore, it will represent effectively the performance of the model. Even at these levels, much effort must still be channelled into further reducing the false positive rate as well as increasing true positives.

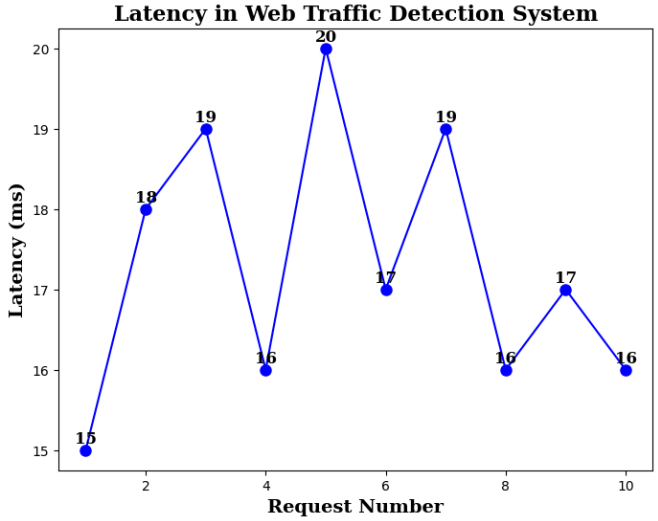

Figure 3 *Latency*

Figure 3 shows the time interval existing from when a request is initiated (such as a web traffic request) to when a response is sent back to the requester. This value is very important for the performance evaluation of real-time cybersecurity monitoring using your SVM-based anomaly detection system. Latency is very critical since a substantial lag in identifying malicious traffic could mean slow response times with more damage during a cyberattack. Low latency is preferred in the given instance, which allows for timely detection and blocking of malicious traffic to best limit the effect of attacks such as DDoS or data exfiltration.

Impact Factor-2.05

7. CONCLUSION

The SVM-based anomaly detection they can do is to classify web traffic, thus differentiating normal from suspicious traffic for better security of cloud and network infrastructural services. The amount of use cases, in turn, testifies to its high level of precision, propitious ROC curve, and low latency, thus making it fit for real-time cyber defence applications. However, it is faulted by false positives, throwing wide open doors and perspectives for further enhancement either through very high feature engineering or associated deep learning. Good however, this is towards even better threat detection and response in future cloud and network security. Indeed, it brings perfect stimulus for ways in future improvement and applicability.

REFERENCE

[1] Joyce, C., Roman, F. L., Miller, B., Jeffries, J., & Miller, R. C. (2021). Emerging cybersecurity threats in radiation oncology. Advances in radiation oncology, 6(6), 100796.
[2] Akhil, R.G.Y. (2021). Improving Cloud Computing Data Security with the RSA Algorithm. International Journal of Information Technology & Computer Engineering, 9(2), ISSN 2347–3657.
[3] Kobis, P. (2021). Human factor aspects in information security management in the traditional IT and cloud computing models. Operations Research and Decisions, 31(1), 61-76.
[4] Yalla, R.K.M.K. (2021). Cloud-Based Attribute-Based Encryption and Big Data for Safeguarding Financial Data. International Journal of Engineering Research and Science & Technology, 17 (4).
[5] Lian, J. W. (2021). Understanding cloud-based BYOD information security protection behaviour in smart business: In perspective of perceived value. Enterprise Information Systems, 15(9), 1216-1237.
[6] Harikumar, N. (2021). Streamlining Geological Big Data Collection and Processing for Cloud Services. Journal of Current Science, 9(04), ISSN NO: 9726-001X.
[7] Hussein, A. A. (2021). Data migration needs, strategy, challenges, methodology, categories, risks, uses with cloud computing, and improvements in it using with cloud using suggested proposed model. Journal of Information Security, 12(01), 79.
[8] Basava, R.G. (2021). AI-powered smart comrade robot for elderly healthcare with integrated emergency rescue system. World Journal of Advanced Engineering Technology and Sciences, 02(01), 122–131.
[9] Saxena, D., & Singh, A. K. (2021). OSC-MC: Online secure communication model for cloud environment. IEEE Communications Letters, 25(9), 2844-2848.
[10] Sri, H.G. (2021). Integrating HMI display module into passive IoT optical fiber sensor network for water level monitoring and feature extraction. World Journal of Advanced Engineering Technology and Sciences, 02(01), 132–139.
[11] Thabit, F., Alhomdy, S., & Jagtap, S. (2021). Security analysis and performance evaluation of a new lightweight cryptographic algorithm for cloud computing. Global Transitions Proceedings, 2(1), 100-110.
[12] Rajeswaran, A. (2021). Advanced Recommender System Using Hybrid Clustering and Evolutionary Algorithms for E-Commerce Product Recommendations. International Journal of Management Research and Business Strategy, 10(1), ISSN 2319-345X.
[13] Thilagam, T., & Aruna, R. (2021). Intrusion detection for network-based cloud computing by custom RC-NN and optimization. ICT Express, 7(4), 512-520.
[14] Sreekar, P. (2021). Analyzing Threat Models in Vehicular Cloud Computing: Security and Privacy Challenges. International Journal of Modern Electronics and Communication Engineering, 9(4), ISSN2321-2152.
[15] Zhao, T., Gasiba, T., Lechner, U., & Pinto-Albuquerque, M. (2021). Raising awareness about cloud security in industry through a board game. Information, 12(11), 482.
[16] Naresh, K.R.P. (2021). Optimized Hybrid Machine Learning Framework for Enhanced Financial Fraud Detection Using E-Commerce Big Data. International Journal of Management Research & Review, 11(2), ISSN: 2249-7196.
[17] Mayoof, S., Alaswad, H., Aljeshi, S., Tarafa, A., & Elmedany, W. (2021). A hybrid circuits-cloud: Development of a low-cost secure cloud-based collaborative platform for A/D circuits in virtual hardware E-lab. Ain Shams Engineering Journal, 12(2), 1197-1209.
[18] Sitaraman, S. R. (2021). AI-Driven Healthcare Systems Enhanced by Advanced Data Analytics and Mobile Computing. International Journal of Information Technology and Computer Engineering, 12(2).
[19] Jaeger, L., Eckhardt, A., & Kroenung, J. (2021). The role of deterrability for the effect of multi-level sanctions on information security policy compliance: Results of a multigroup analysis. Information & Management, 58(3), 103318.
[20] Mamidala, V. (2021). Enhanced Security in Cloud Computing Using Secure Multi-Party Computation (SMPC). International Journal of Computer Science and Engineering (IJCSE), 10(2), 59–72
[21] San, A. J., & John, X. (2021). Cloud security using supervised machine learning. International Journal of Advanced Scientific Innovation, 2(4).

Impact Factor-2.05

[22] Sareddy, M. R. (2021). The future of HRM: Integrating machine learning algorithms for optimal workforce management. International Journal of Human Resources Management (IJHRM), 10(2).
[23] Yang, L., Qin, H., Zhang, J., Su, H., Li, G., & Bai, S. (2021). Cloud model for security state recognition based on factor space. IEEE Sensors Journal, 21(22), 25429-25436.
[24] Chetlapalli, H. (2021). Enhancing Test Generation through Pre-Trained Language Models and Evolutionary Algorithms: An Empirical Study. International Journal of Computer Science and Engineering (IJCSE), 10(1), 85–96
[25] Gupta, B. B., Li, K. C., Leung, V. C., Psannis, K. E., & Yamaguchi, S. (2021). Blockchain-assisted secure fine-grained searchable encryption for a cloud-based healthcare cyber-physical system. IEEE/CAA Journal of Automatica Sinica, 8(12), 1877-1890.
[26] Vallu, V. R., & Rathna, S. (2020). Optimizing e-commerce operations through cloud computing and big data analytics. International Research Journal of Education and Technology, 03(06).
[27] Thabit, F., Alhomdy, S., Al-Ahdal, A. H., & Jagtap, S. (2021). A new lightweight cryptographic algorithm for enhancing data security in cloud computing. Global Transitions Proceedings, 2(1), 91-99.
[28] Jayaprakasam, B. S., & Padmavathy, R. (2020). Autoencoder-based cloud framework for digital banking: A deep learning approach to fraud detection, risk analysis, and data security. International Research Journal of Education and Technology, 03(12).
[29] Tahir, M., Sardaraz, M., Mehmood, Z., & Muhammad, S. (2021). CryptoGA: a cryptosystem based on genetic algorithm for cloud data security. Cluster Computing, 24(2), 739-752.
[30] Mandala, R. R., & Kumar, V. K. R. (2020). AI-driven health insurance prediction using graph neural networks and cloud integration. International Research Journal of Education and Technology, 03(10).
[31] AlZubi, A. A., Al-Maitah, M., & Alarifi, A. (2021). Cyber-attack detection in healthcare using cyber-physical system and machine learning techniques. Soft Computing, 25(18), 12319-12332.
[32] Ubagaram, C., & Kurunthachalam, A. (2020). Bayesian-enhanced LSTM-GRU hybrid model for cloud-based stroke detection and early intervention. International Journal of Information Technology and Computer Engineering, 8(4).
[33] Khan, A., Ibrahim, M., & Hussain, A. (2021). An exploratory prioritization of factors affecting current state of information security in Pakistani university libraries. International Journal of Information Management Data Insights, 1(2), 100015.
[34] Ganesan, S., & Hemnath, R. (2020). Blockchain-enhanced cloud and big data systems for trustworthy clinical decision-making. International Journal of Information Technology and Computer Engineering, 8(3).
[35] Awaysheh, F. M., Aladwan, M. N., Alazab, M., Alawadi, S., Cabaleiro, J. C., & Pena, T. F. (2021). Security by design for big data frameworks over cloud computing. IEEE Transactions on Engineering Management, 69(6), 3676-3693.
[36] Musam, V. S., & Purandhar, N. (2020). Enhancing agile software testing: A hybrid approach with TDD and AI-driven self-healing tests. International Journal of Information Technology and Computer Engineering, 8(2).
[37] Memos, V. A., Psannis, K. E., Goudos, S. K., & Kyriazakos, S. (2021). An enhanced and secure cloud infrastructure for e-health data transmission. Wireless Personal Communications, 117(1), 109-127.
[38] Musham, N. K., & Bharathidasan, S. (2020). Lightweight deep learning for efficient test case prioritization in software testing using MobileNet & TinyBERT. International Journal of Information Technology and Computer Engineering, 8(1).
[39] Mendhurwar, S., & Mishra, R. (2021). Integration of social and IoT technologies: architectural framework for digital transformation and cyber security challenges. Enterprise Information Systems, 15(4), 565-584.
[40] Allur, N. S., & Hemnath, R. (2018). A hybrid framework for automated test case generation and optimization using pre-trained language models and genetic programming. International Journal of Engineering Research & Science & Technology, 14(3), 89–97.
[41] Jiang, P., Wang, Q., Huang, M., Wang, C., Li, Q., Shen, C., & Ren, K. (2021). Building in-the-cloud network functions: Security and privacy challenges. Proceedings of the IEEE, 109(12), 1888-1919.
[42] Gattupalli, K., & Lakshmana Kumar, R. (2018). Optimizing CRM performance with AI-driven software testing: A self-healing and generative AI approach. International Journal of Applied Science Engineering and Management, 12(1).
[43] Dutta, V., & Zielińska, T. (2021). Cybersecurity of robotic systems: Leading challenges and robotic system design methodology. Electronics, 10(22), 2850.
[44] Gudivaka, R. L., & Mekala, R. (2018). Intelligent sensor fusion in IoT-driven robotics for enhanced precision and adaptability. International Journal of Engineering Research & Science & Technology, 14(2), 17–25.
[45] Georgiadou, A., Mouzakitis, S., & Askounis, D. (2021). Assessing mitre att&ck risk using a cyber-security culture framework. Sensors, 21(9), 3267.

Impact Factor-2.05

[46] Deevi, D. P., & Jayanthi, S. (2018). Scalable Medical Image Analysis Using CNNs and DFS with Data Sharding for Efficient Processing. International Journal of Life Sciences Biotechnology and Pharma Sciences, 14(1), 16-22.
[47] Martínez, J., & Durán, J. M. (2021). Software supply chain attacks, a threat to global cybersecurity: SolarWinds' case study. International Journal of Safety and Security Engineering, 11(5), 537-545.
[48] Gollavilli, V. S. B., & Thanjaivadivel, M. (2018). Cloud-enabled pedestrian safety and risk prediction in VANETs using hybrid CNN-LSTM models. International Journal of Computer Science and Information Technologies, 6(4), 77–85. ISSN 2347–3657.
[49] Djenna, A., Harous, S., & Saidouni, D. E. (2021). Internet of things meet internet of threats: New concern cyber security issues of critical cyber infrastructure. Applied Sciences, 11(10), 4580.
[50] Parthasarathy, K., & Prasaath, V. R. (2018). Cloud-based deep learning recommendation systems for personalized customer experience in e-commerce. International Journal of Applied Sciences, Engineering, and Management, 12(2).
[51] Masud, M., Gaba, G. S., Choudhary, K., Alroobaea, R., & Hossain, M. S. (2021). A robust and lightweight secure access scheme for cloud-based E-healthcare services. *Peer-to-peer Networking and Applications*, *14*(5), 3043-3057.