Power System Technology
ISSN:1000-3673

Received: 16-01-2024 Revised: 12-02-2024 Accepted: 07-03-2024

Smart Network Forensics with Generative Adversarial Networks Leveraging Blockchain for Anomaly Detection and Immutable Audit Trails

Yan Lei[1], Zhu Chaoyang[2], Iqbal Alam[3] and Muhammad Azhar Mushtaq
Tianjin Huayuan Times Metal Products Co., Ltd.
yongruishangwu2024@outlook.com
International Institute of Engineering Psychology , Denver, USA)
zcy0919psy@iioep.org
Nanyang Academy of Sciences (NASS)
iqbalalam15111980@gmail.com
Department of Information Technology
University of Sargodha
azhar.mushtaq@uos.edu.pk

Abstract:- Analyzing the specificity of the cybersecurity domain, the problem of ensuring the security and integrity of smart networks is multifaceted. This research explores the complexity of smart network forensics and seeks to meet theses challenges through different approaches. First, to establish the subject of the investigation, the context is described, which includes factors such as ever-fluctuating network traffic and increasing threat types. Further, a thorough analysis of the literature and research work available in the field of network forensics, anomaly detection methodologies, generative adversarial networks, and blockchain technology bring new perspectives and information to the discussion. From this perspective, the proposed methodology contributes towards devising a novel concept. Drawing on the prospects of using GANs for detecting anomalies, this research investigates how GANs can be employed to add synthetic data to training sets and improve the efficiency of smart networks in detecting anomalies. Similarly, Blockchain becomes a valuable asset in creating unalterable audit trails, and providing accountability and recoverability of any examined evidence. By incorporating these state-of-the-art approaches into the proposed work, this research aims at enhancing the reliability of smart network forensics to advance more effective cybersecurity awareness and threat analysis in complex and ever-evolving networks.

Keywords: Smart Network Security, Cybersecurity, Interconnected Networks, Threat Detection, Emerging Technologies.

Power System Technology
ISSN:1000-3673

Received: 16-01-2024 Revised: 12-02-2024 Accepted: 07-03-2024

1. Introduction

Smart network forensics is an important segment in current cybersecurity due to its unique approach to addressing the detection, investigation, and prevention of security breaches in complex and connected systems[1]. With the advent of IoT devices, cloud computing platforms and integrated systems, the nature and /or strength of threats have increased making it essential for the field to have teams, which would employ specialized methods in forensic sciences. While CT low level and system level computer forensics typically involves the examination of an evidence source as an isolated, localized computer or system, smart network forensics takes the opposite approach and recognizes the computers and transmission of data as an interconnected network [2]. Some of the challenges in smart network forensics include the avalanche of input and output data that is produced by the layered smart networked devices, the constantly transforming and evolving network structures and settings and the distributed nature of smart network forensics evidence across the multiple devices and geographical locations [3]. In order to overcome these challenges, scholars and practitioners have designed and applied certain methods and instruments including, for example, machine learning for identifying anomalies, network traffic analysing tools, and blockchain for verification of forensic data's credibility with the help of cryptographic hash functions [4]. Finally, I would like assert that smart network forensics is one of the most important fields in contemporary cybersecurity, and the development and continual improvement of it is an imperative due to constant shifts in threats, targets, and network structures.

Anomaly detection in smart networks is one of the substantial specialties of cybersecurity focused on detecting something that is out of the ordinary or does not conform with network norms [5]. Due to the complex and intertwined characteristics of smart networks, just relying on the conventional security policies is jeopardizing the safety of the whole network environment and data, and thus it is vital to integrate anomaly detection to the strategy. The paper overviews the chosen anomaly detection methods more suitable for SNs, statistical methods, machine learning, and behavioral analysis strategies [6]. Typical statistical traffic analysis involves calculating mean and standard deviations on the traffic matrix to identify patterns of traffic deviating from the normal benchmark on the network. Supervised, unsupervised, and semi-supervised approaches that employ data mining and statistical analysis utilize information from prior network activity to enable models with capability to detect inconsistency [7]. Anomalous behaviour analysis techniques are based on the observation of normal behaviours of network entities and the identification of deviations to these regularities. Moreover, ensemble techniques, the combination of different techniques, and deep learning approaches are used more frequently to improve the effectiveness of the approaches in smart networks for anomaly detection. Hence, concerning the global target goal of producing competent cybersecurity experts with adequate knowledge and skills to deal with attacks in

Power System Technology
ISSN:1000-3673
Received: 16-01-2024 Revised: 12-02-2024 Accepted: 07-03-2024

smart networks, this study seeks to offer a detailed insight into anomalous behaviour detection approaches as a basic toolkit for smart network defence.

Table 1. Attacks on IoT Networks

Attacks Types	Explanation
Malware and Ransomware	Malicious programs that are downloaded and installed on IoT gadgets and then cause damage, steal information, or turn the gadgets into part of a botnet. Data on a device is encrypted and then locked until a ransom is paid
Man-in-the-Middle	The connection between IoT devices and the network may be intercepted by hackers, allowing them to eavesdrop, alter data, or insert harmful instructions. This leads to compromised security, altered data, or outright device control.
Physical Attacks	Physically accessing or tampering with an IoT device with the intent of stealing data, changing its behavior, or obtaining control over it. To identify and prevent such attacks, strong physical security measures are required.
Privilege Escalation	Gaining administrative access by exploiting flaws in the software or configuration of an IoT device. Because of this, malicious actors may get access to private information, change the way a device normally operates, or even go beyond its limits.
Information Leakage	The disclosure of private information, such as user passwords, configuration settings, or personal data, by IoT devices without permission. Those who would steal identities or get access illegally or maliciously take advantage of this vulnerability.
Replay Attacks	A method of recording and then playing back authorized interaction between IoT gadgets. Because to this, malicious acts, entry into protected regions, and authentication bypass are all possible.
DNS Attacks	DNS hijacking is the practice of diverting traffic from legitimate websites to malicious ones. Because of this, unauthorized parties may gain access to or modify information sent from an IoT device to its intended recipient.
Firmware Attacks	Taking advantage of security holes in the firmware of embedded systems used in IoT devices. Software that has been compromised may be used to take over a device, modify its behavior, or install malicious software. The

Power System Technology
ISSN:1000-3673
Received: 16-01-2024 Revised: 12-02-2024 Accepted: 07-03-2024

	security and functioning of a device may be severely compromised by an attack on its firmware.

The groundbreaking concepts of GANs have powered this tool into becoming a new frontier in the cyber security domain where several factors hailing from varied threat detection, vulnerability analysis, and adversarial robustness can be discovered. Understanding GAN's capacities, functions and its potential for utilizing cybersecurity is the main priority of this research which can contribute to the improvement of Security Science in the context of the modern threats [8]. Deep Learning models such as GANs are used to detect anomalies because they can provide nearly realistic synthetic data to be used to model small deviations and noises that could signify malicious activity in the traffic or system behavior. However, GANs' use will prove vital in data augmentation, where it will be critical in generating a broad dataset with increased generality for training enery machine learning models in cybersecurity. Moreover, GANs are used in the creation of adversarial examples to exploit and outline potential weaknesses and limitations of ML-based security systems [9]. This review also assesses the relevant ethical and privacy issues related to GANs in cyber security, with an emphasis laid on the need to avoid misuse and plan for ways of preventing adverse social effects that may arise from their implementation. In so doing, this paper believes that it can uncover the various applications of GANs in cybersecurity while highlighting their strengths and weaknesses in a bid to enhance the research about cybersecurity and GANs to improve development of powerful and robust cybersecurity solutions in the future [10].

Blockchain emerging as a revolutionary technology has changed many industries including the field of forensics by providing an efficient and secure decentralized solution for storing records. This introductory article promises an extensive exploration of the key concepts and primary use cases of block chain technology specifically within forensic sciences as well as the potential of this technology for revolutionization of processes related to the collection, examination, storage, and dissemination of digital evidence. Blockchain, in its simple form, can be defined as distributed ledger technology that provides the main functionality of maintaining a decentralized record of transactions between parties [11]. As a result of having a distributed structure and consensus algorithms, blockchain enables snippets to be responsive to manipulating data, making it suitable for capturing and storing forensic evidence and building applications with tamper-proof history.

Also, many smart contracts provide fully executabale and auditable approaches to conduct forensic investigations, thereby improving the organization and efficiency of investigations and preventing corruption. In addition, it is aimed that, by providing blockchain-enabled platforms, efficient and reliable collaboration and information sharing among forensic investigators, law

Power System Technology
ISSN:1000-3673
Received: 16-01-2024 Revised: 12-02-2024 Accepted: 07-03-2024

enforcement agencies, and other relevant stakeholders may be offered. However, there is now a concern or rather the following issues stemming from the use of blockchain technology in the forensic field which include scalability, interoperability, and the issue of regulations. These challenges warrant a multi-faceted solution that involves all sectors ranging from technological improvements to policy-making and inter-sectorial cooperation [12]. It is therefore the intention of this research to explain the principles of Blockchain in the context of the forensic field and explore its various applications, with the ultimate purpose of outlining its possible utilization and advancement, alongside offering recommendations on its adoption within forensic practices.

While current smart network security implementations present a number of contemporary issues attributed to active evolution of network connectivity and threat. This exploration goes further towards the extended practices of smart network security to identify specific issues that have to be addressed and launched on. The first and obvious issue to look at lies in the fact that smart networks are large and complex – they consist of devices, protocols, and services. Overall, maintaining proper security measures in such vast and diverse environments becomes a challenge in terms of identifying, controlling, and enforcing. Instead, these difficulties intensify due to the emergence of IoT devices, which often do not have high-quality security as a significant number of users might not focus on this aspect [13]. Another challenge relates to the fact that smart network infrastructures are almost constantly in a state of flux, due to such factors as variability in network topology and configuration, traffic flow data, and so on. There are certain inherent limitations that come with traditional security approaches because these do not work well in new and constantly evolving environments and hence there may be some areas which are completely uncovered or even vulnerable to the attackers. Also, new connectivity of Smart networks create new attack planes and methodologies combined with the deployment of more advanced attack strategies such as lateral motion and supply chain disturbances with higher probabilities [14]. Moreover, smart networking had consequences on regulation compliance due to the legal aspect of data security and privacy which makes it even more challenging to implement sound security practices for organizations that have concerns on compliance to regulations and laws in their respective countries. These are issues that cannot be single-handedly solved by any individual or organization and instead, they involve the need to embrace and implement new technologies, culturally acceptable model/framework for implementing security, acceptable risk management models/frameworks, and the need to tap on the expertise of other stakeholders. This paper therefore seeks to analyse the challenges witnessed in current smart network security practice so that smart network can improve on its security defence mechanisms to provide robust solutions that can withstand cyber threats in order to improve the compliance of organizations to meeting standards set for security by the international community [15].

Power System Technology
ISSN:1000-3673
Received: 16-01-2024 Revised: 12-02-2024 Accepted: 07-03-2024

The aims and objectives of the research briefly describe the overall goals and limits of the study exercise, and they help in creating a clear understanding of what is expected to be achieved and areas of focus in the research. In this particular case, the objectives are understood as the main aims and objectives of the study to be conducted, whereas the scope defines the context and specific conditions in which all the research action should be made. Specific goals may cover such areas as the definition of research questions and hypotheses that are to be explored, or analysis of specific phenomena or relationships, or the introduction of new research methodologies or theoretical concepts in a given field or discipline. At the same time, the study context defines the research objectives and defines such parameters as the population under study, its geographical area, the period under consideration, and possible restrictions affecting the analysis or conclusiveness of the results. If the objectives and scope of the study are defined and established properly, then it will be easier for the researcher to work towards and achieve the research goals, and it also enables stakeholders understand what the actual research proactively aims at discovering or exploring.

2. Literature Review

The literature review of smart network security has given an extensive outline of the research and publications available in the field of smart network security, and the security measures that should be taken in smart networks. This section will seek to provide a comprehensive review and discussion of existing literature in the domain which covers virtually all aspects of the problem from the network structures, the threats, the chinks that malicious actors can exploit, the measures that can be taken to minimize such dangers, and much more [16]. Consolidates the information and methodologies obtained from the current state of literature to create a foundation of awareness regarding smart network security research. Furthermore, it reviews studies and synthesizes the data to discover recurring patterns, trends, and research deficits, which can help shape the subsequent parts of the research and further paths for study and investigation. This section adds to the development of knowledge in smart network security literature through a systematic review and offers a premise for approaching potential future challenges and openings based on the current study [17].

The evolution of the threat landscape in smart networks describes the action, transition and development of cybersecurity threats in smart networks as well as the capabilities and susceptibilities of smart networks to hostile acts. This section describes the background of threats to smart networks where the origins can be traced back to typical cyber threats and state-of-the-art and targeted threats that are designed for smart devices, IoT systems, and connected systems [18]. By providing an illustration of hostile acts in cyberspace in history, is designed to explain theenvironmental forces shaping the increasing complexity and evolution of threats: technology, incentives, geopolitics, and society. Moreover, it reveals new types of threats and their use of technologies, including IoT botnets, ransomware controlling smart devices, and

Power System Technology
ISSN:1000-3673
Received: 16-01-2024 Revised: 12-02-2024 Accepted: 07-03-2024

supply chain attacks on connected systems . To further strengthen its argument, this section gives a brief insight on the rise of threat modeling by offering a historical perspective on the topic This section illustrates the dynamism of threats and the importance of a smart network to be capable of responding to the threats as and when they surface.

The investigation on traditional security models and their drawbacks in smart networks provides the reader with insight into the present paradigms and strategies implemented in order to protect networked context, as well as the issues and inadequacies encountered while studying smart networks. The following sub section is focused on the typical approaches used in network security environment such as firewalls, IDSs, antivirus, and security, encryption and tried to define whether these merits the need for smart networks [19]. It explains why traditional security measures are not effective on smart networks – scalability problems, invisibility of IoT devices, inability to capture never-before-seen attacks, and putting all of the work into a single, defined edge. In this section, when exploring the limitations of conventional security strategies, the reader will understand why developing smart network security solutions that are new and can cope with emerging threats is very important, taking into consideration that security solutions should be multifocal and follow the tendencies to implement proactive threat intelligence, anomaly detection, behavioral analysis, and extensive security based on the decentralized approach [20]. To seeks to provide deeper understanding and revelations into conventional security systems and where they fail resulting to form strategies that will prevent smart networks and their day-to-day operational capabilities from being compromised by current emerging and future threats in cyber space.

It highlights the discovered patterns and novel ideas, techniques and ideas that agency the extra creation and advancement in smart network security. As for the emerging ideas, concepts, and techniques reshaping the paradigm of smart network security, this section will name and discuss such developments as artificial intelligence (AI), machine learning (ML), blockchain technology, edge computing, and software-defined networking (SDN). They explore how these developing technologies are applied in increasing threat, recognizing events of incident, asserting anomaly, and protecting data in smart networks [21]. It also studies emerging trends and strategies including Zero-Trust architecture, Dynamic Security Architecture, and Deception Security Architecture that has changed a conventional network security view in Smart environments. This section is brought as an outlook on when, how, and why the future directions of smart network security will bring better solutions and features in regard to potential challenges and impacts since organization administrators and cybersecurity experts need guidance to decide how and where to proceed in the future. In this way, from the prospective point of view, it accentuates information on the need to implement innovative approaches and to be aware of new tendencies as the only way to minimize threats and to protect smart networks steadily confronting with new types of cyber threats [22].

Power System Technology
ISSN:1000-3673
Received: 16-01-2024 Revised: 12-02-2024 Accepted: 07-03-2024

The analysis of the shortcomings and the gaps in the current literature on smart network security shows the factors and aspects that have not been adequately covered in the literature to help unveil some of the issues that make the security of the smart networks rather difficult. Here it highlights and discusses the major concerns, limitations, and voids characterizing conventional and contemporary approaches to smart network security based on different perspectives including technological, methodological, theoretical, and pragmatic views [23]. Among them, some of the critical areas covered by the book are the ability to secure fluid and evolving network structures, the absence of methodological frameworks for comparing and measuring the effectiveness of the security approaches, and the shortage of the real datasets and references that would help author and readers to ground their investigations and assumptions. It aims at identifying the shortcomings such as the lack of knowledge about the new threats and risks to Smart Networks or non-converged attack models, the lack of interdisciplinary thinking and cross-cutting research methodologies, and the lack of communication and cooperation between the academic community, industrial partners, and government. In this section, the discussion assesses the shortcomings of previous research and indicates areas for further research and improvement to help in finding new approaches, methods, and solutions for smart network security that can cope with the current threats and prevent sophisticated attacks in the future effectively [23]. It presents the hope and efforts to further strengthen the understanding and collaboration of various existing problems and deficiencies to further improve the development reinforcement of smart network security and construction of strong anti-cyber attack network security systems.

Considering the existing trends and prospects of further investigations in the domain of smart network security offers a visionary outlook at the future tendencies of cybersecurity for smart networks. This analyses the opportunities for future research, development and cooperation in the field of smart network security with reference to theoretical and practical aspects. It outlines current and potential trends and issues that define the future of smart network security, such as technological innovation, threats and opportunities, revisions in the laws and rules, and social factors. It suggests possible research directions and themes that may include the advancement of AI-based security solutions, the application of Blockchain technology for increasing data reliability and trust, analysis of new techniques in threat identification based on machine learning and behavioral analytics, and examine the nature of users and user-related security concerns in smart networks [24]. As posing perspectives and directions for future research, this section has the purpose of provoking and orienting scholars, practitioners, and policymakers to investigate new frontiers, to found out new challenges, and to enhance the state of the art in smart network security. Thus, one can state that only through putting efforts together and implementing an interdisciplinary approach, the researchers can contribute to the development of new approaches, guidelines, and policy, which will help to strengthen the internet, its ecosystems, and protect them from existing and emerging threats [25].

Power System Technology
ISSN:1000-3673

Received: 16-01-2024 Revised: 12-02-2024 Accepted: 07-03-2024

3. Prposed Methodology

The research and analysis techniques adopted for this study are diverse and extensive, to capture the dynamics and contingencies of smart network security. Firstly, there is a methodological approach which encompasses both qualitative and quantitative data collection and analysis methods in order to provide a comprehensive view of the threats and possibilities to the field of smart network forensics. Survey research uses literature studies, case analysis and expert interviews to discover trends evidenced in the current field, and to evaluate current approaches to smart network forensics. Whereas, quantitative methods consist of collecting numerical data, applying algorithms, statistical models and machine learning to identifying patterns, trends, and predict future security threats in smart networks. In particular, more modern types of using neural networks, including GANs, are applied to create fake data required for training both anomaly detection algorithms and making them less vulnerable to adversarial attacks. Furthermore, in aspects of smart network forensic, blockchain technology is incorporated to build tamper-proof audit trails to improve the retrievability and quality of the acquired digital evidence. Smart contracts are designed to be self-executing, which makes it easier to detect security breaches and trace security threats and unlawful actions in a transparent setting due to the use of distributed ledgers based on blockchain technology. In addition, simulation and emulation of intelligent network environments, as well as a range of experimentations, are used to assess the efficiency of the suggested security solutions in controlled settings. This means emulating scenarios where the approach will be implemented, installing the sensing infrastructure, and launching probing attacks to evaluate the effectiveness of the proposed strategies. Furthermore, cooperation and information exchange with other industries, universities and other educational establishments, as well as participation in cybersecurity associations and events are encouraged. To this end, the research employs a systematic and cross-disciplinary approach and seeks to (a) build on the current literature and knowledge in smart network forensics; (b) contribute to the creation of novel security solutions and paradigms; and (c) bolster the security and stability of networked environments against emerging threats.

Power System Technology
ISSN:1000-3673

Received: 16-01-2024 Revised: 12-02-2024 Accepted: 07-03-2024

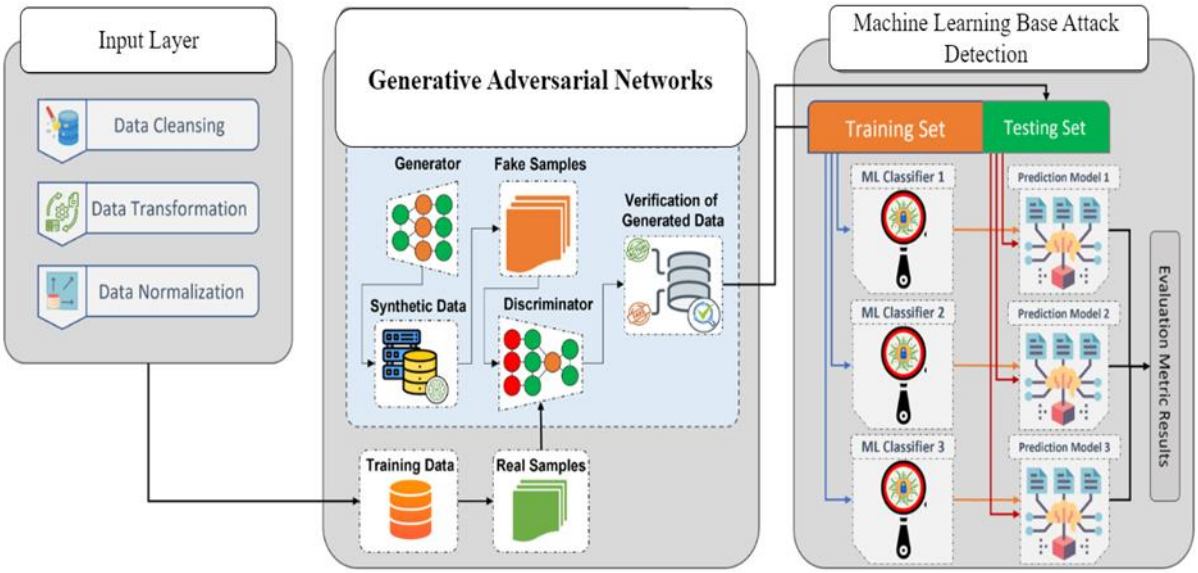

Figure 1. Proposed Flow Diagram

The idea of analyzing network attacks in the era of cybersecurity is a delicate subject because of constantly emerging new methods to detect suspicious network traffic and activity. In doing so, this applied research work identifies a cutting-edge technological intervention that would help remain relevant in today's world: machine learning through the use of Generative Adversarial Networks (GANs). In this system, there is a constant training mode where the system is constantly learning how better to enable it to detect such threats and prevent them.

It starts from network traffic raw data that can be noisy, and contain entries or event with measurement errors or incorrect entries. This data is further processed for cleansing in order to eliminate incompatibilities and inaccuracies to make it suitable for training the desired machine learning models. There comes data cleaning where the data that had been preprocessed undergoes transformation to be specific for the GAN models. This may require normalization, scaling, or some other form of processing to adjust the data points into a form than can be easily grasped by a GAN and manipulated to the required extents.

The core of the system is consequently innervate in the GAN itself. This component operates in two parts: The two characteristic components can be identified as the generator and the discriminator. The generator assumes the role of an active concept at the center of this process and cognition; it employs random noise as a starting point. This noise, denoted mathematically as "z", forms the basis for the generator's artistic process – creating an artificial data set which behaves in a realistic fashion, at least insofar as network traffic is concerned. This 'noise' is essential for teaching the mechanism its parameters concerning the distinction between normal work, attempts at sabotage or malevolent actions.

Power System Technology
ISSN:1000-3673
Received: 16-01-2024 Revised: 12-02-2024 Accepted: 07-03-2024

However, the role of the generator is not without opposition as the following sections indicate. The other half of the GAN, the discriminator, therefore plays a cynical role as it can readily locate fake images. It is subscribed by another module which feeds it with the actual network traffic data (real samples) in addition to the synthetic data not real at all but fake samples generated by its twin. What the discriminator aims at is to filter out all the fake data samples with as finest a scrutiny as possible while admitting the real ones. It achieves this in that it provides the end consumer with a probability score ranging from 0 to 1. A higher score should be closer to 1, which means that the sample is very likely to be from real traffic data, whereas, a score that is closer to 0 implies that the sample is highly likely to be a fabricated data set by the generator.

The training process is also recursive where the generator is trained side-by-side with the discriminator. But while this is happening, the discriminator, which is working to classify real from fake, gets better and better with the new fake data being generated by the generator. In this regard, the competition that continues to exist between them even at the fundamental level helps in the learning process of the two components. The generator is always working towards making better and more convincing forgeries all the time while the discriminator is equally improving its outlook and adeptness in differentiating fake items from the original ones.

The information utilized to train the precise system is not exclusively the set of images generated by the generator. The real network traffic data is also helpful in determining the accuracy of the paper's findings since it corroborates the simulation results. It is further divided into training set and a testing set. The training set finds its application in training the different models in machine learning, which constitutes the key components of the attack detection system. These models, initially established as ML Classifiers , rely on the integrated dataset of actual traffic data along with the synthesized data produced by the GAN. By so doing, the models are able to understand patterns and signatures that seem not to be those of normal networks traffic and may therefore be containing some form of attack.

The trained models then graduate to ML Classifiers, and once trained, they become Prediction Models. These are the models that are poised to defend the system; the models that are trained to inspect and diagnose the new, unknown network traffic data. Given inputs, they produce classifications and it is probable that they can detect anomalous traffic while labeling seemingly normal traffic generated by legitimate users.

Efficiency of the system is monitored from many parameters to ensure that it delivers optimal results. These could be referred as the "Evaluation Metric Results" in the diagram may include accuracy, precision, recall and some other suitable measurements specific to the detection of the listed attacks. Again, these metrics will help security staff determine the status of the system and look out for any areas of optimization.

Power System Technology
ISSN:1000-3673

Received: 16-01-2024 Revised: 12-02-2024 Accepted: 07-03-2024

3.1 Systematic Algorithms

(a) Initialize Blockchain:

- Define genesis block
- Create empty list of blocks

(b) Define Smart Network Forensics Functions:

- Preprocess Data ():
- Clean and normalize network data
- Extract features from network packets
- Train GAN ():

(c) Initialize generator and discriminator networks

- Define loss functions (e.g., binary cross-entropy)
- Compile GAN model
- Train GAN model on preprocessed data
- Generate Synthetic Data ():
- Use trained generator to produce synthetic network data
- Detect Anomalies ():
- Preprocess real and synthetic data
- Train anomaly detection model (e.g., autoencoder)
- Detect anomalies in real and synthetic data
- Create Immutable Audit Trail ():
- Define block structure with fields (e.g., timestamp, data, hash)
- Generate hash for each block using cryptographic hash function
- Link blocks together to form a chain
- Append blocks to blockchain
- Verify Blockchain Integrity():
- Iterate through blocks in blockchain
- Verify hash of each block matches hash of previous block
- Ensure integrity of blockchain

Power System Technology
ISSN:1000-3673
Received: 16-01-2024 Revised: 12-02-2024 Accepted: 07-03-2024

- Analyze Blockchain ():
  - Retrieve and analyze audit trail data from blockchain
  - Identify patterns, anomalies, and security incidents

  Main ():

(d) Initialize blockchain

- Load and preprocess network data
- Train GAN on preprocessed data
- Generate synthetic data using trained GAN
- Detect anomalies in real and synthetic data
- Create immutable audit trail using blockchain
- Verify integrity of blockchain
- Analyze blockchain data for security insights

The following pseudo code encapsulates the logical architecture that forms the foundational model for enabling smart network forensics based on blockchain and GANs. To begin with, involves the starting creation of the blockchain where the first block referred to as the genesis block is created and an empty list of blockages to secure an unaltered trail. Next, the functions for Smart Network Forensics are described as follows: The data preprocessing process includes cleaning and normalizing of data along with feature extraction from the packets harvested from the network. Subsequently, the skills of constructing GAN are utilised to train the GAN on the preprocessed data to generate synthetic network data for anomaly detection . These are then estimated by analyzing the real and synthetic datasets to train and develop an anomaly detector model, e. g. , an autoencoder. The concept of a block that can be used to create an immutable audit trail would then include a time stamp, the data, and hash fields and additional new hash fields would be computed from the data in the block using cryptographic hash functions and subsequent blocks would point to the hash of the previous block and include another hash field for the newly generated hash from the data in the new block. The way the integrity of the blockchain is got is by checking on blocks and hashing them where the result should match with the one before the next. Last but not the least, raw blockchain data is processed in order to extract audit trail data and subsequently, audit trails are examined to find out patterns, irregularities and security breaches. The main function manages all the operations of the system including creating the blockchain, importing the network data and pre-processing it, training the GAN, generating the fake data, checking the anomalies, creating the secure audit trail block chain, verifying the integrity of block chain and analyzing them for security purposes. As a

Power System Technology
ISSN:1000-3673
Received: 16-01-2024 Revised: 12-02-2024 Accepted: 07-03-2024

result of this study, a resilient and structured framework for SNF is proposed with the utilization of blockchain and GANs as a means of fortifying security and identifying irregularities.

4. Results and Discussions

AIDS as the acronym for intrusion detection systems is equivalent to watchdogs of your network, consistently scanning the system for abnormal behaviors. They use different methods like matching current traffic patterns with the analysis result of previous attacks, or they define anomalies as any behavior that is inconsistent with the norm. These analyses assistance in identifying attempted unauthorized access, malicious activity, and security policy violation taking place over your network and defending it against a range of threats.

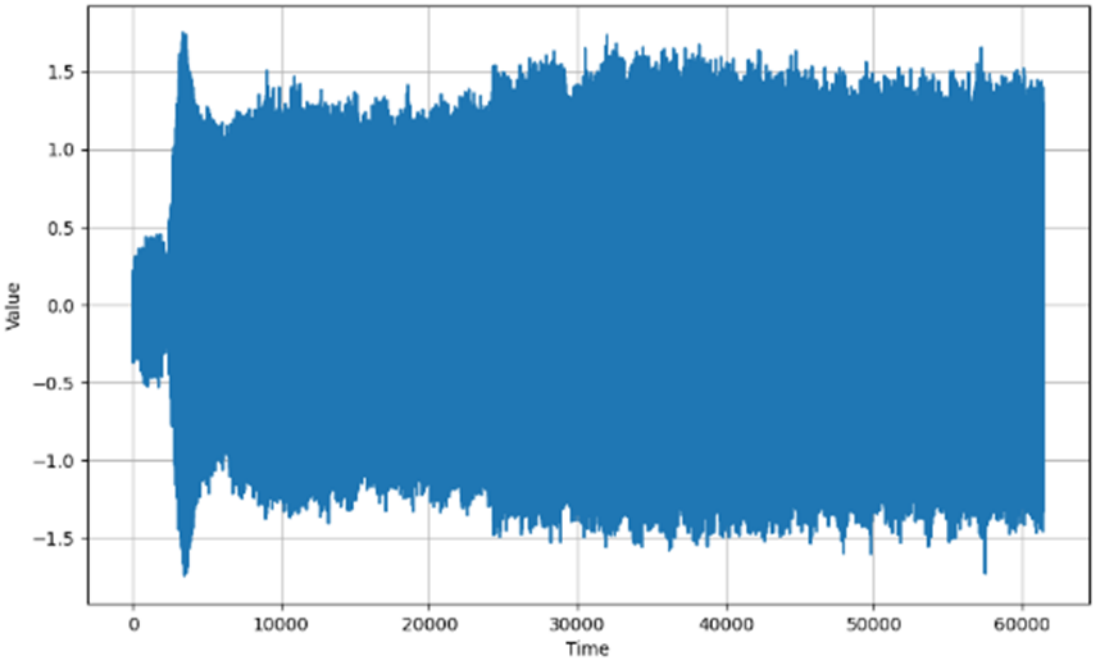

Figure 2. Time Complexity

Intrusion Detection System (IDS) should be noted to be performing operations of a network sentinel of a certain kind. Nodes installed throughout continuously catalog activity so that the information can funnel it to an analytical core. In this engine, many methods are used to detect initial signs of an attack or any change in behavior compared to the norm. In case any suspicious activity is identified, the IDS raises alert and may also launch specific countermeasures to contain threats. Security personnel are required to manage the IDS activity by controlling it from a central console, monitor the alerts, and overall maintenance of the system.

Power System Technology
ISSN:1000-3673
Received: 16-01-2024 Revised: 12-02-2024 Accepted: 07-03-2024

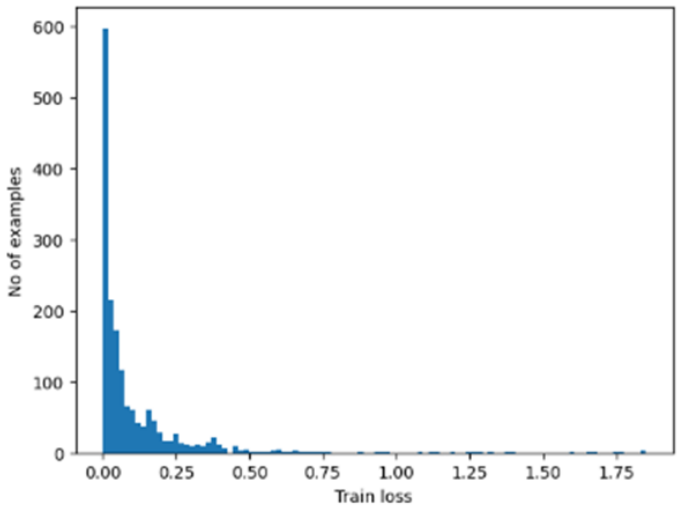

Figure 3. Number of Dataset During Training

Detectors collect information about activity and pass it to analyzer which search for anomalous behavior or signs of an attack. Whenever there is something suspicious, an alert is produced, action like prevention or reporting to security agents is initiated. This makes a central hub that security professionals can use to oversee the system, look into the alarms, and keep the network safe. This brief description encapsulates the concept of an Intrusion Detection System (IDS), a vigilant watchdog that protects your network.

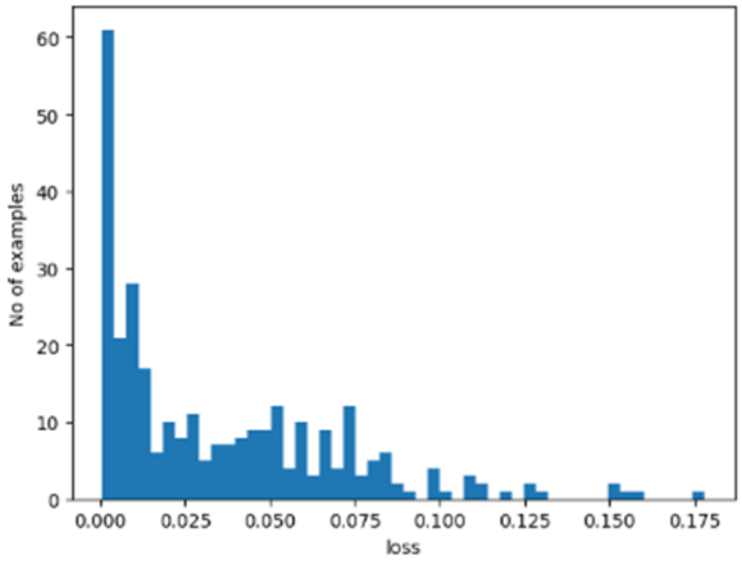

Figure 4. Error Rate

Power System Technology
ISSN:1000-3673

Received: 16-01-2024 Revised: 12-02-2024 Accepted: 07-03-2024

5. Conclusion

Consequently, this research aims to introduce a new concept of network forensics through using GAN for synthetic data generation, blockchain for a tamper-proof log and smart contract for self-executive measures. This framework has the potential to radically enhance network security by enhancing the tools for detection of anomalous behavior, providing forensically sound data storage, and integrating incident handling with a proactive approach toward network protection, thus opening the doors to a new age of defensive network architecture. Peculiarities of computational cost, blockchain, and smart contracts pose certain questions that need to be solved for the widespread adoption of the network security; however, this research serves as a breakthrough to a more enhanced network security environment.

Funding: Tianjin Science and Technology Plan Project—Technological Innovation Guidance Special Fund-22YDLQSN0050.

Refrences

[1] Cholevas, C., Angeli, E., Sereti, Z., Mavrikos, E., & Tsekouras, G. E. (2024). Anomaly Detection in Blockchain Networks Using Unsupervised Learning: A Survey. Algorithms, 17(5), 201.

[2] Ali, S., Li, Q., & Yousafzai, A. (2024). Blockchain and federated learning-based intrusion detection approaches for edge-enabled industrial IoT networks: A survey. Ad Hoc Networks, 152, 103320.

[3] Ponnusamy, S., Antari, J., Bhaladhare, P. R., Potgantwar, A. D., & Kalyanaraman, S. (Eds.). (2024). Enhancing Security in Public Spaces Through Generative Adversarial Networks (GANs). IGI Global.

[4] Kumar, C., & Chittora, P. (2024). Deep-Learning and Blockchain-Empowered Secure Data Sharing for Smart Grid Infrastructure. Arabian Journal for Science and Engineering, 1-14.

[5] Alqahtany, S. S., & Syed, T. A. (2024). ForensicTransMonitor: A Comprehensive Blockchain Approach to Reinvent Digital Forensics and Evidence Management. Information, 15(2), 109.

[6] Kearns, L., Alam, A., & Allison, J. Synthetic Media Authentication Threats: Detection Using a Combination of Neural Network and Blockchain Technology. Available at SSRN 4658121.

[7] Liu, Y., Yu, F. R., Li, X., Ji, H., & Leung, V. C. (2020). Blockchain and machine learning for communications and networking systems. ieee communications surveys & tutorials, 22(2), 1392-1431.

[8] Kamišalić, A., Kramberger, R., & Fister Jr, I. (2021). Synergy of blockchain technology and data mining techniques for anomaly detection. Applied Sciences, 11(17), 7987.

Power System Technology
ISSN:1000-3673

Received: 16-01-2024 Revised: 12-02-2024 Accepted: 07-03-2024

[9] George, A. S. (2023). Securing the future of finance: how AI, Blockchain, and machine learning safeguard emerging Neobank technology against evolving cyber threats. Partners Universal Innovative Research Publication, 1(1), 54-66.

[10] Kumar, R., Kumar, P., Tripathi, R., Gupta, G. P., Gadekallu, T. R., & Srivastava, G. (2021). SP2F: A secured privacy-preserving framework for smart agricultural Unmanned Aerial Vehicles. Computer Networks, 187, 107819.

[11] Sarhan, M., Lo, W. W., Layeghy, S., & Portmann, M. (2022). HBFL: A hierarchical blockchain-based federated learning framework for collaborative IoT intrusion detection. Computers and Electrical Engineering, 103, 108379.

[12] Varma, I. M., & Kumar, N. (2023). A comprehensive survey on SDN and blockchain-based secure vehicular networks. Vehicular Communications, 100663.

[13] Rahman, M. A., Hossain, M. S., Islam, M. S., Alrajeh, N. A., & Muhammad, G. (2020). Secure and provenance enhanced internet of health things framework: A blockchain managed federated learning approach. Ieee Access, 8, 205071-205087.

[14] Wijesekara, P. A. D. S. N., & Gunawardena, S. (2023). A Review of blockchain technology in knowledge-defined networking, its application, benefits, and challenges. Network, 3(3), 343-421.

[15] Jiang, Y., Ma, B., Wang, X., Yu, G., Yu, P., Wang, Z., ... & Liu, R. P. (2023). Blockchained Federated Learning for Internet of Things: A Comprehensive Survey. ACM Computing Surveys.

[16] Bendiab, G., Hameurlaine, A., Germanos, G., Kolokotronis, N., & Shiaeles, S. (2023). Autonomous vehicles security: Challenges and solutions using blockchain and artificial intelligence. IEEE Transactions on Intelligent Transportation Systems, 24(4), 3614-3637.

[17] Mothukuri, V., Parizi, R. M., Pouriyeh, S., Dehghantanha, A., & Choo, K. K. R. (2021). FabricFL: Blockchain-in-the-loop federated learning for trusted decentralized systems. IEEE Systems Journal, 16(3), 3711-3722.

[18] Wang, Y., Su, Z., Zhang, N., Xing, R., Liu, D., Luan, T. H., & Shen, X. (2022). A survey on metaverse: Fundamentals, security, and privacy. IEEE Communications Surveys & Tutorials, 25(1), 319-352.

[19] Sey, C., Lei, H., Qian, W., Li, X., Fiasam, L. D., Kodjiku, S. L., ... & Agyemang, I. O. (2022). Vblock: A blockchain-based tamper-proofing data protection model for internet of vehicle networks. Sensors, 22(20), 8083.

[20] Moore, E., Imteaj, A., Rezapour, S., & Amini, M. H. (2023). A survey on secure and private federated learning using blockchain: Theory and application in resource-constrained computing. IEEE Internet of Things Journal.

[21] Gambín, Á. F., Yazidi, A., Vasilakos, A., Haugerud, H., & Djenouri, Y. (2024). Deepfakes: current and future trends. Artificial Intelligence Review, 57(3), 64.

Power System Technology
ISSN:1000-3673

Received: 16-01-2024 Revised: 12-02-2024 Accepted: 07-03-2024

[22] Myrzashova, R., Alsamhi, S. H., Shvetsov, A. V., Hawbani, A., & Wei, X. (2023). Blockchain meets federated learning in healthcare: A systematic review with challenges and opportunities. IEEE Internet of Things Journal.

[23] Muthamizharasan, M. M., & Hemamalini, M. (Eds.). (2024). Computational Intelligence and Its Applications (ICCIA-2024).

[24] Huang, K., Goertzel, B., Wu, D., & Xie, A. (2024). GenAI Model Security. In Generative AI Security: Theories and Practices (pp. 163-198). Cham: Springer Nature Switzerland.

[25] Ahmad, J., Zia, M. U., Naqvi, I. H., Chattha, J. N., Butt, F. A., Huang, T., & Xiang, W. (2024). Machine learning and blockchain technologies for cybersecurity in connected vehicles. Wiley Interdisciplinary Reviews: Data Mining and Knowledge Discovery, 14(1), e1515.