2025

ANALYSIS OF SIEM SYSTEM AND ITS APPLICATION FOR CAMPUS NETWORK INFRASTRUCTURE USING DEEP LEARNING APPROACH

Zoha Irfan and Prof. Dr. Sohail Asghar

ABSTRACT

This thesis investigates enhancing Security Information and Event Management (SIEM) systems by integrating deep learning for advanced anomaly detection in campus networks. Traditional SIEM tools like Wazuh rely on static rules, resulting in high false positives and limited adaptability. A hybrid framework was developed combining Suricata for packet inspection, Wazuh for centralized monitoring, and deep learning models including Deep Embedded Clustering (DEC), LSTM, and CNN for intelligent threat detection. Logs from IoT-23 datasets allowed detection of cyberattacks such as botnets and DoS. LSTM achieved the highest detection accuracy, while DEC effectively identified unknown threats. A VMware virtual testbed validated real-time detection and alerting, showing improved precision and lower false positives compared to rule-based methods. This research provides a scalable, adaptive, and proactive cybersecurity solution for academic networks and lays the foundation for intelligent SIEM systems capable of responding to modern threats.

Keywords: SIEM, Machine Learning, Deep Learning, Cybersecurity, LSTM, DEC, Network Security, IoT, Anomaly Detection, Campus Networks.

MALWARE DETECTION FOR CLOUD ENVIRONMENT: USING SHALLOW CONVOLUTIONAL NEURAL NETWORK

Khaliq ur Rehman and Dr. Danish Mehmood

ABSTRACT

As cloud computing becomes integral to IT, cyber threats targeting cloud systems have grown increasingly sophisticated. Traditional signature-based malware detection struggles against novel, mutating, or evasive threats. This study designs a shallow Convolutional Neural Network (CNN) for fast, reliable, and cost-effective malware detection in cloud environments. Testing on Malimg, Microsoft BIG 2015, and Malevis datasets against AlexNet and ResNet-50 demonstrated the shallow CNN's high performance, achieving results nearly as effective as deeper networks while being 30% faster and occupying only 10 MB. Its lightweight design allows real-time threat detection on resource-constrained cloud and edge devices without manual feature engineering. By overcoming computational bottlenecks and ensuring scalability, this shallow CNN offers an efficient solution for cloud and edge security, supporting rapid identification of emerging malware threats.

Keywords: Cloud Security, Malware Detection, CNN, Shallow Neural Network, Real-Time Detection, Edge Computing, Lightweight Model, Cybersecurity, EDR, Scalability.

ANOMALY DETECTION IN UNMANNED AERIAL VESICLES THROUGH MACHINE LEARNING

Talat Hussain Hashmi and Dr. Shahzad Latif

ABSTRACT

Unmanned Aerial Vehicles (UAVs) are increasingly used in surveillance, disaster response, and agriculture, yet remain vulnerable to GPS spoofing attacks that mislead navigation and compromise mission safety. This thesis presents a machine learning-based framework for GPS spoofing detection, designed for real-time deployment in resource-constrained UAV environments. Seven supervised learning models, including Random Forest, Logistic Regression, K-Nearest Neighbors, SVM, Decision Tree, Multi-Layer Perceptron, and Naive Bayes, were benchmarked using a Group K-Fold protocol. Physics-informed feature engineering, including delta-based positional metrics and composite speed, improved detection by capturing motion inconsistencies indicative of spoofing. Results showed Random Forest achieved 100% detection rate and zero false alarm rate with sub-millisecond inference. Lightweight classifiers validated rapid, accurate prediction, outperforming previous benchmarks. Limitations include dataset homogeneity, CPU-only testing, and lack of explainability analysis. Future work should expand cross-dataset validation, explore temporal and ensemble architectures, and integrate explainable AI. This study advances UAV cybersecurity with a robust, efficient, and deployment-ready detection framework.

Keywords: UAV, GPS Spoofing, Machine Learning, Random Forest, Logistic Regression, Cybersecurity, Real-Time Detection, Feature Engineering, Lightweight Models.

2025

NEXT-GENERATION DEEP FAKE DETECTION: HYBRIDIZING DEEP LEARNING AND ERROR LEAVE ANALYSIS

Muhammad Faraz Asghar and Dr. Danish Mahmood

ASTRACT

As modern technologies have taken shape to produce multiple fake contents; audios, images and videos. The proliferation of these contents has created a serious concern for the law enforcement agencies due to their perception management capability. In this study we have explored one of the important components of these fake contents; the fake images. These images can be broadly categorized into two categories; such as tempered images and deep fake images. Since 2007 Error Level Analysis (ELA) has been used for image forensic by DF experts, however this technique can only detect tempered images. Furthermore; it requires to be integrated with other techniques for better results. In this research we have proposed a hybrid framework with the integration of ELA and deep learning models to detect both tempered and deepfake images. Moreover; the study has developed a new dataset for experiment purposes. The proposed framework and dataset have been tested with multiple deep learning models (EfficientNetB0, DenseNet201, ResNet152 and InceptionV3) for performance analysis in image classification. At the end of the study; the results have been compared with the State of the Art (SOTA) techniques in which EfficientNetB0 remained standoff with training and testing accuracy of 98.85% and 98.69% respectively.

Keywords: Fake images, Tempered images, Deepfake images, Error level analysis, Machine learning, Deep learning, Artificial intelligence

A LIGHTWEIGHT AUTHENTICATION MECHANISM FOR CLOUD ASSISTANT IOT

Sadaf Rasheed and Dr. Danish Mehmood

ABSTRACT

In the evolving landscape of the Internet of Things (IoT), the integration of cloud services has significantly enhanced functionality but also introduced substantial security challenges. Traditional cryptographic authentication methods, although robust, often lack efficiency in resource-constrained IoT ecosystems, creating a crucial need for adaptive and scalable solutions. To overcome these limitations, this research introduces a hybrid authentication model that synergistically combines Identity-Based Encryption (IBE) with Elliptic Curve Cryptography (ECC) using the BN254 curve and session tokens. This approach enables secure, efficient, and scalable authentication by leveraging cloud resources to offload computationally intensive cryptographic operations, thereby reducing the processing burden on IoT devices. The research methodology encompasses theoretical analysis, prototype development, and empirical evaluation. A realistic simulation environment using Docker containers emulated heterogeneous IoT device capabilities and interactions with cloud servers. Performance evaluations demonstrated improvements in authentication latency, resource efficiency, and scalability compared to existing solutions. Security assessments using formal verification tools confirmed the model's robustness against threats such as replay attacks, man-in-the-middle attacks, and insider threats. This study contributes to cybersecurity literature by providing a practical, efficient, and secure authentication solution tailored for cloud-assisted IoT (CAIoT) environments. Future directions include enhancing cryptographic strength with advanced elliptic curves and expanding applicability to dynamic IoT networks.

Keywords: IoT Authentication, Cloud-Assisted IoT, Identity-Based Encryption, Elliptic Curve Cryptography, Lightweight Cryptography, Cybersecurity.

2024

SIMULATION AND ANALYSIS PF CYBER THREATS IN BLOCK CHAIN WITH POSSIBLE MEASURES AND MITIGATIONS

Syed Noman Ali Jaffri and Dr. Ahsan Abdullah

ASTRACT

Blockchain technology, (decentralized and immutable architecture), has become a cornerstone in various industries, yet its ecosystem remains susceptible to evolving cyber threats [1]. This thesis addresses the security gaps within blockchain platforms, smart contracts, decentralized applications, and ecosystem integrations by simulating and analyzing prevalent cyberattacks. Focusing on Denial of Service, Distributed Denial of Service, Man-in-the-Middle (MitM), and Sybil attacks, the study employs penetration testing tools such as Metasploit and Bettercap to replicate real-world attack scenarios in controlled environments. The simulations reveal significant vulnerabilities, DoS/DDoS attacks disrupt network operations (resource exhaustion), MitM attacks compromise transactional integrity via traffic interception and Sybil attacks undermine consensus mechanisms through fraudulent node proliferation. To counter these threats, tailored mitigation strategies are proposed, including network slicing, traffic filtering using ACLs, bandwidth throttling, cryptographic enhancements, and consensus algorithm refinements like Proof-of-Stake and reputation-based systems [2]. Key contributions include a holistic vulnerability assessment across blockchain modules, validated through testing, and the development of a decentralized DDoS mitigation framework leveraging verifiable delay functions (VDFs). The findings underscore the necessity of integrating blockchain-specific security measures with traditional protocols to enhance resilience against sophisticated threats. Future work will simulate 51% attacks, integrate AI for threat detection, address quantum crypto scalability, and explore ethical-legal frameworks balancing security and compliance in decentralized systems.

Keywords: Blockchain, Vulnerabilities, DoS, DDoS, MitM, Sybil Attacks, Consensus Protocols, AI Integration, Quantum Cryptography.

2024

DETECTION OF INTRUSION ATTACKS IN CAN BUS OF ELECTRIC VEHICLES USING COMPUTATIONAL INTELLIGENCE

Ahsan Ullah and Dr. Shahzad Latif

ASTRACT

The CAN (Controller Area Network) bus, is the most popular protocol used in automobile networks. But the in-vehicle CAN bus is vulnerable to major network security threats because it lacks network security protections. Nevertheless, The majority of intruder detection techniques cannot be implemented in the in-vehicle network system due to the resourceconstrained ECUs. This study proposes an enhanced intrusion detection model to identify attacks on the Controller Area Network (CAN) in autonomous cars. The ADAM optimizer was meticulously fine-tuned to optimize the LSTM model's learning process, enhancing its ability to detect subtle anomalies that indicate malicious activity. By strategically combining LSTM and ADAM, the proposed hybrid model showcases robust capabilities, achieving remarkable detection rates across various attack scenarios. The results of the study demonstrate the exceptional efficacy of the proposed hybrid LSTMADAM model. Notably, the model achieved a remarkable 99% accuracy for both replay and diagnostic attacks highlighting its capacity to effectively identify intrusions that target vehicle diagnostic and communication systems. Furthermore, the model achieved a 97% accuracy against fuzzingh and DoS attacks, demonstrating its robust performance across a spectrum of attack types. These findings underscore the potential of our approach to significantly bolster CAN bus security, offering a reliable and efficient solution for enhancing the cyber resilience of autonomous vehicles against a wide range of cyber threats in the increasingly connected automotive landscape. This research contributes a practical, high-performance IDS that can be deployed within the resource-limited automotive environment, directly addressing the growing security concerns surrounding modern vehicle networks.

Keywords: Controller Area Network bus, Electronic Control Units, Intrusion detection system, Cyber-Physical Systems

2024

SECURING SMART BUILDINGS: UTILIZING HONEYPOTS FOR CYBER DECEPTION AND THREAT ANALYSIS

Muhammad Husnain and Dr. Danish Mehmood

ASTRACT

The smart building concept is increasingly popular for enhancing convenience and efficiency, but it faces significant cybersecurity threats, including unauthorized access, malware, and DDoS attacks. The proliferation of IoT devices has created an expansive attack surface due to their inherent vulnerabilities, such as limited computing resources, poor security designs, and flawed configurations. These weaknesses expose smart buildings to potential exploitation, risking operational integrity and user privacy. Honeypots and honeynets offer a promising solution by providing detailed insight into attacker behaviors, deflecting threats, and enabling real-time analysis of cyberattacks. Honeypots and honeynets are powerful tools for protecting assets within a network as they offer valuable insights into adversary behavior by diverting the attention of potential attackers and siphoning off their resources. However, the cybersecurity threat landscape constantly evolves, and professional attackers are always working to uncover and bypass honeypots. Once an adversary successfully identifies a deception mechanism in place, they may change their tactics, leave the target or potentially cause significant harm to the network. This study presents a customized honeypot framework specifically designed for smart buildings, incorporating deception capabilities to address challenges like honeypot detectability and attack evasion. Results from experimental deployments showed the framework's effectiveness in attracting a diverse range of cyberattacks, including brute force, reconnaissance, and exploitation of critical vulnerabilities. Detailed analysis of the collected data revealed prevalent attack vectors, the use of sophisticated malware payloads, and exploitation patterns targeting smart building infrastructure. By analyzing attacker tactics, techniques, and procedures (TTPs), the research provides a foundation for proactive threat mitigation strategies tailored to the evolving cybersecurity landscape of smart buildings.

Keywords: IoT, Smart Buildings, IOT Threat Landscape, Cyber Attack, Cyber Deception, Honeypot

2024

ENERGY-EFFICIENT INTRUSION DETECTION ALGORITHM FOR RESOURCE CONSTRAINED DEVICES

Hamza Javed and Dr. Shahzad Latif

ASTRACT

Internet of Things (IoT) technologies, pivotal in today's interconnected devices, face significant challenges including high energy consumption and security vulnerabilities. These issues, stemming from constraints like limited battery power and processing capabilities, expose IoT devices to cyber threats. In response, this research explores the development of energy-efficient Intrusion Detection Systems (IDS) tailored for IoT devices, using Federated Learning (FL) to enhance data privacy and detection accuracy. FL permits multiple devices to collaboratively train models without sharing raw data, thus bolstering security and privacy. Our study introduces the Whale Optimization Algorithm (WOA) as a novel method to minimize resource consumption and computational costs. By integrating WOA with FL, the proposed IDS achieves a substantial improvement in energy efficiency while ensuring robust intrusion detection. This hybrid approach not only preserves data privacy but also enhances the accuracy of detecting IoT threats, supporting the dual goals of security and sustainability in IoT networks. Experimental results reveal that the combination of XGBoost and Federated Learning optimized with WOA outperformed traditional methods, achieving an accuracy of 99.17% and an F1-score of 0.9143. The energy efficiency of our model was significantly higher compared to other models tested, such as those using simple XGBoost or standard Federated Learning approaches. The optimized model demonstrated its ability to reduce operational costs and carbon emissions effectively, making it a compelling solution for energy-sensitive IoT environments. In summary, the proposed model addresses the critical needs of IoT security and energy efficiency. It stands out by leveraging advanced optimization techniques to refine model performance, proving highly effective in real-world scenarios where resource conservation and data security are paramount. This approach sets a new benchmark for developing sustainable and secure IoT systems, indicating a promising direction for future research in IoT cybersecurity.

Keywords: Intrusion Detection Systems (IDS), Internet of Things (IoT), Federated Learning (FL). Whale Optimization Algorithm (WOA)

2024

DETECTING ADVANCE PERSISTENT THREATS USING SIEM AND MACHINE LEARNING BASED USER AND ENTITY BEHAVIOR ANALYTICS

Syed Humza Sajjad and Dr. Sohail Asghar

ASTRACT

Advanced Persistent Threats (APTs) pose a significant challenge to modern cybersecurity due to their stealthy, adaptive, and prolonged nature, often evading traditional security mechanisms and leading to delayed detection and response. This research presents a novel approach that integrates Security Information and Event Management (SIEM) with Machine Learning-based User and Entity Behavior Analytics (UEBA) to enhance the detection of APTs by analyzing deviations in behavioral patterns. The proposed model aims to effectively distinguish between legitimate and malicious activities, thereby addressing the limitations of conventional methods that suffer from high false positive and false negative rates. The model is evaluated using two widely recognized datasets, NSL-KDD and CTU-13, which represent diverse network attack scenarios. Experimental results demonstrate that the proposed approach achieves high detec- tion performance, with the model reaching an accuracy of 97.5%, precision of 96.3%, recall of 97.2%, and F1-score of 96.75% on the NSL-KDD dataset, and an accuracy of 96.1%, precision of 94.4%, recall of 95.3%, and F1-score of 94.85% on the CTU-13 dataset. These results indi- cate a significant reduction in false alerts and improved reliability in threat identification. The outcomes of this study highlight the potential of combining SIEM and machine learning-based UEBA as an effective strategy for detecting APTs, contributing to the development of more intelligent and adaptive cybersecurity defense systems.

Keywords: Advance Persistent Threats, UEBA, SIEM, Machine Learning, Isolation Forest, Random Forest

2024

DETECT RUMORS ON TWITTER BY PROMOTING PAKISTAN'S ELECTION 2024 CAMPAIGN WITH GENERATIVE AI LEARNING

Asma Yasmeen and Dr. Sohail Asghar

ABSTRACT

The increasing spread of misinformation and rumors on social media platforms poses a significant challenge, particularly in politically sensitive environments such as election campaigns. This thesis explores the integration of Generative Adversarial Networks (GANs) and Recurrent Neural Networks (RNNs) to develop a robust rumor detection framework for Pakistan's Election 2024 campaign on Twitter. By leveraging GAN-based adversarial training, the proposed model enhances the ability to distinguish between factual content and misleading narratives, adapting to the dynamic nature of social media discussions. The research introduces a dual-network architecture, where the GAN's generator produces adversarial misinformation samples, while the RNN-based discriminator learns to classify real and fake content more effectively over time. This self-improving model refines misinformation detection by continuously learning from evolving rumor patterns. The study evaluates multiple machine learning techniques, incorporating text-based sentiment analysis, social engagement features, and linguistic markers to improve classification accuracy. Challenges such as data scarcity, high-dimensional feature extraction, and adversarial misinformation tactics are addressed through semi-supervised learning approaches and domain-specific dataset augmentation. Experimental results demonstrate that the GAN-RNN model achieves 90% accuracy, 91% precision, and 89% F1-score, outperforming state-of-the-art methods such as BERT (88% accuracy) and SVM (82% accuracy). The framework's ability to capture temporal dynamics and multilingual nuances enables real-time detection of adversarial misinformation, reducing false positives by 37% in politically charged contexts. Future work will focus on integrating transformer-based embeddings to enhance semantic granularity, expanding multilingual support for Urdu-English code-switched content, and deploying the framework for global election monitoring. These advancements aim to strengthen real-time adaptability while addressing ethical concerns such as algorithmic bias and transparency.

Keywords: Rumor Detection, Generative Adversarial Networks (GANs), Recurrent Neural Networks (RNNs), Misinformation, Social Media Analysis, Pakistan Election 2024, Cybersecurity, Natural Language Processing (NLP).

2024

ADDRESSING POTENTIAL FALSE POSITIVE AND FALSE NEGATIVE RATES IN ML-POWERED UEBA SYSTEM

Irfan Nazir and Dr. Sohail Asghar

ABSTRACT

In the modern digital era, securing sensitive systems against cyber threats is essential. This thesis addresses a key limitation in current machine learning-powered User and Entity Behavior Analytics (UEBA) systems the high rate of false positives (FP) and false negatives (FN), which weakens threat detection and incident response efficiency. The objective of this research is to develop a hybrid model combining Random Forest (RF) and Support Vector Machine (SVM) algorithms, integrated with anomaly detection techniques, to enhance detection accuracy and reduce misclassification in cybersecurity alerts. For evaluation, the KDD dataset was used. After thorough preprocessing and feature extraction, the hybrid model was implemented and tested. The proposed approach achieved an accuracy of 99.14%, precision of 98.97%, recall of 98.56%, and an F1-score of 98.76%. These results indicate a significant reduction in false alerts compared to traditional models, demonstrating improved reliability and efficiency. The findings highlight that the integration of ensemble learning with anomaly-based detection not only boosts the accuracy of UEBA systems but also supports timely and intelligent decision-making in security operations. This contributes to reducing alert fatigue, improving response prioritization, and strengthening overall network defense. Furthermore, the system was tested in a simulated environment that mimics real-world traffic, verifying its capability in practical scenarios. The proposed model can be extended for integration with SIEM and XDR platforms to automate alert handling. Future work will explore deep learning models for even higher adaptability and precision in dynamic threat landscapes.

Keywords: UEBA, Machine Learning, False Positives, False Negatives, Anomaly Detection.

2024

SECURE BILLING IN SMART GRID USING BLOCKCHAIN

Mueed Gul Durrani and Dr. Danish Mehmood

ABSTRACT

Electricity Service Providers (ESP) can utilize a consortium block chain to create a new billing system for Smart Grid (SG), a complex electricity network that oversees electricity generation, distribution, transmission, and consumption. The goal of the SG is to decrease costs, increase efficiency and transparency through control, analysis, communication, and observation. To provide optimal billing with lower computational expense, a novel blockchain-based billing mechanism can be put in place. This research underscores the importance of verifiable billing, where both consumers and presumes can calculate the cost of electricity and ensure accuracy using both ends of the service. For energy transactions, a blockchain-based security framework is explored in the research that also delves into the privacy and security of smart meter communication. To improve security, efficiency, and cost-effectiveness for both electricity consumers and producers, the implementation of Proof of Authority (PoA) consensus algorithm in the consortium blockchain is proposed. By doing so, low gas fees can be achieved and scalability can be enhanced, which will aid in the development and growth of the SG. This study is valuable in contributing to the progression of the SG.

Keywords: Smart Grid, Consortium Blockchain, Proof of Authority, Proof of Work, Eliptic Curve Cryptography.

2024

CYBER SECURITY OF CC TLDS OF PAKISTAN-ISSUE AND WAY FORWARD

Syed Junaid Imam and Dr.Danish Mehmood

ABSTRACT

Country Code Top-Level Domains (ccTLDs) are important/critical national data resources associated with Internet governance. Therefore, it is of paramount importance that all stakeholder stake the appropriate measures to ensure the cyber security of Pakistan's ccTLDs, i.e. .pk and Internationalized Domain Names (IDN). The purpose of the thesis is to evaluate existing arrangements/measures taken by stakeholders in this regard and propose remedial measures/improvements required for the secure operation of ccTLDs in Pakistan. However, before discussing/analyzing the measures it is essential to understand the history of the evolution of DNS; the roles and responsibilities of various stakeholders including IANA, RFC 1591-1994, Internet Corporation for Assigned Names Numbers (ICANN), Registry Operators, Registrants, Registrars, Domain Name System (DNS) Root Zone/Servers, Country Code Name Supporting Organization (ccNSO), Government Advisory Committee (GAC), Internet Community, and exhibit the basic building block required for Bottom-Up consensus-driven approach. In addition, it is important to understand that the accurate working of the Internet is seriously reliant on DNS Security (DNSSEC), using public key cryptography and digital signatures i.e. DNSSEC strengthens Data origin authentication and Data integrity protection.DNSSEC is not automatically enabled: it needs to be precisely empowered and configured at recursive resolvers by respective network operators as well as by TLDs (ccTLDs) owners at the zone's authoritative servers. The thesis has identified that it is of paramount importance for the Government to get involved in the technical and administrative management of sublevel domain names that Pakistanis mostly own. In the case of ".pk": 1) DNSSEC has not been deployed so far, which poses serious vulnerabilities for exploiting the most common threats like DNS Spoofing /Cache Poisoning. 2) All the personal data, used for registration of domain names under .pk are being kept outside the country subject to be regulated under the local laws of that country (instead of Pakistan) including privacy and access rights e.g. xiii LIST OF TABLES General Data Protection Regulations (GDPR). Moreover, After the stewardship transition of Internet Assigned Numbers Authority (IANA) functions to ICANN, it has also become imperative for the governments to get their right share in policy development and decision-making process at ICANN through effective and meaningful participation for providing secure and efficient internet services to their users. However, the same is possible through ownership / authorized membership at ccNSO and effective supervision of registry and registrar operations of ccTLDs (".pk", "IDN"). This thesis highlighted some key factors and issues related to the administration and operation of ccTLDs (.pk, IDN), violations (non-accomplishment of

responsibilities) committed by their Managers (Pakistan Network Information Center and National Telecommunication Corporation), focusing on vulnerabilities that arise due to the absence of governmental and technical controls, hence offering security breaches or compromising cyber security. After carrying out the comparison and taking guidance from international models / current best practices for the administration operation of ccTLDs, suggesting the corrections measures in the present governance/supervision model and potential administrative structure/business model to be used for the ccTLDs to run the registry with responsibility, enhance cyber security, and services back to the internet community (not-for-profit or profit-for-purpose).

Keywords: DNS, IANA, ICANN, Policy Development Process, ccNSO, ccTLDs, .pk, IDN, PKNIC, NTC, DNSSEC, Cybersecurity, Zone Authoritative Servers, Not-For-Profit.

2024

ANOMALY DETECTION USING DEEP LEARNING FOR BODY AREA NETWORKS

Muhammad Abbas and Dr. Fadia Shah

ABSTRACT

The emergence of the Internet of Healthcare Things (IoHT) brings with it the potential to revolutionize healthcare services, with wireless body area networks (WBANs) playing a significant role. These networks, composed of miniature devices, offer the capability to improve patient quality of life by continuously monitoring physiological data and transmitting it to healthcare providers. However, ensuring the reliability and accuracy of this data is crucial for effective decision-making in healthcare settings. Anomaly detection in WBANs has become a critical area of research, aiming to identify aberrant patterns in collected data that may arise from sensor faults, errors, or even malicious activities. Traditional anomaly detection methods, primarily based on statistical and machine learning techniques, face challenges in handling the vast streams of data generated by WBANs and detecting novel contextual anomalies. To address these challenges, a novel approach is proposed in this thesis. The model combines the use of correlations existing among different physiological data attributes with the hybrid Convolutional Long Short-Term Memory (ConvLSTM) techniques. ConvLSTM combines the strengths of convolutional neural networks (CNNs) and long short-term memory (LSTM) networks, enabling it to effectively detect both simple point anomalies and contextual anomalies in the big data streams of WBANs. Experimental evaluations of the proposed model demonstrate promising results, with an average F1 measure of 98% and accuracy of 99% reported across different datasets. This performance significantly outperforms traditional CNN and LSTM approaches, which achieved only 64% accuracy when used separately.

Keywords: Anomaly Detection; Wireless Body Area Networks; Spatiotemporal Correlation; Convolutional Neural Networks; Long Short-term Memory.

2024

INVESTIGATING CYBER THREATS AND MALWARE GENERATION BY GENERATIVE AI

Werisha and Dr. Danish Mehmood

ABSTRACT

Generative AI (GenAI) represents a significant advancement in artificial intelligence, allowing the creation of complex outputs such as text, images, and code. Despite its transformative potential in various sectors, GenAI introduces substantial cybersecurity threats such as social engineering, phishing attacks, ransomware, and other forms of malware. This study systematically investigates the impact of GenAI on the landscape of cybersecurity threats, analyzing its capabilities and assessing the ease with which malware can be created and deployed using these technologies. Through a series of experiments, the creation of advanced malware by a script kiddie utilizing GenAI chatbots is being explored, specifically focusing on the capabilities of the GenAI chatbot. The study sheds light on the generation of functional malware using PowerShell scripts and discusses the challenges involved in bypassing GenAI's safety protocols. In particular, the detection rate of malware created by these chatbots is found to be alarmingly low, ranging from 30 to 33 percent on VirusTotal, signaling a significant vulnerability in current cybersecurity defenses. The experiment successfully demonstrated the generation of ransomware using Generative AI, which was tested against 75 antivirus solutions, of which only 25 were able to detect it as malicious. This underscores the inadequacy of traditional security measures, revealing critical vulnerabilities in AI-generated malware detection. These findings underscore the grave need for advanced cybersecurity strategies capable of addressing the unique threats posed by AI-driven tools. The study calls for urgent collaboration between AI developers and cybersecurity professionals to create robust frameworks that can mitigate these risks, ensuring that the benefits of GenAI are harnessed without compromising security. Furthermore, as GenAI continues to evolve, continuous monitoring and adaptation of security measures are crucial to prevent the escalation of AI-powered cyber threats in the future.

Keywords: Generative AI, cyber-attacks, GenAI capabilities, malware generation.

2024

ROOT DETECTION AND COUNTERMEASURES FOR SECURING ANDROID BANKING APPLICATIONS

Muhammad Tariq and Dr. Ahsan Abdullah

ABSTRACT

The popularity of Android has increased by over 1.4 billion users, highlighting its critical role in facilitating financial transactions through various applications. However, the rise in Android smartphones, which has brought with it the basic risks associated with rooted devices, underscores the need for robust security measures in the financial sector. Several root detection techniques exist in the market and are used in various applications. Despite their global use, these techniques are not foolproof, as there are available root evasion methods capable of easily bypassing them. This research aims to assess the accuracy of current root detection techniques used in the market. The work includes developing a prototype with various root detection techniques. It also involves setting up an attack on this prototype application after initially testing it on both rooted and non-rooted Android operating system-based devices to evaluate the accuracy of the detection techniques. These techniques accurately detect roots when no root evasion techniques are employed. Subsequently, this prototype APK is subjected to acomprehensive analysis by launching an attack with the help of Frida tools. An attack was launched on this prototype containing single and combined root detection techniques, and as a result, all these root detection techniques were successfully bypassed, including Google's latest Google Play Integrity API. Resource utilization analysis shows that RootBeer has the lowest average processor usage (9.33%), while command execution exhibited the highest (20.67%). BusyBox utilized the least memory (2.67 MB), whereas Root Beerused the most (9 MB). RootBeer effectively manages processing resources, evidenced by its lowest processor load, despite using a comprehensive set of checks. In conclusion, this work shows that bypassing root detection is not difficult if the app relies on basic functions to detect a rooted device. To make the bypassing process more challenging, it is recommended that developers implement multiple and more advanced root detection techniques.

Keywords: Android Root Detection, Application Security, Banking Apps Security.

2024

A DECENTRALIZED AUTHENTICATION MODEL FOR THE METAVERSE USING AI-BASED BLOCKCHAIN TECHNOLOGY

Haris Javed and Dr. Ahsan Abdullah

ABSTRACT

The rise of the Metaverse has heightened the demand for advanced authentication models to ensure secure interactions and reliable identity verification in virtual spaces. Traditional centralized models are inadequate, exhibiting vulnerabilities to single points of failure, data breaches, and privacy concerns. Existing blockchain-based authentication systems face significant scalability issues, resulting in slow processing times and high energy consumption. To address these challenges, this thesis proposes a novel decentralized authentication model that leverages AI-based blockchain technology to enhance security, privacy, and scalability in the metaverse. The model utilizes blockchain's immutable ledger for transparent identity verification, while AI-driven algorithms facilitate real-time authentication, face detection, fingerprint and adaptive trust scoring. By employing smart contracts, the model validates user interactions and identity credentials without the need for intermediaries, ensuring data integrity and reducing latency by up to 60%. A prototype implementation demonstrates the model's effectiveness in real-world scenarios, achieving a 95% accuracy rate in identity verification and reducing unauthorized access incidents by 85%. Furthermore, user engagement increased by 30% due to the simplified authentication processes. The findings underscore the feasibility and advantages of integrating AI and blockchain for secure, autonomous authentication in the metaverse. The conclusion reflects on the significance of the findings, addresses limitations, and proposes future work focusing on optimization and integration with emerging technologies. This technology fusion forms the backbone of an innovative authentication application designed for the dynamic Metaverse environment.

Keywords: Blockchain, Metaverse, Artificial Intelligence, Decentralized Authentication.

2023

A HYBRID INTRUSION DETECTION SYSTEM BASED ON OPTIMAL FEATURE SELECTION AND EVOLUTIONARY ALGORITHM FOR WIRED NETWORKS

Husnain Babar and Dr. Muhammad Imran

ABSTRACT

The field of cyber security encounters ongoing difficulties in identifying and preventing attacks in networks, the pervasive threat of cyber-attacks demands continual advancements in intrusion detection systems (IDS) to safeguard network integrity. Traditional intrusion detection systems face challenges of handling high dimensional data and class imbalance. Addressing the formidable challenges posed by class imbalance and high-dimensional data, this research proposes a novel hybrid IDS approach. Leveraging Ant Colony Optimization (ACO), the algorithm strategically navigates complex datasets to identify salient features, effectively mitigating the complexities associated with high-dimensional data. Subsequently, a Weighted Stacking Classifier amalgamates the strengths of Random Forest, AdaBoost, and Gradient Boosting classifiers, fortifying the system's ability to handle class imbalance robustly. By strategically enhancing the importance of base classifiers with favorable training outcomes and diminishing the influence of those yielding inferior results, the hybrid IDS endeavors to optimize classification efficacy. The experimentation, conducted exclusively on the NSL-KDD dataset demonstrates the efficacy of the proposed model, yielding remarkable results. With an accuracy of 90.13%, precision of 88.87%, recall of 91.23%, and F1-score of 87.33%, the hybrid IDS exhibits superior performance in detecting malicious activity.The findings underscore the viability of the proposed hybrid IDS as a potent tool in the ongoing battle against cyber threats, positioning it for real-world deployment across diverse networks.

Keywords: Intrusion Detection System, Ant Colony Optimization, Feature Selection, Weighted Stacking Classifier, High-Dimensional Data, Class Imbalance, Ensemble Classifier.

2023

A HYBRID INTRUSION DETECTION SYSTEM BASED ON OPTIMAL FEATURE SELECTION AND EVOLUTIONARY ALGORITHM FOR WIRED NETWORKS

Husnain Babar and Dr. Muhammad Imran

ABSTRACT

The field of cybersecurity encounters ongoing difficulties in identifying and preventing attacks in networks, the pervasive threat of cyber-attacks demands continual advancements in intrusion detection systems (IDS) to safeguard network integrity. Traditional intrusion detection systems face challenges of handling high dimensional data and class imbalance.Addressing the formidable challenges posed by class imbalance and high-dimensional data, this research proposes a novel hybrid IDS approach. Leveraging Ant Colony Optimization (ACO), the algorithm strategically navigates complex datasets to identify salient features, effectively mitigating the complexities associated with high-dimensional data. Subsequently, a Weighted Stacking Classifier amalgamates the strengths of Random Forest, AdaBoost, and Gradient Boosting classifiers, fortifying the system's ability to handle class imbalance robustly.By strategically enhancing the importance of base classifiers with favorable training outcomes and diminishing the influence of those yielding inferior results, the hybrid IDS endeavors to optimize classification efficacy.The experimentation, conducted exclusively on the NSL-KDD dataset demonstrates the efficacy of the proposed model, yielding remarkable results. With an accuracy of 90.13%, precision of 88.87%, recall of 91.23%, and F1-score of 87.33%, the hybrid IDS exhibits superior performance in detecting malicious activity.The findings underscore the viability of the proposed hybrid IDS as a potent tool in the ongoing battle against cyber threats, positioning it for real-world deployment across diverse networks.

Keywords: Intrusion Detection System, Ant colony optimization,Feature selection,Weighted stacking classifier, High-dimensional data,Class imbalance,Ensemble Classifier.