Annals of the University of Craiova, Mathematics and Computer Science Series
Volume 49(1), 2022, Pages 174–182, DOI:
ISSN: 1223-6934

Predicting future community intrusions using a novel type and encryption mechanism architecture for attack node mitigation

Sangeetha Prabhu, P.S. Nethravathi, Cristi Spulbar, and Ramona Birau

Abstract. The recent exponential rise in the number of cyber-attacks has demanded intensive study into community intrusion detection, prediction, and mitigation systems. Even though there are a variety of intrusion detection technologies available, predicting future community intrusions is still a work in progress. Existing approaches rely on statistical and/or superficial device mastery techniques to solve the problem, and as a result, feature selection and engineering are required. The truth is that no single classifier can provide the highest level of accuracy for all five types of training data set. Cyber-attack detection is a technique for detecting cyber-attacks as they emerge on a laptop or network device, intending to compromise the gadget's security. As a result, using a novel type and encryption mechanism, this paper offered a unique architecture for attack node mitigation. The input UNSW-NB15 dataset is first acquired and divided into training and testing statistics. First and foremost, the information is pre-processed and capabilities are retrieved in the training section. The Taxicab Woodpecker Mating Algorithm (TWMA) is then used to select the critical characteristics. The attacked and non-attacked information are then classified using the BRELU-ResNet (Bernoulli's Leaky Rectified Linear Unit - Residual Neural Community) classifier. The encrypted at Ease Hash Probability-Based Elliptic-Curve Cryptography (ESHP-ECC) technique is used to encrypt the ordinary facts, which are subsequently kept in the security log report. Following that, using Euclidean distance, the shortest course distance is estimated. Finally, the records are decrypted using a set of principles known as Decrypted Relaxed Hash Probability-Based Elliptic-Curve Cryptography (DSHP-ECC). If the input appears in the log file during testing, it is regarded as attacked data and is prevented from being transmitted. If it isn't found, the procedure of detecting cyber-attacks continues.

2020 *Mathematics Subject Classification.*
Key words and phrases. Cyber-attack detection; BAIT approaches; Cryptosystem; ResNet; Feature extraction; Woodpecker Mating Algorithm (WMA); Elliptic Curve Cryptography (ECC).

1. Introduction

The digital revolution of large-scale manufacturing environments promotes the use of big data analytic in fixing plant outages, equipment breakdowns, fault prediction, and ensuring cybersecurity through the extension of computer networks and interconnectivity of computers in cyber-physical systems [16, 18]. In recent decades, the topic of cyber-defense has piqued researchers' attention, particularly as cyber-physical networks have become extremely malicious cyber-attacks that could threaten any part of the unexploited cyber surface [14]. This emphasizes the significance of putting in place efficient identification algorithms and robust solution mechanisms that protect both

the cyber and physical facets of the infrastructure ? a crucial prerequisite for improving operational technologies [14, 22]. Many contributions have been made throughout this field of operational technologies by the process automation and control group in particular.

CPS (Cyber-Physical Systems) is a term used to describe the mixture of computational, communication, and physical components [9, 12]. Cyber-Physical Systems CPS is a modeling tool that can be used to simulate a wide range of applications, including sophisticated critical infrastructures. Indeed, the widespread integration of Cyber-Physical Systems in vital infrastructures has increased their significance in sustaining economic growth, and their stability and durability have become essential in all facets of modern life [17, 5]. Security incidents and component faults are two of the biggest abnormalities that can disrupt CPS's daily function. Since CPS are so essential to contemporary society's day-to-day activities, they've become a tempting choice for cybercriminals. Because of their extensive use, their attack surface has grown significantly [6]. Various components of the CPS, like every other physical control device, will malfunction at the same time. Both faults and attacks can cause the machine to behave abnormally, but the consequences can be somewhat different. CPS operators may select the appropriate rehabilitation actions that mitigate the detrimental consequences of irregular behavior as they can differentiate [1]. Defining the criteria that could lead to such distinction is a difficult challenge that necessitates a thorough examination of individual components in a CPS structure before arriving at a holistic solution [2, 15].

A malfunction that influences any of CPS's components will cause it to behave abnormally (nodes). Fault detection in CPS has proven to be a difficult challenge due to the system's complexity and large size, as well as the fact that flawed activity is a complex and diverse problem [13]. Traditional CPS fault detection methods focus on the operator's knowledge, while more recent approaches, which characterize the modern IoT age, rely on sensor and alarm data. Machine learning methods and human expertise are combined in certain IoT solutions for fault diagnosis [7, 5]. For example, Artificial Neural Networks, which are adaptive structures inspired by biological systems, are used in fault detection in power and smart grid systems. RBF and SVM are two popular methods in artificial neural networks. Other methods [3] make use of logic to avoid latent faults that can occur when a stable environment is caused by a control system for a failure condition. Existing CPS security procedures are usually classified according to the security triad of secrecy, transparency, and availability [20, 10]. A security purpose is often linked to the appropriated mitigating measures that seek to defend a CPS system defined by a particular system model from an adversary.

The proposed model works so that the system is first trained on the dataset, including the DDoS attack and ransomware components. The model examines if it contains malware from DDoS or from Ransomware. When tested, we use trained information or data set to provide the results on attack existence and what sort of attack we offer the extracted characteristics of input. When the model identifies the attacker node, it is removed via the BAIT technique from the network.The rest of the paper could be written as follows: the second segment examines the related studies that are relevant to the proposed technique. The recommended strategy, known as a unique way of BRELU-ResNet based completely cyber-assault detection machine

with BAIT-based approach for mitigation, is explained in section three. Section 4 depicts the findings and discussion for the suggested strategy, which is entirely based on performance indicators. Finally, step five brings the paper to a close with destiny work.

2. Literature review

Wang et al. [20] published a scenario-based two-stage sparse cyber-attack model for smart grids with complete and partial network details in 2018. The proven cyber-attacks were successfully detected, and a security mechanism based on interval state estimation (ISE) was implemented in a novel way. The upper and lower limits of each state variable were modeled as a dual optimization problem in this process, to maximize the function variable's variance cycles. Furthermore, a popular deep learning algorithm, the stacked auto-encoder (SAE), was utilized to collect nonlinear and non-stationary features in electric load results. Such features were then used to increase predictive performance for electric loads, resulting in state variables with a narrow width. A parametric Gaussian distribution was used to represent the variance of forecasting errors. Comprehensive studies on numerous IEEE benchmarks have been used to show the validity of the current cyber-attack models and security mechanisms.

In 2019, Defu et al. [19] presented a machine learning-based attack detection model for power systems that were trained using data and logs obtained by phasor measurement units (PMUs). The findings demonstrate that the data processing method could increase the model's precision, and the AWV model could efficiently identify 37 different types of power grid behaviors. The feature development engineering was completed, and the data was then sent to various machine learning models, with the random forest being selected as AdaBoost's simple classifier. Finally, various comparison criteria were used to equate the proposed model to other ones. The experimental findings show that this model can reach a 93.91 percent accuracy rate and a 93.6 percent identification rate, which is better than eight recently established techniques.

In 2020 Mariam et al. [11] established a recovery strategy for the optimal re-closure of the trickled transmission lines. In specific, a framework for deep strengthening learning (RL) has been created to enable the strategy to adapt the unpredictable cyber-attack scenarios and to take decision-making capabilities in real-time. In this context, an environment has been set up for simulating power system dynamics and generating training data during the attack-recovery process. The profound RL strategy to determine the optimal lock-up time was trained with this information. Numerical outcomes demonstrate that the approach utilized would minimize cyber-attack effects in different circumstances.

Integrity attacks on CPSs were studied by means of Mo and Sinopoli [8] in 2012 the usage of discrete linear time-invariant structures. The researchers were able to characterise the available additives of the system kingdom and estimate the error underneath attack a good way to verify the gadget's resilience to integrity attacks. Additionally they used an ellipsoidal approach to find the on hand set's outer approximations. But, in a few cases where the accessible set is unbounded, the attacker can be capable of undermine the system.

3. Methodology

3.1. Proposed model for Cyber-Attack Detection and Mitigation System. Over the last few years, the increasing incidence of Cyber-Physical Systems (CPS) attacks has increased concerns regarding industrial control machine cybersecurity. ICS cybersecurity efforts today rely heavily on firewalls, statistics valves, and other intrusion detection and prevention systems, which may not be enough to combat escalating cyber threats from persistent attackers. Previous research has developed a framework for identifying assaults using a deep learning technique. Even though the attack node in the network was detected, it was no longer deactivated. As a solution to this challenge, an upgraded and effective adversary model will be presented. As a result, this work presents a novel architecture for assault node mitigation based on a unique class and encryption approach. Initially, the input data is divided into two categories: training data (80 percentage) and testing data (20 percentage). The total training data is initially pre-processed. The next step is to extract features from the training dataset as input. The feature is tailored for determining the critical capabilities utilizing TWMA in the 0.33 stage. The suggested BRELU-ResNet classifier is then used to train the characteristic. The classifier divides the data into attack and non-attack categories. If the data is attack data, use the BAIT technique to record the Source IP Address into a secure log file. Following that, if the information is updated regularly, the data are prepared for transmission. The records are first encrypted using the ESHP-ECC method before being sent. Following that, using Euclidean distance, the shortest route distance is estimated. The records are decrypted using the DSHP-ECC method at the destination. During testing, the checking facts are first checked in the Security Log File (SLF). If the source IP address of the data is already known, the records are blocked or an assault is identified. The proposed structure is depicted as a block diagram in Figure 1.

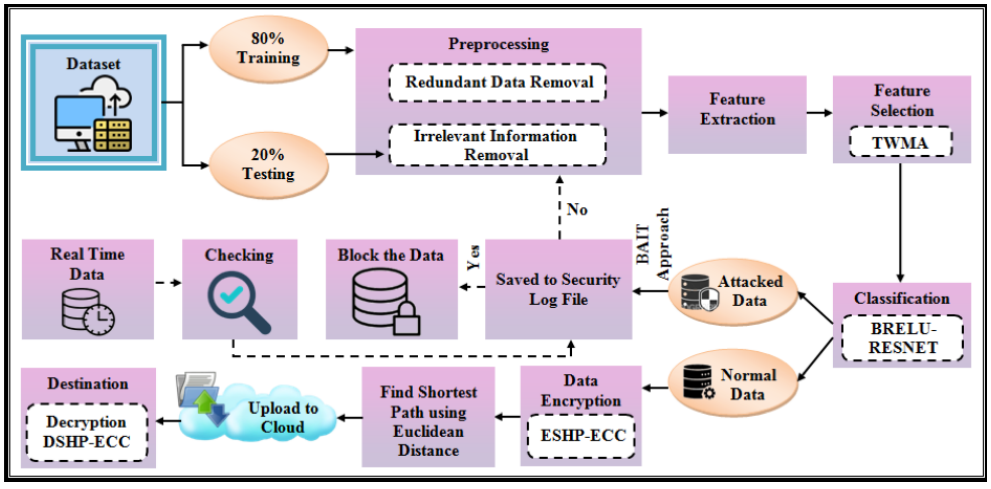

FIGURE 1. The framework for the proposed cyber-attack detection and mitigation system (Jiang, Wang, Wang, and Wu, 2020) [8].

3.2. Data Encryption Using ESHP-ECC. Elliptic-curve cryptography (ECC) is a public-key cryptosystem based on the elliptic curve hypothesis, which is a secure asymmetric encryption scheme used for data security. It generates public and private keys for each user through the elliptic curve properties. These keys are then used to encrypt and decrypt the data. In a conventional ECC technique, the keys are generated randomly. So, the attackers may easily hack the key information. To address the problem, the probability of ones and zeros are generated based on the randomly generated key value. Also, the key values are converted into a hash value using the secure hash method. Due to the alterations in the general ECC, the proposed technique is called as Encrypted Secure Hash Probability-based Elliptic-curve cryptography (ESHP-ECC) algorithm. The encryption process of ESHP-ECC is detailed below,

- At first, the elliptic curve equation used for key generation is given by,

$$Y^2 = X^3 + aX + b, \tag{1}$$

where in (1), a, b denotes the integers.

- Then, a random number (η) is generated from $([1, n-1])$ and the probability of ones and zeros of this random number is calculated, defined as the private key. After that, the public key (ρ) is calculated as,

$$\rho = \eta * B. \tag{2}$$

Here, B describes the point on the elliptic curve.

- Thereafter, these public and private keys are converted into a hash value using a secure hashing method. Secure Hashing Algorithm (SHA) is a cryptographic hash function that takes the keys as the input and produces a 160-bit (20-byte) hash value. The private and public keys after hashing are represented as η and ρ accordingly.

- Consider, M be the message to be transmitted and it has the point Q on the elliptic curve. Randomly select σ from $[1, n-1]$. Two cyphertexts $(C^{(1)}, C^{(2)})$ are calculated using equations (3), (4),

$$C^{(1)} = \sigma * B \tag{3}$$

$$C^{(2)} = Q + \sigma * \rho \tag{4}$$

where, $(C^{(1)}, C^{(2)})$ defines the encrypted message that is transmitted to the cloud server through the shortest path.

3.3. Decryption through DSHP-ECC. The encrypted message in equation 4 is decrypted using the below equation,

$$Q = C^{(2)} - \eta * C^{(1)}, \tag{5}$$

where, Q specifies the original message.

4. Results

This section focuses on the specific findings of the suggested structure's final consequence. The exhibition inspection, such as the relative inquiry, is performed to demonstrate the feasibility of the work. The suggested concept is carried out with the use of MATLAB, and the open source UNSW- NB15 dataset is utilized for this

work. These results focuses on the specific examination of the suggested structure's final consequence. The exhibition inspection, such as the relative inquiry, is performed to demonstrate the feasibility of the work.

4.1. Performance analysis of the proposed BRELU-RESNET. The suggested BRELU-ResNet is compared with existing methodologies such as CNN, ANN, Adaptive Network-based Fuzzy Inference System in terms of sensitivity, False positive rate (FPR), accuracy, False negative rate (FNR), precision, recall, specificity, F-Measure, and Matthews correlation coefficient (MCC) (ANFIS). The comparative analysis is also done with the existing techniques to state the effectiveness of the model.

Table 1: Performance analysis of proposed BRELU-ResNet with respect to FPR, FNR, and MCC.

Techniques	FPR	FNR	MCC
Proposed BRELU-ResNet	22.46	1.66	77.38
CNN	36.38	2.19	66.24
ANN	41.16	4.22	51.12
ANFIS	55.58	2.83	50.6

Table 1 depicts the performance evaluation of the proposed BRELU-ResNet and other existing techniques concerning FPR, FNR, and MCC. The lower value of FPR and FNR efficiently discards the misclassification or miss-prediction error.

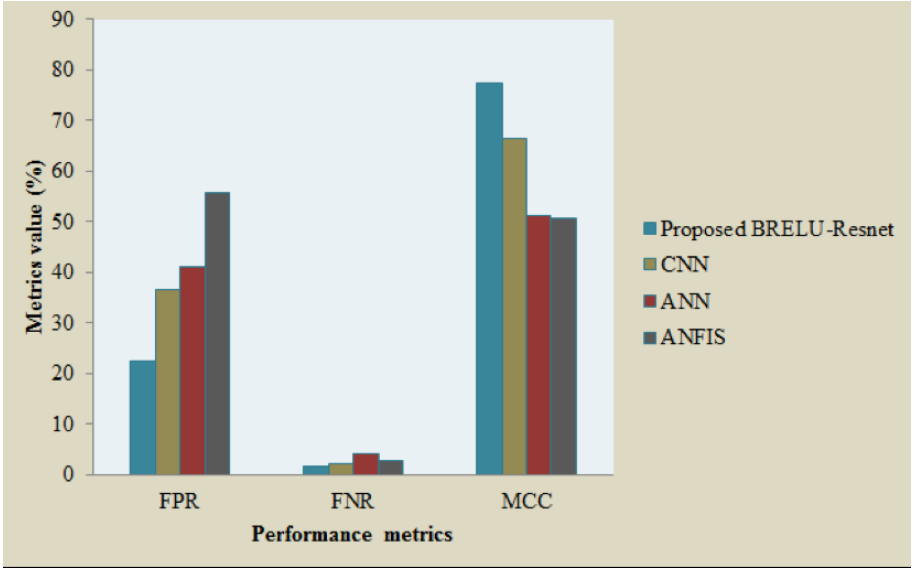

FIGURE 2. Comparative analysis of proposed BRELU-ResNet in terms of FNR, FPR, and MCC

Figure 2 compares the evaluation metrics such as FNR, FPR, and MCC of the proposed work with the existing works. The consequence of the model is determined by the low value of FPR and FNR rates and the high value of MCC.

5. Discussion

According to the results obtained in the previous section, the proposed method achieves 22.46 percentage of FPR and 1.66 percentage of FNR values. But the average FPR and FNR values of the existing techniques are 44.37 percentage and 3.0 percentage respectively. Conversely, the higher MCC value denotes the robustness of the model; here, the proposed method obtains 77.38 percentage of MCC, while the existing techniques obtain the average MCC value of 55.98 percentage.

Hence, it is revealed that the proposed work is more reliable and outperforms the existing approaches. In accordance with the significance of the model is resolute by the FNR and FPR rates of the proposed work are low and the MCC rate achieved by the proposed work is higher than the existing approaches. Hence, the proposed method outperforms the other state-of-art methods and delivers better outcomes in the cyber-attack detection process.

6. Conclusion

The research proposes a novel strategy for detecting and mitigating cyber-attacks using a BRELU- ResNet -based system with aBAIT-based mechanism. This method applied to a number of tasks involving the green detection of cyber-attacks. The work goes through pre-processing, function extraction, function choosing, and categorization for intrusion detection. The categorization step effectively determines if the facts are routine or malicious. The facts transfer operation begins if the records are normal. The encryption and decryption techniques are carried out in accordance with the SHP-ECC set of principles to ensure security. After that, the experimental assessment is completed, in which the overall performance evaluation and comparison analysis of the offered strategies are carried out in terms of a few overall performance metrics with the goal of validating the proposed algorithm's efficacy. The new approach can deal with a variety of uncertainty and produce more promising outcomes. The suggested technique achieves 22.46 percent of FPR, 1.66 percent of FNR, and 77.38 percent of MCCusing publicly available datasets named the UNSW-NB 15 dataset. On average, the suggested cyber-assault detection system surpasses current state-of-the-art technologies and remains more reliable and robust. The study will be expanded in the future with a few sophisticated neural networks, as well as a focus on unique sorts of practical assaults.

References

[1] M. Aamir and S.M.A. Zaidi, Clustering-based semi-supervised machine learning for DDoS attack classification, *Journal of King Saud University - Computer and Information Sciences* **7** (2019), no. 2, 1–11. DOI: 10.1016/j.jksuci.2019.02.003

[2] A. Al-Abassi, H. Karimipour, A. Dehghantanha, and R. M. Parizi, An ensemble deep learning-based cyber-attack detection in the industrial control system, *IEEE Access* **8** (2020), no. 5, 83965–83973. DOI: 10.1109/ACCESS.2020.2992249

[3] M. Marsaline Beno, I.R. Valarmathi, S.M. Swamy, and B. R. Rajakumar, Threshold prediction for segmenting tumors from brain MRI scans, *International Journal of Imaging Systems and Technology* **24** (2014), no. 2, 129–137. DOI: 10.1002/ima.22087

[4] X. Fang, M. Xu, S. Xu, and P. Zhao, A deep learning framework for predicting cyberattacks rates, *Eurasip Journal on Information Security* **2019** (2019), no. 1, 1–11. DOI: 10.1186/s13635-019-0090-6

[5] T. Gopalakrishnan, D. Ruby, F. Al-Turjman, D. Gupta, I.V. Pustokhina, D.A. Pustokhin, and K. Shankar, Deep learning enabled data offloading with a cyber-attack detection model in mobile edge computing systems, *IEEE Access* **8** (2020), no. 1, 185938–185949. DOI: 10.1109/ACCESS.2020.3030726

[6] B. Hussain, Q. Du, B. Sun, and Z. Han,, Deep Learning-Based DDoS-Attack Detection for Cyber- Physical System over 5G Network, *IEEE Transactions on Industrial Informatics* **17** (2021), no. 2, 860–870. DOI: 10.1109/TII.2020.2974520

[7] A.E. Ibor, F.A. Oladeji, O.B. Okunoye, and O.O. Ekabua, The conceptualization of Cyberattack prediction with deep learning, *Cybersecurity* **3** (2020), no. 1, 1–13. DOI: 10.1186/s42400-020-00053-7

[8] K. Jiang, W. Wang, A. Wang, and H. Wu, Network Intrusion Detection Combined Hybrid Sampling with Deep Hierarchical Network, *IEEE Access* **8** (2020), no. 3, 32464–32476. DOI: 10.1109/ACCESS.2020.2973730

[9] V. Kanimozhi and T.P. Jacob, Artificial Intelligence outflanks all other machine learning classifiers in Network Intrusion Detection System on the realistic cyber dataset CSE-CIC-IDS 2018 using cloud computing, *ICT Express* **8** (2020), no. 1, 1–8. DOI: 10.1016/j.icte.2020.12.004

[10] N.M. Karie, V.R. Kebande, and H.S. Venter, Diverging deep learning cognitive computing techniques into cyber forensics, *Forensic Science International: Synergy* **17** (2019), no. 1, 61–67. DOI: 10.1016/j.fsisyn.2019.03.006

[11] M. Elnour, N. Meskin, K. Khan, and R. Jain, A dual-isolation-forests-based attack detection framework for industrial control systems, *IEEE Access* **8** (2020), no. 3, 36639–36651. DOI: 10.1109/ACCESS.2020.2975066

[12] U. Noor, Z. Anwar, T. Amjad, and K.K.R. Choo, A machine learning-based FinTech cyber threat attribution framework using high-level indicators of compromise, *Future Generation Computer Systems* **9** (2019), no. 6, 227–242. DOI: 10.1016/j.future.2019.02.013

[13] Y. Pan, F. Sun, Z. Teng, J. White, D.C. Schmidt, J. Staples, and L. Krause, Detecting web attacks with end-to-end deep learning, *Journal of Internet Services and Applications* **10** (2019), no. 1, 2–22. DOI: 10.1186/s13174-019-0115-x

[14] D.T. Ramotsoela, G.P. Hancke, and A.M. Abu-Mahfouz, Attack detection in water distribution systems using machine learning, *Human-Centric Computing and Information Science* **9** (2019), no. 1, 1–26. DOI: 10.1186/s13673-019-0175-8

[15] M. Saharkhizan, A. Azmoodeh, A. Dehghantanha, K.K.R. Choo, and R.M. Parizi, An Ensemble of Deep Recurrent Neural Networks for Detecting IoT Cyber Attacks Using Network Traffic, *IEEE Internet of Things Journal* **7** (2020), no. 9, 8852–8859. DOI: 10.1109/JIOT.2020.2996425

[16] A. Samy, H. Yu, and H. Zhang, Fog-Based Attack Detection Framework for Internet of Things Using Deep Learning., *IEEE Access* **8** (2020), no. Dl, 74571–74585. DOI: 10.1109/ACCESS.2020.2988854

[17] M. Shafiq, Z. Tian, Y. Sun, X. Du, and M. Guizani, Selection of effective machine learning algorithm and Bot-IoT attacks traffic identification for the internet of things in a smart city, *Future Generation Computer Systems* **10** (2020), no. 7, 443–442. DOI: 10.1016/j.future.2020.02.017

[18] A. Subroto and A. Apriyana, Cyber risk prediction through social media big data analytics and statistical machine learning, *Journal of Big Data* **6** (2019), no. 1, 1–19. DOI: 10.1186/s40537-019-0216-1

[19] D. Wang, X. Wang, Y. Zhang, and L. Jin, Detection of power grid disturbances and cyber-attacks based on machine learning, *Journal of Information Security and Applications* **46** (2019), no. 1, 42–52. DOI: 10.1016/j.jisa.2019.02.008

[20] H. Wang, J. Ruan, Z. Ma, B. Zhou, X. Fu, and G. Cao, Deep learning aided interval state prediction for improving cybersecurity in the energy internet, *Energy* **17** (2019), no. 4, 1292–1304. DOI: 10.1016/j.energy.2019.03.009

[21] H. Wang, J. Ruan, G. Wang, B. Zhou, Y. Liu, X. Fu, and J. Peng, Deep Learning-Based Interval State Estimation of AC Smart Grids Against Sparse Cyber Attacks, *IEEE Transactions on Industrial Informatics* **14** (2018), no. 11, 4766–4778. DOI: 10.1109/TII.2018.2804669

[22] Y. Xin, L. Kong, Z. Liu, Y. Chen, Y. Li, H. Zhu, M. Gao, H. Hou, and C. Wang, Machine Learning and Deep Learning Methods for Cybersecurity, *IEEE Access* **6** (2018), no. 1, 35365–35381. DOI: 10.1109/ACCESS.2018.2836950

(Sangeetha Prabhu) College of Computer Science and Information Science, Srinivas University, Mangalore, India. ORCID ID 0000-0002-8026-1133
E-mail address: sangeethaprabhu96@gmail.com

(P.S. Nethravathi) College of Computer Science and Information Science, Srinivas University, Mangalore, India. ORCID ID 0000-0002-0088-3355
E-mail address: nethrakumar590@gmail.com

(Cristi Spulbar) Faculty of Economics and Business Administration, University of Craiova, Romania. ORCID ID 0000-0002-3909-9496
E-mail address: cristi_spulbar@yahoo.com

(Ramona Birau) C-tin Brancusi University of Targu Jiu, Faculty of Education Science, Law and Public Administration, Romania. ORCID ID 0000-0003-1638-4291
E-mail address: ramona.f.birau@gmail.com