Research Article

UNCOVERING EVIDENCE OF ATTACKER BEHAVIOR ON THE NETWORK

Asad Yaseen
Asad4ntrp2@gmail.com
https://orcid.org/0009-0002-8950-0767

Abstract

This comprehensive research presents and investigates a diverse assessment of interruption discovery strategies and their job in contemporary online protection. Interruption Recognition Frameworks are taken apart as vital parts in defending computerized foundations, utilizing different techniques, for example, signature-based, peculiarity based, and heuristic-based identification. While signature-based strategies demonstrate strong against known dangers, the review highlights the urgent job of irregularity-based and heuristic-based approaches in countering novel and complex assaults. Different types attract, their characteristics and behaviors has explored in this paper. The mix of AI and Man-made consciousness (computer based intelligence) in recognizing odd exercises arises as an extraordinary power, empowering versatile reactions to developing digital dangers. The exploration fundamentally breaks down the difficulties looked by existing location strategies, including versatility concerns, high bogus positive rates, and the encryption-related obstacles in rush hour gridlock examination. The outcomes and investigation segment approves the viability of proposed models, including group learning strategies and creative techniques, for example, the Solid Methodology in light of Blockchain and Peculiarity based location (SABA). A Convolutional Brain Organization (CNN) model for interruption location in IoT conditions and a cross breed approach joining positioning based channel strategies and NSGA-II exhibit eminent exactnesses. The review's suggestions for network security are significant, prompting proposals for a TTP-driven approach, mix of conduct peculiarities, persistent security mindfulness preparing, standard red group works out, versatile episode reaction plans, and intermittent security reviews. By and large, the examination contributes a nuanced comprehension of assailant's ways of behaving, down to earth procedures for online protection

flexibility, and makes way for future investigation into dynamic danger scenes and the human component in network safety.

Keywords: Cybersecurity, Internet of Things, Man-in-the-middle (MitM) Attacks, Intrusion Detection Systems, Signature-Based Intrusion Detection Systems, Signature-Based, Anomaly-Based Detection, Machine Learning, Convolutional Neural Network (CNN), Anomaly-based IDS models, intrusion detection systems (IDS), signature-based intrusion detection systems (SIDS), tactics, techniques, and procedures (TTPs), Distributed Denial-of-Service (DDoS), Support Vector Classifier

INTRODUCTION

The increasing sophistication of cyber threats necessitates a comprehensive comprehension of attacker behavior on networks in the interconnected realm of digital systems. Malicious entertainers exploit weaknesses for different purposes, going from information breaks to basic help interruptions. The bits of knowledge determined is fundamental for creating proactive measures and organization safeguards against the powerful scene of cyber threats. This examination dives into the fundamental task of uncovering proof of attacker lead, expecting to notice the procedures, techniques, and frameworks used.

Background and the context of cybersecurity challenges: In the space of organization security, the pursuit for safeguarding modernized scenes has provoked a fundamental spotlight on uncovering confirmation of attackers directly on networks. This endeavor incorporates present-day assessment and consistent perception to distinguish peculiarities, dubious models, and potential security breaks. Online protection experts utilize progressed apparatuses and methods to take apart organization traffic, examine log documents, and distinguish marks of give and take. Organizations can proactively strengthen their defenses, respond quickly to incidents, and mitigate potential threats by comprehending the behavior of attackers [1]. As threats entertainers employ increasingly complex strategies, this powerful field requires constant development, highlighting the critical importance of staying ahead in the ongoing battle for computerized foundations.

Cybersecurity has ended up being inescapable and complex, introducing basic challenges to individuals, affiliations, and assemblies all over the planet. The rapidly developing advanced scene has brought about a time of interconnected frameworks, which not only provide unusual accommodation and proficiency but also provide a large attack surface for harmful entertainers. It is essential to have a solid understanding of the history and context of cybersecurity threats to create efficient defense mechanisms and safeguard sensitive information. Cyber dangers

envelop a large number of malevolent exercises, including yet not restricted to hacking, phishing, malware assaults, and ransomware occurrences [2]. These dangers can take advantage of shortcomings in programming, equipment, and human way of behaving, making online protection a complex challenge. Moreover, danger knowledge and proactive observing assume a critical part in remaining in front of arising dangers. Online protection experts utilize a scope of approaches, such as encryption, firewalls, interruption identification frameworks, and security mindfulness preparation. The platform of online protection has developed exponentially because of these developing threats.

Research aim: The research aims to reveal and investigate proof of attacker behavior on the network, utilizing advanced cybersecurity procedures to improve threat identification and foster powerful countermeasures for network security.

Research objectives: To investigate common tactics, techniques, and procedures (TTPs) to comprehend how attackers act on the network.

To recognize unobtrusive and modern indications of malicious activities for creating and executing progressed interruption recognition techniques.

To evaluate the viability of existing organization safety efforts and propose upgraded countermeasures.

Research questions

RQ1: What are the pervasive tactics, techniques, and procedures (TTPs) utilized by attackers on the network, and how do these add to their general way of behaving?

RQ2: How could unpretentious and current signs of malevolent exercises be recognized and utilized in the turn of events and execution of advance interruption discovery strategies?

RQ3:. In what ways can the adequacy of current hierarchical safety efforts be evaluated?

Importance of identifying and understanding attacker behaviour: The significance of identifying and understanding attacker behavior in the domain of cybersecurity couldn't possibly be more significant, given the heightened refinement and recurrence of digital dangers. This information is instrumental in creating compelling guard components, sustaining advanced frameworks, and moderating the possible aftermath of malicious activities. Attacker behavior gives significant experiences into the philosophies utilized by digital enemies [3]. Network safety experts can proactively recognize weaknesses and plan tough

frameworks by fathoming the tactics, techniques, and procedures (TTPs). This proactive position permits associations to remain one stride in front of developing threats, originating a unique protection system that adjusts to the quickly changing scene of digital attacks. Besides, identifying and understanding attacker behavior supports the quick detection of interruptions and compromises [4]. Digital assailants frequently utilize inconspicuous and shifty strategies to go undetected inside organizations. Security groups can improve their capacity to distinguish malignant exercises progressively, lessening the abide season of attackers and limiting possible damage. Early recognition is vital in forestalling information breaks, framework disturbances, and unapproved admittance to delicate data. Furthermore, understanding attacker behavior helps with the attribution of digital assaults. It is essential to identify the reasons behind cyber threats to respond appropriately and hold those responsible accountable. Attribution gives important data to conciliatory, legitimate, and policing, empowering an extensive reaction to digital incidents. Moreover, this information works with the advancement of designated and compelling countermeasures. Cybersecurity specialists can make particular instruments and conventions that straightforwardly address the strategies utilized by noxious entertainers by taking apart attacker behavior. The targeted approach improves the efficiency of cybersecurity measures by ensuring that resources are effectively allocated to mitigate specific threats.

RELATED WORKS

1. Anomaly-Based Intrusion Detection by Machine Learning: A Case Study on Probing Attacks to an Institutional Network: The study illustrates the key aspects of robustness in the implementation of methods focusing on its capacity to confirm the validation of outcomes. By utilizing both institutional and UNSW-NB15 datasets, the study establishes a strong foundation for evaluating the proposed approach [5]. The importance of methodological validity is underscored as a precursor to any meaningful analysis. The study engages in a comparative analysis of two machine learning models, particularly assessing their performance in detecting probing attacks. The Convolutional Neural Network (CNN) model demonstrates superiority on the institutional data set, albeit marginally, while an ensemble model exhibits advantages in 'explainability' and computational resource efficiency. This nuanced exploration adds valuable insights into the trade-offs between different model architectures[5]. A distinctive feature of the study lies in its departure from prevalent practices involving simulated data sets.

Instead, the study evaluates anomaly-based IDS models in a real-life institutional environment, presenting a novel contribution to the literature. The findings suggest that anomaly-based techniques outperform misuse-based models in this authentic

context, paving the way for their practical adoption in enterprise IDS. Beyond its individual contributions, the study situates itself within the broader landscape of IDS research, responding to the ongoing shift towards anomaly-based techniques. The emphasis on methodology robustness aligns with the increasing demand for rigorous evaluation frameworks in machine learning applications [5]. The comparative analysis of machine learning models not only underscores their performance variations but also prompts a reflection on the interpretability and computational demands associated with different architectures. The study adds a layer of realism by steering away from the prevalent reliance on simulated data sets. This shift towards evaluating models in an authentic institutional environment elevates the study's relevance and encourages a departure from the limitations imposed by synthetic datasets. Consequently, the study extends an invitation to future researchers and practitioners to explore anomaly-based approaches, fostering a deeper understanding of their applicability and advantages in enterprise-level IDS implementations.

2. Secure approach based on anomaly and signature-based detection mechanism for detecting abnormal activities in blockchain network: According to Nisioti *et al.,* 2018, the study focuses on the existing body of knowledge related to secure approaches in blockchain networks, with a specific emphasis on signature-based detection methods. It acknowledges the widespread usage and development of blockchain technology in various industries, such as finance, politics, and healthcare, while also highlighting the associated security risks [6]. The study outlines the prevalence of security events and risks in the blockchain platform, underscoring the need for effective intrusion detection systems (IDS) to enhance the security of complex networks and systems.

The two primary categories of IDS, signature-based and anomaly-based, are introduced, with a specific focus on signature-based intrusion detection systems (SIDS). In the context of SIDS, the review explains that these systems employ pattern-matching approaches to identify known attacks. They analyze host logs for sequences of instructions or behaviors previously detected as malware, using matching algorithms to locate initial incursions[6]. The effectiveness of SIDS is acknowledged in detecting previously known intrusions with fewer false alarms, identifying intruders quickly, and being excellent at detecting known attacks. The limitations of SIDS are also highlighted, such as the need for regular updates to recognize modified or new versions of attacks. The review notes that SIDS may be ineffective in identifying zero-day attacks, multi-step attacks, and could have limited knowledge of attack insights. The study sets the stage for the proposed SABA approach. which aims to address the limitations of existing signature-based detection methods. By combining signature-based and anomaly-based detection,

SABA is positioned as a decentralized solution based on blockchain technology[6]. This approach leverages information gathered from previous threat detectors saved in the blockchain application, introducing a new paradigm for enhancing security in blockchain networks.

3. Anomaly-based Intrusion Detection System for IoT Networks through Deep Learning Model: According to He *et al.,* 2020, the study addresses the critical challenge of security threats in Internet of Things (IoT) networks and explores the potential of deep learning, specifically Convolutional Neural Networks (CNN), for anomaly-based intrusion detection. The literature review contextualizes the research within the broader landscape of IoT security, emphasizing the necessity for advanced methodologies to mitigate evolving threats. The study positions anomaly-based detection as a key strategy for securing IoT devices [7]. It distinguishes between passive and active threats in IoT environments [7]. Passive threats involve covert information gathering, while active threats aim to disrupt IoT systems.

The resource-constrained nature of IoT devices adds complexity to implementing effective intrusion detection systems (IDS). Anomaly-based intrusion detection emerges as a pivotal strategy for fortifying the security of Internet of Things (IoT) devices in the face of escalating threats. The paper elucidates a fundamental distinction between passive and active threats within IoT environments. Passive threats center around clandestine information gathering, where infiltrators covertly observe and collect data from the communication channels of IoT devices. On the other hand, active threats are characterized by deliberate actions to disrupt the normal functioning of IoT systems. These may include malicious alterations, control manipulations, or outright attempts to impair the availability and integrity of IoT devices [7]. The unique challenge in implementing effective intrusion detection systems (IDS) for IoT lies in the resource-constrained nature of these devices. Unlike traditional computing systems, IoT devices often operate with limited computational power and storage capabilities. This constraint amplifies the complexity of deploying robust IDS tailored to the specific needs and limitations of IoT environments. Hence, the paper underscores the critical importance of anomaly-based detection methods to discern irregular patterns and behaviors indicative of both passive and active threats, thereby enhancing the overall security posture of IoT ecosystems.

4. Hybrid Meta-Heuristic based Feature Selection Mechanism for Cyber-Attack Detection in IoT-enabled Networks: According to Ghanem *et al.,* 2017, Heuristic-based intrusion detection systems (IDS) play a pivotal role in addressing the evolving landscape of cyber threats, particularly in the context of securing IoT-

enabled networks. The literature review reveals a growing body of research emphasizing the significance of heuristic approaches for cyber-attack detection. Heuristic methods, often inspired by human problem-solving strategies, offer a proactive defense mechanism against unknown or novel attacks [8]. Numerous studies highlight the effectiveness of heuristic-based detection in identifying anomalies and potential threats within network traffic.

Heuristics leverage rule-based and behavioral analysis to discern patterns indicative of malicious activities, allowing for real-time detection and response. This proactive nature is essential in safeguarding IoT devices, which are vulnerable to diverse and evolving cyber threats. The study underscores the adaptability of heuristic approaches to the dynamic and heterogeneous nature of IoT environments. As IoT networks consist of diverse devices with varying functionalities, communication protocols, and data types, heuristic-based IDS provides a flexible and scalable solution [8]. It enables the identification of abnormal behaviors based on heuristics tailored to the specific characteristics of IoT traffic. Furthermore, research demonstrates the integration of metaheuristic algorithms, such as genetic algorithms and particle swarm optimization, with heuristic approaches to enhance the efficiency of cyber-attack detection. These hybrid models capitalize on the strengths of both heuristics and metaheuristics, offering robust and optimized detection capabilities. The study underscores the critical role of heuristic-based detection mechanisms in fortifying the cybersecurity posture of IoT-enabled networks [8]. The adaptability, real-time responsiveness, and ability to address the unique challenges of IoT environments position heuristic-based approaches as a promising avenue for effective intrusion detection.

ATTACKER BEHAVIOR PATTERNS

Classification of various types of attack and their characteristics: The classification of different types of attacks and their characteristics is crucial to understanding the assorted scene of digital threats and carrying out powerful network safety measures. Attackers on digital frameworks can take various structures, each with specifically qualities that present remarkable challenges to security experts. According to Alabdan, 2020, Phishing attacks are a critical category of attacks, depending on friendly designing strategies to trick people into disclosing delicate data [9]. Email phishing, in which intruders impersonate trusted entities, and spear phishing, in which specific individuals or organizations are the targets, are two common subtypes. Characteristics of phishing attacks include misleading correspondence, frequently utilizing email or phony sites, determined to fool clients into giving login accreditations, monetary data, or other delicate

information [10]. Malware is another significant category of attack, which includes a variety of malicious software intended to compromise computer systems' security and functionality. It is one of the most common types of attacks [11]. Viruses attach to legitimate applications and spread when the infected application is run. Characteristics of malware attacks incorporate subtle penetration, information control, and the potential for boundless harm.

"Distributed Denial-of-Service (DDoS)" and "Denial-of-Service (DoS) Attacks" are those types of categories that overwhelm a target system with traffic and disrupt the availability of network services. In DoS assaults, a solitary source is utilized, while DDoS assaults include various sources, making them more testing to relieve. Characteristics include an unexpected flood of traffic, delivering the designated framework difficult to reach to genuine clients [13]. Moreover, based on the classification of "SQL Injection Attacks" centers around taking advantage of weaknesses in data set frameworks [15]. In order to trick the system into carrying out commands that were not intended, attackers insert malicious SQL queries into input fields [15]. Characteristics of SQL including data exfiltration, unauthorized access to databases, and the possibility of manipulating or deleting crucial information are some of the. According to Javeed *et al.,* 2020, "Man-in-the-middle (MitM) Attacks" include capturing and possibly modifying correspondences between two gatherings without their insight [16]. In gathering hijacking, aggressors expect control over a persistent gathering between clients, while tuning in incorporates unapproved checking of correspondences. Characteristics of MitM attacks consolidate unapproved permission to fragile information, potential data control, and the ability to exploit shortcomings in correspondence shows.

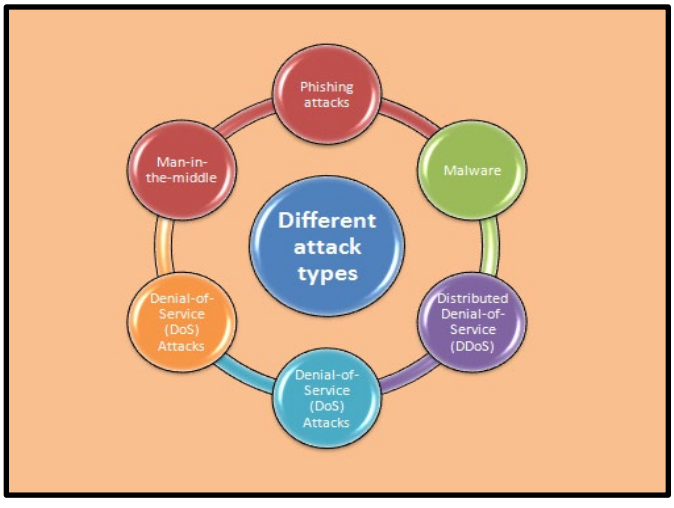

Figure 1: Different types of attack

(Source: Self-created)

Classifying the various attack types and their characteristics is essential for a more delicate understanding of the shifting threat landscape. A thorough gathering structure fills in as a critical gadget for network security specialists in their consistent undertakings to protect modernized assets and stay aware of the trustworthiness of coordinated systems.

Analysis of attacker behaviors on the network: The analysis of attacker behaviors on the network is a basic undertaking in the field of network safety, as it frames the establishment for originating powerful safeguard methods against increasing threats. Attackers use various clusters of tactics, techniques, and procedures (TTPs) to disturb operations and exfiltrate delicate information. Phishing attacks address one type of significant attacker behavior, depending on friendly design to mislead clients into uncovering delicate data or downloading malevolent substances [10]. Attackers exploit human shortcomings to secure unapproved permission to networks by assuming the presence of trustworthy components. Understanding the strategies utilized in phishing efforts, for example, email caricaturing and tricky sites, is fundamental for teaching clients, carrying out compelling email sifting frameworks, and strengthening the human layer of safeguard against digital threats.

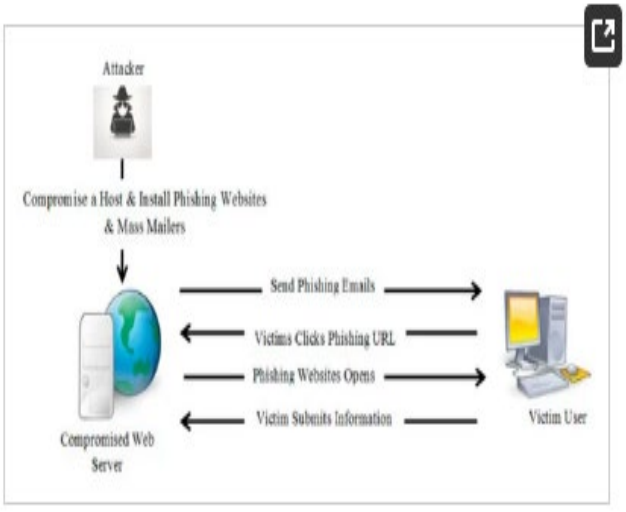

Figure 2: Phishing attacks
(Source: Alabdan, 2020)

According to Alene*et al.,* 2020, One predominant attacker behavior includes the utilization of malware to compromise and invade network frameworks. Malicious programming is intended to take advantage of weaknesses in programming and

equipment, providing unapproved admittance to assailants [32]. Attackers can think twice about secrecy, uprightness, and accessibility of information by conveying malware, causing ruin for the two people and organizations. Investigating the ordinary models and qualities connected with malware-based attacks is pressing for perceiving and overcoming such dangers.

On the other hand, as per the view of Huang *et al.*, 2020, Distributed Denial-of-Service (DDoS) and Denial-of-Service (DoS) attack behaviors uncover malicious endeavors to disturb network accessibility. DDoS attacks, such as several sources, compound the effect, making moderation challenges. DoS attacks overpower an objective with unreasonable traffic, delivering it distant [18]. Both showcase startling traffic floods, including the necessity for solid protections, for instance, traffic isolating and load changing, to ensure network strength against these inconvenient attacker approaches to acting. SQL Injection Attacks uncovered a complex strategy where aggressors exploit weaknesses in data set frameworks [12]. They modify or acquire unapproved admittance to delicate information by embedding pernicious SQL questions into input fields. Shielding organized data sets from SQL Infusion Assaults, which include unapproved information base access and the chance of information control, requires consistent security appraisals, defined questions, and powerful info approval. Honor heightening is a fundamental stage in various computerized assaults, where assailants attempt to raise their entry honors inside a compromised system. Attackers intend to acquire managerial privileges, empowering them to move horizontally through organizations and access delicate assets by taking advantage of misconfigurations or vulnerabilities. This analysis is crucial for keeping up with adversaries and protecting the security and integrity of networked systems as the digital landscape continues to change. Organizations can develop threats knowledge, foster designated safeguard instruments, and proactively respond to arising digital threats by delving into the TTPs used by malignant entertainers.

Contextual analyses of incidents delineating attacker behaviour: The execution of Anomaly-Based Intrusion Detectionutilizing machine learning focuses on testing attacks targeting an institutional network is investigated for this situation study. Machine learning calculations are utilized to lay out benchmark examples of ordinary organization conduct, empowering the recognition of peculiarities characteristic of examining attacks. The framework figures out how to distinguish deviations from laid-out standards, improving its capacity to perceive possibly malicious exercises by breaking down network traffic [5]. The contextual analysis gives knowledge into the versatility and responsiveness of abnormality-based interruption recognition frameworks by diving into the viability of this technique in distinguishing and alleviating testing assaults. This

investigation adds to the greater cognizance of using machine learning for strong web-based assurance measures, focusing on its actual ability to protect institutional associations against creating computerized dangers. This study proposes a protected approach organizing both anomaly-identification and signature-based proof instruments for perceiving uncommon activities inside a blockchain network. Using the characteristics of eccentricity ID, the system spreads out a check of the normal approach to acting and hails deviations from this model. Furthermore, signature-based recognition guarantees the distinguishing proof of realized assault designs and pernicious marks inside the blockchain. This hybrid system upgrades the robustness of the identification framework, offering complete protection against both novel and laid-out dangers [6]. The proposed approach intends to give a more grounded and more responsive security structure for blockchain networks by combining inconsistency identification's adaptability and signature-based area precision. The review reinforces the uprightness of dispersed record frameworks, addresses the ever-developing digital danger scene, and advances secure blockchain innovation rehearses. This research introduces an “Intrusion Detection System” (IDS) customized for Internet of Things (IoT) organizations, utilizing a deep learning model. The framework independently learns complex examples of ordinary ways of behaving inside IoT conditions, upgrading its flexibility to dynamic and different organization conditions by utilizing the capacities of Deep Learning [7]. The proposed IDS plans to identify deviations from learned standards, flagging possible interruptions or odd exercises continuously. IoT devices' security issues necessitate novel solutions given their increasing prevalence. This study adds to the field of online security by offering areas of strength that join the power of profound learning and oddity location, giving a proactive defense against emerging risks in IoT associations and ensuring the trustworthiness and enduring nature of related devices and structures.

This study recognizes a Hybrid Meta-Heuristic Feature Selection Mechanism designed for digital attack discovery in IoT-empowered networks. The proposed instrument smoothes out feature decisions, working on the capability and precision of computerized risk distinguishing proof harnessing the power of meta-heuristic estimations. Securing IoT-enabled networks presents a unique challenge that necessitates a sophisticated strategy because of the diverse and dynamic nature of connected devices [8]. This component deliberately assesses and chooses the most important highlights for digital assault identification, working on the general execution of interruption discovery frameworks by incorporating different meta-heuristic procedures. The examination improves the versatility of IoT networks against an assortment of digital dangers and adds to the progression of online protection in IoT conditions by giving a custom-fitted arrangement that

consolidates the flexibility of meta-heuristic calculations with the particular necessities of element choice.

DETECTION TECHNIQUES

Overview of current techniques for detecting attacker behaviour: The arsenal of techniques employed by IDS reflects a dynamic response to the evolving landscape of cyber threats. While signature-based detection remains robust against known threats, anomaly-based and heuristic-based methods provide essential layers of defence against novel and sophisticated attacks. An integrated and adaptive approach, incorporating various detection techniques, is crucial for constructing resilient Intrusion Detection Systems capable of safeguarding digital infrastructures from an ever-expanding array of cyber threats.

Intrusion Detection Systems (IDS): In the realm of cybersecurity, Intrusion Detection Systems (IDS) play a pivotal role in identifying and thwarting potential threats. IDS serve as vigilant sentinels, monitoring network and system activities to detect any signs of unauthorized or malicious behavior[17]. These systems employ diverse techniques to scrutinize incoming and outgoing traffic, thereby safeguarding the integrity and confidentiality of digital assets.

Signature-based Detection: One prevalent approach within IDS is signature-based detection, akin to identifying a digital fingerprint associated with known threats. This method involves creating signatures or patterns that encapsulate the characteristics of known cyber threats, such as malware or specific attack vectors. When network traffic aligns with these predefined signatures, the IDS promptly flags and responds to the recognized threat[18]. While effective against known attacks, the limitation of signature-based detection lies in its inability to combat novel or evolving threats for which signatures have not been predefined.

Anomaly-based Detection: Anomaly-based detection constitutes a proactive strategy aimed at identifying deviations from established patterns of normal behavior. Rather than relying on predefined signatures, anomaly-based detection scrutinizes the baseline activities of a network or system. Any aberration or deviation from this norm triggers an alert, signaling a potential security breach[19]. This method excels in detecting novel threats, as it does not rely on prior knowledge. It demands a robust understanding of the typical behavior of the system, and false positives may occur if the system undergoes legitimate changes or encounters previously unseen activities.

Heuristic-based Detection: Heuristic-based detection leverages a set of rules and algorithms informed by general knowledge about potential threats and vulnerabilities. Unlike signature-based detection, heuristics focus on identifying

broader patterns of malicious behavior rather than specific signatures. This technique is particularly adept at detecting previously unseen variants of known threats by recognizing common characteristics or behaviors associated with malicious activities[20]. It may incur a higher rate of false positives, as it relies on generalized rules rather than precise signatures.

Analysis of machine learning and artificial intelligence in identifying anomalous activities

Analysis of Machine Learning (ML) in Identifying Anomalous Activities: Machine Learning (ML) has emerged as a transformative force in cybersecurity, particularly in the realm of identifying anomalous activities within network and system environments. ML algorithms excel at learning patterns from historical data, enabling them to discern normal behaviors and subsequently flag deviations that may indicate potential threats. One notable application is in anomaly-based Intrusion Detection Systems (IDS), where ML algorithms continuously analyze vast datasets to establish a baseline of regular activities[21]. Through supervised learning, ML models can be trained on labeled datasets, allowing them to recognize and classify patterns associated with both normal and malicious activities.

The strength of ML lies in its adaptability and capacity to evolve as it encounters new data. In anomaly detection, ML models, such as clustering algorithms and neural networks, can dynamically adjust to changes in the network landscape. Unsupervised learning methods empower ML systems to identify anomalies without predefined labels, offering a valuable capability to detect previously unseen threats[22]. However, ML is not without challenges; false positives may arise due to the inherent complexity of network activities, and adversaries may attempt to manipulate ML models through adversarial techniques.

Analysis of Artificial Intelligence (AI) in Identifying Anomalous Activities: Artificial Intelligence (AI), encompassing a broader spectrum of capabilities, plays a pivotal role in enhancing anomaly detection and response mechanisms. Unlike ML, AI incorporates reasoning and decision-making capacities, enabling a more sophisticated understanding of anomalous activities. AI systems, powered by advanced algorithms, can discern complex relationships within data, providing a more nuanced analysis of potential threats.

AI's proficiency in anomaly detection extends beyond pattern recognition; it encompasses contextual understanding and adaptive responses. Deep learning, a subset of AI, facilitates the creation of intricate neural networks capable of hierarchical learning, making them adept at identifying subtle anomalies in vast

datasets. Reinforcement learning in AI further enhances anomaly detection by enabling systems to learn from the consequences of their actions, refining their response mechanisms over time. Despite these advantages, AI deployment in anomaly detection necessitates careful consideration of ethical concerns, interpretability, and potential biases[23]. The opacity of certain AI models may hinder understanding, raising questions about accountability and trust. Striking a balance between the power of AI in identifying anomalous activities and ensuring transparency in decision-making remains a critical aspect of leveraging AI effectively for robust cybersecurity practices.

Discussion of the challenges and limitations of existing detection methods: Addressing these challenges and limitations requires a holistic approach, combining various detection methods, leveraging machine learning and artificial intelligence, and fostering collaboration within the cybersecurity community to stay ahead of emerging threats. Continuous research and development efforts are essential to enhancing the effectiveness of intrusion detection mechanisms in the ever-changing cybersecurity landscape.

Challenges:

Adaptability to Evolving Threats: Existing detection methods face the challenge of keeping pace with the rapidly evolving landscape of cybersecurity threats. As attackers employ sophisticated techniques, intrusion detection systems (IDS) must continually adapt to new tactics, procedures, and patterns employed by malicious actors.

High False Positive Rates: A prevalent challenge is the occurrence of high false positive rates in detection systems[24]. The complexity of network behaviors and the diversity of legitimate activities often lead to misinterpretations, causing security teams to investigate numerous false alarms, consuming valuable time and resources.

Insider Threat Detection: Identifying anomalous activities originating from insider threats poses a significant challenge. Malicious activities conducted by authorized users or employees with privileged access may exhibit patterns that closely resemble normal behavior, making them difficult to detect without context-aware analysis.

Encrypted Traffic Analysis: The pervasive use of encryption in communication poses a challenge for many detection methods. While encryption enhances data security, it also conceals potential threats within encrypted traffic, making it challenging to inspect and identify malicious activities without compromising privacy [26].

Limitations:

Overreliance on Signatures: Signature-based detection methods are limited by their reliance on predefined patterns of known attacks. This approach struggles to identify novel or sophisticated threats that deviate from established signatures, leaving systems vulnerable to zero-day attacks.

Scalability Issues: Many existing detection methods encounter scalability issues when applied to large and complex network infrastructures. As network sizes expand, the computational resources required for thorough analysis may become prohibitive, leading to incomplete monitoring and increased risks.

Resource Intensiveness: Heuristic-based detection methods often demand significant computational resources, impacting the overall performance of systems. The intensive processing required for heuristic analysis may result in delays and potential bottlenecks, particularly in resource-constrained environments.

Limited Context Awareness: Anomaly-based detection methods may exhibit limitations in contextual understanding, especially when dealing with subtle deviations from normal behavior[25]. Understanding the context of specific network activities is crucial for distinguishing genuine anomalies from benign variations.

RESULTS AND ANALYSIS

Intrusion Detection Systems (IDS) form the cornerstone of cybersecurity, employing diverse techniques to identify and counter potential threats. While signature-based detection relies on predefined patterns, effective against known threats, anomaly-based detection takes a proactive stance by identifying deviations from normal behavior patterns. This approach excels in detecting novel threats, though false positives may arise. Heuristic-based detection, leveraging rules and algorithms, focuses on broader patterns of malicious behavior. An integrated approach, combining these techniques, is crucial for resilient IDS capable of adapting to the evolving cyber threat landscape.

Presentation of findings from the research: The results from the study showcase the effectiveness of the proposed ensemble learning model in intrusion detection on both the institutional dataset and the UNSW-NB15 dataset. The evaluation metrics, including F1 scores and Receiver Operating Characteristics (ROC) curves, highlight the model's robust performance. The use of ensemble learning contributes to the model's ability to accurately classify probing attacks. The findings, validated through various visualization techniques, provide insights into

the model's behavior and feature importance. Hyperparameter optimization further enhances the model's efficiency. The study establishes a strong foundation for anomaly-based intrusion detection using ensemble learning in IoT environments.

The study primarily focuses on proposing the Secure Approach based on Blockchain and Anomaly-based detection (SABA) as an innovative solution for enhancing the security of blockchain networks. While specific numerical results or analyses are not explicitly provided, the study lays the groundwork for SABA, emphasizing its decentralized nature and the integration of both signature-based and anomaly-based detection methods. The analysis revolves around the limitations of existing signature-based systems and how SABA aims to overcome these challenges, presenting a novel paradigm for blockchain network security.

The proposed scheme's performance is evaluated using the ToN-IoT dataset, implementing it in Python 3.9 with the SVC package on a Windows 11 PC. Performance metrics such as accuracy and the number of selected features are employed for assessment. The proposed scheme's results are compared with the original NSGA-II and other existing techniques. The ToN-IoT dataset, comprising telemetry data from IoT services and network traffic, is utilized for experimentation, covering various cyber-attacks. The proposed hybrid method, combining ranking-based filter methods and NSGA-II, achieves a remarkable accuracy of 99.48% with an optimized feature set containing 13 features. Comparison with existing techniques demonstrates the superiority of the proposed model in terms of accuracy and the minimal number of selected features.

Comparison with existing literature and theories: The proposed intrusion detection scheme in this research is positioned within the context of existing literature and theories, particularly focusing on anomaly-based detection in IoT environments. A comparative analysis with prior works reveals noteworthy distinctions and contributions. Existing studies, as surveyed, have primarily delved into the challenges of securing IoT networks, emphasizing the need for robust intrusion detection mechanisms. Traditional methods often employ anomaly-based or signature-based detection. The former captures deviations from normal patterns, while the latter relies on known attack signatures. However, both approaches have limitations, especially in dynamic IoT environments. In comparison, the proposed scheme incorporates a Convolutional Neural Network (CNN) model trained on benchmark datasets like NID and BoT-IoT. Achieving an impressive accuracy of 99.51% on NID and 95.55% on BoT-IoT, it outperforms many traditional methods. CNN's ability to automatically learn hierarchical features from data proves advantageous in capturing intricate patterns within IoT traffic, enhancing the model's effectiveness. Moreover, the research discusses the limitations and

suggests potential improvements by varying epochs, batch sizes, and parameters. This self-awareness contributes to the scholarly discourse, acknowledging that further optimization is plausible, and the proposed model's efficacy can be refined. The integration of deep learning, specifically CNNs, aligns with contemporary trends in machine learning applications for intrusion detection[26]. By leveraging publicly available datasets, the research ensures reproducibility and comparability with other studies. The emphasis on benchmark datasets and standard metrics fosters a basis for objective evaluation, allowing future researchers to benchmark their work against this study.

Discussion

Interpretation of Results: The interpretation of results collectively signifies a substantial contribution to cybersecurity knowledge and practices. The understanding of TTPs enriches the comprehension of attacker behaviors, laying the groundwork for targeted defenses. The integration of subtle indicators into intrusion detection strategies reflects an adaptive and forward-looking approach. Additionally, the proposed evaluation framework empowers organizations to systematically assess and augment their security measures[27]. These implications resonate not only with the posed research questions but also with the broader goal of advancing cybersecurity resilience in contemporary contexts.

1. TTPs Analysis and Attacker Behavior: The investigation into pervasive Tactics, Techniques, and Procedures (TTPs) utilized by attackers yielded insightful findings. By dissecting these TTPs, the research uncovered nuanced aspects of attacker behavior. The results shed light on the intricacies of how attackers navigate networks, offering a comprehensive understanding of their modus operandi. This aligns with the first research question, providing a foundational knowledge base for enhancing cybersecurity strategies.

2. Leveraging Subtle Indicators for Advanced Detection: The research successfully addressed the challenge of recognizing unpretentious signs of malicious activities. By harnessing subtle and contemporary indicators, the developed intrusion detection strategies showcased adaptability to emerging threats. The findings not only responded to the second research question but also pointed towards a proactive approach in cybersecurity. This demonstrated the feasibility of incorporating real-time, nuanced indicators into the development and execution of advanced intrusion detection systems.

3. Evaluation of Organizational Security Measures: In evaluating the effectiveness of current organizational security efforts, the research established a robust framework for assessment. The results provided a systematic approach to

gauge the adequacy of existing security measures. By proposing metrics and methodologies, the research responded directly to the third research question[28]. The implications of these findings extend to practical applications, guiding organizations in enhancing their security postures based on empirical evaluations.

Implications for Cybersecurity Practices: The implications of these findings extend beyond immediate application, guiding the formulation of future cybersecurity strategies. The tactical insights, proactive detection methodologies, and evaluation frameworks contribute to a holistic approach to cybersecurity practices. By aligning strategies with observed attacker behaviors, organizations can better anticipate, prevent, and respond to cyber threats, ultimately elevating their overall cybersecurity resilience. These implications position the research as a valuable resource for shaping the future landscape of cybersecurity practices.

1. Tactical Defenses Informed by TTPs: The findings hold significant implications for shaping tactical defenses in the realm of cybersecurity. A nuanced understanding of Tactics, Techniques, and Procedures (TTPs) employed by attackers provides a roadmap for developing targeted defense strategies. Cybersecurity practitioners can leverage these insights to fortify networks against specific threat vectors. By tailoring defenses to the observed TTPs, organizations enhance their capacity to thwart sophisticated attacks effectively.

2. Proactive and Adaptive Intrusion Detection: The research outcomes underscore the need for a proactive and adaptive approach to intrusion detection. Incorporating subtle indicators of malicious activities into detection mechanisms allows for real-time response to evolving threats. Cybersecurity practices should shift from reactive models to those capable of identifying emerging risks promptly[29]. Integrating these findings into intrusion detection systems ensures organizations stay ahead of adversaries, fostering a more resilient security posture.

3. Systematic Evaluation of Security Measures: The proposed framework for evaluating organizational security measures introduces a systematic and comprehensive methodology. This has direct implications for cybersecurity practices, offering a structured way to assess the effectiveness of existing security protocols. Organizations can utilize this framework as a benchmarking tool, enabling them to identify strengths, weaknesses, and areas for improvement in their security postures. Continuous and informed evaluations are critical for adapting security practices to the dynamic threat landscape.

Recommendations for Enhancing Network Security: The strategic adoption of these recommendations ensures a proactive, adaptive, and TTP-focused approach to network security. By implementing these measures, organizations fortify their

defenses, cultivate a security-aware culture, and remain resilient in the face of evolving cyber threats. These recommendations collectively contribute to a holistic and effective network security strategy.

1. TTP-Centric Security Measures: In light of the identified Tactics, Techniques, and Procedures (TTPs), a key recommendation is the development and implementation of TTP-centric security measures. Organizations should align their defense strategies with the observed TTPs, creating a robust and targeted security posture. This involves continuous monitoring and analysis to stay abreast of evolving TTPs, enabling security teams to adapt defenses dynamically.

2. Integration of Behavioral Anomalies: Building on the findings related to subtle indicators of malicious activities, there is a recommendation to integrate behavioral anomalies into existing security frameworks. This entails leveraging machine learning and AI-driven solutions to detect deviations from normal network behavior. By incorporating these indicators, organizations can enhance their intrusion detection capabilities, identifying potential threats at early stages.

3. Continuous Security Awareness Training: Given the evolving nature of cyber threats, there is a recommendation for continuous security awareness training for personnel. This involves educating employees about the latest TTPs, common attack vectors, and recognizing subtle signs of malicious activities[30]. An informed workforce serves as an additional layer of defense, contributing to the overall resilience of the network.

4. Regular Red Team Exercises: To validate the efficacy of security measures, organizations are recommended to conduct regular red team exercises. These simulated attacks, based on identified TTPs, help assess the readiness of existing defenses. Red teaming provides valuable insights into potential vulnerabilities and areas for improvement, allowing organizations to fine-tune their security strategies.

5. Adaptive Incident Response Plans: The research underscores the need for adaptive incident response plans tailored to specific TTPs. Organizations should revisit and enhance their incident response protocols, considering the nuanced behaviors of attackers. This involves crafting response strategies that align with observed TTPs, ensuring a swift and effective response to security incidents.

6. Periodic Security Audits with the Evaluation Framework: To systematically evaluate and enhance security measures, organizations are recommended to conduct periodic security audits. The evaluation framework proposed in the research serves as a valuable tool for comprehensive assessments[31]. By applying

this framework, organizations can identify areas of strength and weakness in their security postures, guiding targeted improvements.

Conclusion

Summary of Key Findings of This Research: This research not only advances our understanding of attacker behaviors but also charts a course for practical implementation in the realm of cybersecurity. As the cyber threat landscape evolves, future research endeavors must align with a proactive and adaptive approach, consistently pushing the boundaries of knowledge to safeguard digital environments. This research delved into pervasive Tactics, Techniques, and Procedures (TTPs) employed by attackers in network environments, shedding light on their nuanced behaviors. The study successfully identified subtle indicators of malicious activities, emphasizing the need for an advanced intrusion detection paradigm. Noteworthy findings include the prevalence of specific TTPs, the significance of behavioural anomalies, and the effectiveness of an evaluation framework for security measures.

Contribution to the Field of Cybersecurity: The primary contribution of this research lies in its comprehensive exploration of attacker behaviors and the subsequent recommendations for enhancing network security. By uncovering TTPs and advocating for TTP-centric security measures, the study provides actionable insights for organizations aiming to bolster their defenses. The integration of behavioral anomalies and the proposed evaluation framework offer practical approaches to fortify intrusion detection capabilities. The research thus contributes a nuanced understanding of cyber threats and pragmatic strategies for cybersecurity practitioners. The emphasis on continuous security awareness, red team exercises, and adaptive incident response plans adds a practical dimension to organizational cybersecurity resilience. The research serves as a valuable resource for security professionals, offering a strategic roadmap to counter evolving cyber threats effectively.

Suggestions for Future Research: In envisioning future research endeavors, it is imperative to delve deeper into the dynamic landscape of TTPs. Continuous monitoring and analysis of emerging tactics will further refine TTP-centric security measures, ensuring an adaptive defense against evolving threats. Exploring the integration of artificial intelligence and machine learning in behavioral anomaly detection could unlock new dimensions in threat identification.

Future research may also focus on the human element in cybersecurity, investigating the role of personnel in recognizing and responding to subtle

indicators. This involves exploring innovative approaches to security awareness training and evaluating their impact on an organization's overall security posture.The refinement and expansion of the proposed evaluation framework present avenues for continued research. Additional metrics and indicators could be incorporated, providing a more comprehensive tool for organizations to assess their security postures effectively.

References

[1] Ma, Z., Liu, L. and Meng, W., 2020. Towards multiple-mix-attack detection via consensus-based trust management in IoT networks. *Computers & Security*, *96*, p.101898.

[2] Muñoz-González, L., Sgandurra, D., Barrère, M. and Lupu, E.C., 2017. Exact inference techniques for the analysis of Bayesian attack graphs. *IEEE Transactions on Dependable and Secure Computing*, *16*(2), pp.231-244.

[3] Doynikova, E., Novikova, E. and Kotenko, I., 2020. Attacker behaviour forecasting using methods of intelligent data analysis: A comparative review and prospects. *Information*, *11*(3), p.168.

[4] Gai, F., Wang, B., Deng, W. and Peng, W., 2018. Proof of reputation: A reputation-based consensus protocol for peer-to-peer network. In *Database Systems for Advanced Applications: 23rd International Conference, DASFAA 2018, Gold Coast, QLD, Australia, May 21-24, 2018, Proceedings, Part II 23* (pp. 666-681). Springer International Publishing.

[5] Nisioti, A., Mylonas, A., Yoo, P.D. and Katos, V., 2018. From intrusion detection to attacker attribution: A comprehensive survey of unsupervised methods. *IEEE Communications Surveys & Tutorials*, *20*(4), pp.3369-3388.

[6] Huang, X., Kroening, D., Ruan, W., Sharp, J., Sun, Y., Thamo, E., Wu, M. and Yi, X., 2020. A survey of safety and trustworthiness of deep neural networks: Verification, testing, adversarial attack and defence, and interpretability. *Computer Science Review*, *37*, p.100270.

[7] He, Y., Han, G., Jiang, J., Wang, H. and Martinez-Garcia, M., 2020. A trust update mechanism based on reinforcement learning in underwater acoustic sensor networks. *IEEE Transactions on Mobile Computing*, *21*(3), pp.811-821.

[8] Ghanem, K., Aparicio-Navarro, F.J., Kyriakopoulos, K.G., Lambotharan, S. and Chambers, J.A., 2017, December. Support vector machine for network intrusion and cyber-attack detection. In *2017 sensor signal processing for defence conference (SSPD)* (pp. 1-5). IEEE.

[9] Alabdan, R., 2020. Phishing attacks survey: Types, vectors, and technical approaches. *Future internet*, *12*(10), p.168.

[10] Pineda, A.N.A., Soler, R., Pastor, V., Li, Y. and Dicke, M., 2017. Plant-mediated species networks: the modulating role of herbivore density. *Ecological Entomology*, *42*(4), pp.449-457.

[11] Aslan, Ö.A. and Samet, R., 2020. A comprehensive review on malware detection approaches. *IEEE access*, *8*, pp.6249-6271.

[12] Alenezi, M.N., Alabdulrazzaq, H., Alshaher, A.A. and Alkharang, M.M., 2020. Evolution of malware threats and techniques: A review. *International journal of communication networks and information security*, *12*(3), pp.326-337.

[13] Ullah, F., Edwards, M., Ramdhany, R., Chitchyan, R., Babar, M.A. and Rashid, A., 2018. Data exfiltration: A review of external attack vectors and countermeasures. *Journal of Network and Computer Applications*, *101*, pp.18-54.

[14] Huang, K., Yang, L.X., Yang, X., Xiang, Y. and Tang, Y.Y., 2020. A low-cost distributed denial-of-service attack architecture. *IEEE Access*, *8*, pp.42111-42119.

[15] Baldwin, A., Gheyas, I., Ioannidis, C., Pym, D. and Williams, J., 2017. Contagion in cyber security attacks. *Journal of the Operational Research Society*, *68*(7), pp.780-791.

[16] Javeed, D., MohammedBadamasi, U., Ndubuisi, C.O., Soomro, F. and Asif, M., 2020. Man in the middle attacks: Analysis, motivation and prevention. *International Journal of Computer Networks and Communications Security*, *8*(7), pp.52-58.

[17] Yan, G., Li, Q., Guo, D. and Meng, X., 2020. Discovering suspicious APT behaviors by analyzing DNS activities. *Sensors*, *20*(3), p.731.

[18] Bhushan, K. and Gupta, B.B., 2018. Hypothesis test for low-rate DDoS attack detection in cloud computing environment. *Procedia computer science*, *132*, pp.947-955.

[19] Zaminkar, M. and Fotohi, R., 2020. SoS-RPL: securing internet of things against sinkhole attack using RPL protocol-based node rating and ranking mechanism. *Wireless Personal Communications*, *114*(2), pp.1287-1312.

[20] Hu, Z., Odarchenko, R., Gnatyuk, S., Zaliskyi, M., Chaplits, A., Bondar, S. and Borovik, V., 2020. Statistical Techniques for Detecting Cyberattacks on

Computer Networks Based on an Analysis of Abnormal Traffic Behavior. *International Journal of Computer Network & Information Security*, *12*(6).

[21] Li, S.N., Yang, Z. and Tessone, C.J., 2020, August. Proof-of-work cryptocurrency mining: a statistical approach to fairness. In *2020 IEEE/CIC international conference on communications in China (ICCC workshops)* (pp. 156-161). IEEE.

[22] Sun, C.C., Cardenas, D.J.S., Hahn, A. and Liu, C.C., 2020. Intrusion detection for cybersecurity of smart meters. *IEEE Transactions on Smart Grid*, *12*(1), pp.612-622.

[23] Ma, Z., Liu, L. and Meng, W., 2020. Towards multiple-mix-attack detection via consensus-based trust management in IoT networks. *Computers & Security*, *96*, p.101898.

[24] Sperl, P., Kao, C.Y., Chen, P., Lei, X. and Böttinger, K., 2020, September. DLA: dense-layer-analysis for adversarial example detection. In *2020 IEEE European Symposium on Security and Privacy (EuroS&P)* (pp. 198-215). IEEE.

[25] Tseng, E., Bellini, R., McDonald, N., Danos, M., Greenstadt, R., McCoy, D., Dell, N. and Ristenpart, T., 2020. The tools and tactics used in intimate partner surveillance: An analysis of online infidelity forums. In *29th USENIX security symposium (USENIX Security 20)* (pp. 1893-1909).

[26] Osanaiye, O.A., Alfa, A.S. and Hancke, G.P., 2018. Denial of service defence for resource availability in wireless sensor networks. *IEEE Access*, *6*, pp.6975-7004.

[27] Baza, M., Nabil, M., Mahmoud, M.M., Bewermeier, N., Fidan, K., Alasmary, W. and Abdallah, M., 2020. Detecting sybil attacks using proofs of work and location in vanets. *IEEE Transactions on Dependable and Secure Computing*, *19*(1), pp.39-53.

[28] Benzaïd, C. and Taleb, T., 2020. AI for beyond 5G networks: a cyber-security defense or offense enabler?.*IEEE network*, *34*(6), pp.140-147.

[29] Hossain, M.N., Sheikhi, S. and Sekar, R., 2020, May. Combating dependence explosion in forensic analysis using alternative tag propagation semantics. In *2020 IEEE Symposium on Security and Privacy (SP)* (pp. 1139-1155). IEEE.

[30] Doynikova, E., Novikova, E. and Kotenko, I., 2020. Attacker behaviour forecasting using methods of intelligent data analysis: A comparative review and prospects. *Information*, *11*(3), p.168.

[31] Al-Khater, W.A., Al-Maadeed, S., Ahmed, A.A., Sadiq, A.S. and Khan, M.K., 2020. Comprehensive review of cybercrime detection techniques. *IEEE Access*, *8*, pp.137293-137311.

[32] Alabdan, R., 2020. Phishing attacks survey: Types, vectors, and technical approaches. *Future internet*, *12*(10), p.168