IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received 23 March 2023, accepted 22 April 2023, date of publication 8 May 2023, date of current version 17 May 2023.

Digital Object Identifier 10.1109/ACCESS.2023.3273904

RESEARCH ARTICLE

Imperative Node Evaluator With Self Replication Mode for Network Intrusion Detection

RAGINI MOKKAPATI AND D. VENKATA LAKSHMI
School of Computer Science and Engineering, VIT–AP University, Amaravati 522237, India
Corresponding author: D. Venkata Lakshmi (venkatalakshmi.d@vitap.ac.in)

ABSTRACT In recent years, network expansion has increased exponentially, making security a pressing issue for modern systems. Monitoring user activity for abnormalities is a useful fraud detection strategy. The ability of a system to efficiently discover new, previously unknown vulnerabilities and respond in a way that minimises damage and, ideally, removes the threat, is one of the most important open research topics in the field of cyber security. This research provides a blueprint for an intrusion detection system that employs pattern matching and self-replication among other methods. As the system detects potentially dangerous symptoms in the surroundings, it compares them to the events that have become apparent so far to find a pattern that may explain their occurrence. Once this happens, it alerts other nodes in the system to keep an eye out for harmful event sequences, and it initiates the defence mechanism that lessens the number of false intrusion alarms. Using natural intrusion detection and self-healing idea, this research outlines a novel method for network security. An Imperative Node Evaluator with Self Replication Code and Auto Triggering Mode (INE-SRC-ATM) is proposed in this research for auto healing of the network if intrusion occurs and also to perform auto triggering of nodes for securing the network and reducing the false alarms. To activate the self-healing mechanism, the IDS must first identify and assess the impact of hostile actions on the network. This means that the self-healing process begins when the damage caused by malevolent activity is identified. The proposed model self triggering model immediately triggers when there is a dissimilarity on attributes that improve the network security levels. The proposed model when contrasted with the traditional model performs high in intrusion detection in terms of self replication triggering accuracy and intrusion detection accuracy levels.

INDEX TERMS Intrusion detection, network security, imperative node evaluator, self replication code, auto triggering, false alarms, malicious action, pattern matching.

I. INTRODUCTION

Detecting intrusions into a computer network involves continuously monitoring and analyzing system and network activity as the usage of internet increased in the modern society [1]. Researchers have devised a complete defence - in-depth solution for securing these networks. To identify, prevent, and respond to an attack [2], IDSs automate the process of analyzing network traffic. It keeps an eye on what's happening on the network, analyses the data, and keeps track of any suspicious activity [3]. When it detects potentially harmful activity, an immediate alert is sent to the administrator. IDS detection methods can be broken down into two broad classes: detection of abnormal behavior and detection of misuse [4]. The purpose of intrusion detection is to identify any out-of-the-ordinary behavior that may indicate an upcoming security breach. On the other hand, intrusion detection employs commonly exploited security gaps in order to trigger alerts and pinpoint infiltrations [5]. While IDS have proven their ability to detect a wide variety of network attacks and have evolved into a comprehensive defense-in-depth infrastructure, they face a significant challenge in the form of the enormous volume of alarms they produce [6], the vast majority of which are false positives [7]. There will be performance degradation in IDS effectiveness as a result of this. Another issue is that a human analyst would be overwhelmed by the sheer volume of alarms.

The associate editor coordinating the review of this manuscript and approving it for publication was Gongbo Zhou.

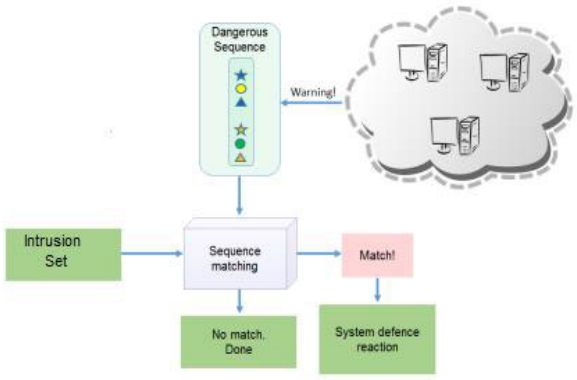

FIGURE 1. Self repair auto trigger IDS model.

While IDSs are commonly employed to identify online threats, they suffer from the drawback of producing an overwhelming amount of false positives and warnings. In addition, this will reduce the effectiveness of the IDS [8]. Many scientists are now driven by this issue to find a way to differentiate between significant and less important events and so reduce false positives in alerts. The main issues in informatics are the security [9], privacy [10], and secrecy of electronic data. Information about workers, customers, products, studies, and finances is collected by many different types of organizations, including the government, the military, corporations, financial and medical institutions, and individual firms. These days, most data is gathered, processed, and stored digitally on computers before being transported through networks. It can be challenging work to keep a healthcare facility safe from both insider and outsider threats to its assets, such as patient health records [11]. In order to detect malicious activity early, Intrusion Detection and Prevention Systems (IDPS) can be a very useful tool.

Using IDPS, it may be possible to detect an attack and either alert the proper authorities or prevent it from succeeding. There are a wide variety of dangers and methods of attack against computers and networks [12], and this is only expected to increase as management information systems become more sophisticated and widespread. As the number of attacks and vulnerabilities increases, and as misuse detection functions are unable to identify attacks for which no signatures exist yet, researchers are urged to advocate for an intrusion detection mechanism that is capable of identifying novel attacks through anomaly detection models [13]. An ID creates a standard for typical behavior and flag anything that deviates significantly from that as suspicious [14]. Anomaly detection may mistakenly label benign, everyday behavior as malicious, prompting an unnecessary response [15]. The self repair IDS with auto IDS trigger model is shown in Figure 1.

For self-healing or self replication of IDS to work, it doesn't always have to be fixed immediately [16]. Depending on the needs of the application and the best possible efficiency [17], self-healing systems may opt to do self-healing in either an offline or online mode. Autonomously selecting the optimal moment to shut down the service, do the repair [18], and then resume the service can be a more cost-effective self-healing option when the application does not have severe real-time requirements and is insensitive to short periods of down time [19]. However, in this work, online self-healing methods are focused due to the fact that many large-scale database systems crucial to businesses are required to be available continuously and can only be halted for repair at high cost [20]. Online self-healing necessitates not only the ability to autonomously find and repair the damage in real time, but also the ability to preserve the system's functionality [21]. The signature records the specific behaviours associated with a particular attack. This realistic strategy narrowly targets attacks, which increases accuracy while decreasing false positives. Signature-based detection can quickly and effectively identify malicious events because of its rapid processing for known threats and low false positive rates.

Self-healing is the term used to describe a system that can both detect and stop attacks, and repair any damage that may have occurred during data transmission in the network [22]. A self-healing system is one that can identify deviation from a normal system and apply a remedial action that can identify intruders and understand their impact, and can reverse from new states to the normal state by triggering the IDS to reduce the false alarms and to improve the network performance [23]. In this research, a novel approach is proposed to intrusion detection self replication, one that takes advantage of the detection of intrusion and the recognition of threat signals. As soon as the system detects potentially harmful symptoms in the environment, it compares them to the events that have transpired thus far to identify a pattern that may explain the emergence of the symptoms. A defence mechanism is activated, and other instances of the system are alerted to potentially harmful event sequences. Self-healing is the capacity of a system to detect when its normal operation has been disrupted and to make the necessary corrections to return to normal operation without any external intervention. The proposed model performs two operations, the first is a process of finding problems and stopping further damage from occurring, and the second is self-healing or repairing those problems by triggering the IDS to reduce false alarms in the network.

II. LITERATURE SURVEY

To defend a smart-grid system from unknown assailants with unexpected and dynamic behaviours, Hao et al. [2] suggested a unique defence approach called Adaptive Markov Strategy (AMS). In the event of self-play, AMS is guaranteed to converge to Nash Equilibrium (NE), and in the case of a stationary attacker, it converges to a best response. Considering the category of data integrity assaults in which an attacker succeeds to insert fake voltage information into the smart controller at a substation, users can gauge AMS's efficacy. A blackout or load shedding could result from such an attack. Several scale-dependent IEEE standard test cases are used in the extended simulations.

Even though it's been around for a while, the Controller Area Network (CAN) is still the most popular choice for in-vehicle networking because it doesn't have built-in security or authentication. The multiple communication technologies included in modern automobiles including Bluetooth, Wi-Fi, and cellular radio make them vulnerable to cyber attacks. Detecting and blocking cyber attacks on vehicles is, thus, an immediate necessity. Freitas De Araujo-Filho et al. [3] presented a new autonomous Intrusion Prevention System (IPS) for automotive CANs that can identify and prevent assaults without requiring access to information that is normally only available to car makers or modifying the architecture of the Electronic Control Units (ECUs). The author verified the accuracy and data tracks of two machine learning techniques for detecting fuzzing and spoofing attacks. Faster detection and identification of attacking frames are possible with less data.

It is expected that Service Oriented Architecture (SOA), built on top of the SOME/IP middleware and an Ethernet high transmission layer, will soon become standard in automobile networks. It has the potential to satisfy the expanding requirements for software components in contemporary automobiles, such as network connectivity and modularity. Quality-of-Service (QoS) agreements are an essential component of the cars of the future due to the wide variety of service requirements and the time-sensitive nature of network operations. Nevertheless, dynamic QoS selection is not possible with the current crop of middleware solutions. In this research, Çakir et al. [4] introduced a service-oriented middleware for quality-of-service-aware vehicular communication. The author contributed a multi-protocol stack that can handle the many types of communication based on the needs identified in an in-depth needs assessment, as well as a protocol for dynamic QoS negotiation. The author conducted a case study to confirm the viability of our method, and tested its efficacy using a simulation model of a real-world automobile network. This research shows that QoS-aware communication can succeed where others have failed, so long as the cross-traffic during negotiations does not exceed 70% of the available bandwidth and the network's setup time is kept to an acceptable minimum.

Cyber-attacks Misconduct in sensing and actuation, significant damage to physical things, and security issues are all possible outcomes of CPSs. Although machine learning methods have been presented as a means of protecting CPSs from cyber attack, detecting fresh assaults is difficult due to a lack of labelled data. Generative Adversarial Networks (GANs), an unsupervised method that implicitly models the system, show promise as a means of detecting cyber-attacks. However, there are stringent latency requirements for the detection of cyber-attacks against CPSs, as the attacks must be halted prior to the system being hacked. Here, Araujo-Filho et al. [5] proposed FID-GAN, an innovative GAN-based unsupervised IDS for CPSs based on the fog. The IDS is proposed for a fog design, which helps meet low-latency requirements by moving compute resources toward the final nodes. The suggested architecture uses a reconstruction loss derived from the restoration of data samples projected to the latent space to improve detection rates. Like minded approaches have difficulty computing the reconstruction loss, making them unfeasible for latency-sensitive applications. Training an algorithm that speeds up the computation of the reconstruction loss is one way we deal with this issue.

Defending the entire network is no longer sufficient in a world when organizations are adopting new IT working patterns like Bring Your Own Device (BYOD) and remote working. In recent years, a novel security architecture known as Zero Trust Architecture (ZTA) has emerged, with a focus on the breach approach as the primary threat model. Until proven otherwise, the ZTA treats every endpoint as potentially malicious. However, even after authentication has been confirmed by the endpoint, attacks using Advanced Persistent Threats (APT) can still take control of an authorized session through that endpoint. This makes the endpoint the weak spot of ZTA since they can undertake a variety of user/device centered harmful operations in addition to lateral movement. In this study, Alevizos et al. [6] proposed a Blockchain-enabled Intrusion Detection and Prevention System (BIDPS) that augments Zero Trust Architecture (ZTA) onto endpoints as a means of effectively discouraging Advanced Persistent Threat (APT) attack capabilities. The primary goals of the BIDPS are to identify and thwart attackers' approaches and tactics according to MITRE's ATT&CK enterprise matrix before the lateral mobility stage, and to migrate trust from the endpoint to the blockchain, hence establishing an inalterable system of explicit trust.

The model for preventing cyber intrusions is an innovative approach to cyber defence that makes use of an intelligent defensive system. It is not only able to spot suspicious activity, but to act swiftly in response to it as well. In this research, semi-supervised clustering and the idea of deep learning are used by Xian et al. [7] to the field of cyber intrusion prevention. The current trend in the evolution of neural networks is deep learning on the basis of deep structures. When it comes to preventing cyber intrusions with a low recognition error rate, semi-supervised learning can be quite useful with the combination of a huge number of unidentified cyber traffic data and a small quantity of labeled cyber traffic data. Because of its low incidence of error, technology based on Discriminative Deep Belief Networks (DDBN) has become a topic of intense study in the field of cyber intrusion prevention. To address the issue of high classification error rates in the cyber intrusion prevention model, this work proposes employing DDBN for large-scale semi-supervised deep learning based on local and non-local regularization. The suggested DDBN model has the lowest error rate in comparison to the Hopfield, Support Vector Machine (SVM), Generative Adversarial Network (GAN), and Deep Belief Network-Random Forest (DBN-RFS) classifiers for cyber intrusion prevention. Because of this, the proposed method can boost the IDS's efficiency.

In order to provide low-cost, high-efficiency, ubiquitous 5G services, mobile small cell technologies are seen as a key component of the 5G infrastructure. As a result, Network Coding (NC) technology is anticipated as a viable option for the wireless network of mobile small cells to boost its throughput and functionality. However, due to NC's flaws, NC-enabled mobile small cells are susceptible to pollution attacks. The following transmission of coded packets of the same iteration from the source node to the destination nodes may still be contaminated by the attackers, despite the fact that there are a number of works on pollution attack detection. Thus, in this study, Parsamehr et al. [11] described an intrusion detection and location-aware prevention (IDLP) method that not only detects the polluted packets and drops them, but also identifies the attacker's precise location to block them and avoid packet pollution in subsequent transmissions. Power grids today can be monitored and regulated from farther away than ever before with the widespread adoption of Information And Communication Technologies (ICT) in the distribution system. But this rapidly expanding interconnectedness also means that the modern distribution grid is more susceptible to disruptions. Therefore, there is a pressing need for study of intrusion/anomaly detection systems at the distribution layer. While much emphasis has been paid to securing the Supervisory Control and Data Acquisition and individual nodes, research on Intrusion Detection Systems for the power grid has largely ignored the possibility of coordinated cyber attacks on many nodes. Distributed systems have not yet had a comprehensive strategy for cyber security implemented. Appiah-Kubi et al. [12] introduced a new method for preventing intrusions into distribution systems by utilizing a multi-agent system.

In the realm of cyber defence, Network Intrusion Detection (NID) system is important. However, the main problem with the current machine learning-based NID research is that their experimental settings don't mirror real-world scenarios where new, unknown assaults are continually appearing. Their overestimation of detection capacity can be traced back to the fact that all test attack types are known in training and therefore test cases would share features with the training data. Seo et al. [13] presented a novel approach to populating test data with fresh, up-to-date traffic that includes novel attack types not present in training data. The prediction accuracy of existing detectors is reduced by around 20% in the suggested environment, relative to what has been published. In addition, an in-depth investigation of detection accuracy by attack types has shown that the current models excel at detecting some attack types, but struggle to detect others, such as DoS, DDoS, web attack, and port scan. The author presented a new neural detector, MHSA, built on a multi-head self-attention mechanism, whose architecture is more suited to capturing dispersed pieces of evidence in network traffic.

The increasing prevalence of embedded electronics in modern automobiles has exposed the formerly secure vehicular system to the possibility of cyber attacks via both direct and indirect access to the vehicle's internal networks, including the controller area network (CAN). Despite the growing prevalence of cyber and physical attacks on vehicles, the CAN bus does not employ a security standard to defend them. To mitigate this threat, Olufowobi et al. [14] presented SAIDuCANT, a specification-based IDS that employs anomaly-based learning algorithm with the real-time model as input and introduced a novel technique to extract the CAN bus's real-time model parameters. The author used a publicly available CAN dataset gathered from real-world settings and CAN logs acquired from two passenger vehicles to measure SAIDuCANT's efficacy. As demonstrated by the experiments, SAIDuCANT was able to identify data injection assaults with a negligible false positive rate.

Once operated solely by mechanical parts, today's cars now feature integrated circuits for a variety of functions. While these gadgets' in-car communications enhance safety and comfort, they are also susceptible to cyber-physical threats and attacks. Intrusion detection systems are a tried and true method of spotting intrusion attempts and other suspicious activity. Unpredictable anomalies in the network cause sudden shifts in the statistical properties of the messages. Olufowobi et al. [15] presented a method for detecting data software vulnerabilities on the CAN bus using an anomaly-based intrusion detection strategy based on the cumulative sum (CUSUM) activity recognition algorithm. To cut down on false alarms and lag time, the author used the change-point algorithm necessitates. The author tested the detection method in three different attack situations using a real dataset derived from a running automobile.

Electronic Control Units (ECUs) are installed in automobiles to improve the system's overall performance and communication. Such connection, however, leaves an unprotected internal CAN vulnerable to cyberattacks. Supervisory modules like IDS have been developed for detecting malicious messages in CAN networks without requiring changes to existing ECUs or generating excessive network traffic. While cutting-edge solutions may be vehicle dependent, conventional IDS methods rely on time and frequency thresholding, which results in high false alarm rates. Bozdal et al. [16] introduced a wavelet-based method for evaluating CAN network transmission patterns, with the goal of pinpointing the location of any observable behaviour changes in CAN data. Using real-world vehicle traffic from two separate research institutions, the proposed Wavelet-based Intrusion Detection System (WINDS) is put through its paces in a variety of attack scenarios before being enhanced to include more extensive attack scenarios using synthetic attacks. The method is examined, and the results are compared to those obtained using the state-of-the-art solutions and the traditional frequency-based approach.

Self-organizing mapping is a technique for creating artificial neural networks that can be used to efficiently represent the topology of high-dimensional data for uses such as network intrusion detection. Nonetheless, it is still difficult to faithfully describe the topology of network traffic data that has an uneven distribution, which degrades the effectiveness

of measures like DoS attack detection. As a result, Qu et al. [17] offered a novel model of statistically-enhanced directed batch growth self-organizing mapping, update the definition of the growth limit used to evaluate/control neuron expansion, and for the first time incorporate the inner distribution component for fine-grained data distinguishing. Numerical experiments on two datasets (KDD99 and CICIDS2017) show that the proposed model's use of statistical concepts significantly improves key performance metrics for DoS attack detection. These metrics include detection rate, false positive rate, and training time.

Cognitive computing, artificial intelligence, big data, and the Internet of Things (IoT) have come a long way in recent years, and the result is a convergence of the real and virtual that is altering people's daily routines. Although cognitive computing has greatly aided in the study and implementation of Cyber-Physical Systems (CPSs), there are still substantial challenges to the reliability and widespread use of CPSs due to specific security vulnerabilities. Therefore, it is important to identify, analyze, and predict better in order to improve the effectiveness of intrusion detection and to clarify and address the flaws of existing intrusion detection methods for CPSs. To enhance between-class learning, Gao et al. [18] first presented a unique self-learning spatial distribution technique called Euclidean distance-based between-class learning (EBC learning), which uses the ED calculated among k -nearest neighbors of various classes to make predictions. In addition, the author presented a cognitive computing-based intrusion detection approach for industrial CPSs based on EBC learning and the border-line SMOTE and random forest (BSBC-RF) architecture. The suggested EBC learning has significant spatial constraint capability, as evidenced by experimental findings over an actual industrial traffic dataset, and can boost prediction and recognition performance.

The cyber physical system relies heavily on Wireless Sensor Networks (WSNs), which are self-organizing, multi-hop networks made up of many individual sensors. Blackhole, grayhole, flooding, and scheduling attacks are some examples of common attacks in WSN that can do significant damage rapidly. Furthermore, due to the limited resources of sensor nodes and the huge amount of redundancy in addition to high correlation of network data, intrusion detection techniques for WSN suffer from the limitations of poor detection rate, substantial calculation overhead, and high false alarm rate. In light of these issues, Jiang et al. [19] presented SLGBM, a novel intrusion detection technique tailored specifically for WSNs. To begin, the original traffic data's feature space data dimension is decreased using the Sequence Backward Selection (SBS) algorithm to lessen the computing burden. Then, various network assaults are identified using a LightGBM algorithm.

When it comes to keeping a network of computers and other electronic devices safe from harm, IDSs are crucial components. False alarm rates can be kept low while the ADR for attacks is kept high with the help of a misuse IDS. Misuse IDSs, on the other hand, are hampered by a lack of agility due to their inability to adjust to novel and unknown settings. The problem is too huge for humans to handle on their own, what with the vast scale of today's networks and the complexity of massive data on network traffic. For this reason, Papamartzivanos et al. [20] offered a new approach that integrates the strengths of self-taught learning with those of the MAPE-K framework to produce an extensible, adaptable, and self-sufficient abuse IDS.

III. PROPOSED FRAMEWORK

In order to prevent attackers from gaining access to sensitive data or services across a network, intrusion detection and prevention systems monitor for suspicious activity. In common parlance, an intrusion is any form of illegal interference [27], which is almost often done maliciously. The goal of an attack is to gain access to an organization's internal network so that malicious actors can gather intelligence about the firm, such as its software systems, operating systems, tools/utilities, and software applications. People from outside the company typically carry out intrusions. Internally authorized individuals may commit such assaults by misusing their authority or by going outside the scope of their authorization, and it is necessary to secure against such intrusions as well.

The self-healing features of a computer employ the scheduler's activity as a source of pattern data to trigger an automatic threat warning production module [28]. Consequently, the warning sign is gleaned from keeping monitoring the system performance indicators such outbound network traffic and thread activity. The auto triggering model executes the self-healing feature as part of its scheduler. All fixes and upgrades have been applied and there have been no warnings about any potential security issues. An Imperative Node Evaluator is considered from the network that has best performance among the nodes in the network and this node will monitor the network nodes transactions and their behavior for malicious actions detection and triggers the self replication model when an intrusion is identified.

Parameters such as event type, anomaly value, and risk value are calculated based on event analysis. It is important to keep in mind that various anomaly detection algorithms offer varying means through which an event's anomalous value might be determined. The estimated anomaly score can vary widely depending on the method used, which in turn affects the inferences made when looking for potentially harmful events. A running timeline is maintained, and new occurrences are added as soon as they have been analyzed. To be useful for event sequence matching, the timeline should only provide an event category or particular attributes of events, rather than the actual unique events themselves. Comparable analysis and categorization of event sequences can be performed on a timeline of occurrences, as is done with event classification. New events are added to the classification system, which may result in a reclassification if the event profiles alter. The proposed model work flow is presented in Figure 2.

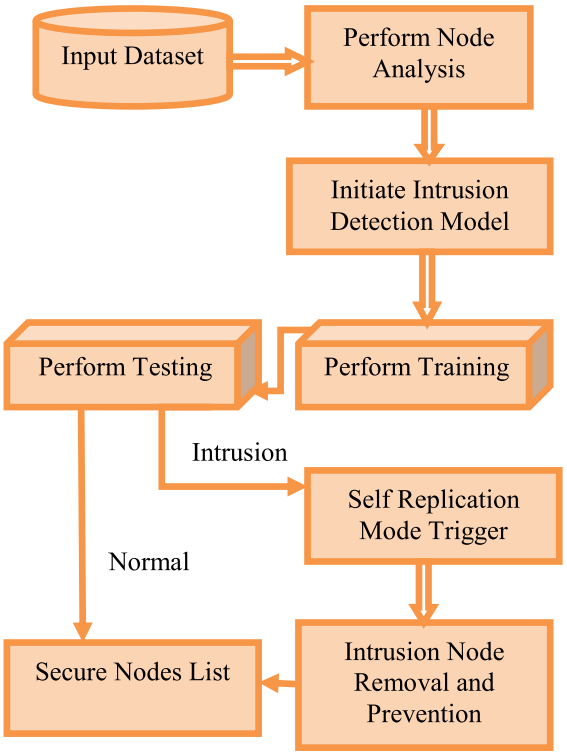

FIGURE 2. Proposed model framework.

The proposed model Pseudo code is explained that performs self replication to avoid attacks in the network.

Begin
- Input Network dataset *NDset*
- Split the Dataset into 80:20 for training and testing
- Consider the dataset *NDset* and analyze the records in the dataset.
- While r in *NDset* do
  - Calculate the packet delivery rate *PDRset* and nodes $N(r)$ that have maximum PDR only will be considered.
  - Calculate the node energy consumption *enerconsm* and nodes *N(r)* that has less energy consumption only will be considered for data transmission.
- Done
- The eveauator node *EV(r)* is considered that monitors the network.
- The intrusion detection set *IDset* is generated based on the dissimilar values.
- While $N(i)$ in *NDset* do
  - $N(i)$ values are analyzed with the normal network parameter values and the dissimilarity is checked.
  - The self replication alarm is triggered based on the dissimilarity values.
  - Nodes *N(r')* that has dissimilarity is predicted and removed from the network.
- Done

End

The network of reliable machines sends out a warning signal. After an attack has been detected and the liable sequences of events have been determined, the information is broadcasted to every machine in the network. When a potentially harmful sequence of events coincides with the chronology, a protective response is triggered. If no match is found, normal operation will proceed. An Imperative Node Evaluator with Self Replication Code and Auto Triggering Mode Model is proposed in this research for auto healing of the network if intrusion occurs and also to perform auto triggering of nodes with for securing the network and reducing the false alarms.

Algorithm INE-SRC-ATM

{

Input: Network Dataset $\{ND_{set}\}$

Output: Intrusion Causing Nodes, AlarmSet $\{IC_{set}, Alm_{set}\}$

Step-1: Initially the nodes in the network will be registered and the nodes will be analyzed with their behavior in data transmission rate. The node analysis is performed as

Consider nodes list {n1,n2,.....nN} and the transactions list {t1,t2,....tN}

$$NodeList\,[N] = \sum_{p=1}^{N} nodebaseaddr\,(p) + \tau\,(n, n+1) + \max\,(trans\,(t, t+1)) + \delta(PDR\,(n)) \quad (1)$$

Here τ is the model used to extract the node transaction attributes to the next neighbor node and δ is the nodes attributes that consider the maximum packets delivered.

Step-2: The registered nodes performance is calculated based on the node transmission, energy levels, computational complexity levels. The nodes with best performance is considered to be part of the network and the network parameter evealuation lilst is generated as

$$NodeList = \sum_{p=1}^{N} \frac{getNode\,(p) + getNode\,(p+1) + \gamma(p)}{maxrange(p)} \quad (2)$$

Here p is the current node, γ is the node maximum attribute transmission limit and the maxrange is the scope of availability of node in the network for data transmissions.

Step-3: The node packet delivery performance is calculated as

$$NodePDR\,(N) = \sum_{p=1}^{N} \frac{\omega\,(p) + count(GP(p))}{\sigma\,(p) + \sigma\,(p+1)} \quad (3)$$

Here ω is the model considering the total packets transmitted to current node, GP is the generated packets count. σ is the received packets count.

Step-4: The nodes energy consumption is also considered as a performance metric and the nodes energy consumption levels are performed as

$$NodeEner\,(N) = \sum_{p=1}^{N} \frac{EAlloc\,(p) - f(\Delta NodePDR\,(p))}{L} \quad (4)$$

Here f is the function used for calculating the node energy consumption during packet delivery. L is the total allocated energy levels.

Step-5: After registering the nodes in the network, then the node performance analysis will be done and then for network monitoring, the evaluator node is considered for monitoring the behavior of nodes. The evaluator node is considered as (5) and (6), shown at the bottom of the next page, β is the node transactions that are having maximum dissimilar attributes, G is the loss rate when extracting the node attributes.

Step-6: If the evaluator node is facing any issues, then the new evaluator node is selected among the previous evaluator node secondary. Every evaluator node will maintain two nodes as secondary nodes and the best one will be the evaluator node if the present evaluator node is removed. The process of selecting the new evaluator node is

$$\begin{aligned} &UpdEN\,[M] \\ &= \sum_{p=1}^{N} \frac{getaddr\,(EN\,(p))}{\delta\,(EN\,(p))} \\ &\quad \times \begin{cases} mindist\,(EN\,(p)\,, NodeList\,(p+1)) \\ \quad +\delta\,(\max\,(EvalNode\,(p))) \\ EN\,(p) \longleftarrow \\ returnEN\,(p) \quad Otherwise \end{cases} \\ &\quad if\ \ getaddr\ \ (EN\,(p)) == NULL \end{aligned} \tag{7}$$

Step-7: The intrusion detection will be performed based in the attribute dissimilarity and the network's administrator can be alerted to prospective attacks and protected against further access with the help of an intrusion detection and prevention system. The process of intrusion detection among nodes {n1,n2,….nN} is performed by maintaining attribute set {A1, A2,….,AN} with normal range dissimilarity set {DS1,DS2,…..,DSN} as

$$\begin{aligned} &IntrDSet(EN[M]) \\ &= \delta \left(\sum_{p=1}^{N} \left(\begin{array}{l} \sum_{q=1}^{p} \left(\begin{array}{l} \frac{diff\,(p,p+1)+diff\,(q,q+1))}{\max(diff\,(\beta))} \\ -\frac{\min(G(p,p+1))}{\min(G(q,q+1))} \\ -DS(p,q) \end{array} \right) \\ +\min(Ndis(p,p+1)+\max(A(p,q)) \end{array} \right) \end{aligned} \tag{8}$$

Step-8: The self replication model is triggered that raises an alarm in case of intrusion and the nodes causing intrusions will be removed from the network and the communication is re initiated. The self replication model is performed by initiating the automatic IDS when nodes are identified in the intrusion detected set. The self replication is performed as

$$\begin{aligned} &\text{Nset} \\ &\leftarrow \text{len(IntrDset)} \\ &\text{Fset} \\ &\leftarrow \max(\text{diff(p,q)}) + \max(\text{diff(p}+1, \text{q}+1)) \end{aligned} \tag{9}$$

$$\begin{aligned} &ITrig(Nset(M)) \\ &= \left[\sum_{p=1}^{N} \left(\begin{array}{l} \max\,range(EN\,(IntrDSet(p,q),))- \\ loss\,(Fset(\delta)) \end{array} \right)^2 + Th \right] \end{aligned} \tag{10}$$

$$\begin{aligned} &SelfReplicaMode(ITrif\,(M)) \\ &= \lambda(Fset(p,p+1)) + \sum_{p=1}^{M} \max(Nset(q,q+1)) \\ &\{ValT \leftarrow [\max(\lambda(Fset(p,p+1)))+\max(\lambda(Fset(q,q+1))]^2 \end{aligned} \tag{11}$$

Here Th is the threshold value considered for auto triggering model. λ is the function used for generating a copy of the IDS model.

Step-9: The intrusion prevention and removal model is helpful in successful data transmission with high security levels. The Process of alarm triggering and the node removal process is performed as

$$\begin{aligned} &AlarmT\ (SelfReplicaMode\,(M)) \\ &= \int_{p=1}^{M} Max\ (NodeList\ (\delta)) + \text{Loss}(\tau))) \\ &\quad + \lambda * \frac{\delta(ITrig\ (\text{p}))}{\text{len(SelfReplication (p, q))}} - Nset\ (p,q) \\ &\quad - \frac{nodebaseaddr\ (NodeList\ (p))}{\beta} \end{aligned} \tag{12}$$

}

IV. RESULTS AND DISCUSSIONS

The tests were performed in the Tensorflow 2.1 environment on a Intel(R) Core(TM) i5-7200U CPU with 2.50GHz with 16GB of RAM and executed in Anaconda Jupyter. The proposed model is tested with 1050 iterations for analyzing the model performance in intrusion detection. All forms of illicit network traffic and computer activities that can bypass a traditional firewall can be detected by an Intrusion Detection System. Network-based attacks including privilege escalation, illegal logins, and access to sensitive files, as well as malware, fall under this category. Users necessitate security in order to protect their systems against intrusion by unauthorized parties. There is a lot of focus on IDSs these days because they are an integral aspect of system security. Network security can be improved with the use of intrusion detection systems (IDSs), which monitor network traffic from a central location.

More and more, learning approaches are being used to detect network intrusions, which in turn aid the network administrator in taking preventative actions. For better cyber defences, it's crucial to assess existing intrusion detection systems. The success of IDS can be gauged by its accuracy in classifying events as either attacks or benign activity. An efficient self replication auto triggering model for intrusion detection is proposed that considers a model that will be automatically triggered if unusual or malicious traffic is found.

TABLE 1. Node analysis time levels.

Nodes in Network	Models Considered				
	INE-SRC-ATM	SLSD-IDS	IDCPS-GAN	IPS-CAN	AMS
100	16.5	15.0	19.0	22.0	26.0
200	18.0	17.5	20.0	24.5	29.5
300	19.5	20.0	21.5	27.0	32.0
400	21.0	22.5	24.0	29.5	35.5
500	22.5	25.0	27.5	32.0	39.0
600	24.0	27.5	30.0	34.5	42.5

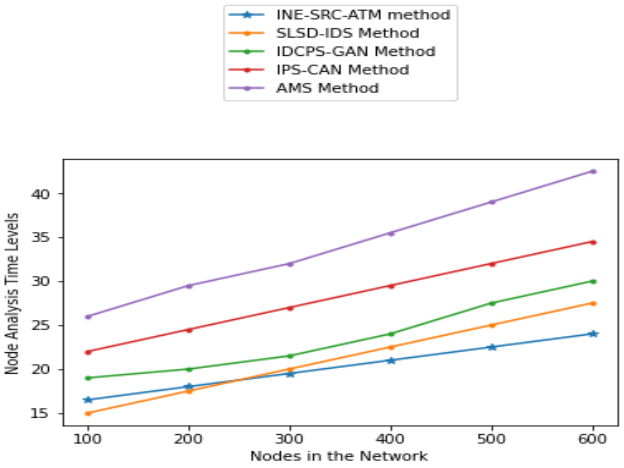

FIGURE 3. Node analysis time levels.

TABLE 2. Evaluator node considering accuracy levels.

Nodes in Network	Models Considered				
	INE-SRC-ATM	SLSD-IDS	IDCPS-GAN	IPS-CAN	AMS
100	86.0	81.0	77.5	73.0	69.0
200	88.0	83.5	79.0	75.0	71.5
300	90.5	85.0	81.0	77.5	73.0
400	92.0	87.5	83.0	79.0	75.0
500	94.0	89.0	85.5	81.0	77.5
600	96.0	91.0	87.0	83.5	79.0

The proposed model effectively reduces the false alarms by keenly monitoring the nodes and the traffic. An Imperative Node Evaluator with Self Replication Code and Auto Triggering Mode (INE-SRC-ATM) Model is proposed in this research for auto healing of the network if intrusion occurs and also to perform auto triggering of nodes with for securing the network and reducing the false alarms. The proposed model is compared with the traditional Self-Learning Spatial Distribution-Based Intrusion Detection for Industrial Cyber-Physical System (SLSD-IDS) [1], adaptive Markov strategy (AMS) [2], intrusion prevention system (IPS) for automotive controller area network (IPS-CAN) [3] and Intrusion Detection for Cyber–Physical Systems Using Generative Adversarial Networks (IDCPS-GAN) [5].The proposed model when contrasted with the traditional model exhibit better performance.

The proposed model initially registers the nodes in the network and the nodes attributes will be analyzed. The node analysis indicates the performance levels of the nodes that are registered in the network. The Node analysis time levels of the proposed and existing models are shown in Table 1 and figure 3.

The proposed model considers Evaluator Node for monitoring the registered node behavior. The proposed model node performance levels and transmission capabilities are analyzed and then the network performance can be monitored. The Evaluator Node Considering Accuracy Levels of the proposed and traditional models are shown in Table 2 and Figure 4.

The Evaluator node is used to monitor the entire network. The evaluator node if compromised, the performance will be degraded and the delay will be increased. The proposed

$$Ndis\,[L] = \sum_{p=1}^{N} \frac{N - (p - 1 * p)}{len(NodeList)}$$

$$EvalNode[EN] = \sum_{p=1}^{N} \sum_{q=j}^{p} Min(Ndis\,(p)) + \min_{0 \le p \le N} (\delta(PDR(p, q))) + minener(q, p) \tag{5}$$

$$\mathrm{EN\,[M]} = \frac{\sum_{p=1}^{N} \sum_{q=1}^{\mathrm{p}} |\max\,(\mathrm{EvalNode\,(q,\,p)})|^2 - \max\,(\beta) + \min(\mathrm{G\,(p,\,q)})}{\mathrm{len(EvalNode\,[EN])}} \tag{6}$$

TABLE 3. Evaluator node selection time levels.

Nodes in Network	Models Considered				
	INE-SRC-ATM	SLSD-IDS	IDCPS-GAN	IPS-CAN	AMS
100	7.5	9.5	11.0	14.0	17.0
200	10.0	11.0	13.5	16.5	19.5
300	12.0	13.5	16.8	19.7	22.6
400	14.5	16.0	18.5	21.5	24.0
500	17.0	19.5	21.0	24.3	27.5
600	19.0	22.0	23.5	26.5	29.5

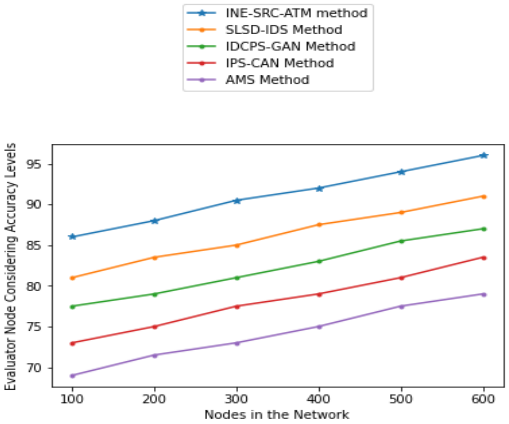

FIGURE 4. Evaluator node considering accuracy levels.

model evaluator node consider two nodes as secondary and if there is any issue with the evaluator node, the better secondary node will be considered for monitoring the network. The new evaluator node selection time levels are shown in Table 3 and Figure 5.

Any dynamical system's action that results in the creation of a copy of itself is considered self-replicating. The proposed model used a self replication IDS models that is used to automatically detect the intrusions and remove them from the network for secure data transmission. The self replication model triggers the IDS model to generate a copy of self IDS model that also removes the intrusion and alarm the network administrator for achieving secure data transmission. The Self Replication Triggering Time Levels and Self Replication Triggering Accuracy Levels are represented in Table 4 and Figure 6.

The self replication model creates a duplicate copy of the IDS tracking model that detects and removes the intrusions in the network. The Self Replication Triggering Accuracy Levels of the proposed and existing models are shown in Table 5 and Figure 7.

TABLE 4. Self replication triggering time levels.

Nodes in Network	Models Considered				
	INE-SRC-ATM	SLSD-IDS	IDCPS-GAN	IPS-CAN	AMS
100	12.0	14.5	17.7	19.0	21.5
200	14.0	17.4	19.5	22.5	23.0
300	16.5	19.5	22.0	25.0	25.5
400	18.0	22.0	24.5	27.5	28.0
500	20.8	24.7	27.3	30.0	31.5
600	22.0	27.0	29.5	32.5	34.0

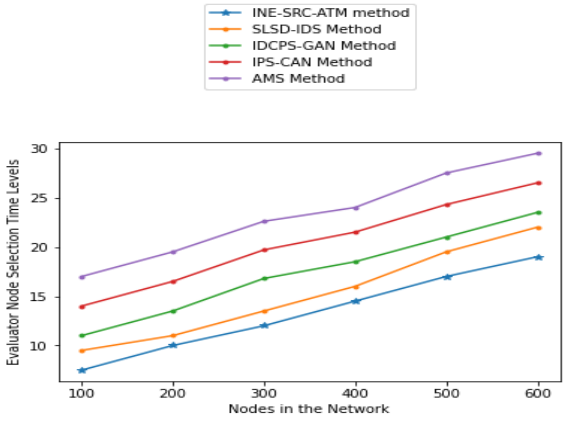

FIGURE 5. Evaluator node selection time levels.

TABLE 5. Self replication triggering accuracy levels.

Nodes in Network	Models Considered				
	INE-SRC-ATM	SLSD-IDS	IDCPS-GAN	IPS-CAN	AMS
100	82.0	79.5	67.0	65.0	63.8
200	84.0	81.0	71.0	67.8	66.0
300	86.0	83.5	73.6	69.8	68.5
400	88.0	86.5	75.0	71.3	70.0
500	90.0	88.0	77.8	74.7	73.4
600	92.0	91.4	79.0	76.7	75.0

An IDS is a software designed to keep an eye on a network or set of systems for signs of intrusion. Event and security information management systems often collect reports of

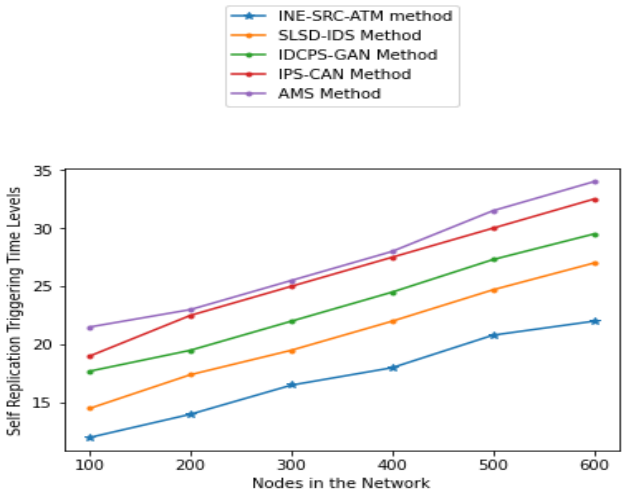

FIGURE 6. Self replication triggering time levels.

TABLE 6. Intrusion detection time levels.

Nodes in Network	Models Considered				
	INE-SRC-ATM	SLSD-IDS	IDCPS-GAN	IPS-CAN	AMS
100	17.0	19,5	21.5	23.0	
200	19.4	21.4	23.6	25.7	
300	22.0	23.7	25.6	27.4	
400	24.5	25,3	28.0	30.4	
500	27.0	27.9	31.0	33.0	
600	29.0	30.0	34.0	35.0	

intrusion activity and violations and either forward them to an administrator or store them in one centralized location. The Intrusion Detection Time Levels of the proposed and existing models are shown in Table 6 and Figure 8.

The False Positive Rate (FPR), also known as the False Alarm Rate (FAR), is the percentage of times when benign data is incorrectly identified as malicious activity. The proposed model false alarm rate is less than the traditional models. The FAR levels of the proposed and traditional models are shown in Table 7 and Figure 9.

A network's traffic can be monitored by IDS, which then sends out alerts if it detects any malicious behavior. IDS is a software designed to search for malicious behavior or policy violations within a system or network. An intrusion prevention system (IPS) is a type of network security technology that keeps a network under constant surveillance for malicious activity and responds accordingly to stop it, typically by reporting, blocking, or dumping the offending traffic. Unlike an IDS, which can just notify an administrator

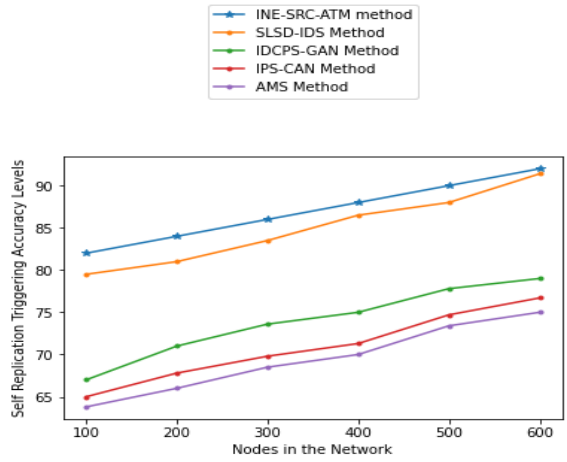

FIGURE 7. Self replication triggering accuracy levels.

TABLE 7. False alarm rate levels.

Nodes in Network	Models Considered				
	INE-SRC-ATM	SLSD-IDS	IDCPS-GAN	IPS-CAN	AMS
100	4	7.8	11	14	21
200	4.6	8.6	12	15.6	21.5
300	5	9.3	14	16	23
400	5.4	10	16	17.6	23.9
500	5.7	11.3	17	18	24
600	6.1	11.8	18.6	18.3	25

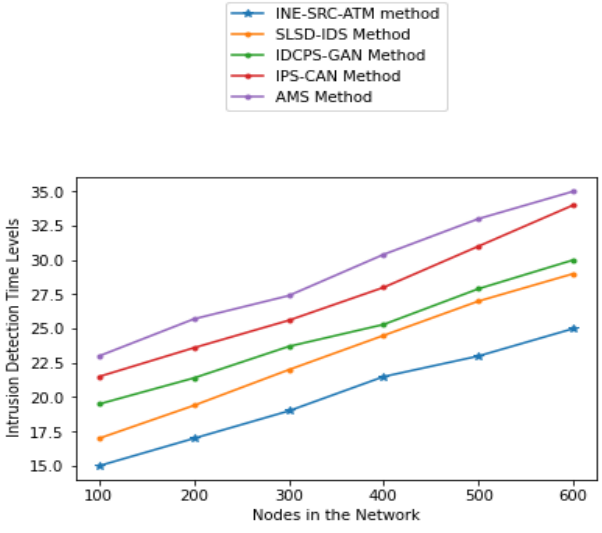

FIGURE 8. Intrusion detection time levels.

to harmful activity, this system can actively stop it. The Table 8 and Figure 10 represents the Intrusion Detection and

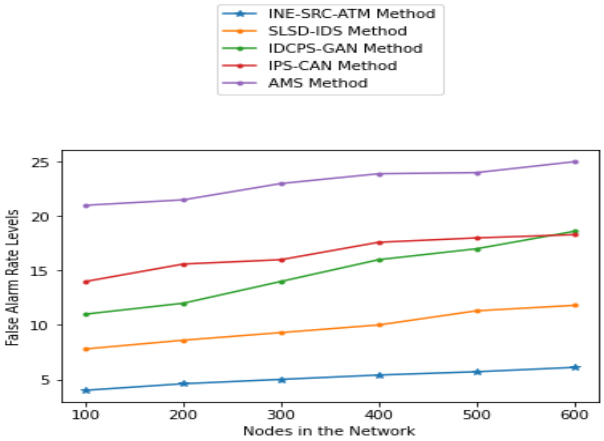

FIGURE 9. False alarm rate levels.

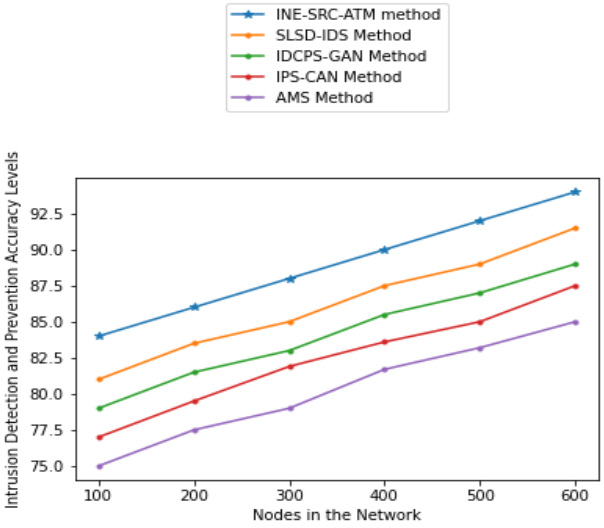

FIGURE 10. Intrusion detection and prevention accuracy levels.

TABLE 8. Intrusion detection and prevention accuracy levels.

Nodes in Network	Models Considered				
	INE-SRC-ATM	SLSD-IDS	IDCPS-GAN	IPS-CAN	AMS
100	84.0	81.0	79.0	77.0	75.0
200	86.0	83.5	81.5	79.5	77.5
300	88.0	85.0	83.0	81.9	79.0
400	90.0	87.5	85.5	83.6	81.7
500	92.0	89.0	87.0	85.0	83.2
600	94.0	91.5	89.0	87.5	85.0

Prevention Accuracy Levels of the existing and proposed model.

V. CONCLUSION

Using the framework of auto triggering theory, this research introduced the idea of a self-repairing network intrusion detection system. This method can prevent assaults that haven't been seen before, unlike signature-based approaches. Furthermore, this method allows differentiating between new legitimate behavior and new harmful behavior, allowing for a more targeted response than is possible with pure anomaly detection approaches, which react to any new behavior in the system. In highly dynamic systems, where novel behaviors develop continuously, this allows for a significant reduction in the amount of false positive alarms. When potentially harmful events are broadcast across the network, defensive measures can spread rapidly to other servers, thwarting the attack before it can do any real damage. An Imperative Node Evaluator with Self Replication Code and Auto Triggering Mode Model is proposed in this research for auto healing of the network if intrusion occurs and also to perform auto triggering of nodes with for securing the network and reducing the false alarms. The proposed model achieves 97% intrusion detection accuracy and self replication accuracy. While there has been progress in reducing false positives, there is still room for development. In addition, most methods employ an offline mode, which necessitates the development of automated methods that can reduce false positives in real time. Finally, researchers have a lot of room to work until they find a way to eliminate or drastically cut down on these false positives, which would greatly improve IDS's overall effectiveness. The feature dimensionality reduction model can also be applied on the intrusion detection model for reduction of time complexity for better performance.

REFERENCES

[1] R. Heartfield, G. Loukas, A. Bezemskij, and E. Panaousis, "Self-configurable cyber-physical intrusion detection for smart homes using reinforcement learning," *IEEE Trans. Inf. Forensics Security*, vol. 16, pp. 1720–1735, 2020, doi: 10.1109/TIFS.2020.3042049.

[2] J. Hao, E. Kang, J. Sun, Z. Wang, Z. Meng, X. Li, and Z. Ming, "An adaptive Markov strategy for defending smart grid false data injection from malicious attackers," *IEEE Trans. Smart Grid*, vol. 9, no. 4, pp. 2398–2408, Jul. 2018, doi: 10.1109/TSG.2016.2610582.

[3] P. F. De Araujo-Filho, A. J. Pinheiro, G. Kaddoum, D. R. Campelo, and F. L. Soares, "An efficient intrusion prevention system for CAN: Hindering cyber-attacks with a low-cost platform," *IEEE Access*, vol. 9, pp. 166855–166869, 2021, doi: 10.1109/ACCESS.2021.3136147.

[4] M. Cakir, T. Hackel, S. Reider, P. Meyer, F. Korf, and T. C. Schmidt, "A QoS aware approach to service-oriented communication in future automotive networks," in *Proc. IEEE Veh. Netw. Conf. (VNC)*, Dec. 2019, pp. 1–8.

[5] P. F. de Araujo-Filho, G. Kaddoum, D. R. Campelo, A. G. Santos, D. Macêdo, and C. Zanchettin, "Intrusion detection for cyber-physical systems using generative adversarial networks in fog environment," *IEEE Internet Things J.*, vol. 8, no. 8, pp. 6247–6256, Apr. 2021.

[6] L. Alevizos, M. H. Eiza, V. T. Ta, Q. Shi, and J. Read, "Blockchain-enabled intrusion detection and prevention system of APTs within zero trust architecture," *IEEE Access*, vol. 10, pp. 89270–89288, 2022, doi: 10.1109/ACCESS.2022.3200165.

[7] G. Xian, "Cyber intrusion prevention for large-scale semi-supervised deep learning based on local and non-local regularization," *IEEE Access*, vol. 8, pp. 55526–55539, 2020, doi: 10.1109/ACCESS.2020.2981162.

[8] M. Nam, S. Park, and D. S. Kim, "Intrusion detection method using bi-directional GPT for in-vehicle controller area networks," *IEEE Access*, vol. 9, pp. 124931–124944, 2021.

[9] R. Islam, R. U. D. Refat, S. M. Yerram, and H. Malik, "Graph-based intrusion detection system for controller area networks," *IEEE Trans. Intell. Transp. Syst.*, vol. 23, no. 3, pp. 1727–1736, Mar. 2020.
[10] J. Ashraf, A. D. Bakhshi, N. Moustafa, H. Khurshid, A. Javed, and A. Beheshti, "Novel deep learning-enabled LSTM autoencoder architecture for discovering anomalous events from intelligent transportation systems," *IEEE Trans. Intell. Transp. Syst.*, vol. 22, no. 7, pp. 4507–4518, Jul. 2021.
[11] R. Parsamehr, G. Mantas, J. Rodriguez, and J.-F. Martinez-Ortega, "IDLP: An efficient intrusion detection and location-aware prevention mechanism for network coding-enabled mobile small cells," *IEEE Access*, vol. 8, pp. 43863–43875, 2020, doi: 10.1109/ACCESS.2020.2977428.
[12] J. Appiah-Kubi and C.-C. Liu, "Decentralized intrusion prevention (DIP) against co-ordinated cyberattacks on distribution automation systems," *IEEE Open Access J. Power Energy*, vol. 7, pp. 389–402, 2020, doi: 10.1109/OAJPE.2020.3029805.
[13] S. Seo, S. Han, J. Park, S. Shim, H.-E. Ryu, B. Cho, and S. Lee, "Hunt for unseen intrusion: Multi-head self-attention neural detector," *IEEE Access*, vol. 9, pp. 129635–129647, 2021, doi: 10.1109/ACCESS.2021.3113124.
[14] H. Olufowobi, C. Young, J. Zambreno, and G. Bloom, "SAIDuCANT: Specification-based automotive intrusion detection using controller area network (CAN) timing," *IEEE Trans. Veh. Technol.*, vol. 69, no. 2, pp. 1484–1494, Feb. 2020.
[15] H. Olufowobi, U. Ezeobi, E. Muhati, G. Robinson, C. Young, J. Zambreno, and G. Bloom, "Anomaly detection approach using adaptive cumulative sum algorithm for controller area network," in *Proc. ACM Workshop Automot. Cybersecurity*, Mar. 2019, pp. 25–30.
[16] M. Bozdal, M. Samie, and I. K. Jennions, "WINDS: A wavelet-based intrusion detection system for controller area network (CAN)," *IEEE Access*, vol. 9, pp. 58621–58633, 2021.
[17] X. Qu, L. Yang, K. Guo, L. Ma, T. Feng, S. Ren, and M. Sun, "Statistics-enhanced direct batch growth self-organizing mapping for efficient DoS attack detection," *IEEE Access*, vol. 7, pp. 78434–78441, 2019, doi: 10.1109/ACCESS.2019.2922737.
[18] Y. Gao, J. Chen, H. Miao, B. Song, Y. Lu, and W. Pan, "Self-learning spatial distribution-based intrusion detection for industrial cyber-physical systems," *IEEE Trans. Computat. Social Syst.*, vol. 9, no. 6, pp. 1693–1702, Dec. 2022, doi: 10.1109/TCSS.2021.3135586.
[19] S. Jiang, J. Zhao, and X. Xu, "SLGBM: An intrusion detection mechanism for wireless sensor networks in smart environments," *IEEE Access*, vol. 8, pp. 169548–169558, 2020, doi: 10.1109/ACCESS.2020.3024219.
[20] D. Papamartzivanos, F. G. Mármol, and G. Kambourakis, "Introducing deep learning self-adaptive misuse network intrusion detection systems," *IEEE Access*, vol. 7, pp. 13546–13560, 2019, doi: 10.1109/ACCESS.2019.2893871.
[21] A. Nisioti, A. Mylonas, P. D. Yoo, and V. Katos, "From intrusion detection to attacker attribution: A comprehensive survey of unsupervised methods," *IEEE Commun. Surveys Tuts.*, vol. 20, no. 4, pp. 3369–3388, 4th Quart., 2018.
[22] H. Choi, M. Kim, G. Lee, and W. Kim, "Unsupervised learning approach for network intrusion detection system using autoencoders," *J. Supercomput.*, vol. 75, no. 9, pp. 5597–5621, Sep. 2019.
[23] Z. K. Maseer, R. Yusof, S. A. Mostafa, N. Bahaman, O. Musa, and B. Ali Saleh Al-rimy, "DeepIoT.IDS: Hybrid deep learning for enhancing IoT network intrusion detection," *Comput., Mater. Continua*, vol. 69, no. 3, pp. 3945–3966, 2021.
[24] M. Marchetti and D. Stabili, "Anomaly detection of CAN bus messages through analysis of ID sequences," in *Proc. IEEE Intell. Vehicles Symp. (IV)*, Jun. 2017, pp. 1577–1583.
[25] E. Seo, H. M. Song, and H. K. Kim, "GIDS: GAN based intrusion detection system for in-vehicle network," in *Proc. 16th Annu. Conf. Privacy, Secur. Trust (PST)*, Aug. 2018, pp. 1–6.
[26] H. M. Song, J. Woo, and H. K. Kim, "In-vehicle network intrusion detection using deep convolutional neural network," *Veh. Commun.*, vol. 21, Jan. 2020, Art. no. 100198.
[27] L. Yang, A. Moubayed, and A. Shami, "MTH-IDS: A multitiered hybrid intrusion detection system for Internet of Vehicles," *IEEE Internet Things J.*, vol. 9, no. 1, pp. 616–632, Jan. 2022.
[28] H.-J. Xing and M. Ji, "Robust one-class support vector machine with rescaled Hinge loss function," *Pattern Recognit.*, vol. 84, pp. 152–164, Dec. 2018.

RAGINI MOKKAPATI received the M.Tech. degree from ANU, Guntur. She is a full time Ph.D. Research Scholar with the School of Computer Science and Engineering, VIT–AP University, Amaravati. She has 11 years of teaching experience. Her research interests include deep learning and machine learning.

D. VENKATA LAKSHMI received the master's and Ph.D. degrees from the University of Hyderabad, Hyderabad, India, in 1993 and 2008, respectively. Her Ph.D. research project titled "On Vector Valued Amalgam Spaces." She was with the Faculty of Mathematics, Bapatla Engineering College, Bapatla, India, from 1996 to 2021. Currently, she has been a Professor with the School of Computer Science and Engineering, VIT–AP University, India, since 2021. She has more than 24 years of teaching experience and 12 years of research experience. She has published more than 35 research articles in national and international journals. Her research interests include machine learning, artificial intelligence, graph theory, and theoretical computer science.