Mitigating DDoS Attacks in Virtual Machine Migration: An In-Depth Security Framework Utilizing Deep Learning and Advanced Encryption Techniques

Venkata Subramanian N., Shankar Sriram V S.

Abstract:** Safeguarding virtual machines (VMs) during migration is essential to avert Service Level Agreement (SLA) violations. This research article presents a robust security framework that utilizes deep learning and advanced encryption methods to reduce the impact of Distributed Denial of Service (DDoS) attacks during virtual machine migration. The study introduces an Improved Sparrow Search Algorithm-based Deep Neural Network (ISSA-DNN) for classifying DDoS attacks. It utilises Advanced Encryption Standard-Elliptic Curve Cryptography (AES-ECC) to safeguard virtual machine images. The primary objective is to mitigate the risks associated with VM migration by identifying DDoS attacks and safeguarding VMs using advanced cryptographic techniques. The research utilises the Canadian Institute for Cybersecurity Distributed Denial of Service (CICDDoS) dataset, implementing preprocessing procedures such as duplicate elimination, feature selection via Random Forest, and normalisation to enhance the precision of the DNN classifier. The ISSA-DNN approach enhances hyperparameter optimization by inverse mutation-based sparrow search, yielding a precise attack classification model. Furthermore, the research incorporates AES-ECC for encrypting VM images, amalgamating AES's computational efficiency with ECC's improved security. In contrast to conventional methods, this hybrid encryption approach enhances throughput and reduces encryption and decryption durations, making it suitable for high-throughput and real-time applications. Experimental findings indicate that the proposed ISSA-DNN attains a classification accuracy of 98.79%, surpassing current state-of-the-art techniques. The AES-ECC encryption technique markedly enhances performance metrics, safeguarding the security of virtual machines during migration. This proactive security policy safeguards sensitive data and ensures compliance with regulatory standards. In conclusion, the established framework offers a comprehensive solution for mitigating DDoS attacks and safeguarding VM migration via advanced deep learning and encryption methodologies. Integrating ISSA-DNN for attack classification and AES-ECC for encryption provides a robust approach to enhancing cybersecurity in cloud environments.

***Keywords:** AES-ECC Hybrid Encryption, Cloud Infrastructure Security, Deep Neural Network (DNN) for Cybersecurity, Distributed Denial of Service (DDoS) Attack Detection, Random Forest Feature Selection, Virtual Machine (VM) Migration Security*

Manuscript received on 27 December 2024 | First Revised Manuscript received on 02 January 2025 | Second Revised Manuscript received on 07 January 2025 | Manuscript Accepted on 15 January 2025 | Manuscript published on 30 January 2025.
*Correspondence Author(s)

Dr. Venkata Subramanian N.*, School of Computing, SASTRA Deemed-to-be University, Thanjavur (Tamil Nadu), India. Email ID: tyrvenkat@mca.sastra.edu, ORCID ID: 0000-0001-8096-742X

Dr. Shankar Sriram V S., Centre for Information Super Highway (CISH), School of Computing, SASTRA Deemed-to-be University, Thanjavur (Tamil Nadu), India. Email ID: sriram@it.sastra.edu ORCID ID: 0000-0001-7870-7944

I. INTRODUCTION

The cloud has revolutionised resource utilisation by prioritising demand over geography. Although cloud computing offers numerous benefits, it also presents certain obstacles, with security being a prominent concern. Security has gained significant importance in Infrastructure as a Service (IaaS), where resources are shared and accessed by multiple users. [1]. Distributed Denial of Service (DDoS) attacks pose a significant threat to cloud services, potentially causing substantial harm to these systems. A DDoS attack is [2] A significant attack that explicitly aims to disrupt the availability of cloud services, rendering them inaccessible to users. Cloud computing poses a higher level of risk compared to traditional infrastructure-based systems. Upon initiating an attack on a physical machine (PM), the utilization of resources escalates expeditiously [3]. Hence, cloud management implements autoscaling to allocate additional resources to the server. This ongoing resource allocation process might result in significant resource wastage if an attack remains undetected and unmitigated. In addition, many virtual machines (VMs) are operated on a single physical server [4]When an attacker targets a VM, it has a detrimental impact on the other VMs operating on the same server [5]. The expenses and importance of hosting, maintaining, and securing PMs and VMs have significantly increased. Therefore, analysing and classifying network data is crucial to prevent additional attacks during virtual machine migration. Due to the rise in invasions, the expansion of data dimensions, and the advancements in deep learning [6]Researchers have started exploring deep learning for detecting DDoS attacks [7].

In recent years, Deep Neural Networks (DNNs) have been used to detect DDoS attacks [8]. Thus, the proposed system employs DNN to categorize DDoS attacks accurately. Nevertheless, a comprehensive dataset should be preprocessed to train the attack classification model. In addition, it guarantees the security of the VM to be migrated [9]. The Advanced Encryption Standard (AES) has been employed to encrypt the VM image.

AES is chosen for its notable efficiency in computation and robust security measures. The symmetric key used in

AES has been enhanced with additional security measures, utilising Elliptic Curve Cryptography (ECC), to protect its integrity further. The subsequent step involves encrypting and migrating the VMs.

II. LITERATURE SURVEY

In the dynamic landscape of cloud computing, live VM migration has become a critical aspect for ensuring resource optimization, load balancing, and efficient infrastructure utilization. However, with the increasing threat of distributed denial of service (DDoS) attacks, it is imperative that organizations carefully consider the classification of DDoS attacks and the security of VM images using cryptographic techniques during live VM migration.

A. DDoS Attack Classification

Researchers in the cloud computing environment have developed numerous detection and prevention models to counter Distributed Denial of Service (DDoS) attacks. Many DL and cloud-based machine learning methodologies are employed to conduct these investigations. An overview of the publications is presented below.

Phan et al [10]. Proposed a new defence mechanism against DDoS attacks by combining machine learning and an improved IP Filtering scheme called enhanced History-based IP Filtering (eHIPF). This approach aims to improve the detection rate and speed of traffic classification compared to the traditional HIPF method. To detect DDoS attacks on cloud platforms, Bhardwaj et al [11]. Developed the Naive Auto Encoder (AE) with a Deep Neural Network (DNN) model. David et al [12]. Developed a detection technique for DDoS attacks based on entropy using a Generalized Auto Regressive Conditional Heteroskedasticity (GARCH) model. Prathyusha et al [13]. Implemented the Artificial Immune System in the cloud environment to defend against DDoS attacks by meticulously selecting relevant attributes. Vuong et al [14]. Proposed a sophisticated machine-learning approach to identify and classify malicious attacks. Gupta et al [15]. Designed a Network Intrusion Detection System (NIDS) using LSTM and the Improved One-vs-One (I-OVO) approach. Wei et al [16]. Proposed a hybrid approach integrating two deep learning algorithms to identify and classify DDoS attacks effectively. Khempetch et al [17]. Introduced the CIC-DDoS2019 dataset to address shortcomings and propose a new classification system for DDoS attacks. Agarwal et al [18]. Proposed an approach that successfully integrates feature selection, a whale optimization technique, and a DNN to counteract DDoS attacks. Batchu et al [19]. Proposed an innovative approach to tackle challenges associated with DDoS attack detection, utilizing data preparation, adaptive synthetic oversampling, SHAP feature importance, and recursive feature elimination.

As indicated by the publications above, real-time detection of DDoS attacks is challenging due to extraneous attributes, ambiguity, and an unbalanced class distribution. Traditional detection systems demonstrate limited efficacy in discerning intricate attack patterns, exhibit deficiencies in comprehending complex attack mechanisms, and encounter challenges when confronted with diverse types of attacks.

B. Cryptographic Security for VM Images

Preserving the confidentiality, integrity, and authenticity of virtual environments requires that VM images be protected cryptographically. Organisations can protect highly sensitive information by reducing the likelihood of unauthorised access or manipulation and implementing encryption protocols. The security of VM images is of the utmost importance, given the increasing reliance on virtualisation and the expanding use of cloud computing; therefore, a cryptographic security framework is indispensable.

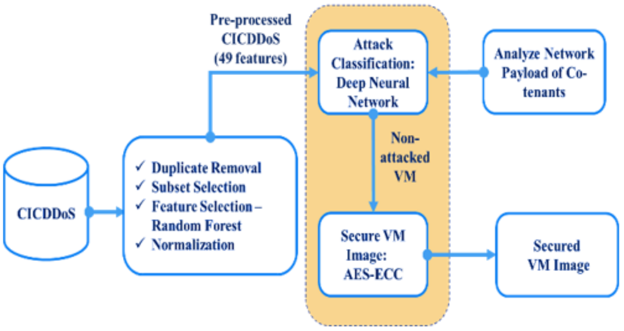
The research conducted by Disha H. Parekh et al [20]. Focuses on enhancing security in cloud computing by addressing vulnerabilities associated with third parties and proposing a practical model that integrates Public-Key Infrastructure to bolster cryptography. Further, a two-tier cryptographic protocol [21] Symmetric (AES) and asymmetric (ECC) algorithms have been proposed to safeguard data integrity and privacy while enhancing operational speed. Additionally, Ashish Nanda et al [22]. Developed a novel routing protocol featuring a hybrid encryption technique to reinforce multilayer security, demonstrating improved performance through reduced encryption time—lastly, Aliev et al [23]. Introduced a matrix-based security system for vehicle ad-hoc networks that outperforms existing privacy measures, while Bechir Alaya et al [24]. Implemented a multi-objective algorithm that optimises performance metrics through a sophisticated key management method, incorporating symmetric and asymmetric encryption strategies. The authors [25] Advocate using AES and ECC to bolster system security, though this hybrid method increases computational costs and time. To ensure secure cloud services, algorithms like AES, DES, and Blowfish [26] Maintain data integrity, prevent user conflicts, and safeguard individual data. Service providers manage prompt and controlled access to data. Rehman et al [21]. Combined ECC and AES to hide cloud data, address key size issues, and optimize memory with minimal computational resources. Still, they couldn't prevent denial-of-service, reply, plaintext, and impersonation attacks. P. Chinnasamy et al [27]. Integrated ECC and Blowfish, offering enhanced security and confidentiality for patient data compared to existing systems. Vikas K. Soman et al [28]. Explored a hybrid cryptographic method for secure cloud data storage, addressing security concerns. Francis K. Mupila et al [29]. Developed a framework with encrypted certificates and token accumulation based on user location, improving security against data loss and cyberattacks, though further research on practicality and scalability is needed. Saxena et al [30]. Introduced a secure VM deployment algorithm using WOGA, reducing latency and enabling energy-efficient resource allocation. Fursan Thabit et al [31]. Presented a two-layer homomorphic encryption technique that enhances data security with better encryption time and memory use. Binita Thakkar et al [32]. Created a multilevel encryption method that combines DES, mixed transposition, and Blowfish, thereby strengthening data security but requiring further implementation research. Fagul Pandey et al [33]. Developed a software-based private key generation using user emails, ensuring randomness and reliability in data transmission security.

The aforementioned research findings indicate that an effective encryption model and a streamlined system for classifying DDoS attacks are imperative for migrating the VM image.

III. IMPROVED DEEP NEURAL NETWORK FOR ATTACK CLASSIFICATION AND VM SECURITY ENFORCEMENT

In a Live VM Migration, security vulnerabilities are more likely to occur if resources are not anticipated in advance and the destination is chosen without considering potential security threats that may arise during the migration. Hence, the proposed system incorporates two key strategies: classification of DDoS attacks and security enforcement for VMs designated for migration.

However, preprocessing is required before executing the two strategies listed above.


Pre-processed CICDDoS (49 features)
Attack Classification: Deep Neural Network
Analyze Network Payload of Co-tenants
CICDDoS
✓ Duplicate Removal
✓ Subset Selection
✓ Feature Selection – Random Forest
✓ Normalization
Non-attacked VM
Secure VM Image: AES-ECC
Secured VM Image

[Fig.1: Overview of the Proposed ISSA-DNN-ENC]

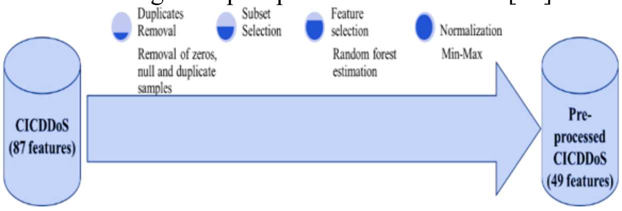
However, preprocessing is required before executing the two strategies listed above. The Canadian Institute for Cyber Security Distributed Denial of Service (CICDDoS) dataset has been considered for validation purposes. It has undergone various preprocessing steps, including duplicate removal, feature selection, and normalisation. For the classification of DDoS attacks, an Improved Sparrow Search algorithm-based Deep Neural Network (ISSA-DNN) is utilised, and the underlying cause of physical machine overload has been identified. Consequently, VM images are encrypted. The overview architecture of the proposed ISSA-DNN-ENC system is depicted in Fig. 1.

The proposed system is organized into three distinct phases. The first phase focuses on pre-processing, followed by the second phase, which involves attack classification. The final phase consists of implementing encryption measures to ensure VM security.

A. Data Preprocessing

Data preprocessing plays a crucial role in analysing the CICDDoS dataset due to the presence of intricate and noisy data. The effectiveness of the classification model is significantly impacted by the data quality, emphasizing the importance of preprocessing [34]. To minimise overfitting or bias in analysis, suitable preprocessing techniques should be implemented to enhance the model's precision and reliability.

Hence, the dataset is first processed to eliminate duplicates, and then a subset is chosen. To balance the dataset for subsequent classification, an equal number of samples from all attack types were randomly selected, proportionate to the number of benign samples present in the dataset [35].

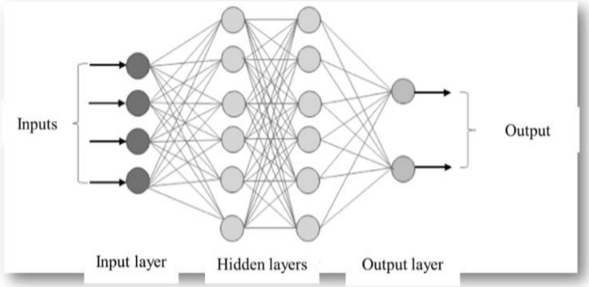


[Fig.2: An Outline of the Preprocessing Phase]

The feature selection process enables the identification and selection of the key features that are important for classification. Furthermore, Random Forest is employed as a feature selector in the proposed system since it offers advantages like high-dimensional data handling, robustness in overfitting, and suitability for ensemble learning in class imbalance problems. The selected features are normalized to align the different scales of values in the same range. An outline of the preprocessing is presented in Fig. 2.

B. Attacks Classification using Improved Sparrow Search-Based Deep Neural Network (ISSA-DNN)

The proposed system categorises network traffic by assessing the likelihood of a DDoS attack on a physical machine using a deep neural network (DNN). The DNN uses a multi-layered architecture, inferring intricate patterns and correlations. The research introduces a novel inverse mutation-based sparrow search method to optimize hyperparameters and improve performance. An overview of the DNN architecture as a binary classifier is drawn in Fig. 3.



[Fig.3: Overview of the DNN Architecture as a Binary Classifier]

The Sparrow search algorithm (SSA) [36] It is a traditional method used to find food for sparrows. It involves producers and scroungers, with the best sparrows acting as producers. However, due to its searchability, SSA can fall into a local minima trap. Inversion mutation, a proposed alternative, enhances population variety and minimises this issue [37]. This technique can be applied to the sparrow's search optimization life cycle to generate novel solutions and prevent stagnation in local optima.

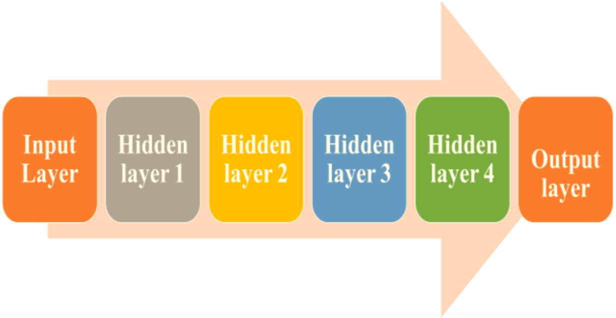
i. Improved Sparrow Search Algorithm (ISSA)

The algorithm involves initializing parameters such as population size, learning rate, number of hidden layers, batch size, number of epochs, and searching space area. The fitness value of the total number of sparrows is calculated using the G_y function, with producers with higher fitness values preceding the search process. Inversion mutations are applied to avoid local optimums. The location of producers is updated using the formula.

$$y_{a,b}^{i+1} = \begin{cases} y_{a,b}^{i} * exp\left(\frac{-a}{\hbar * I_m}\right), if W_1 < S_v \\ y_{a,b}^{i} + D * V, if W_2 \geq S_v \end{cases} \quad \dots \quad (1)$$

ii. Attack Classification

This system aims to classify network traffic by evaluating the probability of a DDoS attack against the physical machine. Attack classification is performed using a DNN. To enhance the performance of the attack classification, the hyperparameters of the DNN are tuned using inverse mutation-based SSA. A DNN is generally identical to a neural network (NN), with the key distinction being that a DNN contains four or more hidden layers positioned between the input and output layers. A massive dataset significantly enhances the efficacy of this DL approach. Fig. 4 shows the proposed DNN architecture layer arrangement.



[Fig.4: Layers Arrangement of Proposed DNN Architecture]

The proposed DNN architecture comprises the following components: an input layer, four hidden layers, and a dense output layer. Eqs. (2) through (14) represent the computation procedure for each layer.

$$C_{h1} = Wt_1 .\mathrm{x} + bs_1 \quad \dots \quad (2)$$

$$Actv_1 = \mathrm{ReLU}(C_{h1}) \quad \dots \quad (3)$$

$$Actv_1 = \mathrm{ReLU}(C_{h1}) \quad \dots \quad (4)$$

$$Drp_1 = Dropout(Actv_1) \quad \dots \quad (5)$$

$$C_{h2} = Wt_2 .Drp_1 + bs_2 \quad \dots \quad (6)$$

$$Actv_2 = \mathrm{ReLU}\ (C_{h2}) \quad \dots \quad (7)$$

$$Drp_2 = Dropout(Actv_2) \quad \dots \quad (8)$$

$$C_{h3} = Wt_3 .Drp_2 + bs_3 \quad \dots \quad (9)$$

$$Actv_3 = \mathrm{ReLU}\ (C_{h3}) \quad \dots \quad (10)$$

$$Drp_3 = Dropout(Actv_3) \quad \dots \quad (11)$$

$$C_{h4} = Wt_4 .Drp_4 + bs_4 \quad \dots \quad (12)$$

$$Actv_4 = \mathrm{ReLU}\ (C_{h4}) \quad \dots \quad (13)$$

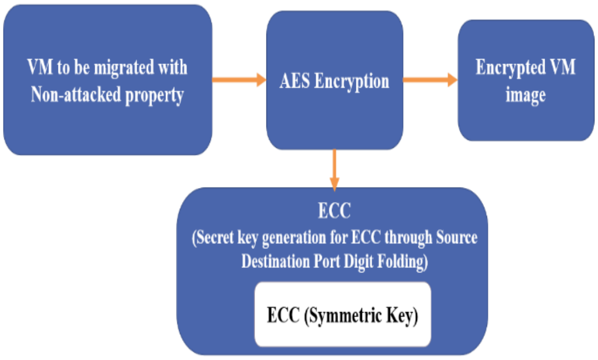
$$Drp_4 = Dropout(Actv_4) \quad \dots \quad (14)$$

$$FBC = \sigma\left(Wt_o .Drp_4 + bs_0\right) \quad \dots \quad (15)$$

Where, $C_{h1}, C_{h2}, C_{h3}, C_{h4}$ Are the outputs of the first and second hidden layers, Wt_1 Is the weight factor of the first hidden layer, which is multiplied by the input x in the first hidden layer? Wt_2 Is the weight factor of the second hidden layer, which is multiplied by the first dropout value in the second hidden layer? Wt_3 Is the weight factor of the third hidden layer, which is multiplied by the second dropout value in the third hidden layer? Wt_4 Is the weight factor of the fourth hidden layer, which is multiplied by the third dropout value in the fourth hidden layer? bs_1, bs_2, bs_3, bs_4 Are the bias terms for the first to fourth hidden layers, and $Actv_1, Actv_2, Actv_3, Actv_4$ Are the activation functions output for four hidden layers? $FBC\ It\ It\ It$ It is the final binary classification output.

iii. VM Security (AES-ECC)

VM image security safeguards digital data against corruption, fraud, and unauthorized access during migration [38]. Hardware-based solutions limit read and write privileges, whereas software-based solutions utilise encryption to protect against unauthorised access. This proposed system utilises a software-based security solution, where the symmetric key is encrypted using ECC and the VM image is encrypted using AES. This enhances the security of the symmetric key. The proposed encryption procedure is illustrated in Fig. 5.


VM to be migrated with Non-attacked property
AES Encryption
Encrypted VM image
ECC
(Secret key generation for ECC through Source Destination Port Digit Folding)
ECC (Symmetric Key)

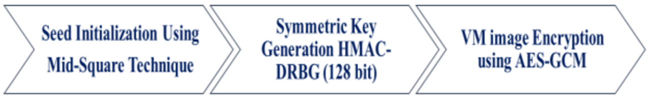
[Fig.5: Layout of the Proposed VM Image Encryption]

iv. Symmetric Key Generation using HMAC-Based Deterministic Random Bit Generator (HMAC-DRBG)

The CICDDoS dataset utilises source and destination ports to analyse network traffic, detect abnormalities, understand protocols, and identify trends in DDoS attacks. These ports are used in symmetric key generation using the HMAC-based Deterministic Random Bit Generator (HMAC-DRBG) [39]. The process involves two phases: seed initialization using the mid-square technique, which generates unique keys, and key generation using HMC-DRBG. Secure implementation requires attention to entropy sources, reseeding techniques, compliance with standards, and safe management of generated keys. Reputable cryptographic libraries should adhere to these standards.

v. VM Image Encryption using Advanced Encryption Standard

The Advanced Encryption Standard (AES) is a crucial component of modern cryptography, protecting confidential data. It uses a symmetric-key encryption technique and processes data in fixed-size blocks with key sizes of 128, 192, or 256 bits. [40]. AES offers various data security modes, including Galois/Counter Mode (GCM), Electronic Code Book (ECB) [41]Cypher-Block Chaining (CBC), and Counter Mode (CTR) [42]. The AES-GCM mode, used in this research, utilises the Counter (CTR) mode for encryption, enabling parallel block encryption. This design allows parallelization of software and hardware implementations, enhancing AES's performance. However, its parallelism and combined encryption/authentication capability make it more efficient for handling larger VM images [43]. Fig. 6 illustrates the phases of VM Image Encryption.


Seed Initialization Using Mid-Square Technique
Symmetric Key Generation HMAC-DRBG (128 bit)
VM image Encryption using AES-GCM

[Fig.6: Phases of VM Image Encryption]

The pseudocode for the VM image encryption is shown in pseudocode 1.

Pseudocode 1 VM Image Encryption

```
# Step 1: Initial Seed Generation
function mid_sqr_seed_gen (SDP):
    #SDP – Concatenated Source and Destination Port numbers
    sqr = Pow (SDP,2) IS_mid_digs = extr_mid_digs(sqr)
    If len(IS_mid_digs >= thrshld):
        return substr(IS_mid_digs,16)
    Else:
        mid_sqr_seed_gen(IS_mid_digs)
# Step 2: HMAC-DRBG-Based KeyGen
function gen_sym_key(IS_mid_digs):
    sym_k=HMAC_DRBG(concat(IS_mid_digs,spl_chars))
    return sym_k
# Step 3: AES-GCM Enc
function Enc_AES (VM_Image, sym_k):
    in_v = gen_in_v() # Init_Vector Gen
    Enc_VM_image = AES_GCM.Enc (VM_Image, sym_k, in_v)
    return Enc_VM_image
```

vi. Symmetric Key Security using Elliptic Curve Cryptography (ECC)

The elliptic curve cryptographic system (ECC) generates public and private keys using mathematical principles derived from elliptic curves. ECC [44] It is faster and has a shorter secret key than RSA. [45]. This work proposes an improved ECC to enhance system security. The standard form generates two types of keys, while the improved form generates a third key (secret key) using the Source Destination Port Digit Folding technique. This secret key is used for both encryption and decryption, further enhancing security. The ECC is used as the cryptographic key algorithm where the elliptical curve is defined as,

$$h^3 = (u^3 + uv + z) mod\ PRM \quad \dots \quad (19)$$

Where u, z Are two integer constants, h, v Denote the parameters that define the function and PRM It is a larger prime number. The user can encrypt the message with the receiver's public key, and the receiver will decrypt the data using their private key. Private and public keys are generated to perform encryption and decryption. The equation used to create the public key is,

$$P = \sigma * R \quad \dots \quad (15)$$

Where P denotes the public key, R denotes the randomly generated private key using the secp256r1 specification, σIs the point on the curve? Additionally, the secret key is obtained using the digit folding method, as outlined in Eqs. (16) and (17).

$$\varepsilon = median\ (small\ prime, large\ prime) \ \dots \quad (16)$$

$$F_d = (A + B + C)\ mod\ \varepsilon \quad \dots \quad (17)$$

Where, $A, B$and C denotes the prerequisite keys with the concatenated value of source and destination port numbers, broken into three parts, ε Value has been determined by calculating the median between small and larger prime numbers within the source and destination port numbers. Hence, F_dThe generated secret key will play a role in the encryption and decryption process. To execute encryption, Equations (18) and (19) show the output: two ciphertexts derived from the input data (symmetric key), a secret key that is generated, and the public key of the recipient.

$$T_1 = (\sigma * \Psi) * F_d \quad \dots \quad (18)$$

$$T_2 = (S_K + P * \Psi) * F_d \quad \dots \quad (19)$$

Where Ψ It is a random number within the range (1, n-1), S_K Is the input to be encrypted? σ Is the point on the curve? F_d is the secret key, P is the public key, T_1 *and* T_2 Are the generated ciphertexts. During the encryption process, the secret key was multiplied by two ciphertexts.

During the decryption process, two ciphertexts, the recipient's private and secret keys, are used to extract the symmetric key. The extracted symmetric key can decrypt the VM image using the AES technique in the destination system. The decryption process can be visualised using Eq. (20).

$$SymKey = \frac{T_2 - R * T_1}{F_d} \quad \dots \quad (20)$$

IV. EXPERIMENTAL ANALYSIS

The proposed system aims to categorise DDoS attacks and implement security measures for securely migrating virtual machines. It is implemented using Python and the CICDDoS dataset. The model's efficacy is assessed by comparing its results with those of other models, as shown in Fig. 7.

Experimental Analysis
Performance analysis on Feature Selection
Performance Analysis of Attacks classification
Performance Analysis of VM Image security

[Fig.7: Experimental Analysis of Proposed System]

A. Dataset Description

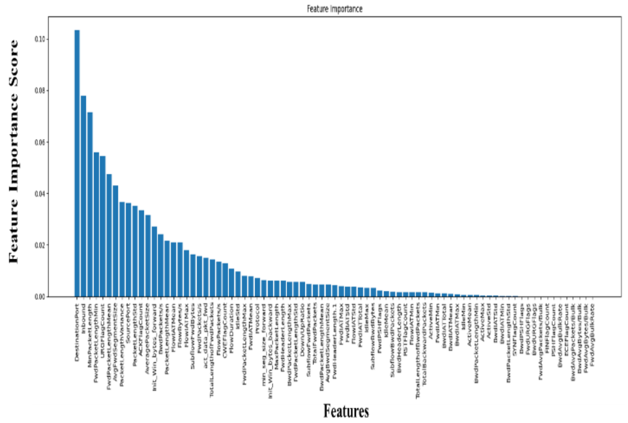
CICDoS-2019 presents real-world DDoS attacks and network traffic analysis results using CICFlowMeter-V3, labelled by IP addresses, ports, protocols, and attacks [40].

B. Performance Analysis of Feature Selection

The effectiveness of the Random Forest feature selection technique is evaluated by calculating the significance of each feature in the CICDDoS dataset using the Random Forest Estimator. A total of 49 essential Features (Table 1) were identified with improved accuracy, as shown in Fig. 8.

Table 1: List of Selected Features from the CICDDoS Dataset using Random Forest

S.No	Features	S.No	Features
1	Source IP	26	Fwd PSH Flags
2	Source Port	27	Fwd Header Length
3	Destination IP	28	Fwd Packets/s
4	Destination Port	29	Bwd Packets/s
5	Protocol	30	Min Packet Length
6	Flow Duration	31	Max Packet Length
7	Total Fwd Packets	32	Act data pkt fwd
8	TotalLen Fwd Packets	33	Idle Std
9	Fwd Packet Length Max	34	PKT Length Mean
10	Fwd Packet Length Min	35	Packet Length Std
11	Fwd Packet Length Mean	36	Packet Length Variance
12	Fwd Packet Length Std	37	ACK Flag Count
13	Bwd Packet Length Max	38	URG Flag Count
14	Bwd Packet Length Mean	39	Down/Up Ratio
15	Init_Win_bytes_backward	40	Average Packet Size
16	Idle Mean	41	Avg Fwd Segment Size
17	Inbound	42	Avg Bwd Segment Size
18	FlowBytes/s	43	Fwd Header Length
19	Flow Packets/s	44	Subflow Fwd Packets
20	Flow IAT Mean	45	Subflow Fwd Bytes
21	Flow IAT Std	46	Subflow Bwd Bytes
22	Flow IAT Max	47	Init_Win bytes forward
23	Fwd IAT Total	48	Min seg size forward
24	Fwd IAT Mean	49	Idle Max
25	Fwd IAT Max		



[Fig.8: Calculated Features Importance using Random Forest]

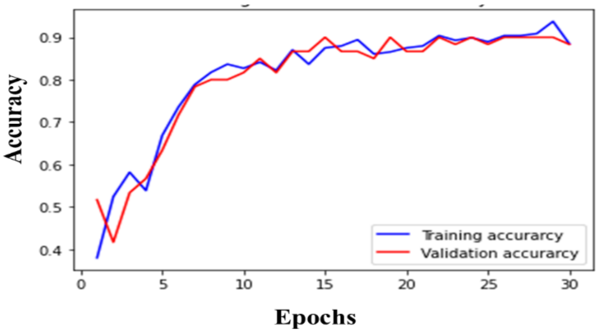
C. Performance Analysis of ISSA-DNN-Based Classification

This section discusses the use of ISSA to determine the optimal configuration of network hyperparameters for accurate classification. The proposed ISSA-DNN achieves superior outcomes with optimal parameters of 64:16 neurons, 120 batches, a learning rate of 0.001, and 30 epochs. The results are compared with existing models, including Generative Adversarial Networks (GAN), LSTM, Multi-Layer Perceptron (MLP), CNN, and Feature Selection-Whale Optimisation Algorithm-Deep Neural Network (FS–WOA–DNN). Table 2 tabulates the accuracy, precision, recall, and f-measure of the proposed ISSA-DNN.

Table 2: Performance Analysis of ISSA-DNN-Based Classification

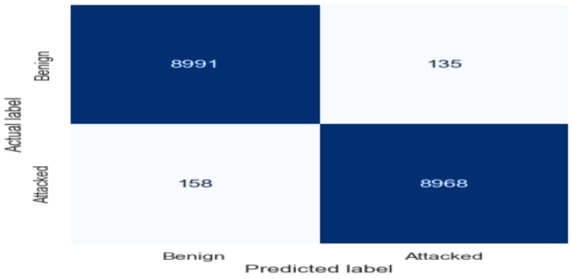
Techniques / Metrics	Accuracy (%)	Precision (%)	Recall (%)	F-Measure (%)
GAN [46]	94.38	94.08	97.89	95.94
LSTM [47]	90.29	90.12	89.43	89.77
MLP [48]	92.12	92.12	84.68	88.80
CNN [49]	94.08	96.32	86.29	91.02
FS-WOA–DNN [18]	95.35	96.9	90.71	96.28
Proposed ISSA-DNN	98.79	98.51	98.26	98.33

In Table 2, the ISSA-DNN classification model outperforms existing models in terms of accuracy, precision, recall, and f-measure values. It enhances these by 3.44%, 1.61%, 7.55%, and 2.05% compared to the existing FS-WOA-DNN technique, achieving a classification accuracy of 98.79% (Fig. 9).



[Fig.9: Accuracy Graph of the Proposed ISSA-DNN Classification System]

However, there is no significant improvement after 30 epochs, as shown in Fig. 10, which represents the confusion matrix of the proposed classification system.



[Fig.10: Confusion Matrix of the Proposed ISSA-DNN Classification System]

From Fig. 10, it is evident from the confusion matrix that the proposed ISSA-DNN accurately classifies 8,991 samples as legitimate and 8,968 as malicious.

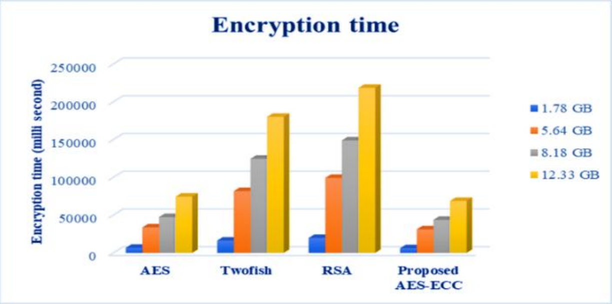
D. Performance Analysis of AES-ECC-Based Cryptography

The performance of the proposed AES-ECC is evaluated in terms of encryption time, decryption time, and throughput. The outcomes are compared with those of Conventional AES, Twofish, and Rivest-Shamir-Adleman (RSA) approaches.

Published By:
Blue Eyes Intelligence Engineering
and Sciences Publication (BEIESP)
© Copyright: All rights reserved.

i. Encryption Time

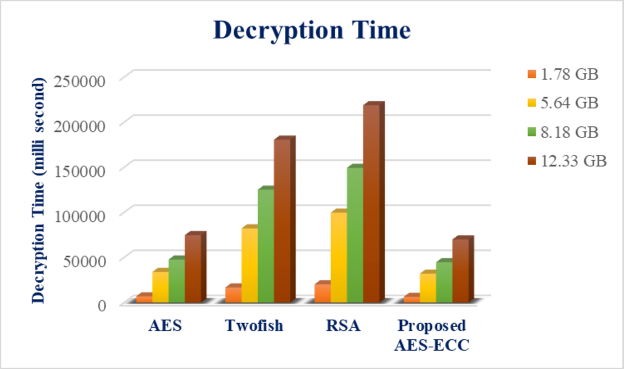
The proposed cryptographic solution significantly reduces encryption time (Fig. 11) by 13109 and 9620 ms compared to existing models (1.78 GB VM image), particularly for real-time or high-throughput applications. This is achieved by utilising four virtual machine images (1.78 GB, 5.64 GB, 8.18 GB, and 12.33 GB) and considering factors such as cryptographic strength, key management, algorithm agility, and compliance with standards.



[Fig.11: Performance Analysis in Terms of Encryption Time]

ii. Decryption Time

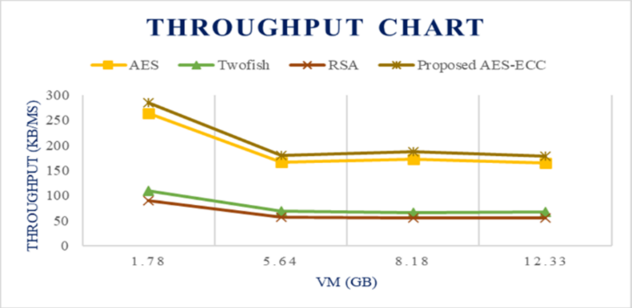
Compared to existing models, the proposed system's security is evaluated based on its decryption time (Fig. 12). Using four virtual machine images, the system demonstrates that AES-ECC takes 13310 and 9821 ms less time to decrypt than Twofish and RSA, respectively.



[Fig.12: Performance Analysis in Terms of Decryption Time]

iii. Throughout Time

Throughput time is crucial in cryptographic analysis, as it assesses the speed of a cryptographic algorithm's data encryption or decryption. It significantly impacts performance, usability, and practicality.



[Fig.13: Performance Analysis in Terms of Throughput Time]

The research comparing proposed and existing models showed that AES-ECC outperformed RSA and Twofish in terms of throughput (Fig. 13), achieving a higher rate of 195 kbps.

V. CONCLUSION

This research aims to minimize security risks during migration by incorporating an advanced cryptographic framework and a DDoS attack classification system. An Improved Sparrow Search Algorithm-based Deep Neural Network (ISSA-DNN) is suggested to ensure virtual machine security and classify DDoS attacks. The research commences with preparatory procedures, including normalising the CIC-DDoS dataset, feature selection using Random Forest (RF), subset selection, and duplicate elimination. The Grid Search identifies essential features, while the RF technique calculates the significance score for each feature. The DNN classifier achieves an accuracy of 98.79% for pre-processed data, which is 3.8% higher than the present FS-WOA-DNN method. The encryption of virtual machines intended for migration ensures compliance with regulatory standards and safeguards sensitive information. The results suggest that VM images encrypted with AES-ECC exhibit superior speed, as evidenced by reduced encryption and decryption times and increased throughput compared to RSA and Twofish. The AES-ECC-based VM image encryption and ISSA-DNN-based DDoS attack classification ensure optimal security during VM migration.

DECLARATION STATEMENT

After aggregating input from all authors, I must verify the accuracy of the following information as the article's author.

- **Conflicts of Interest/Competing Interests:** Based on my understanding, this article does not have any conflicts of interest.
- **Funding Support:** This article has not been sponsored or funded by any organization or agency. The independence of this research is a crucial factor in affirming its impartiality, as it was conducted without any external influence.
- **Ethical Approval and Consent to Participate:** The data provided in this article is exempt from the requirement for ethical approval or participant consent.
- **Data Access Statement and Material Availability:** The adequate resources of this article are publicly accessible.
- **Author's Contributions:** The authorship of this article is contributed equally to all participating individuals.

REFERENCES

1. F. Khoda Parast, C. Sindhav, S. Nikam, H. Izadi Yekta, K. B. Kent, and S. Hakak, "Cloud computing security: A survey of service-based models," Comput. Secur., vol. 114, p. 102580, Mar. 2022, DOI: https://doi.org/10.1016/j.cose.2021.102580
2. H. Lin, C. Wu, and M. Masdari, "A comprehensive survey of network traffic anomalies and DDoS attacks detection schemes using fuzzy techniques," Comput. Electr. Eng., vol. 104, p. 108466, 2022, DOI: https://doi.org/10.1016/j.compeleceng.2022.108466
3. X. Jing, Z. Yan, and W. Pedrycz, "Security Data Collection and Data Analytics in the Internet: A Survey," IEEE Commun. Surv. Tutorials,

vol. 21, no. 1, pp. 586–618, 2019, DOI: https://doi.org/10.1109/COMST.2018.2863942

4. R. Kumar and R. Goyal, "On cloud security requirements, threats, vulnerabilities and countermeasures: A survey," Comput. Sci. Rev.., vol. 33, pp. 1–48, 2019, DOI: https://doi.org/10.1016/j.cosrev.2019.05.002
5. H. Tabrizchi and M. Kuchaki Rafsanjani, "A survey on security challenges in cloud computing: issues, threats, and solutions," J. Supercomput., vol. 76, no. 12, pp. 9493–9532, 2020, DOI: https://doi.org/10.1007/s11227-020-03213-1
6. K. B. V., N. D. G., and P. S. Hiremath, "Detection of DDoS Attacks in Software Defined Networks," in 2018 3rd International Conference on Computational Systems and Information Technology for Sustainable Solutions (CSITSS), 2018, pp. 265–270. DOI: https://doi.org/10.1109/CSITSS.2018.8768551
7. J. Ali, B. Roh, B. Lee, J. Oh, and M. Adil, "A Machine Learning Framework for Prevention of Software-Defined Networking controller from DDoS Attacks and dimensionality reduction of big data," in 2020 International Conference on Information and Communication Technology Convergence (ICTC), 2020, pp. 515–519. DOI: https://doi.org/10.1109/ICTC49870.2020.9289504
8. A. E. Cil, K. Yildiz, and A. Buldu, "Detection of DDoS attacks with feed forward based deep neural network model," Expert Syst. Appl., vol. 169, p. 114520, 2021, DOI: https://doi.org/10.1016/j.eswa.2020.114520
9. M. Albanese, A. De Benedictis, D. D. J. de Macedo, and F. Messina, "Security and trust in cloud application life-cycle management," Futur. Gener. Comput. Syst., vol. 111, pp. 934–936, 2020, DOI: https://doi.org/10.1016/j.future.2020.01.025
10. T. V Phan and M. Park, "Efficient Distributed Denial-of-Service Attack Defence in SDN-Based Cloud," IEEE Access, vol. 7, pp. 18701–18714, 2019, DOI: https://doi.org/10.1109/ACCESS.2019.2896783
11. A. Bhardwaj, V. Mangat, and R. Vig, "Hyperband Tuned Deep Neural Network With Well Posed Stacked Sparse AutoEncoder for Detection of DDoS Attacks in Cloud," IEEE Access, vol. 8, pp. 181916–181929, 2020, DOI: https://doi.org/10.1109/ACCESS.2020.3028690
12. J. David and C. Thomas, "Detection of distributed denial of service attacks based on information theoretic approach in time series models," J. Inf. Secur. Appl., vol. 55, p. 102621, 2020, DOI: https://doi.org/10.1016/j.jisa.2020.102621
13. D. J. Prathyusha and G. Kannayaram, "A cognitive mechanism for mitigating DDoS attacks using the artificial immune system in a cloud environment," Evol. Intell., vol. 14, no. 2, pp. 607–618, 2021, DOI: https://doi.org/10.1007/s12065-019-00340-4
14. T.-H. Vuong, C.-V. N. Thi, and Q.-T. Ha, "N-Tier Machine Learning-Based Architecture for DDoS Attack Detection," in Intelligent Information and Database Systems, 2021, pp. 375–385, DOI: https://doi.org/10.1007/978-3-031-09484-2_2
15. N. Gupta, V. Jindal, and P. Bedi, "LIO-IDS: Handling class imbalance using LSTM and improved one-vs-one technique in intrusion detection system," Comput. Networks, vol. 192, p. 108076, 2021, DOI: https://doi.org/10.1016/j.comnet.2021.108076
16. Y. Wei, J. Jang-Jaccard, F. Sabrina, A. Singh, W. Xu, and S. Camtepe, "AE-MLP: A Hybrid Deep Learning Approach for DDoS Detection and Classification," IEEE Access, vol. 9, pp. 146810–146821, 2021, DOI: https://doi.org/10.1109/ACCESS.2021.3123791
17. T. Khempetch and P. Wuttidittachotti, "DDoS attack detection using deep learning," vol. 10, no. 2, pp. 382-388, 2021, DOI: https://doi.org/10.11591/ijai.v10.i2.pp382-388
18. A. Agarwal, M. Khari, and R. Singh, "Detection of DDOS Attack using Deep Learning Model in Cloud Storage Application," Wirel. Pers. Commun., vol. 127, no. 1, pp. 419–439, 2022, DOI: https://doi.org/10.1007/s11277-021-08271-z
19. R. K. Batchu and H. Seetha, "An integrated approach explaining the detection of distributed denial of service attacks," Comput. Networks, vol. 216, p. 109269, 2022, DOI: https://doi.org/10.1016/j.comnet.2022.109269
20. D. H. Parekh and R. Sridaran, "Mitigating cloud security threats using public-key infrastructure," in Cyber Security: Proceedings of CSI 2015, 2018, pp. 165–177, doi: https://doi.org/10.1007/978-981-10-8536-9_17
21. S. Rehman, N. Talat Bajwa, M. A. Shah, A. O. Aseeri, and A. Anjum, "Hybrid AES-ECC Model for the Security of Data over Cloud Storage," Electronics, vol. 10, no. 21, 2021, DOI: https://doi.org/10.3390/electronics10212673
22. A. Nanda, P. Nanda, X. He, A. Jamdagni, and D. Puthal, "A hybrid encryption technique for Secure-GLOR: The adaptive secure routing protocol for dynamic wireless mesh networks," Futur. Gener. Comput. Syst., vol. 109, pp. 521–530, 2020, DOI: https://doi.org/10.1016/j.future.2018.05.065
23. H. Aliev and H.-W. Kim, "Matrix-Based Dynamic Authentication With Conditional Privacy-Preservation for Vehicular Network Security," IEEE Access, vol. 8, pp. 200883–200896, 2020, DOI: https://doi.org/10.1109/ACCESS.2020.3035845
24. B. Alaya and L. SELLAMI, "Clustering method and symmetric/asymmetric cryptography scheme adapted to securing urban VANET networks," J. Inf. Secur. Appl., vol. 58, p. 102779, 2021, DOI: https://doi.org/10.1016/j.jisa.2021.102779
25. D. K. R. Shukla, V. K. R. Dwivedi, and M. C. Trivedi, "Encryption algorithm in cloud computing," Mater. Today Proc., vol. 37, pp. 1869–1875, 2021, DOI: https://doi.org/10.1016/j.matpr.2020.07.452
26. H. S. Yahia et al., "Comprehensive survey for cloud computing based nature-inspired algorithms optimization scheduling," Asian J. Res. Comput. Sci., vol. 8, no. 2, pp. 1–16, 2021, DOI: https://doi.org/10.9734/ajrcos/2021/v8i230195
27. P. Chinnasamy, S. Padmavathi, R. Swathy, and S. Rakesh, "Efficient Data Security Using Hybrid Cryptography on Cloud Computing," in Inventive Communication and Computational Technologies, 2021, pp. 537–547, DOI: https://doi.org/10.1007/978-981-15-7345-3_46
28. V. K. Soman and V. Natarajan, "Analysis of Hybrid Data Security Algorithms for Cloud," in Second International Conference on Networks and Advances in Computational Technologies, 2021, pp. 231–242, DOI: https://doi.org/10.1007/978-3-030-49500-8_20
29. F. K. Mupila and H. Gupta, "An Innovative Authentication Model for the Enhancement of Cloud Security," in Innovations in Computer Science and Engineering, 2021, pp. 447–455, DOI: https://doi.org/10.1007/978-981-33-4543-0_48
30. D. Saxena, I. Gupta, J. Kumar, A. K. Singh, and X. Wen, "A Secure and Multiobjective Virtual Machine Placement Framework for Cloud Data Centre," IEEE Syst. J., vol. 16, no. 2, pp. 3163–3174, 2022, DOI: https://doi.org/10.1109/JSYST.2021.3092521
31. F. Thabit, O. Can, S. Alhomdy, G. H. Al-Gaphari, and S. Jagtap, "A Novel Effective Lightweight Homomorphic Cryptographic Algorithm for data security in cloud computing," Int. J. Intell. Networks, vol. 3, pp. 16–30, 2022, DOI: https://doi.org/10.1016/j.ijin.2022.04.001
32. B. Thakkar and B. Thankachan, "An Approach for Enhancing Security of Data over Cloud Using Multilevel Algorithm," in Congress on Intelligent Systems, 2022, pp. 305–318, DOI: https://doi.org/10.1007/978-981-16-9416-5_22
33. F. Pandey, P. Dash, D. Samanta, and M. Sarma, "Efficient and provably secure intelligent geometrical method of secret key generation for cryptographic applications," Comput. Electr. Eng., vol. 101, p. 107947, 2022, DOI: https://doi.org/10.1016/j.compeleceng.2022.107947
34. R. K. Batchu and H. Seetha, "A generalized machine learning model for DDoS attacks detection using hybrid feature selection and hyperparameter tuning," Comput. Networks, vol. 200, p. 108498, 2021, DOI: https://doi.org/10.1016/j.comnet.2021.108498
35. D. Akgun, S. Hizal, and U. Cavusoglu, "A new DDoS attacks intrusion detection model based on deep learning for cybersecurity," Comput. Secur., vol. 118, p. 102748, 2022, DOI: https://doi.org/10.1016/j.cose.2022.102748
36. J. Xue and B. Shen, "A novel swarm intelligence optimization approach: sparrow search algorithm," Syst. Sci. & Control Eng., vol. 8, no. 1, pp. 22–34, 2020, DOI: https://doi.org/10.1080/21642583.2019.1708830
37. R. Kumar, M. Memoria, A. Gupta, and M. Awasthi, "Critical Analysis of Genetic Algorithm under Crossover and Mutation Rate," in 2021 3rd International Conference on Advances in Computing, Communication Control and Networking (ICAC3N), 2021, pp. 976–980. DOI:: https://doi.org/10.1109/ICAC3N53548.2021.9725640
38. C. E. L. BALMANY, Z. TBATOU, A. ASIMI, and M. BAMAROUF, "Secure Virtual Machine Image Storage Process into a Trusted Zone-based Cloud Storage," Comput. Secur., vol. 120, p. 102815, 2022, DOI: https://doi.org/10.1016/j.cose.2022.102815
39. D. N. Tran, B. L. Vu, and X. N. Tien, "Improved Deterministic Usage of the Elliptic Curve Digital Signature Algorithm with Scrypt," in 2023 IEEE Statistical Signal Processing Workshop (SSP), 2023, pp. 611–615. DOI: https://doi.org/10.1109/SSP53291.2023.10207927
40. R. Banoth and R. Regar, Classical and Modern Cryptography for Beginners. Springer Nature, 2023, DOI: https://doi.org/10.1007/978-3-031-32959-3
41. R. Banoth and R. Regar, "Security Standards for Classical and Modern Cryptography," in Classical and Modern Cryptography for Beginners, Cham: Springer Nature Switzerland, 2023, pp. 47–83. DOI: https://doi.org/10.1007/978-3-031-32959-3_2
42. V. S. Shetty, R. Anusha, D. Kumar M.J., and P. Hegde N., "A Survey on Performance Analysis of Block Cypher Algorithms," in 2020 International Conference on Inventive Computation Technologies

(ICICT), 2020, pp. 167–174. DOI: https://doi.org/10.1109/ICICT48043.2020.9112491

43. P. Oktivasari, M. Agustin, R. E. M. Akbar, A. Kurniawan, A. R. Zain, and F. A. Murad, "Analysis of ECG Image File Encryption using ECDH and AES-GCM Algorithm," in 2022 7th International Workshop on Big Data and Information Security (IWBIS), 2022, pp. 75–80. DOI: https://doi.org/10.1109/IWBIS56557.2022.9924954
44. R. Banoth and R. Regar, "Asymmetric Key Cryptography," in Classical and Modern Cryptography for Beginners, Cham: Springer Nature Switzerland, 2023, pp. 109–165. DOI: https://doi.org/10.1007/978-3-031-32959-3_4
45. M. Ma, "Comparison between RSA and ECC," in 2021 2nd International Seminar on Artificial Intelligence, Networking and Information Technology (AINIT), 2021, pp. 642–645. DOI: https://doi.org/10.1109/AINIT54228.2021.00129
46. M. P. Novaes, L. F. Carvalho, J. Lloret, and M. L. Proença, "Adversarial Deep Learning approach detection and defence against DDoS attacks in SDN environments," Futur. Gener. Comput. Syst., vol. 125, pp. 156–167, Dec. 2021, DOI: https://doi.org/10.1016/j.future.2021.06.047
47. R. Priyadarshini and R. K. Barik, "A deep learning based intelligent framework to mitigate DDoS attack in fog environment," J. King Saud Univ. - Comput. Inf. Sci., vol. 34, no. 3, pp. 825–831, 2022, DOI: https://doi.org/10.1016/j.jksuci.2019.04.010
48. M. Wang, Y. Lu, and J. Qin, "A dynamic MLP-based DDoS attack detection method using feature selection and feedback," Comput. Secur., vol. 88, p. 101645, 2020, DOI: https://doi.org/10.1016/j.cose.2019.101645
49. M. V. O. de Assis, L. F. Carvalho, J. J. P. C. Rodrigues, J. Lloret, and M. L. Proença Jr, "Near real-time security system applied to SDN environments in IoT networks using a convolutional neural network," Comput. Electr. Eng., vol. 86, p. 106738, 2020, DOI: https://doi.org/10.1016/j.compeleceng.2020.106738

AUTHOR'S PROFILE

Dr. N. Venkata Subramanian, a dedicated member of SASTRA Deemed University since 2009, has made significant contributions to the institution through teaching, research, and service. In 2024, he earned his Ph.D., marking an important milestone in his academic journey. He has consistently published research in Scopus and SCIE-indexed journals, demonstrating a strong commitment to advancing knowledge and upholding high standards of scholarly excellence. This dedication to research and academic rigour makes him a valuable asset to the SASTRA community.

Dr. Shankar Sriram V.S. is the Dean of the School of Computing at SASTRA Deemed University, Thanjavur, Tamil Nadu, India. He holds a Master's degree in Computer Applications from Madurai Kamaraj University, Madurai, India. He also received his Master's degree in Engineering from Thapar University, Punjab, India. He was conferred a Ph.D. in Information and Network Security from Birla Institute of Technology, Mesra, India. He has been in Academia for the past 22 years. He is a member of IEEE. He was awarded the IBM Shared University Research (SUR) Award in 2017 and received research funding from various organisations. His current area of research includes information and network security, cloud computing, big data analytics, machine learning, deep learning, bioinformatics, and graph-based data mining.

Disclaimer/Publisher's Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of the Blue Eyes Intelligence Engineering and Sciences Publication (BEIESP)/ journal and/or the editor(s). The Blue Eyes Intelligence Engineering and Sciences Publication (BEIESP) and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.