DOI: 10.21917/ijct.2024.0483

EFFECTIVE CLUSTERING AND CERTIFICATELESS ENCRYPTION TECHNIQUES IN THE MILITARY DOMAIN FOR ATTACK DETECTION

S. Rajesh[1], M.S. Premapriya[2], A. Jayasmruthi[3] and V. Muthu Lakshmi[4]
[1,3]Department of Computer Science and Engineering, Sri Ramakrishna Institute of Technology, India
[2]Department of Management Studies, Anna University Regional Campus, Coimbatore, India
[4]Department of Information Technology, Sri Ramakrishna Engineering College, India

Abstract

The goal of a wireless sensor network (WSN) is to connect numerous nodes via a multi-hop self-organizing network. A variety of sensor nodes are arranged and positioned in relation to other nodes to provide safe data exchange. Sensor nodes watch as a sink node processes the data. The network includes a variety of assaults, including floods, wormhole, black hole, sinkhole, and so on. One of the most challenging tasks in WSN is secure routing because of the existence of attacks. The technology of attack detection is employed to identify attacks and enhances the security of data transmission. It provides a way to ignore network threats, enabling secure communication. Most recent efforts have been focused on implementing secure data communication in wireless sensor networks. However, the more accurate detection attack was not achieved. Numerous intrusion attackers are available to compromise network data packet communication. To provide better data distribution amongst soldiers in a combat environment, this wireless network invader node needs to be identified. Hence, in a WSN context, data transmission with a military scenario entails armed men engaged in combat, such as fighter aircraft, tankers, and shot ships. Finding intrusion attackers is a difficult task, especially in the highly dynamic military wireless sensor network. Therefore, different techniques are developed in WSN for achieving attack detection accuracy with minimal delay and maximum data delivery rate.

Keywords:

WSN, Secure Routing, Black Hole Attack Detection, Floods, Sink Hole Wormhole, Certificateless Signcryption Secure Communication

1. INTRODUCTION

. Sensor Networks are initially planned for military process and observation. WSNs have emerged as an admirable tool for military applications involving intrusion detection, various parameters examining, information gathering and smart logistics support in an unknown deployed area. In the military, the defined network renders various services such as information collection, battlefield surveillance and attack detection. WSNs play a crucial work in military actions due to their competence of real time transmission [11]. These networks present several benefits over habitual sensor devices such as fault tolerance, low budget deployment and so on. In case of adversary attack, some nodes may be damaged but, node damage in WSNs does not affect the whole network.

WSN also helps to distribute significant information quickly and reliably to the right individual or organization at the right time. This considerably improves the competence of combat operations. Here, WSN is used for intrusion detection and data transmission in military field [12]. Security is a key challenge in this application. The foremost functions of the WSN are to examine the enemy activities and managing the activities of the army. In WSN, sink is used to gather and process the information from various nodes. Sensor nodes are employed to sense the environment for intruder detection and to manage military action [13]-[17]. Nodes in the network examine the particular events and thus periodically send the data to the sink node. In case of intruder behaviours, the nodes send the data to the sink node. The sink node receives the information and then takes the necessary actions like notifying the command in charge for that region.

There are many intrusion attackers presented to affect the data packet communication in the network. If the node attackers are in the network, then the node is called as intruder node. This intruder node in the wireless network needs to be determined to give the higher data delivery between the soldiers in a military field. Thus, the data communication with military scenario in WSN involves the armed soldiers occupied in the battlefield like fighter level surface, tankers, and shot ships. The detection of intrusion attackers is a demanding task particularly in highly dynamic military WSN.

The novelty of this work lies in the integration of advanced certificateless signcryption techniques with spatial correlation and Gaussian kernel-based clustering for enhancing the security and accuracy of intrusion detection in Wireless Sensor Networks (WSNs), particularly in military applications. By employing the Spatially Correlated Boltzmann Lamport Session Certificateless Signcryption (SCB-LSCS) method, the proposed approach effectively identifies secure routing paths by detecting and eliminating malicious nodes, thus minimizing packet loss and enhancing data transfer reliability. The unique use of a probabilistic distribution function based on energy for selecting cluster heads and the Lamport Session Discrete Certificateless Signcryption further strengthens data security during communication. Additionally, the Gaussian kernel clustered Okamoto–Uchiyama certificateless signcryption (GKCOUCS-SIDNL) technique offers a novel deep learning-based framework for precise attack detection, utilizing mean shift clustering to dynamically adapt to various attack patterns and ensure accurate clustering of sensor nodes. This dual-method approach significantly contributes to improving attack detection accuracy, reducing transmission delays, and maximizing data delivery rates in highly sensitive military environments, marking a substantial advancement in secure WSN communication.

2. LITERATURE REVIEW

The research in secure communication and attack detection in Wireless Sensor Networks (WSNs) has evolved significantly, with various approaches addressing the challenges posed by different types of attacks, such as Denial of Service (DoS) and blackhole attacks. A noteworthy contribution by Rajesh and Jayanthi [1] proposed a clustered certificateless signcryption scheme specifically designed for blackhole attack detection in

secured WSNs, enhancing the security and performance of these networks. This work was further extended in a subsequent study, where Rajesh, Jayanthi, and Mala introduced a spatially correlated Boltzmann deep learning-based signcryption method aimed at detecting DoS attacks and ensuring secure communication in WSNs [2].

The classification of DoS attacks in smart underwater WSNs by Ahmad et al. [3] emphasized the importance of accurate attack detection, leveraging advanced classification techniques to mitigate the impact of such threats. Similarly, Ahmad et al. [4] focused on feature-selection and mutual-clustering approaches, which significantly improved DoS detection and optimized the lifetime of WSNs by reducing unnecessary energy consumption.

To enhance security in WSNs, Aissani and Abbache [5] developed a secure key management system integrated into the cell-LEACH protocol, demonstrating a robust method for maintaining secure communication channels. Alghamdi [6] introduced a convolutional technique to detect malicious nodes in WSNs, thereby strengthening the network's resilience against internal threats. Furthering this line of research, Alghamdi et al. [7] presented a routing-aware detection method that effectively identified malicious nodes through concealed data aggregation, providing an innovative approach to safeguard data integrity in WSNs.

The identification of distributed denial of services (DDoS) anomalies by Ali et al. [8] utilized a combination of entropy and sequential probability ratio test methods, presenting a novel technique for accurate detection of DDoS attacks in WSNs. Almomani and Alenezi [9] explored efficient detection mechanisms for DoS attacks, proposing an approach that balances detection accuracy with resource efficiency, crucial for the constrained environments of WSNs. Additionally, Alsulaiman and Al-Ahmadi [10] conducted a performance evaluation of machine learning techniques for DoS detection in WSNs, providing insights into the effectiveness of various algorithms in enhancing network security.

These studies collectively highlight the advancements in secure communication and attack detection within WSNs, demonstrating a broad spectrum of techniques ranging from deep learning and machine learning to advanced cryptographic methods. The continued exploration of these approaches is vital for developing resilient WSNs capable of withstanding the evolving landscape of cyber threats.

3. PROPOSED METHODOLOGY

The numerous domains of applications such as military observation, electronic healthcare monitoring, vehicular traffic monitoring are used in WSN. In military application, the most important constraints are the value of the enemy's political objective, time, internal public opinion, the international political environment, geography, and nuclear weapons. Military security is a major application area of WSN. The major functions of the WSN are to observe the enemy actions and controlling the activities of the army. The nodes are deployed in the area and monitored as shown in Fig.1.

The base station or sink node is used to collect and process the information from various nodes. The nodes sense the environment to identify the enemy and to coordinate the military activity. Sensors observe during certain events and give periodical messages to the base station. In case of intruder activities, nodes instantly send messages to the base station.

The base station get the information from nodes and take the crucial action like notifying the command in charge for that region or give messages to nodes surrounding that area.

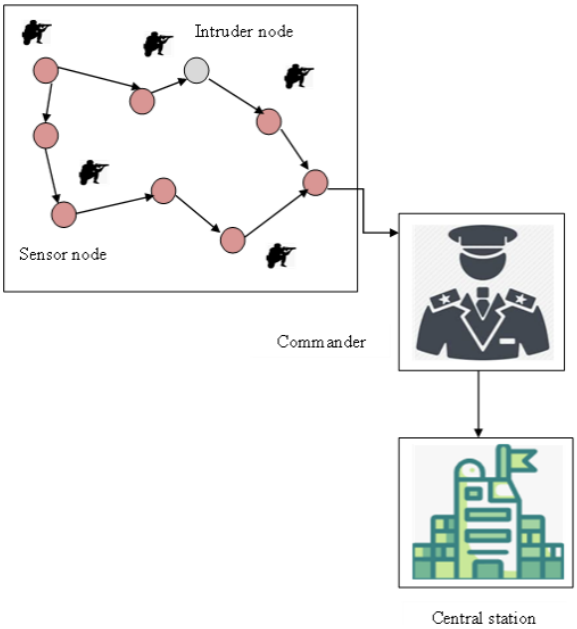

Fig.1. Architecture of Intrusion Detection in Military Environment

The Fig.1 shows the architecture of intrusion detection in military environment. A number of sensor nodes is deployed to work as a soldier in various areas for identifying intrusion attackers in military environment. Then the soldier observes information about the region and sends the message to the sink node (commanders). The commander is used to control the entire soldiers in the military environment. A commander is a person to give the highest operational command and also manages the military forces for secured communication between the soldiers. This helps to find the attacker in the area. If any intruder is entered into the network, then the soldier immediately sends message to the commanders to take necessary actions. Intruder nodes in the network area are hard to detect the attack. Also, security of the data needs to be ensured during the message transmission from soldiers to the commander. Therefore, three different techniques are developed in WSN for achieving attack detection accuracy with minimal delay and maximum data delivery rate.

3.1 PROPOSED ALGORITHM: SCB-LSCS AND GKCOUCS-SIDNL FOR INTRUSION DETECTION AND SECURE DATA TRANSMISSION IN WSNS

Step 1: Network Initialization

- Deploy sensor nodes across the target area, such as a military environment.
- Define the base station (sink node) to collect and process data from the deployed sensor nodes.

Step 2: Spatial Correlation Model for Malicious Node Detection (SCB-LSCS)

- **Node Deployment and Sensing**:
- Nodes continuously monitor the environment and gather data related to potential intrusions.
- Sensor nodes communicate periodically or in response to detected events (e.g., intruder presence) with the base station.
- **Cluster Formation**:
- Use spatial correlation to group nodes into clusters based on proximity and sensing similarities.
- Calculate cluster heads using a probabilistic distribution function that considers the nodes' residual energy levels.
- **Malicious Node Detection:**
- Identify potential malicious nodes within clusters by evaluating the communication patterns and energy anomalies.
- Remove detected malicious nodes from the network to prevent them from participating in data routing.
- **Secure Routing Path Identification:**
- Determine secure routing paths by selecting nodes with the lowest packet loss rates, ensuring reliable data transmission from sensor nodes to the base station.
- **Lamport Session Discrete Certificateless Signcryption:**
- Generate private and public keys using session discrete numbers for each secure communication session.
- Signcrypt data packets at the sensor nodes before transmission to ensure confidentiality and authenticity.

Step 3: Gaussian Kernel Clustered Okamoto–Uchiyama Certificateless Signcryption (GKCOUCS-SIDNL)

- **Input Layer:**
- The number of sensor nodes is input into the deep learning model for processing.
- Hidden Layer 1: Attack Detection using Gaussian Kernel Mean Shift Clustering:
- Apply Gaussian kernel mean shift clustering to the nodes to identify clusters based on the characteristics of potential attacks.
- Compute the mean values for each cluster and group nodes that exhibit similar attack patterns.
- **Attack Detection and Clustering:**
- Calculate the likelihood for each node belonging to specific clusters.
- Nodes that align closely with the cluster mean are grouped together, improving attack detection accuracy.
- **Certificateless Signcryption Process:**
- Implement Pseudo Randomized Okamoto–Uchiyama certificateless signcryption to secure the data transmission between nodes.
- Key Generation: Base station creates and distributes public and private keys.
- Signcryption: Sensor nodes encrypt data and generate a signature before transmission.
- Unsigncryption: The base station verifies the signature; if valid, the message is accepted and decrypted to retrieve the original data.
- **Output Layer:**
- The data is securely transmitted to the authorized receiver node.
- If the received signature is verified, the receiver decrypts the ciphertext and retrieves the original message.

Step 4: Data Delivery and Command Response

- The base station processes received data and takes necessary actions, such as alerting commanders or other response units in case of detected intrusions.
- The system ensures minimal delay and maximum data delivery rates, enhancing overall mission efficiency.

This algorithm ensures robust intrusion detection and secure data transmission in WSNs, particularly suited for high-stakes military applications where reliable and secure communication is critical.

The purpose of the Spatially Correlated Boltzmann Lamport Session Certificateless Signcryption (SCB-LSCS) method is secure data transfer and attack detection. In order to acquire effective data communication and attack detection, the number of soldiers, or nodes, in the network is taken into consideration first. For every sensor node, the spatial correlation model is used. Spatial correlation identifies the assault vectors and locates the best cluster. Each cluster's cluster head is selected using a probabilistic distribution function based on energy. Malicious nodes are found and eliminated for the routing process during this phase. This allows the nodes with the lowest packet loss rate to be identified as having a secure route path. Then, for secure communication, Lamport Session Discrete Certificateless Signcryption is used. In this case, the private and public keys are generated using a session discrete number.

Gaussian kernel clustered Okamoto–Uchiyama certificateless signcryption based Shift invariant deep neural learning (GKCOUCS-SIDNL) technique is developed for accurate attack detection and secure data transmission in WSN. The designed technique includes several layers to find the attack in the network. Number of sensor nodes is considered as input in the input layer. Then the nodes are fed into the hidden layer one. In that layer, various kinds of attacks are determined by using Gaussian kernel mean shift clustering technique. Based on the characteristics of nodes, the number of clusters is determined. Mean value for each cluster is computed depending on the characteristics of the attack. Then the likelihood is computed for each cluster to group the nearby nodes. From that, the node characteristic that is closer to the mean is grouped into the cluster. With this, the attack detection accuracy is improved. After that, the Pseudo randomized Okamoto–Uchiyama certificateless signcryption is applied to carry out the secure data transmission. Here, key generation, signcryption, and unsigncryption processes are employed. Base station creates the public key and private keys in the key generation process. Sensor node encrypts the data and generates the signature. Lastly, signature verification is performed at the receiver side. If the signature is valid, then the receiver gets the original data. Lastly, the authorized receiver node decrypts the ciphertext and gets the original data in the output layer of deep learning.

4. RESULTS AND DISCUSSION

4.1 SIMULATION SETTINGS

Simulation assessment of proposed SCMSC-GMCS technique, SCB-LSCS method and GKCOUCS-SIDNL technique is carried out with the simulation of NS2.34 network simulator. Windows 10 OS, 4GB RAM, core i3-4130 3.40GHZ Processor, 1TB (1000 GB) Hard disk, Internet Protocol, ASUSTek P5G41C-M Motherboard is represented as hardware setting up and it is applied in the proposed and existing methods for conducting experiments. In the simulation process, Dynamic Source Routing (DSR) protocol is used as routing protocol. A^2 (1400 m * 1400 m) is considered with 500 sensor nodes. Random Way point mobility model is used to distribute the sensors nodes in the region. A number of data packets used for simulation varied from 25 to 250 data to analyze the performance of secure data transmission in WSN via detecting various types of attacks.

4.2 PERFORMANCE ANALYSIS

The performance analysis of different proposed technique is conducted by comparing with existing Malicious Node Detection method based on Reputation with Enhanced Low Energy adaptive clustering hierarchy (MNDREL) approach, trustable and secure routing scheme (TSRS) and Deep Learning-based Defense Mechanism (DLDM). Parameters used for performing the simulation are given as follows, Packet Delivery Ratio, Delay, Routing Overhead and Attack Detection.

4.2.1 Performance Analysis of Packet Delivery Ratio:

Packet delivery ratio is calculated as the ratio of number of data packets correctly received at the sink node to the total number of data packets sent from the source node. The unit for computing packet delivery ratio is percentage (%). The method with higher packet delivery is the best for attack detection in the military field which is shown in Table 1.

Table.1. Measure of Packet Delivery Ratio (%)

Data Packets Sent	DLDM	TSRS	MNDREL	Proposed SCB-LSCS	Proposed SCMSC-GMCS
25	70	68	69	76	72
50	71	68.5	69.5	77	73
75	72	69	70	78	74
100	72.5	70	71	78.5	74.5
125	73	71	71.5	79	75
150	73.5	71.5	72	79.5	76
175	74	72	72.5	80	76.5
200	74.5	72.5	73	80.5	77
225	75	73	73.5	81	77.5
250	75.5	73.5	74	81.5	78

As a result, packet delivery ratio of GKCOUCS-SIDNL technique is improved by 8%, 14% and 11% as compared to existing DLDM, trustable and secure routing scheme and MNDREL respectively. Also, packet delivery ratio of SCB-LSCS method is increased by 6%, 12% and 8% as compared to the existing DLDM, trustable and secure routing scheme and MNDREL respectively. Similarly, SCMSC-GMCS enhances the packet delivery ratio by 3%, 9% and 6% than the conventional methods

4.2.2 Performance Analysis of Delay:

In data transmission, delay is computed as the difference of expected arrival time of data packets and the actual arrival time of the packet. Delay is calculated in terms of milliseconds (ms). Lower delay ensures that the technique is more efficient, which is shown in Table 2.

Table.2. Measure of Delay (ms)

Data Packets Sent	DLDM	TSRS	MNDREL	Proposed SCB-LSCS	Proposed SCMSC-GMCS
25	120	115	118	95	103
50	122	117	119	97	104
75	125	119	121	98	106
100	127	121	122	100	107
125	129	123	123	102	108
150	130	125	124	104	109
175	132	127	126	106	111
200	134	129	127	108	113
225	135	130	128	110	114
250	137	132	129	112	115

Simulation results of delay using proposed GKCOUCS-SIDNL technique is minimized by 33%, 41% and 36% as compared to DLDM, trustable and secure routing scheme and MNDREL respectively. Similarly, the delay of SCB-LSCS technique is reduced by 21%, 31% and 25% than the existing methods. In addition, delay in SCMSC-GMCS is decreased by 14%, 25% and 18% as compared to conventional methods.

4.2.3 Performance Analysis of Routing Overhead:

Routing overhead is calculated as the time taken to route data packet to attain secure data communication between source and destination nodes. In other words, it is defined with the total data packets and time taken by each packet for routing. Routing overhead is computed in terms of milliseconds (ms), which is shown in Table 3.

Table.3. Measure of Routing Overhead (ms)

Data Packets Sent	DLDM	TSRS	MNDREL	Proposed SCB-LSCS	Proposed SCMSC-GMCS
25	220	210	215	160	185
50	225	215	218	165	190
75	230	220	220	170	193
100	235	225	225	175	195
125	240	230	230	180	200
150	245	235	235	185	205
175	250	240	240	190	210
200	255	245	245	195	213

225	260	250	248	200	215
250	265	255	250	205	220

Results of GKCOUCS-SIDNL technique illustrates that the routing overhead is minimized by 36%, 57% and 51% as compared to the existing DLDM, trustable, secure routing scheme and MNDREL. Likewise, routing overhead of SCB-LSCS method is decreased by 27%, 51% and 43% than the conventional methods. Proposed SCMSC-GMCS reduces the routing overhead by 15%, 43% and 34% than the existing methods

4.2.4 Performance Analysis of Attack Detection Accuracy:

Attack detection accuracy is computed as the ratio of data packets attack being detected correctly to the total data packet being attacked. It is determined in terms of percentage (%). Higher value of attack detection accuracy indicates the better performance of the method which is shown in Table 4.

Table.4. Measure of Attack Detection Accuracy

Data Packets Sent	DLDM	TSRS	MNDREL	Proposed SCB-LSCS	Proposed SCMSC-GMCS
25	71	65	68	77	74
50	72	66	69	78	75
75	73	67	70	79	76
100	74	68	71	80	77
125	75	69	72	81	78
150	76	70	73	82	79
175	77	71	74	83	80
200	78	72	75	84	81
225	79	73	76	85	82
250	80	74	77	86	83

Simulation results of attack detection accuracy using proposed GKCOUCS-SIDNL technique is improved by 9%, 34% and 29% as compared to the existing DLDM, trustable, secure routing scheme and MNDREL respectively. In addition, attack detection accuracy of SCB-LSCS method is increased by 6%, 29% and 25% than the existing DLDM, trustable, secure routing scheme and MNDREL respectively. SCMSC-GMCS improves the attack detection accuracy by 3%, 26% and 21% as compared to the existing DLDM, trustable, secure routing scheme and MNDREL respectively.

5. CONCLUSIONS

In the simulation conduction, the performance of proposed SCMSC-GMCS technique, SCB-LSCS method and GKCOUCS-SIDNL technique is compared with existing MNDREL approach, trustable and secure routing scheme and DLDM. Results of the proposed and existing methods are compared with various performance metrics. As observed in the results, proposed GKCOUCS-SIDNL technique performs efficient attack detection and secures the data transmission with higher attack detection accuracy, packet delivery ratio and lower delay and routing overhead.

Future work can explore the integration of more advanced machine learning algorithms, such as reinforcement learning, to dynamically adapt to evolving attack patterns in WSNs. Additionally, implementing real-time anomaly detection techniques and expanding the system's applicability to other critical domains, like healthcare and industrial monitoring, could further enhance its versatility and effectiveness. Testing the proposed methods in larger-scale networks with diverse environmental conditions will also help validate and improve the robustness of the solution.

REFERENCES

[1] S. Rajesh and A.N. Jayanthi, "Clustered Certificateless Signcryption for Blackhole Attack Detection in Secured Wireless Sensor Networks", *Tierarztliche Praxis*, Vol.41, pp. 1-9, 2021.

[2] S. Rajesh, A.N. Jayanthi and J. Mala, "Spatially Correlated Boltzmann Deep Learning Lamport Session Discrete Certificateless Signcryption for Dos Attack Detection and Secured WSN Communication", *Proceedings of International Conference on Electronics and Renewable Systems*, pp. 1-13, 2022.

[3] B. Ahmad, W. Jian, R.N. Enam and A. Abbas, "Classification of DoS Attacks in Smart Underwater Wireless Sensor Network", *Wireless Personal Communications*, Vol. 116, No. 2, pp. 1055-1069, 2021.

[4] R. Ahmad, R. Wazirali, Q. Bsoul, T. Abu-Ain and W. Abu-Ain, "Feature-Selection and Mutual-Clustering Approaches to Improve Dos Detection and Maintain WSNS' Lifetime", *Sensors*, Vol. 21, No. 14, pp. 4821-4836, 2021.

[5] S. Aissani and B. Abbache, "Secure Key Management System Integrated in Cell-LEACH", *Wireless Personal Communications*, Vol. 112, No. 4, pp. 2109-2129, 2020.

[6] T.A. Alghamdi, "Convolutional Technique for Enhancing Security in Wireless Sensor Networks Against Malicious Nodes", *Human-Centric Computing and Information Sciences*, Vol. 9, No. 1, pp. 1-10, 2019.

[7] W. Alghamdi, M. Rezvani, H. Wu and S.S. Kanhere, "Routing-Aware and Malicious Node Detection in a Concealed Data Aggregation for WSNs", *ACM Transactions on Sensor Networks*, Vol. 15, No. 2, pp. 1-20, 2019.

[8] B.H. Ali, N. Sulaiman, S.A.R. Al-Haddad, R. Atan, S.L.M. Hassan and M. Alghrairi, "Identification of Distributed Denial of Services Anomalies by using Combination of Entropy and Sequential Probabilities Ratio Test Methods", *Sensors*, Vol. 21, No. 19, pp. 6453-6469, 2021.

[9] I.M. Almomani and M. Alenezi, "Efficient Denial of Service Attacks Detection in Wireless Sensor Networks", *Journal of Information Science and Engineering*, Vol. 34, No. 4, pp. 977-1000, 2018.

[10] L. Alsulaiman and S. Al-Ahmadi, "Performance Evaluation of Machine Learning Techniques for DOS Detection in Wireless Sensor Network", *International Journal of Network Security and Its Applications*, Vol.13, No.2, pp. 1-9, 2021.

[11] M. Ramkumar, J. Logeshwaran and T. Husna, "CEA: Certification based Encryption Algorithm for Enhanced Data Protection in Social Networks", *Fundamentals of*

Applied Mathematics and Soft Computing, Vol. 1, pp. 161-170, 2022.

[12] B. Gobinathan, M.A. Mukunthan, S. Surendran, K. Somasundaram, S.A. Moeed, P. Niranjan and V.P. Sundramurthy, "A Novel Method to Solve Real Time Security Issues in Software Industry using Advanced Cryptographic Techniques", *Scientific Programming*, pp. 1-9, 2021.

[13] V.A.K. Gorantla, S.K. Sriramulugari, B. Gorantla and K. Singh, "Optimizing Performance of Cloud Computing Management Algorithm for High-Traffic Networks", *Proceedings of International Conference on Disruptive Technologies*, pp. 482-487, 2024.

[14] Nakkl Masuda, Goce Jakimoski, Kazuyuki Aihara and Ljupco Kocarev, "Chaotic Block Ciphers: from Theory to Practical Algorithms", *IEEE Transactions on Circuits and Systems I: Regular Papers*, Vol. 53, No. 6, pp. 1341-1352, 2006.

[15] K.T. Atanassov, "Intuitionistic Fuzzy Sets", *Fuzzy Sets and Systems*, Vol. 20, No. 1, pp. 87-96, 1986.

[16] S.F. Sultana and D.C. Shubhangi, "Video Encryption Algorithm and Key Management using Perfect Shuffle", *International Journal of Engineering Research and Applications*, Vol. 7, No. 2, pp. 1-5, 2017.

[17] Mousa Farajallah, Z Fawaz, Safwan E1 Assad and Olivier Dforges, "Efficient Image Encryption and Authentication Scheme based on Chaotic Sequences", *Proceedings of International Conference on Emerging Security Information Systems and Technologies*, pp. 150-155, 2013.