Improving the Cyber Security over Banking Sector by Detecting the Malicious Attacks Using the Wrapper Stepwise Resnet Classifier

Damodharan Kuttiyappan[1*], and Dr Rajasekar V[2]
[1]Ph.D. Research Scholar, SRM Institute of Science and Technology, Chennai,
Tamilnadu, India.
[e-mail: dt3388@srmist.edu.in]
[2]Associate Professor, Computer Science & Engineering, SRMIST, Vadapalani, Chennai
[e-mail: rajasekv2@srmist.edu.in]
* Corresponding author: Damodharan Kuttiyappan

Received August 12, 2022; revised February 14, 2023; accepted May 1, 2023;
published June 30, 2023

Abstract

With the advancement of information technology, criminals employ multiple cyberspaces to promote cybercrime. To combat cybercrime and cyber dangers, banks and financial institutions use artificial intelligence (AI). AI technologies assist the banking sector to develop and grow in many ways. Transparency and explanation of AI's ability are required to preserve trust. Deep learning protects client behavior and interest data. Deep learning techniques may anticipate cyber-attack behavior, allowing for secure banking transactions. This proposed approach is based on a user-centric design that safeguards people's private data over banking. Here, initially, the attack data can be generated over banking transactions. Routing is done for the configuration of the nodes. Then, the obtained data can be preprocessed for removing the errors. Followed by hierarchical network feature extraction can be used to identify the abnormal features related to the attack. Finally, the user data can be protected and the malicious attack in the transmission route can be identified by using the Wrapper stepwise ResNet classifier. The proposed work outperforms other techniques in terms of attack detection and accuracy, and the findings are depicted in the graphical format by employing the Python tool.

Keywords: Cyber security, Malicious attacks, Cyber-physical systems, banking sector, Hierarchical network feature extraction, Wrapper stepwise ResNet.

http://doi.org/10.3837/tiis.2023.06.007 **ISSN : 1976-7277**

1. Introduction

A digital asset is protected by cyber security methods, human behavior, and technologies. The cyber security issues in banking services pose problems as depicted in **Fig. 1**. Cyber-criminals are doubling the potency of the attack tools with half the price; similar to how Moore's law predicts doubling the number of components over a silicon chip every 2 years (thus reducing chip expenses) [1]. The criminal organization involved in illegal operations launches cyber attacks that can cause a Denial of Service (DoS), steal data or state secrets as a result of data breaches, seek payments through ransomware, and so on.

In recent years, researchers have begun investigating recommendations for better cyber security using Artificial Intelligence (AI). Malicious actors use AI to execute highly complicated cyber threats whilst obscuring their trials. But in this work, we look at how AI-based cyber security systems can better ward off attacks and avoid privacy violations [2]. The Internet of Things (IoT), smartphones, and clinical records all present unique security difficulties and concerns for IT professionals. As the need for IT solutions grows, so do the risks of being a victim of a cyber attack. Distributed Denial of Service (DDoS) assault could be used to penetrate the network and digital resources of a specific company or online business, among the many cyber attacks currently available **Fig. 1**.

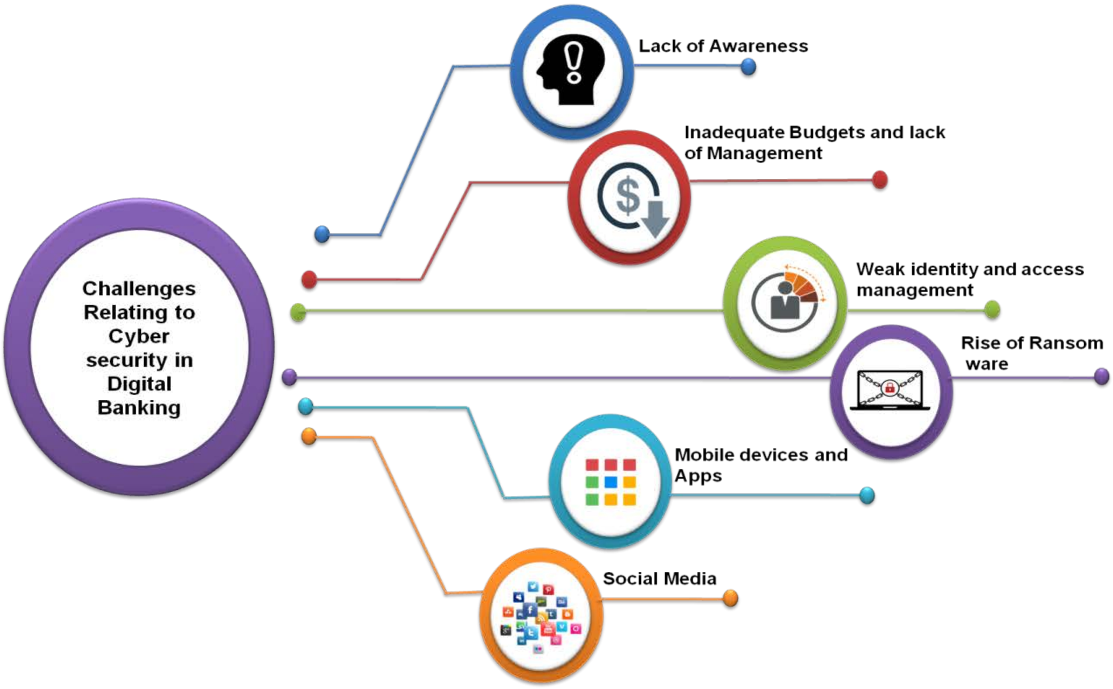
Challenges Relating to Cyber security in Digital Banking
Lack of Awareness
Inadequate Budgets and lack of Management
Weak identity and access management
Rise of Ransom ware
Mobile devices and Apps
Social Media

Fig. 1. Cybersecurity issues in banking services pose problems

Web-based methods are typically unavailable to legitimate people in this assault since a huge proportion of compromised devices are particularly susceptible. The goal of a DDoS assault is to render a computer or network asset inaccessible to the target audience [3]. Two or more people or machines are involved in DDoS assaults, whereas one person or machine is involved in DoS attacks. Whenever a computer crashes with malicious code, a bot is a resultant gadget. DDoS assaults are the primary emphasis of this study. Employing protocols like TCP, UDP, ICMP, and HTTP, could be deployed in the networking, transport, and application layers. DDoS assaults can be carried out by massive quantities of infected machines on the internet.

Attackers gain over a multitude of computers before launching an attack. These systems are susceptible. To take control of the computer, the attacker uses malicious files or another hacking method to attack the system's vulnerabilities [4]. The structure of DDoS assaults and the objectives of the perpetrators are continuously changing. Still, now, criminals are being prosecuted for botnet-based DDoS operations that inflict billions of dollars of harm on their targets [5]. Last year's major cyber attack on the Estonian government's online sites placed this attack tactic into public view. To launch a DDoS attack, there are two methods. Attackers can disrupt a protocol or a program by sending rogue messages to the target (i.e., a vulnerability attack).

Try to disrupt a valid user's accessibility by using frequency band, network components, or router processing ability; or destroy a genuine user's facilities by using CPU, memory, disk/database bandwidth, and I/O bandwidth on a server to overload the system and cause it to crash. The above-mentioned approach is used by malicious users. With the rise of hacking attempts on banks across the country, a new Wrapper stepwise ResNet classifier is presented in this paper.

As a result of our research, we have come up with the following contributions:

- To eliminate the defects, the pre-processing technique is utilized.
- To identify the abnormal features related to the attack, the hierarchical network feature extraction technique is employed.
- To protect the user data and identify the malicious attack in the transmission route, the Wrapper stepwise ResNet classifier is provided.

The additional detail of this paper is organized as follows: topic II-related works with a problem statement, topic III-proposed work, topic IV-performance analysis, and topic V-conclusion.

2. Related Works

Cybersecurity is a hotly debated topic because of its importance in today's digital environment. Several investigators have used a variety of advanced machine-learning techniques. In [6], they presented an intrusion detection technique using ensemble learning's Decision Tree-Recursive Feature Elimination (DT-RFE) characteristic. Preliminary, they offer a DT-RFE to choose characteristics and decrease feature size. Removes superfluous and unrelated information from a database to improve resource quality and decrease runtime. In this work, they combine DT and RFE approaches to create Stacking ensemble learning. In [7], they provided an ML-based DoS detection method. The suggested method relies on signatures collected from internet traffic patterns. The tests used recent datasets. In [8], they suggested a mechanism for high-level and long-term attack prevention. For managing application-level gateways, a deep, as well as machine learning-based adaptive anomaly detection structure, was built. The proposed scheme for increasing cybersecurity was evaluated using typical network statistics. In [9], they offer a method for identifying HTTP DDoS attacks inside the cloud using Information Theoretic Entropy and also the Random

Forest ensemble learning technique. The entropy of incoming data was estimated using a time-based sliding window technique. Entropy estimates that have been higher than normal trigger pretreatment and categorization activities. In [10], The IPv6 network DoS intrusion threat technique seems to be the study basis and information gain percentage. The double dimensionality reduction approach minimizes feature dimensionality and increases the categorization functionality of subsequent classifications. In terms of classification techniques, this paper improves the GR-AD-KNN approach. The method is employed in DoS attack detection. Using the information gain percentage as a weight, unique features can have varying levels of impact. In [11], to discriminate between two common low-rate Attacks, the constant assault and also the pulsating assault, they proposed an expectation of a packet-size approach. In [12], a revised and thorough taxonomy of DDoS assaults was proposed, along with instances about how this categorization corresponds to actual threats. But from the other hand, fresh findings reinforce the fears regarding the growing use of DDoS-enabled viruses within IoT. In [13], an overview of information fusion strategies for heterogeneous multi-source datasets was presented. A big data analytical methodology for targeted cyber-attack identification was proposed on this foundation, as is a correlation test. This method can successfully connect multisource heterogeneous security information and analyze attack purposes. In [14], they presented a quintuple cyber security knowledge base including deduction procedures. For a cyber security knowledge base, they use machine learning to retrieve items and develop taxonomies. The path-ranking technique is used to calculate rule changes. One could train an extractor using the Stanford-named entity recognizer (NER). The goal of this research is to uncover the various cyber attack tactics used by computer hackers to target certain banking sectors, wherein faking, malicious attacks, memory leaks, and merge scripting have been discovered to be positively connected with both public and private sector banks. If they used a bi-directional recurrent neural network and long short-term memory (BRNN-LSTM) to build a deep learning model. The BRNN-LSTM outperforms the statistical technique in terms of accuracy. This study provides a thorough overview of the expanding corpus of studies investigating the ubiquitous consequences of cyber risks upon those banking markets. As the banking industry faces a serious cyber threat, investigators were analyzing the issue from several angles. Many records are supplying theoretical conversations, advanced analytics, and survey responses, but little empirical evidence using actual information. Also, global and regional regulatory authorities provide ideas to ensure banking institutions manage threats. In this study, they consolidate significant literature and policy statements on threats, concentrating on the banking platform's susceptibility. Lastly, they offer numerous novel approaches that could improve our understanding of threats and assist professionals to design a stronger methodology. They proposed a new approach to evaluate Indian bank workers' cyber security efforts. Cyber-attacks were unavoidable, but also how quickly a bank recovers depends on the staff's cyber resilience. In Using a test platform, they show how a DDoS attack affects an IRC server's functionality. They employ a game theory framework for assessing the viability of DDoS attacks against IRC. The study would help security professionals offer effective solutions to diminish attackers' usefulness, rendering attacks less appealing. They suggested combining deep learning to identify pirated software as well as malware-infected documents throughout IoT networks. With source code theft, Tensor flow, a deep learning model, was suggested.

Problem statement

DDoS attacks are difficult to identify and mitigate because of human mistakes and insufficient resources that automatically adapt to the network's changing trends, according to research done several years ago. Automated technologies which can perform (identify and prevent) depending on the traffic's properties and behavior have emerged as a result of this development. A high degree of flexibility in the categorization process, as well as improved identification of malicious activity, has been achieved through the use of technologies based on "artificial intelligence" (AI), especially “machine learning” (ML). It's difficult to strike a balance between both research and the reality of DDoS protection. As a result of this asset, the university intends to use ML in several industries, including banking and finance. DDoS attacks continue to occur regularly, proving that the issue has not been fixed. However, there have been several experiments that have yielded inconsistent findings in the detection and mitigation of assaults in these areas.

3. Proposed Work

In this section, the proposed Wrapper stepwise ResNet classifier is illustrated to identify malicious attacks in the banking network. **Fig. 2** depicts the complete procedure of this research. The presented research contains preprocessing and feature extraction stages to normalize the raw dataset and extract the features related to the attack correspondingly. The hierarchical network model is employed in the feature extraction stage. The proposed technique is utilized in the classification stage to identify the attack to enhance cyber security throughout the banking sector.

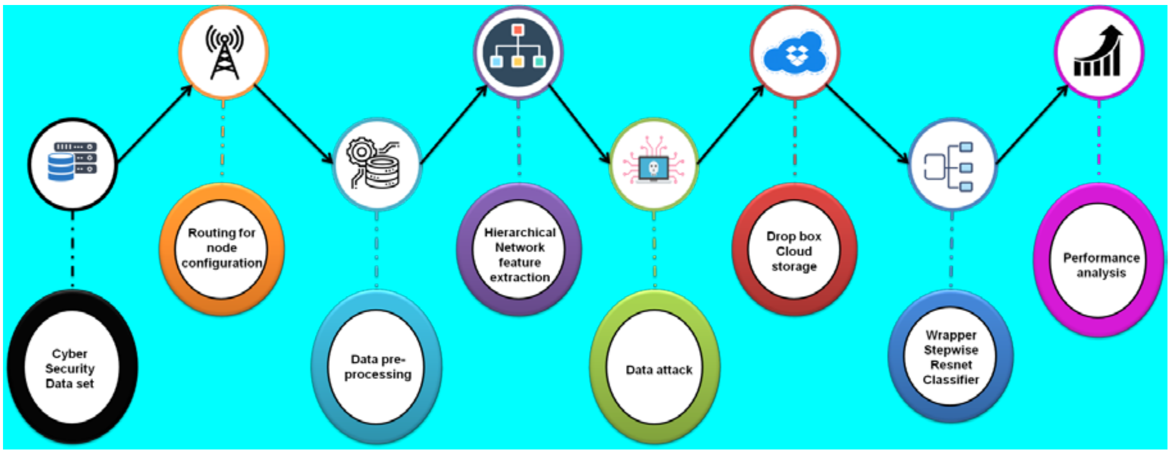
Cyber Security Data set
Routing for node configuration
Data pre-processing
Hierarchical Network feature extraction
Data attack
Drop box Cloud storage
Wrapper Stepwise Resnet Classifier
Performance analysis

Fig. 2. Illustration of the proposed approach as a flow

Dataset

Initially, gather datasets are taken from the "Kaggle" platform to conduct this investigation regarding cyber security enhancement. There are 175,341 reports regarding detecting malware in the database "UNSW-NB 15," which can be found on the Kaggle platform. This dataset is included in this study. The Australian Institute of Cyber Security's Cyber Range Laboratory developed the statistics. This collected data are shall be normalized to eliminate errors or unwanted data in the pre-processing stage.

Data pre-processing

The first stage of this research involves preprocessing, which is used to transform real-world datasets into a format that can be understood. This data is likely to be incorrect and inconsistent throughout most actual datasets that were investigated thus far. When identifying patterns in data transmitted, preprocessing is essential for getting the most accurate findings. For all information retrieval efforts, like malicious detection, data pre-processing is a necessary part of the effort.

Equation (1) defines the q-count in mathematical form as,

$$\mathrm{q} = \left[\frac{\mathrm{B} - \beta}{\tau}\right] - - - - - - (1)$$

Here, β expresses the mean of the information and τ hints at the standard deviation. And q is represented as,

$$\mathrm{q} = \frac{\mathrm{B} - \overline{\mathrm{B}}}{\mathrm{Sd}} - - - - - - (2)$$

Here, $\bar{B}$=mean of the specimen, and Sd points out the standard deviation of the specimens.

The random specimen looks like this:

$$q_k = \delta_0 + \delta_1 B_r + \rho_r - - - - - - (3)$$

The defects that are depending on τ^2 are represented by r.

Ensuring that, as seen below, the defects should not depend on one another.

$$t_m \sim \sqrt{U}\frac{t}{\sqrt{t^2 + u - 1}} - - - - - - (4)$$

Here, t=random parameter.

After that, the standard deviation is used to standardize the variable's moves. The momentary scale deviation is calculated using the formula (5).

$$\mathrm{MMS} = \frac{\mu^{\mathrm{mms}}}{\theta^{\mathrm{mms}}} - - - - - - (5)$$

Here, momentary scale=mms.

$$\mu^{\mathrm{mms}} = \mathrm{Ex}(\mathrm{B} - \beta)^{\mathrm{MMS}} - - - - - - (6)$$

Here, B=random variable, and Ex=predicted values.

$$\theta^{\mathrm{mms}} = \left(\sqrt{Ex(B - \beta)^{MMS}}\right)^2 - - - - - - (7)$$

$$t_u = \frac{mms}{\bar{B}} - - - - - - (8)$$

The coefficient of variance=t_u.

The characteristic scaling procedure will be stopped by setting all of the parameters to 0 or 1. The unison-based normalizing approach is the name for this procedure. The normalized formula would look like this:

$$B' = \frac{(t - t_{min})}{(t_{max} - t_{min})} ------ (9)$$

After this pre-processing stage, the feature extraction procedure is conducted using the hierarchical network to convert the actual data into numerical features or attributes.

Hierarchical network feature extraction

Generally, feature extraction is the way of converting unprocessed or actual data into numerical attributes that may be handled while keeping the actual dataset's information. Hierarchical networks divide a network into different layers, one of which performs a specific purpose in the network. By this, we select the best attributes (DateTime, host, src, proto, type, spt, dpt, srcstr, cc, country, locale, locale abbr, postal code, latitude, and longitude) to play a specific function in that network layer.

With the assistance of pre-processing processes in the lower levels, as shown in **Fig. 3**, we may predict that a hierarchical extracting strategy will provide higher chances of extracting significant features from complicated data. This finally allows for improved identification even with a limited set of features available. A more ordinary procedure of discovering hierarchical feature associations will be achieved by combining non-negativity restriction with basic deep learning architectures.

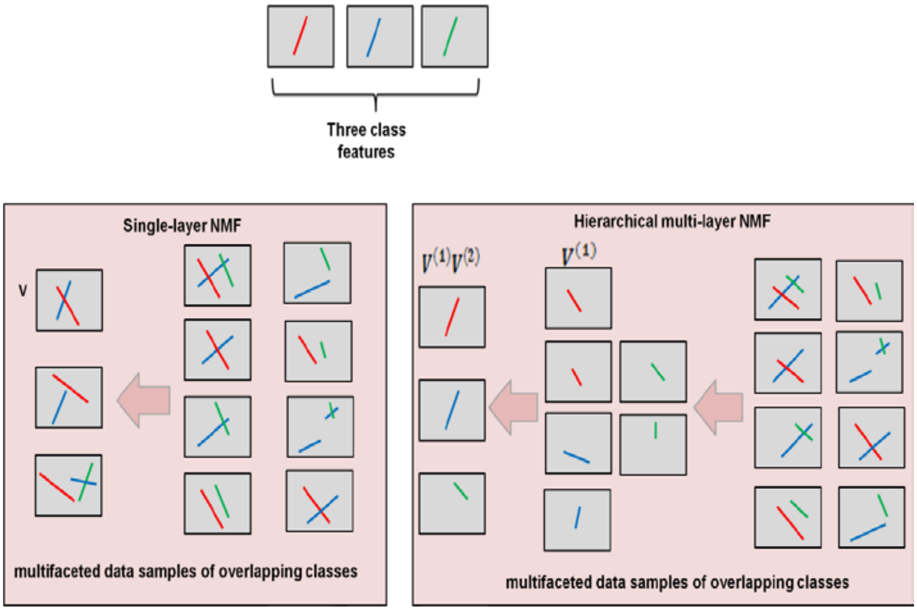
Three class features
Single-layer NMF
V
multifaceted data samples of overlapping classes
Hierarchical multi-layer NMF
$V^{(1)}V^{(2)}$
$V^{(1)}$
multifaceted data samples of overlapping classes

Fig. 3. Multi-layer hierarchical network

The fundamental technique for every layer of this strategy is called NsNMF, which stands for non-smooth non-negative matrix factorization. NsNMF is a version of NMF with the restriction of sparsity. Non-negative input information Q is decomposed into non-negative V & G, which have attributes and related coefficients or information depiction. By doing so, the difference between the actual data Q as well as its recreation VG should be smaller.

A well-known way to extract features is to implement a sparsity restriction. We conducted studies with varied sparsity criteria for every layer to examine the influence of the sparsity restriction. We would use the same beginning for every example of changing sparsity in terms of fairness in our comparisons.

The cost function is seen in equation (10):

$$C = \frac{1}{2}\|Q - VG\|^2 = \frac{1}{2}\sum_{m=1}^{M}\sum_{n=1}^{N}\left(Q_{mn} - \sum_{r=1}^{R} V_{mr}G_{rn}\right)^2 - - - - - (10)$$

A multiplicative update rule is used to adjust V and G inside the rounds, as mentioned in the attached equation (11):

$$V_{mr} \leftarrow V_{mr}\frac{(QG^T)_{mr}}{(VGG^T)_{mr}}, G_{mr} \leftarrow G_{mr}\frac{(V^TQ)_{rn}}{(V^TVG)_{rn}} - - - - - (11)$$

In the following equation (12), a sparsity matrix R is placed as a restriction on a typical single-layer NMF.

$$R = (1-\theta)eye(g) + \frac{\theta}{g}ones(g) - - - - - (12)$$

Here, g=attributes, θ=sparsity factor ranging between 0 and 1, $eye(g)$=identity matrix with (gxg), $ones(g)$=matrix with each element of 1s.

The sparsity of a matrix is lost when it is multiplied by R. The degradation of sparsity is increased when the gets near 1. Each time we perform an alternative change, we divide R by G to get G=RG. The decrease of the sparsity of G causes V to become sparse.

Fig. 4 depicts the hierarchical network's framework and we build a multi-layered structure.

Every layer's output is converted to $D^{(a)}$ before being used as an input next. Then $D^{(a)}$ is calculated by

$$D_{rn}^{(a)} = f\left(G_{rn}^{(a)}\right) - - - - - (13)$$

Here, $G^{(a)}$=output of layer, f(.)=non-linear function, and a=layer's index with a=1, 2,…,A.

The nsNMF can be used to dissolve $D^{(a)}$ into $V^{(a+1)}$ and $G^{(a+1)}$: $D^{(a)}$~$V^{(a+1)}$ $G^{(a+1)}$. This cycle continues till g=G is reached.

Next-layer decomposition of $D^{(a)}$ has the physical sense of obtaining data on how different layers' features combine. We can create more complicated features by figuring out which features from one layer are coupled with others in the next. At first, little building blocks are extracted from the lowest layer, and then they are combined to create more complicated blocks through the subsequent layers **Table 1**.

The resulting data description $D^{(A)}$ is achieved after training up to the last layer. These generated data are stored in Dropbox since users could keep digital files as well as synchronize them to other gadgets. The Dropbox connections let users exchange data files without transferring huge documents. To identify the malicious attacks in the classification stage, the features are collected from the drop box **Fig. 4**.

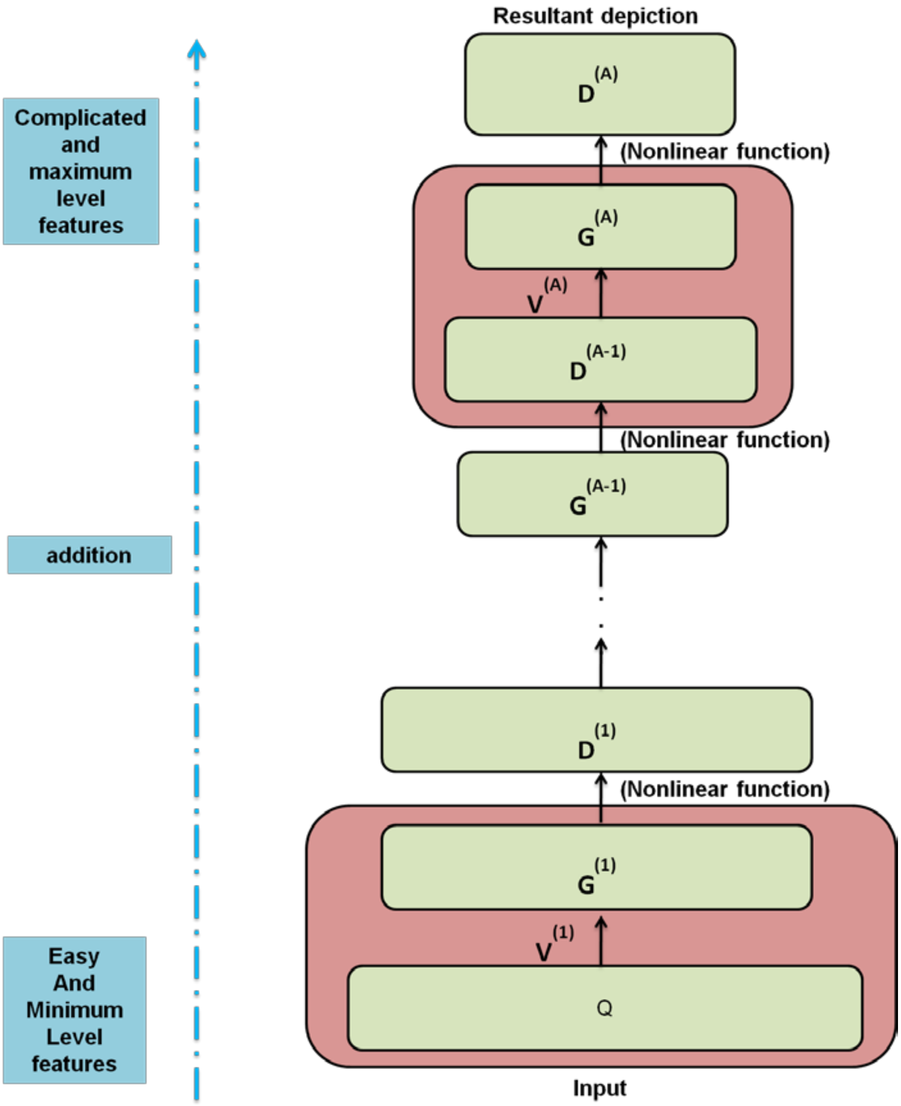

Fig. 4. Hierarchical network feature extraction flow

Table 1. Feature extraction result

#	Columns	Non-Null count	D-Type
0	datetime	451581 non-null	Object
1	host	451581 non-null	Object
2	proto	451581 non-null	Int64
3	type	451581 non-null	Object
4	spt	44811 non-null	float64
5	dpt	406770 non-null	float64
6	srcstr	406770 non-null	float64
7	country	451581 non-null	Object
8	locale	447985 non-null	Object
9	localeabbr	447947 non-null	Object
10	postalcode	342112 non-null	Object
11	latitude	331705 non-null	Object
12	longitude	86478 non-null	Object
13	datetime	448112 non-null	float64
14	host	448153 non-null	float64
15	Unnamed: 15	83 non-null	float64
d-types: float64 (6), int64 (1), object (9) memory usage: 55.1+ MB			

Wrapper stepwise ResNet classifier

In this section, Wrapper stepwise ResNet classifier is utilized to classify the malicious data or attacks. Wrapper stepwise ResNet includes a new identification mapping feature. The ResNet forecasts the delta needed to get it from one layer to another and arrive at the final prediction. The ResNet solves the fading gradient issue by enabling the gradient can pass through an additional shortcut way. So, this classifier takes the data from the drop box as part-wise or step-wise (that means 16 data per step or part) and wraps the two sets of data (16+16) to identify the malicious attacks. The ResNet's identification mapping enables the system to skip a weighted layer unless the present layer isn't required. This avoids the issue of the training examples becoming overfitted.

Fig. 5 displays the design of Wrapper stepwise ResNet and **Fig. 6** depicts the residual learning block. For example, given a set containing characteristics D and labels u, we may try to tackle the associated objective functions to discover it.

$$f_D^* \stackrel{\text{def}}{=} {}^{argmin}{}_{f}L(c,u,f) \qquad f \in D - - - - - (14)$$

Here, D=class, c=characteristics, u=label, f*=” truth” function.

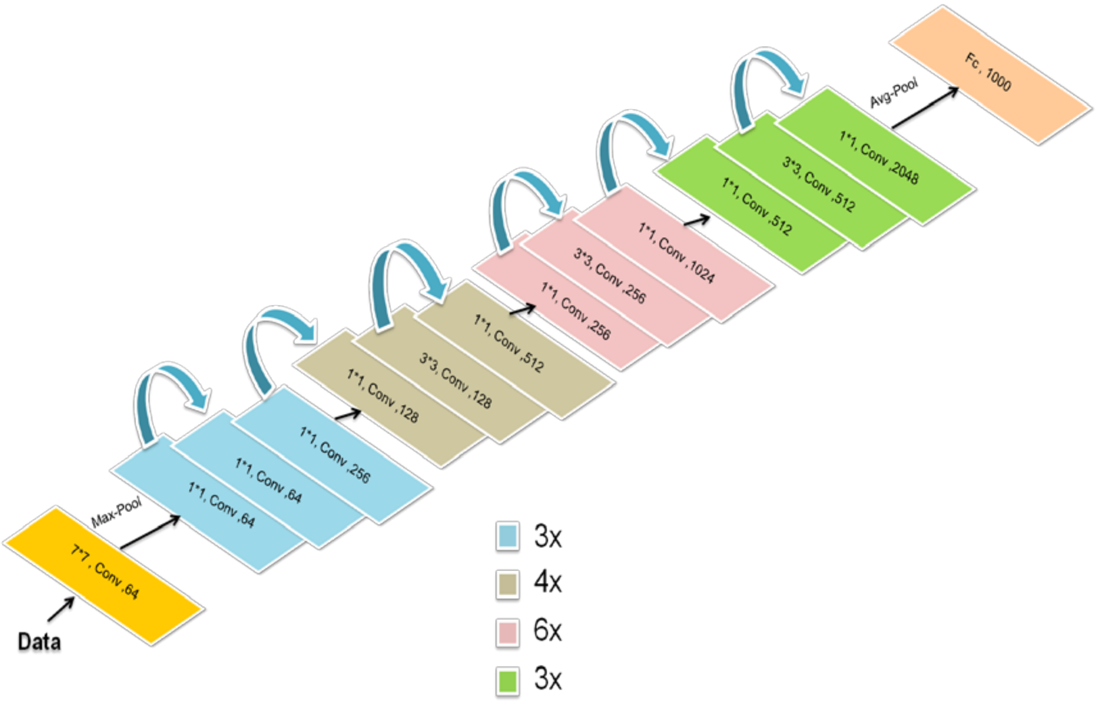

Fig. 5. Wrapper stepwise ResNet

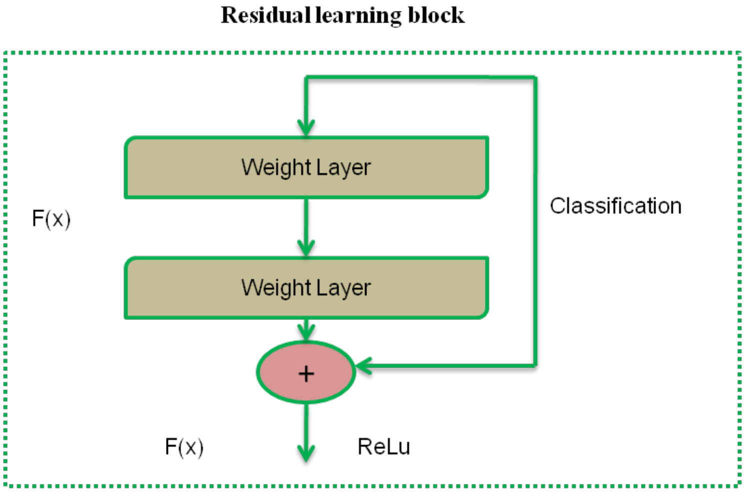

Fig. 6. Residual learning block

4. Performance Analysis

In this section, the investigation of the proposed technique is explained by identifying the malicious attacks in the banking servers regarding cyber security enhancement. During this investigation, the performance metric "accuracy" is obtained by employing the Python tool. This performance metric of our proposed technique is matched with other existing techniques to accomplish our research with the greatest effectiveness in malicious prediction.

Fig. 7 and **Fig. 8** depicted the rates of attacks for each month and hour, correspondingly. In **Fig. 8**, the x-axis indicates the month and the y-axis indicates the attack rate. During the 3rd, 4th, 5th, and 6th months, nearly 54,000 to 70,000 attacks occurred. In the 7th and 8th months, nearly 88,000 to 95,000 attacks have occurred. But, in the 9th month, nearly 20,000 attacks occurred. From this, a small and large amount of attacks have existed in the 9th month and 7th & 8th months, correspondingly. Similarly, in **Fig. 9**, the x-axis indicates the hour and y-axis attack rate. A large amount of attacks (nearly 30,000) is developed in only the 7th hour when compared with overall hours and then a small amount of attacks is developed in other time steps. **Fig. 10** depicts the total attack rate by month. Here, the month and attack are exponentially increased.

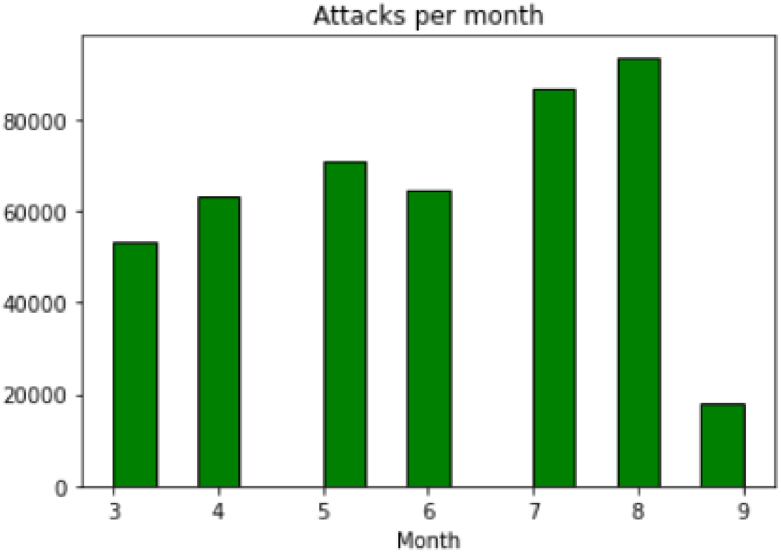

Fig. 7. Attacks per month

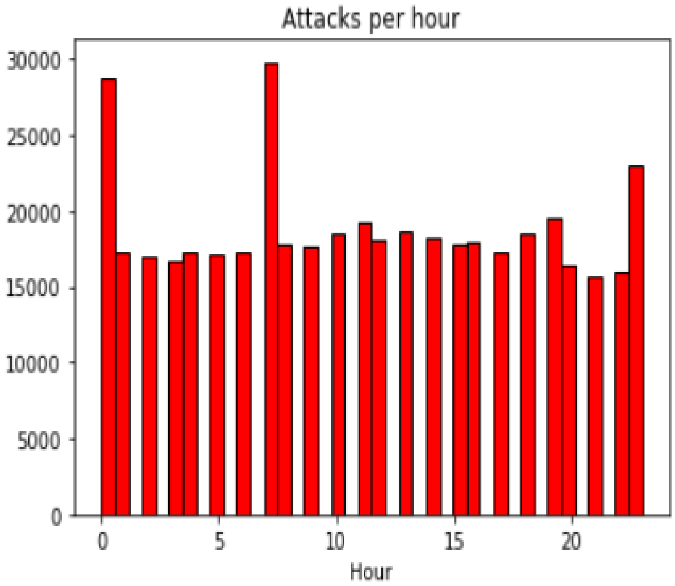

Fig. 8. Attacks per hour

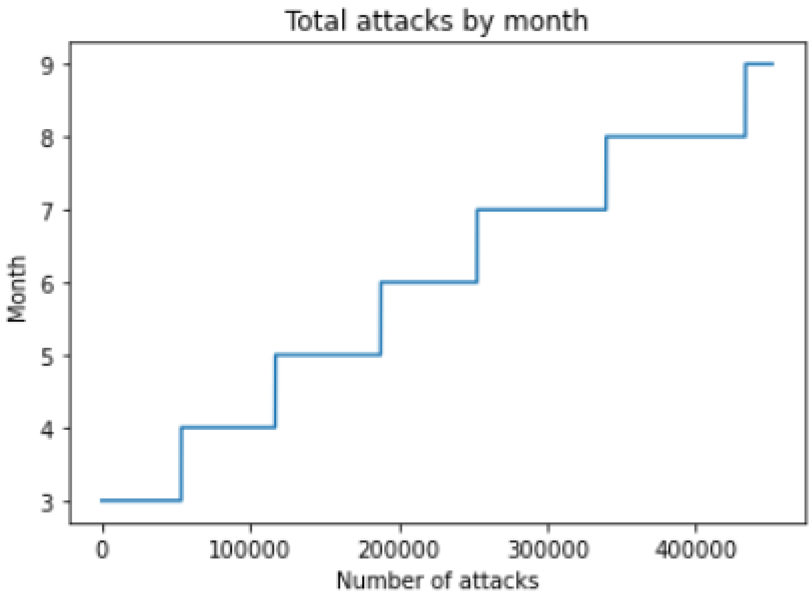

Fig. 9. Total attacks by month

Metric for assessing performance

Malicious attacks can indeed be classified as either positive or negative events. We divided the dataset into 4 trials [i.e., “true positive”, “true negative”, “false positive”, and “false negative”]. Our algorithm forecasts the data individually; therefore we arrange them as per their prediction findings and then use the data as good instances. In this section, the accuracy metric is assessed with our proposed work for predicting malicious attacks. The metric is mentioned below.

Accuracy

It displays the percentage of data in the testing dataset that were correctly classified, as seen in equation (15). Table 1 depicts the accuracy rate for proposed and existing techniques.

$$Ac = \frac{(tp+tn)}{(tp+tn+fp+fn)}$$

(15)

Here, true positive=tp=amount of right forecasts of a positive sample, true negative=tn=amount of right forecasts of a negative sample, false positive=fp=amount of wrong forecasts of a positive sample, and false negative=fn=amount of wrong forecasts of a negative sample **Table 2**.

Table 2. Accuracy (%) for proposed and existing techniques

S.No	Techniques	Accuracy (%)
1.	Auto-IF	95.4
2.	BC + kNN	94.92
3.	STL	93.96
4.	HCRNN	97.5
5.	Wrapper step-wise ResNet [proposed]	98.642

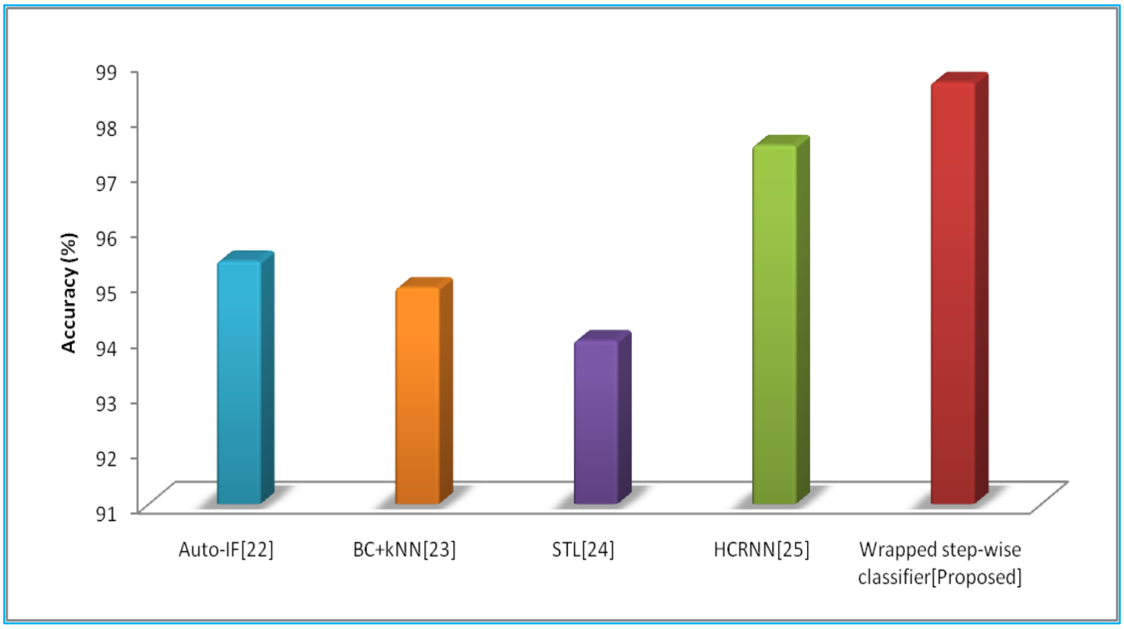

Fig. 10. Comparison of accuracy with proposed and existing techniques

Discussion

Detecting intrusions in the present cyber domain is a controversial subject. Machine learning techniques have been used to detect intrusions in a variety of ways. In this part, we discuss the effectiveness of our proposed technique over the existing techniques by assessing the above-mentioned performance metric regarding cyber security enhancement for the given data. **Fig. 11** depicts the comparison of accuracy with both the proposed and existing techniques regarding the classification of malicious attacks. In there was an inconsistent performance of accuracy in the detection of threats. Just one parameter was performed and this approach detects only the lower-frequency threats. In there are more number problems like the poor depiction of features, inconsistent reduction of dimensionality, and large progress time in the testing and training stages. In there is an incompatible extraction of features as well as knowledge learning and just a single intrusion recognition database. But, our proposed technique overcomes those specified limitations and accomplishes the greatest accuracy (98.642%) over existing techniques.

5. Conclusion

This paper presented a novel Wrapper stepwise ResNet classifier to identify the malicious attacks regarding cyber security enhancement throughout the banking sector. Here, Kaagle cyber security datasets are employed for classifying the malicious attacks. In the first stage, pre-processing was done to eliminate unwanted data or errors from the collected original dataset. After that, the attack-related features are identified in the second stage by employing the hierarchical network approach. The proposed technique was applied to classify the malicious attacks. To accomplish the greatest performance, the proposed technique was compared with certain existing techniques. Finally, we secured a 98.642% accuracy rate for our proposed technique over the existing techniques and the outcome was displayed via the Python tool. If our research will concentrate on the selection of feature sub-sets, then we obtain additional growth in the performance of identification of malicious attacks in upcoming years.

Declaration

Ethics Approval and Consent to Participate:

No participation of humans takes place in this implementation process

Human and Animal Rights:

No violation of Human and Animal Rights is involved.

Funding:

No funding is involved in this work.

Data availability statement:

Data sharing not applicable to this article as no datasets were generated or analyzed during the current study

Conflict of Interest:

Conflict of Interest is not applicable in this work.

Authorship contributions:

All authors are contributed equally to this work

Acknowledgement:

There is no acknowledgement involved in this work.

References

[1] L.A. Maglaras, K.H. Kim, H. Janicke, M.A. Ferrag, S. Rallis, et al., "Cyber security of critical infrastructures," *ICT Express*, vol. 4, no. 1, pp. 42-45, 2018. Article (CrossRef Link)

[2] I.F. Kilincer, F. Ertam, and A. Sengur, "Machine learning methods for cyber security intrusion detection: Datasets and comparative study," *Computer Networks*, vol. 188, p. 107840, 2021. Article (CrossRef Link)

[3] H.H. Jazi, H. Gonzalez, N. Stakhanova and A.A. Ghorbani, "Detecting HTTP-based application layer DoS attacks on web servers in the presence of sampling," *Computer Networks*, vol. 121, pp. 25-36, 2017. Article (CrossRef Link)

[4] S. Behal and K. Kumar, "Detection of DDoS attacks and flash events using information theory metrics–an empirical investigation," *Computer Communications*, vol. 103, pp. 18-28, 2017. Article (CrossRef Link)

[5] N.Z. Bawany, J.A. Shamsi, and K. Salah, "DDoS attack detection and mitigation using SDN: methods, practices, and solutions," *Arabian Journal for Science and Engineering*, vol. 42, no. 2, pp. 425-441, 2017. Article (CrossRef Link).

[6] Y. Jia, Y. Qi, H. Shang, R. Jiang, and A. Li, "A practical approach to constructing a knowledge graph for cyber security," *Engineering*, vol. 4, no. 1, pp. 53-60, 2018. Article (CrossRef Link).

[7] X. Fang, M. Xu, S. Xu, and P. Zhao, "A deep learning framework for predicting cyber attacks rates," *EURASIP Journal on Information security*, vol. 2019, pp. 1-11, 2019. Article (CrossRef Link).

[8] Uddin, M., Ali, M. and Hassan, M.K., "Cyber security hazards and financial system vulnerability: a synthesis of the literature," *Risk Management*, vol. 22, no. 4, pp. 239-309. Article (CrossRef Link).

[9] T. Godbole, S. Gochhait and D. Ghosh, "Developing a Framework to Measure Cyber Resilience Behaviour of Indian Bank Employees," in *ICT with Intelligent Applications*, Springer, Singapore, 2022, pp. 299-309. Article (CrossRef Link).

[10] F. Ullah, H. Naeem, S. Jabbar, S. Khalid, M.A. Latif, et al., "Cyber security threats detection in the internet of things using deep learning approach," *IEEE Access*, vol. 7, pp. 124379-124389, 2019. Article (CrossRef Link).

[11] M. Al-Omari, M. Rawashdeh, F. Qutaishat, H.M. Alshira, and N. Ababneh, "An intelligent tree-based intrusion detection model for cyber security," *Journal of Network and Systems Management*, vol. 29, no. 2, pp. 1-18, 2021. Article (CrossRef Link).

[12] K. Sadaf and J. Sultana, "Intrusion detection based on the autoencoder and isolation forest in fog computing," *IEEE Access*, vol. 8, pp. 167059-167068, 2020. Article (CrossRef Link).

[13] L. Li, Y. Yu, S. Bai, Y. Hou, and X. Chen, "An Effective Two-Step Intrusion Detection Approach Based on Binary Classification and $ k $-NN," *IEEE Access*, vol. 6, pp. 12060-12073, 2017. Article (CrossRef Link).

[14] M. Al-Qatf, Y. Lasheng, M. Al-Habib, and K. Al-Sabahi, "Deep learning approach combining sparse autoencoder with SVM for network intrusion detection," *Ieee Access*, vol. 6, pp. 52843-52856, 2018. Article (CrossRef Link).

Damodharan Kuttiyappan is a Director in Data & Analytics, Natwest Group with over 20 years of experience in holding leadership position across various Domains - Medical, Semiconductor, Automotive and Financial sector. Currently Leading AI/ML and Data Science Portfolio in Data & Analytics Domain. He is a FinOps enthusiast, leading FinOps & Cloud Cost Management in Natwest. He is actively involved in FinOps Foundation. Expertise on Agile transformation, creating vision, defining Roadmap and execution for larger domains. Certified in AML/KYC, CSM, PMP, LeSS. Certified SAFe Agilist and SAFe RTE. He is currently pursing research as an external candidate in SRM Institute of Science and Technology, Vadapalani, Chennai, Tamilnadu, INDIA. He has published an IEEE research papers on his Master and the paper has been awarded as the best paper in International conference held in Croatia. He is interested in Volunteering activities, Gender Balance community, Upskilling freshers out of college to increase their chances of employability. Guest speaker in various prestigious universities.

Dr. Rajasekar. V is working as Associate Professor, SRM Institute of Science and Technology, Vadapalani, Chennai, Tamilnadu, INDIA. He has received B.E., Degree in Computer Science and Engineering, Madras University, Chennai. M.E., Degree in Embedded System Technologies, Anna University, Chennai. PhD from Anna University, Chennai. Research interest includes Image Processing, Object Identification and Classification, Evolutionary Computing. He has got an experience of 20 years in teaching profession. He has so far written 3 patents and published more than 20 research papers in the journal of National and International level.