International Journal of
INTELLIGENT SYSTEMS AND APPLICATIONS IN ENGINEERING
ISSN:2147-6799 www.ijisae.org Original Research Paper

Design and Elevating Cloud Security Through a Comprehensive Integration of Zero Trust Framework

K. Saravanan[1], R. Anitha[2], P. Kamarajapandian[3], Thomas Paul Roy Arockiadoss[4], K. Sambath Kumar[5], R. Hariharan[6]

Submitted: 02/11/2023 **Revised**: 21/12/2023 **Accepted**: 03/01/2024

Abstract: Cloud security is vital as it protects against a myriad of cyber threats, including data breaches and service disruptions, ensuring the integrity, confidentiality, and availability of critical information stored in the cloud. It also establishes a foundation for trust, enabling businesses to harness the benefits of cloud technologies while maintaining the resilience and security of their digital assets. User authentication within the cloud ecosystem is indispensable, constituting a foundational pillar for the security and integrity of digital assets. By validating user identities, organizations establish a crucial defense mechanism, thwarting unauthorized access to sensitive data and resources. This authentication process is pivotal in enforcing stringent access controls, effectively mitigating the risks associated with data breaches and unauthorized transactions. The Zero Trust Framework is a security paradigm commencing with User Identity Verification and advancing through the seamless integration of Multi-Factor Authentication (MFA), Device Health Assessment, and Behavioral Analysis. The dual-layer authentication process establishes a formidable barrier, ensuring access only for legitimate users, while stringent device health checks enforce security criteria compliance. The orchestration of Behavioral Analysis, powered by machine learning, becomes pivotal in continuous monitoring, promptly identifying deviations from typical user behavior. These anomalies act as proactive indicators, triggering investigations into potential security breaches. This integrated security approach, providing a robust foundation for continuous verification in safeguarding against unauthorized access and potential threats.

Keywords: *Cloud Security, User Authentication, Zero Trust Framework, Behavioural Analysis, Multi-Factor Authentication*.

1. Introduction

In contemporary business landscapes, the utilization of cloud computing has become ubiquitous, revolutionizing the way organizations leverage and manage their digital infrastructure. The cloud offers unparalleled flexibility and scalability, allowing enterprises to dynamically scale resources based on demand, optimize operational efficiency, and expedite time-to-market for applications and services [1]. Its utility extends beyond traditional data storage, encompassing diverse functionalities such as data analytics, artificial intelligence, and Internet of Things (IoT) deployments [2].

[1]*Professor, Department of Electronics, SAINTGITS college of Engineering, Kottayam,Kerala,India.Email: saravanan.k@saintgits.org*
[2]*Professor, Department of Biomedical Engineering, Jerusalem College of Engineering (Autonomous), Pallikaranai , Chennai, Tamil Nadu-600100,India.Email: anithagodavarthy@gmail.com*
[3]*Assistant Professor, Department of Computer Science and Engineering, Kommuri Pratap Reddy Institute of Technology, Hyderabad, Telangana-501301, India., Email: kamarajapandianp@gmail.com*
[4]*Professor, Department of Computer Science and Engineering, PSNA College of Engineering and Technology, Dindigul, Tamil Nadu 624622. Email: pauli.dgl@gmail.com*
[5]*Assistant Professor, Department of Electronics and Communication Engineering, Vel Tech Rangarajan Dr.Sagunthala R&D Institute of Science and Technology, Chennai - 62, Tamil Nadu, India. Email : samelectronics.kpm@gmail.com*
[6]*Assistant Professor, Department of Electronics and Communication Engineering, P. S. R Engineering College, Sevalpatti, Sivakasi-626140.Tamil Nadu, India. Email: hariharan061998@gmail.com*

The intrinsic value of cloud computing lies in its ability to democratize access to cutting-edge technologies, enabling even small to medium-sized enterprises to harness powerful computing resources without significant upfront investments.. This democratization fosters innovation and agility, as businesses can rapidly prototype, test, and deploy new solutions with reduced capital expenditure. However, the widespread adoption of cloud computing also brings forth a set of challenges and security considerations [3]. Cybersecurity threats in the cloud environment include data breaches, unauthorized access, and service disruptions. As organizations migrate sensitive data and critical applications to the cloud, they must contend with the imperative of fortifying their security postures [4]. Strategies encompassing robust identity and access management, encryption, continuous monitoring, and adherence to best practices such as the shared responsibility model are pivotal in mitigating these security threats. Furthermore, the evolving regulatory landscape poses compliance challenges for cloud users, necessitating a comprehensive understanding of data residency, privacy regulations, and industry-specific compliance requirements. Addressing these considerations ensures that organizations not only harness the full potential of cloud computing but also do so in a secure, compliant, and resilient manner [5]. The Objectives of the work are:

- Assess the effectiveness of ZTA by evaluating its application in user identity verification, multi-factor authentication (MFA), device health assessment, and behavioral analysis within a cloud environment.
- Measure and analyze the decrease in false positive rates over time as an indicator of the improved accuracy and efficiency of the behavioral analysis system integrated into the ZTA framework.
- Illustrate how the User Identity Verification (UIV) graph represents the continuous monitoring and verification aspect of ZTA, emphasizing the shift from periodic to ongoing authentication processes.
- Showcase how the UIV graph explicitly displays trust decisions for each user, emphasizing the principle of making explicit, context-aware trust decisions based on continuous verification, aligning with ZTA principles.

2. Literature Survey

Traditional Intrusion Detection Systems (IDS) face significant challenges when deployed in cloud environments, rendering them less effective compared to solutions designed for the dynamic nature of cloud infrastructures [6]. Unlike their on-premises counterparts, traditional IDS relies on predefined signatures and patterns to identify known threats. The cloud, however, introduces a range of complexities that traditional IDS struggles to address [7]. In the cloud, resources are highly dynamic, with virtual machines, containers, and serverless architectures constantly being provisioned and de-provisioned [8]. The scalability demands of cloud environments may overwhelm traditional IDS, which may not be able to keep up with the scale and speed of these changes. Limited visibility into these dynamic environments further exacerbates the problem, as the traditional IDS may miss crucial insights into network activities [9]. Additionally, the lack of context awareness is a significant drawback. Cloud environments often involve intricate relationships between services, users, and data. Traditional IDS, relying on static signatures, may generate false positives or miss context-dependent anomalies, diminishing its effectiveness in identifying sophisticated threats [10]. The shift toward microservices, serverless computing, and extensive use of APIs in the cloud presents another challenge. Traditional IDS is not inherently designed to monitor and analyze these technologies effectively, leading to blind spots in threat detection. Integration is key in cloud security, and traditional IDS may struggle to seamlessly integrate with cloud-native security services provided by cloud service providers. The result is a fragmented security landscape that lacks the cohesive protection required in a cloud-centric infrastructure. Encryption further complicates matters [11]. As more traffic in the cloud becomes encrypted, traditional IDS faces limitations in inspecting encrypted communication, reducing its ability to detect certain types of threats that may be hidden within encrypted traffic [12]. In terms of response capabilities, traditional IDS may experience delays in reacting to incidents. Manual analysis is often required, slowing down the incident response process and potentially increasing the impact of a security event. Resource intensiveness is another factor contributing to the less effective nature of traditional IDS in the cloud [13]. The resource demands of traditional IDS may be impractical and less cost-effective in a cloud environment where optimization and efficiency are paramount.The complexity of encrypted traffic in the cloud poses challenges to traditional security measures. Encrypted communication conceals the content from inspection, limiting the effectiveness of signature-based threat detection [14]. Threat actors exploit encryption to hide malicious activities, making it difficult for antivirus solutions to detect and mitigate threats. Decrypting traffic for analysis introduces performance overhead, impacting system efficiency [15]. Key management complexities and the need to balance security with privacy add further intricacies. Addressing these challenges requires advanced security solutions capable of effectively handling encrypted traffic without compromising overall system security and performance in dynamic cloud environments.

A clever IDS framework that makes use of the Likelihood Support Vector Machine (LSVM) and Cuckoo Search Greedy Improvement (CSGO) models to improve WSN security. The most widely used network datasets, including NSL-KDD and UNSW-NB15, are taken into account in this model in order to validate it. The first step in establishing the characteristics of the dataset is preprocessing, which involves filtering, missing value prediction, and the elimination of extraneous information [16].

Approximate computing is one of the major techniques used to achieve high performance and energy efficiency in error resistant computationally intense applications. Low power VLSI design is one of the important factors in the designing of new IoT system or reconstructing the existed IoT system. An inexact reverse carry select adder (IRCSLA) with back carry propagation is presented in this work. Three different types of adder implementations were presented in IRCSLA. The method of back carry propagation is applied to the design of both 16-bit ripple carry adder (RCA) & 16-bit carry select adders [17].

3. Proposed Work

Zero Trust Architecture (ZTA) is a security model designed to enhance the protection of cloud environments by challenging the traditional notion of trust. Instead of relying on the assumption that entities within a network are inherently trustworthy, ZTA adopts the principle of "never trust, always verify." This model aims to minimize the impact of potential security breaches by continuously

verifying the identity, device health, and contextual factors associated with each user and device.

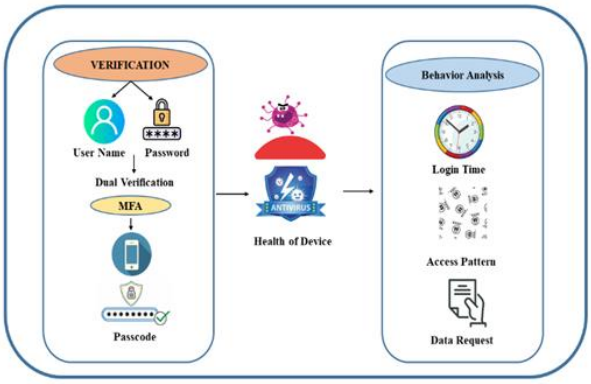

Fig. 1 Workflow of Zero Trust Architecture

The security journey commences with the foundational step of User Identity Verification, necessitating users to authenticate themselves through credentials such as usernames and passwords. To bolster the security posture, a seamless integration of Multi-Factor Authentication (MFA) is introduced, demanding additional layers of identification. This includes the generation of a temporary code sent to the user's mobile device, thereby establishing a dual-layer authentication process that forms a robust checkpoint. This meticulous approach ensures that only legitimate users gain access, significantly enhancing the overall security of the system. Concurrently, a critical aspect of this security framework is the implementation of Device Health Assessment, which rigorously scrutinizes the wellness of the user's device. This assessment aims to ascertain the device's alignment with stringent security standards by conducting a detailed examination. The process involves checking for the presence of up-to-date antivirus software, the application of security patches, and ensuring the absence of any lurking malware. Through the enforcement of these health checks, the system ensures that only devices meeting the prescribed security criteria are granted entry, providing an additional layer of defense against potential threats. The orchestration of Behavioral Analysis emerges as a linchpin in the continuous verification methodology, contributing significantly to the proactive security stance. Leveraging continuous monitoring, advanced machine learning algorithms, and behavioral analysis tools, the system meticulously scrutinizes user actions. By establishing a baseline of typical user behavior, any deviations from this norm are promptly identified. These anomalies serve as red flags, triggering immediate attention and prompting further investigation into potentially unauthorized activities and potential security breaches. In essence, the comprehensive integration of User Identity Verification, Multi-Factor Authentication, Device Health Assessment, and Behavioral Analysis forms a multi-layered security approach. This approach not only safeguards against unauthorized access but also proactively identifies and addresses potential threats. The meticulous examination of user identity, device health, and behavioral patterns establishes a sophisticated security framework, ensuring the continuous and robust protection of the system against evolving security challenges.

3.1 Algorithmic Framework

The input for the behaviour analysis algorithm is the dataset of user behavior features in a cloud environment. These features, such as login times, access patterns, and other relevant behaviors, are organized into sequences. The input includes historical data on user interactions, which is crucial for training the model. Upon execution, the algorithm produces an output that identifies anomalous instances within the user behavior sequences. Using a trained LSTM model, the algorithm predicts future behavior patterns and calculates prediction errors. Anomaly detection is performed by assessing these errors against a predefined threshold. The output includes a set of identified anomalous instances, providing insights into potentially unauthorized or suspicious activities in the cloud environment.

Algorithm: Behaviour analysis for User Authentication

```
# Load and preprocess the data
data = pd.read_csv('user_behavior_data.csv')[['feature1', 'feature2', 'feature3']]
data_scaled = MinMaxScaler().fit_transform(data)
# Create sequences for LSTM training
sequence_length = 10
sequences = np.array([data_scaled[i:i+sequence_length] for i in range(len(data_scaled)-sequence_length)])
labels = np.array([data_scaled[i+sequence_length] for i in range(len(data_scaled)-sequence_length)])
# Split data into training and testing sets
train_size = int(len(sequences) * 0.8)
train_sequences, test_sequences = sequences[:train_size], sequences[train_size:]
train_labels, test_labels = labels[:train_size], labels[train_size:]
# Build the LSTM model
model = Sequential([LSTM(50, return_sequences=True, input_shape=(sequence_length, data.shape[1])),
LSTM(50), Dense(data.shape[1])])
model.compile(optimizer='adam', loss='mean_squared_error')
# Train the model
model.fit(train_sequences, train_labels, epochs=10, batch_size=32)
# Make predictions on the test set
predictions = model.predict(test_sequences)
# Assess anomalies based on prediction errors
```

```
21. prediction_errors = np.abs(predictions - test_labels)
22. anomaly_threshold = 0.1
23. anomalies = np.any(prediction_errors > anomaly_threshold, axis=1)
24. # Identify anomalous instances
25. anomalous_instances = test_sequences[anomalies]
```

This algorithm utilizes an LSTM-based neural network to capture sequential patterns in user behavior. The model is trained on historical data and can subsequently identify anomalies in new data based on prediction errors. The choice of the anomaly threshold is a parameter that can be adjusted based on the specific requirements of the cloud security system.

Mathematical Indication

To express this process mathematically, combination of set notation, probability, and conditional statements are used. Keep in mind that this is a symbolic representation and not a precise mathematical model. Let U be the set of all Users. $C(u)$ represents the credentials (username and password) provided by user u. The identity verification function V can be represented as

$$V(u) = \begin{cases} 1, & if\ C\ (u)\ is\ valid \\ 0, & Otherwise \end{cases} \quad (1)$$

$MFA(u)$ is the MFA function for user u. Let $T(u)$be the temporary code sent to the user's mobile device. MFA can be represented as

$$MFA(u) = \begin{cases} 1, & if\ T(u)\ is\ valid \\ 0, & otherwise \end{cases} \quad (2)$$

$D(u)$ Represents the health assessment for user u device. $A(u)$, (u) , and $M(u)$ Represent the presence of up-to-date antivirus software, application of security patches, and the absence of malware, respectively. The device health assessment function can be defined as

$$D(u) = \begin{cases} 1, & if\ A(u)\ and\ P(u)\ and\ not\ M(u) \\ 0, & otherwise \end{cases}$$

(3)

$B(u)$ is the behavioral analysis function for user u. $N(u)$ Represents the baseline of typical behavior. $Dev(u)$ Is the deviation from the norm for user$u$ Behavioral analysis can be symbolized

$$B(u) = \begin{cases} 1, & if\ B(u)\ is\ within\ acceptable\ limits \\ 0, & otherwise \end{cases}$$

(4)

The overall security verification process can be represented as a combination of these functions

$$Verification(u) = V(u) \times MFA(u) \times D(u) \times B(u)$$

(5)

4. Results

4.1 Dataset Details

The Cloud Behavior dataset emerges as a valuable reservoir meticulously curated for the purpose of delving into the intricacies of user behavior within the dynamic realm of cloud environments. This dataset Sourced from UCI Machine Learning Repository boasts a rich tapestry comprising 1000 entries thoughtfully organized across six key columns as shown in table 1

Table. 1 Cloud user Activity

User ID	Login Time	Access Pattern	Data Request	Feature x	Feature Y
1	2023-01-01 08:00:00	Web Application	Files & Folder	0.75	0.20
2	2023-01-01 09:30:00	Mobile APP	DB queries	0.60	0.40
3	2023-01-01 12:09:00	Web Application	Data update	0.85	0.15
4	2023-01-01 06:15:00	Desktop	Data Analysis	0.70	0.30
5	2023-01-01 10:09:00	Mobile App	File Upload	0.90	0.10

4.2 B A Analysis

To demonstrate the effectiveness of a Zero Trust Architecture (ZTA) in enhancing cloud security False Positive Rates in Behavioral Analysis is done as represented in figure 2.

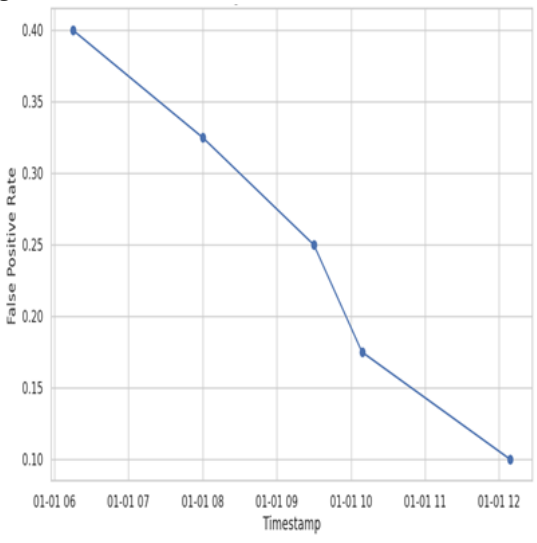

Fig. 2 False Positive Rates Over Time

Table. 2 Output of False Positive Rates Over Time

Malicious	False Positive Rate
0.30	0.400
0.20	0.325
0.40	0.250
0.10	0.175
0.15	0.100

In analyzing the output of table 2 and figure 2, it is evident that the False Positive Rates decrease consistently over time, reflecting a significant improvement in the accuracy of the behavioral analysis system. This reduction in false positives is a crucial indicator of the effectiveness of the Zero Trust Architecture (ZTA) in enhancing cloud security. The consistent decline in false positive rates means that the system is becoming more adept at distinguishing between normal user behaviors and potentially malicious activities. This improvement is essential for ensuring cloud security as it minimizes false alarms, allowing security teams to focus their attention on real security threats rather than being inundated with non-threatening alerts. The progressive refinement of the system's ability to identify genuine security risks aligns seamlessly with the principles of a Zero Trust Architecture. By continuously adapting and learning from user behaviors, the ZTA establishes a robust defense mechanism, providing a higher level of confidence in the security posture of the cloud environment. In conclusion, the observed reduction in false positive rates, as evidenced by the table and graph, not only signifies the efficiency of the behavioral analysis system but also underscores the robust security framework established by the Zero Trust Architecture. This continuous improvement in threat detection contributes significantly to enhancing overall cloud security and mitigating potential risks effectively.

4.3 UIV Analysis

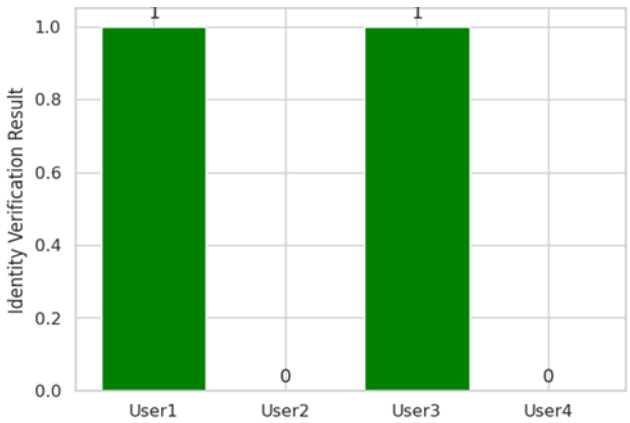

Figure 3 illustrates the User Identity Verification (UIV) function serves as a visual representation of key principles aligned with the Zero Trust security model. Firstly, the concept of continuous verification is depicted, as the graph presents a snapshot of identity verification results for each user. In practical terms, this process would be ongoing, reflecting the Zero Trust principle of continuous monitoring and verification rather than relying on periodic or static authentication methods. Moreover, the graph makes explicit the trust decisions associated with each user by explicitly displaying whether their credentials are valid or not. This transparency in trust decisions resonates with the Zero Trust principle of making explicit, context-aware trust decisions based on continuous verification. Unlike traditional models that assume trust by default, the graph reinforces the idea that trust is earned through continuous and explicit validation.

Furthermore, the graph's representation of individual bars for each user emphasizes a granular level of access control. Trust decisions are made at the user level, illustrating a nuanced approach consistent with the Zero Trust model. This granularity aligns with the idea of applying access controls based on the specific needs and context of each user, reflecting the principle of granular access control within the Zero Trust architecture. While the graph itself may not encapsulate all aspects of Zero Trust, it serves as a visual aid to convey how the identity verification process adheres to fundamental Zero Trust principles. The emphasis on continuous verification, explicit trust decisions, and granular access control reinforces the alignment of the security measures with the core tenets of the Zero Trust model.

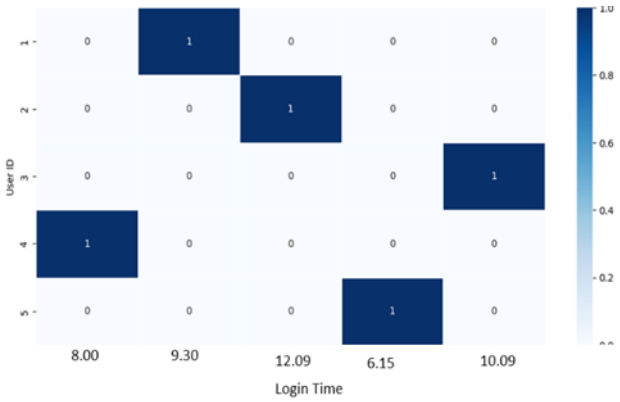

Fig.4 User Activities over Time (Access Pattern)

The heatmap in figure 4 represents user activities over time, with each row corresponding to a user and each column corresponding to a login time. The color intensity at each intersection represents the count of access patterns for a specific user at a given login time. By observing the heatmap, you can identify patterns or spikes in user interactions, and anomalies or unusual activities might be

indicated by unexpected high counts or irregular patterns. This visualization helps security analysts to quickly identify unusual user behavior or spikes in activity, which can be indicative of security threats or unauthorized access. In the context of Zero Trust Architecture, continuous monitoring and anomaly detection through visualizations like heatmaps contribute to enhancing security by promptly identifying and responding to potential security incidents.

5. Conclusion and Future Directions

In conclusion, the integration of Zero Trust Architecture (ZTA) into cloud security, as demonstrated through the User Identity Verification (UIV) function, reflects a paradigm shift from traditional trust models to a more robust and adaptive security framework. The continuous verification approach, exemplified by the dynamic graph, emphasizes the commitment to ongoing scrutiny of user identities, aligning seamlessly with ZTA principles. For future work, it is imperative to further refine and expand the application of ZTA principles within the cloud environment. Continuous enhancement of behavioral analysis tools, machine learning algorithms, and device health assessments can contribute to a more sophisticated and adaptive security posture. Additionally, exploring ways to integrate emerging technologies, such as artificial intelligence and advanced anomaly detection, can further strengthen the overall resilience of the system.

References

[1] .Rasool, R., & Younis, U. (2017). Intrusion detection systems in cloud computing: A contemporary review of techniques and solutions. *Journal of Information Science and Engineering*, *33*, 611-634.

[2] Asharf, J., Moustafa, N., Khurshid, H., Debie, E., Haider, W., & Wahab, A. (2020). A review of intrusion detection systems using machine and deep learning in internet of things: Challenges, solutions and future directions. *Electronics*, *9*(7), 1177.

[3] Arafath, B. N. Y. (2022). *A comparative study between Microservices and Serverless in the cloud* (Master's thesis, OsloMet-storbyuniversitetet).

[4] Aslanpour, M. S., Gill, S. S., & Toosi, A. N. (2020). Performance evaluation metrics for cloud, fog and edge computing: A review, taxonomy, benchmarks and standards for future research. *Internet of Things*, *12*, 100273.

[5] Idhammad, M., Afdel, K., & Belouch, M. (2018). Distributed intrusion detection system for cloud environments based on data mining techniques. *Procedia Computer Science*, *127*, 35-41.

[6] Prabhakaran, V., & Kulandasamy, A. (2021). Integration of recurrent convolutional neural network and optimal encryption scheme for intrusion detection with secure data storage in the cloud. *Computational Intelligence*, *37*(1), 344-370.

[7] Papadogiannaki, E., & Ioannidis, S. (2021). A survey on encrypted network traffic analysis applications, techniques, and countermeasures. *ACM Computing Surveys (CSUR)*, *54*(6), 1-35.

[8] Heidari, A., & Jabraeil Jamali, M. A. (2022). Internet of Things intrusion detection systems: A comprehensive review and future directions. *Cluster Computing*, 1-28.

[9] Liu, J., Tian, Z., Zheng, R., & Liu, L. (2019). A distance-based method for building an encrypted malware traffic identification framework. *IEEE Access*, *7*, 100014-100028.

[10] Zhou, E., Turcotte, J., & De Carli, L. (2020, December). Enabling security analysis of IoT device-to-cloud traffic. In *2020 IEEE 19th International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom)* (pp. 1888-1894). IEEE.

[11] Gopampallikar Vinoda Reddy, Kongara Deepika, Lakshmanan Malliga, Duraivelu Hemanand, Chinnadurai Senthilkumar, Subburayalu Gopalakrishnan, Yousef Farhaoui, “Human action recognition using difference of gaussian and difference of wavelet”, Big Data Mining and Analytics, vol. 6, Issue. 3, pp. 336-346, 2023.

[12] Rajasekhar Turaka, S Ravi Chand, R Anitha, R Arun Prasath, S Ramani, Harish Kumar, S Gopalakrishnan, Yousef Farhaoui, "A novel approach for design energy efficient inexact reverse carry select adders for IoT applications", Journal Results in Engineering, Vol. 18, pp. 101127, Elsevier, 2023.