IJIRSET
International Journal of Innovative Research in
SCIENCE | ENGINEERING | TECHNOLOGY

e-ISSN: 2319-8753 | p-ISSN: 2347-6710

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

Volume 12, Issue 5, May 2023

ISSN INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 8.423

9940 572 462 | 6381 907 438 | ijirset@gmail.com | www.ijirset.com

International Journal of Innovative Research in Science, Engineering and Technology (IJIRSET)

|e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 8.423| A Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 5, May 2023 ||

| DOI:10.15680/IJIRSET.2023.1205496 |

Artificial Intelligence Strategies for Combating IoT-Centric Cyber Attacks

Prof. Abhishek Patel[1], Prof. Pankaj Pali[2], Prof. Saurabh Verma[3] , Prof.Shivam Tiwari[4,]

Vaishnavi Vishwakarma[4], Shivam Chourasiya[5]

Department of CSE, Baderia Global Institute of Engineering and Management, Jabalpur[1], (M.P), India

ABSTRACT: The proliferation of Internet of Things (IoT) devices has revolutionized various sectors, from smart homes to industrial automation, but it has also introduced significant cyber security challenges. IoT-centric cyber attacks exploit vulnerabilities inherent in interconnected devices, posing threats to data integrity, privacy, and overall system stability. This review paper explores the evolving landscape of IoT cyber security and the role of Artificial Intelligence (AI) in mitigating these risks. We systematically analyze the types of IoT-centric cyber attacks, including Distributed Denial of Service (DDoS), man-in-the-middle (MITM), and malware injection attacks. The paper further examines AI-driven strategies for detecting, preventing, and responding to such threats. Key AI techniques such as machine learning, deep learning, and anomaly detection are evaluated for their effectiveness in real-time threat identification and adaptive defense mechanisms. Additionally, the review addresses the integration of AI with traditional cyber security frameworks and highlights emerging trends and challenges in the deployment of AI solutions. By synthesizing current research and practical applications, this paper aims to provide a comprehensive overview of AI strategies that enhance the security posture of IoT ecosystems, offering insights for researchers, practitioners, and policymakers dedicated to advancing cyber security in the IoT domain.

KEYWORDS: smart transportation system", "AI-Driven Vehicle system", "Urban transportation".

I. INTRODUCTION

The Internet of Things (IoT) has transformed various aspects of modern life, from smart homes and healthcare to industrial automation and urban infrastructure. This technological revolution characterized by interconnected devices communicating and exchanging data, offers significant convenience, efficiency, and innovation opportunities. According to recent estimates, the number of IoT devices is expected to surpass 30 billion by 2025, highlighting the rapid adoption and integration of IoT technology across multiple sectors.

However, this pervasive connectivity comes with heightened vulnerabilities. IoT devices, often designed with minimal security considerations, present a broad attack surface for cyber threats. Unlike traditional IT systems, IoT environments encompass a diverse array of devices, many of which lack the computational resources for robust security measures. This diversity and the heterogeneity of IoT devices make them attractive targets for malicious actors. Common cyber threats in IoT environments include distributed denial-of-service (DDoS) attacks, malware propagation, data breaches, and unauthorized access. The implications of such attacks are profound, potentially compromising personal privacy, disrupting critical services, and causing significant financial losses.

In light of these challenges, Artificial Intelligence (AI) emerges as a promising solution to enhance IoT security. AI's ability to analyze vast amounts of data, detect patterns, and respond to anomalies in real-time makes it particularly suited for the dynamic and complex nature of IoT networks. AI-driven techniques, such as machine learning and deep learning, can be employed to identify and mitigate cyber threats with greater accuracy and speed compared to traditional methods. By leveraging AI, it is possible to develop adaptive and proactive security mechanisms that can keep pace with the evolving threat landscape.

This survey paper aims to explore and synthesize the current strategies and advancements in using AI to combat IoT-centric cyber attacks. The objectives of this paper are fourfold: first, to provide a comprehensive background on IoT technology and its vulnerabilities; second, to categorize and analyze the various types of cyber threats specific to IoT environments; third, to evaluate the effectiveness of existing AI-based security solutions; and fourth, to identify emerging trends and future directions in this field. By doing so, this paper seeks to offer valuable insights for researchers, practitioners, and policymakers striving to enhance the security and resilience of IoT ecosystems.

|e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 8.423| A Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 5, May 2023 ||

| DOI:10.15680/IJIRSET.2023.1205496 |

II. OVERVIEW OF IOT CETRIC CYBER ATTACKS

The Internet of Things (IoT) revolution has brought about a vast array of interconnected devices, offering unprecedented convenience and efficiency. However, this connectivity also presents significant security challenges. IoT-centric cyber attacks exploit vulnerabilities in these devices, leading to various adverse outcomes. This overview examines the types, techniques, and notable incidents of IoT-centric cyber attacks.

A. Types of IoT-Centric Cyber Attacks

1. Botnet Attacks

Mirai Botnet: One of the most notorious IoT-based botnets, Mirai, was responsible for a massive Distributed Denial of Service (DDoS) attack in 2016, affecting major websites like Twitter and Netflix.

Hajime Botnet: Unlike Mirai, Hajime is a more sophisticated botnet that appears to be a vigilante, securing devices instead of attacking them. However, its existence indicates the potential for exploitation.

2. DDoS Attacks

IoT devices, often with weak security, can be hijacked to form botnets that launch DDoS attacks. These attacks overwhelm targets with traffic, causing downtime and financial losses.

3. Data Breaches

Ring Security Cameras: In 2019, a series of breaches exposed the vulnerabilities in Ring security cameras, where attackers gained access to live feeds and personal data.

Target Data Breach: In 2013, attackers exploited an HVAC system to gain access to Target's network, resulting in the theft of 40 million credit and debit card records.

Ransomware WannaCry: While not IoT-specific, WannaCry highlighted the potential for ransomware to impact connected devices. Future IoT-specific ransomware could target smart homes or critical infrastructure.

4. Firmware Attacks Attackers can exploit vulnerabilities in device firmware to gain persistent access and control. This can lead to long-term compromises that are hard to detect and mitigate.

5. Man-in-the-Middle (MitM) Attacks By intercepting communication between IoT devices and their control systems, attackers can manipulate data, inject malicious commands, or steal sensitive information.

B. Techniques Used in IoT-Centric Attacks

1. Exploitation of Default Credentials Many IoT devices are shipped with default usernames and passwords, which users often neglect to change. Attackers exploit these defaults to gain unauthorized access.
2. Vulnerability Exploitation: Software bugs and design flaws in IoT devices can be exploited to gain control or disrupt operations. Regular updates and patches are essential but often neglected in IoT devices.
3. Network Traffic Analysis: Attackers can analyze unencrypted traffic from IoT devices to gather sensitive information or inject malicious commands.
4. Physical Access: Physical access to IoT devices can allow attackers to tamper with hardware, install malicious firmware, or extract sensitive data.
5. Notable IoT Cyber Attacks: Mirai Botnet (2016): Leveraged thousands of compromised IoT devices to launch a massive DDoS attack, taking down major websites and highlighting the vulnerabilities in IoT security.
6. Stuxnet (2010): Although not an IoT attack in the conventional sense, Stuxnet demonstrated how targeted malware could disrupt physical infrastructure, a scenario relevant to IoT environments.
7. Jeep Cherokee Hack (2015): Researchers demonstrated how vulnerabilities in the vehicle's IoT systems could allow remote control of critical functions, prompting a recall of 1.4 million vehicles.
8. Vulnerable Smart Toys (2015-2017): Several incidents, including the VTech data breach, exposed the risks associated with connected toys, where attackers accessed personal data of children and their families.
9. Mitigation Strategies: Strong Authentication Implementing robust authentication mechanisms, such as multi-factor authentication (MFA), can significantly reduce unauthorized access.
10. Regular Updates and Patching: Ensuring that IoT devices are regularly updated with the latest security patches can mitigate known vulnerabilities.
11. Network Segmentation: Segregating IoT devices from critical network infrastructure can limit the impact of a compromised device.

|e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 8.423| A Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 5, May 2023 ||

| DOI:10.15680/IJIRSET.2023.1205496 |

12. Encryption: Encrypting data in transit and at rest can prevent attackers from intercepting and manipulating sensitive information.
13. Device Hardening: Disabling unnecessary features and services, changing default credentials, and implementing secure configurations can reduce the attack surface.
14. Security Monitoring: Continuous monitoring of IoT devices for unusual activity can help in early detection and response to potential threats.

III. ROLE OF AI IN CYBER SECURITY

A. The Role of AI in Cyber security: Artificial Intelligence (AI) has rapidly emerged as a critical tool in the field of cyber security, offering advanced solutions to tackle evolving cyber threats. The integration of AI into cyber security practices has brought about significant advancements in threat detection, response, and mitigation. This paper explores the multifaceted role of AI in enhancing cyber security defenses.

B. Enhanced Threat Detection: One of the primary benefits of AI in cyber security is its ability to detect threats more effectively than traditional methods. AI algorithms, particularly those based on machine learning (ML), can analyze vast amounts of data to identify patterns and anomalies that may indicate a cyber threat. Unlike traditional systems that rely on predefined rules and signatures, AI systems learn from historical data and can adapt to new threats without needing explicit reprogramming. For instance, AI can detect zero-day attacks—new and previously unknown vulnerabilities—by recognizing abnormal behavior patterns that deviate from the norm.

C. Real-time Threat Analysis and Response: AI excels in processing large volumes of data in real-time, which is crucial for identifying and responding to threats as they occur. Through techniques such as anomaly detection and predictive analytics, AI systems can provide real-time alerts and automated responses to mitigate potential attacks. For example, AI-driven security information and event management (SIEM) systems can aggregate and analyze log data from various sources to detect suspicious activity, allowing for swift incident response.

D. Automating Routine Security Tasks: Automation is another significant advantage of AI in cyber security. AI can handle repetitive and mundane tasks, such as monitoring network traffic, managing patches, and updating software, freeing up human analysts to focus on more complex issues. This not only increases efficiency but also reduces the likelihood of human error. AI-powered tools can also simulate attacks to test the robustness of security systems, a process known as penetration testing.

E. Enhancing Threat Intelligence: AI contributes to the enhancement of threat intelligence by collecting and analyzing data from diverse sources, including dark web forums, social media, and security blogs. By synthesizing this information, AI can provide actionable insights and predictive analytics to anticipate and counteract potential threats. Natural language processing (NLP), a subset of AI, can be used to parse and understand unstructured data, further enriching the threat intelligence process.

F. Adaptive Security Measures: AI enables adaptive security measures that evolve with the threat landscape. Through continuous learning and adaptation, AI systems can update their models based on new data, ensuring that security measures remain effective against emerging threats. This dynamic approach contrasts with static security measures that can quickly become obsolete as new vulnerabilities are discovered.

G. Challenges and Considerations: Despite its benefits, the implementation of AI in cyber security comes with challenges. AI systems require large datasets to learn effectively, which may raise privacy concerns. Additionally, attackers can use AI to develop more sophisticated attack methods, creating an ongoing arms race between defenders and adversaries. Ensuring the transparency and explain ability of AI decisions is also crucial to maintain trust in these systems.

|e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 8.423| A Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 5, May 2023 ||

| DOI:10.15680/IJIRSET.2023.1205496 |

IV. AI-STRATEGIES FOR COMBATTING IOT-CENTRING CYBER ATTACKS

A. Intrusion Detection Systems (IDS)

1. Types of IDS

Intrusion Detection Systems (IDS) are critical for identifying unauthorized access or breaches in a network. There are three main types of IDS:

Signature-based IDS: This type identifies threats by comparing the network traffic against a database of known attack patterns or signatures. While effective against known threats, it struggles with zero-day exploits.

Anomaly-based IDS: This type detects deviations from a model of normal network behavior. It can identify new and previously unknown threats but may produce false positives due to the dynamic nature of network traffic.

Hybrid IDS: Combining the strengths of both signature-based and anomaly-based approaches, hybrid IDS provides a more robust solution. It uses signatures for known threats while employing anomaly detection for unknown or emerging threats.

2. Role of AI in Enhancing IDS: AI significantly enhances IDS by improving detection accuracy and response times. Machine learning algorithms analyze vast amounts of network data to identify patterns and anomalies. AI-driven IDS can adapt to new threats by learning from previous incidents and continually updating their detection models. This reduces false positives and improves the system's ability to detect sophisticated attacks, including those targeting IoT devices.

B. Network Security Solutions

1. AI-driven Firewalls: Traditional firewalls are rule-based and may not effectively handle the dynamic nature of modern cyber threats. AI-driven firewalls, however, utilize machine learning to monitor and analyze network traffic in real-time. They can identify and block malicious traffic based on learned behaviors rather than static rules, providing a more adaptive and proactive security measure.
2. Intelligent Network Traffic Analysis: AI enhances network traffic analysis by employing advanced algorithms to scrutinize data flows for signs of malicious activity. Intelligent systems can identify unusual patterns indicative of an attack, such as data exhilaration or Distributed Denial of Service (DDoS) attacks. By continuously learning and updating their analysis models, AI-driven tools can stay ahead of evolving threats, ensuring robust network security.
3. Endpoint Security : AI-based Antivirus and Anti-malware Solutions: Traditional antivirus software relies on signature databases to detect malware, which can be ineffective against new or polymorphic threats. AI-based solutions, however, use machine learning to identify malicious behavior patterns. These systems can detect and neutralize unknown malware by analyzing the behavior of files and processes, providing more comprehensive protection for IoT devices.
4. Device Authentication and Access Control: Ensuring that only authorized devices can access a network is crucial for IoT security. AI enhances device authentication by analyzing patterns such as usage habits, location, and device characteristics. AI-driven access control systems can dynamically adjust permissions based on real-time risk assessments, preventing unauthorized access and reducing the likelihood of breaches.
5. Data Security and Privacy AI Techniques for Data Encryption and Secure Communication : AI can optimize data encryption methods, ensuring that communication between IoT devices remains secure. Machine learning algorithms can identify the most effective encryption techniques for different types of data and communication channels, enhancing overall security. Additionally, AI can monitor encrypted traffic to detect potential breaches without decrypting the data, maintaining privacy while ensuring security.
6. AI-driven Privacy-Preserving Mechanisms: Privacy is a significant concern in IoT environments, where vast amounts of sensitive data are collected and transmitted. AI-driven mechanisms can ensure data privacy by employing techniques such as differential privacy and homomorphism encryption. These methods allow data to be analyzed and utilized without exposing the underlying sensitive information, balancing the need for data utility and privacy.

|e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 8.423| A Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 5, May 2023 ||

| DOI:10.15680/IJIRSET.2023.1205496 |

V. CASE STUDIES AND REAL-WORLD APPLICATIONS

The integration of Artificial Intelligence (AI) in combating IoT-centric cyber attacks has shown significant promise across various sectors. This section delves into real-world applications and case studies that highlight the effectiveness of AI strategies in different IoT domains.

A. Industrial IoT (IIoT): In the realm of manufacturing and critical infrastructure, AI strategies are pivotal in safeguarding Industrial IoT (IIoT) systems. AI-driven predictive maintenance and anomaly detection algorithms help in identifying irregularities in machinery performance and network traffic, which can indicate potential cyber threats. For example, Siemens utilizes AI to monitor and analyze data from industrial sensors, ensuring early detection of malfunctions and cyber intrusions. Similarly, General Electric's Predix platform leverages machine learning to enhance the security and efficiency of industrial operations. These AI applications not only enhance operational reliability but also fortify security measures against sophisticated cyber threats targeting critical infrastructure.

B. Smart Homes and Wearable's: Consumer IoT security, encompassing smart homes and wearable devices, has greatly benefited from AI applications. AI algorithms embedded in smart home systems, such as Amazon Alexa and Google Home, analyze user patterns to detect unusual activities and potential security breaches. For instance, AI-powered security cameras from companies like Ring use facial recognition and motion detection to alert homeowners of unauthorized access. Wearable devices, including smart watches, employ AI to monitor biometric data, ensuring the integrity and privacy of personal health information. These AI-enhanced IoT devices provide an additional layer of security, making it harder for attackers to exploit vulnerabilities.

C. Healthcare IoT: In healthcare, the security of medical devices and patient data is paramount. AI-driven solutions play a crucial role in safeguarding healthcare IoT (IoMT) devices. For example, IBM Watson Health employs AI to analyze vast amounts of medical data, identifying patterns that could signify security breaches or device malfunctions. AI algorithms also monitor network traffic to detect anomalies indicative of cyber attacks on medical equipment, such as infusion pumps and pacemakers. These proactive AI strategies ensure that patient data remains confidential and that medical devices function safely and reliably, mitigating the risk of potentially life-threatening cyber incidents.

D. Transportation and Smart Cities: AI is instrumental in securing autonomous vehicles and smart city infrastructures. In autonomous transportation, AI systems from companies like Tesla and Waymo analyze real-time data to detect and respond to cyber threats, ensuring the safety and security of passengers. AI algorithms in smart cities monitor and manage critical infrastructure, including traffic lights, surveillance systems, and public utilities, to prevent and mitigate cyber attacks. For instance, AI solutions deployed in cities like Singapore and Barcelona analyze data from IoT sensors to optimize urban operations and enhance cybersecurity. These AI applications not only improve the efficiency and resilience of smart city systems but also protect against potential disruptions caused by cyber threats.

VI. CHALLENGES AND LIMITATIONS

In the realm of AI-driven strategies for combating IoT-centric cyber attacks, several challenges and limitations must be addressed to ensure effectiveness and fairness. These challenges can be broadly categorized into technical, ethical, and regulatory domains.

A. Technical Challenges-- Scalability and Resource Constraints: One of the foremost technical challenges is the scalability of AI systems. IoT environments are characterized by a vast number of devices, each generating significant amounts of data. The AI models designed to detect and mitigate cyber threats must process and analyze this data in real-time, which demands substantial computational resources. The heterogeneity of IoT devices further complicates this, as different devices have varied capabilities and resource limitations, making it difficult to implement uniform AI solutions across the board.

B. Data Quality and Availability: The efficacy of AI in combating cyber attacks heavily relies on the quality and availability of data. IoT devices often produce noisy, incomplete, or inconsistent data, which can impair the performance of AI models. Additionally, data from IoT devices may be sporadically available due to connectivity issues or device failures. Ensuring continuous, high-quality data streams is crucial for maintaining the reliability of AI-based security measures.

|e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 8.423| A Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 5, May 2023 ||

| DOI:10.15680/IJIRSET.2023.1205496 |

C. Ethical and Privacy Concerns-- Balancing Security with User Privacy: Implementing AI strategies in IoT environments raises significant ethical concerns, particularly around user privacy. AI systems often require extensive data to function effectively, which can include sensitive user information. Striking a balance between robust security measures and the preservation of user privacy is a critical challenge. Excessive data collection and intrusive monitoring can lead to privacy violations and erode user trust.

D. AI Biases and Fairness: AI models can inadvertently perpetuate biases present in the training data, leading to unfair or discriminatory outcomes. In the context of IoT security, this can manifest in the form of biased threat detection and mitigation, where certain devices or user behaviors are unfairly targeted. Ensuring fairness and transparency in AI decision-making processes is essential to avoid reinforcing existing biases and to maintain equitable security measures.Regulatory and Standardization Issues.

E. Lack of Uniform Regulations: The regulatory landscape for IoT security is fragmented, with varying standards and regulations across different regions and industries. This lack of uniformity complicates the implementation of AI-based security solutions, as they must be tailored to comply with diverse regulatory requirements. Harmonizing regulations and establishing common frameworks are necessary to facilitate the widespread adoption of AI in IoT security.

F. Need for Global Standards: The global nature of IoT ecosystems necessitates the development of international standards for AI-driven security measures. Without globally recognized standards, it is challenging to ensure interoperability and consistency across different IoT platforms and devices. Developing and enforcing these standards is crucial for creating a cohesive and effective defense against IoT-centric cyber attacks.

VII. FUTURE DIRECTION AND RESEARCH OPPORTUNITIES

A. Emerging AI Technologies in Cyber security: The landscape of AI-driven cyber security for IoT systems is rapidly evolving with the advent of advanced AI techniques such as federated learning and edge AI. Federated learning offers a decentralized approach to training machine learning models, allowing data to remain on local devices while aggregating model updates centrally. This method enhances privacy and security by minimizing data exposure risks, making it particularly suitable for IoT ecosystems where data sensitivity and heterogeneity are paramount. Edge AI, on the other hand, brings AI computations closer to the data source, reducing latency and bandwidth usage. This proximity facilitates real-time threat detection and response, crucial for time-sensitive IoT applications such as healthcare and autonomous vehicles.

B. Integration with Other Technologies: The integration of AI with block chain technology presents a promising avenue for enhancing IoT security. Block chain's immutable and decentralized ledger can provide a robust framework for securing IoT transactions and data exchanges. By leveraging AI to analyze and manage block chain data, more intelligent and adaptive security measures can be developed. For instance, AI can be used to detect anomalous patterns in block chain transactions, potentially indicating security breaches or fraudulent activities. Furthermore, the advent of quantum computing holds significant implications for cyber security. Quantum computing potential to break traditional cryptographic methods necessitates the development of quantum-resistant algorithms. AI can aid in the design and implementation of these algorithms, ensuring the continued protection of IoT systems in a post-quantum era.

C. Interdisciplinary Research: Addressing the complex challenges posed by IoT-centric cyber attacks requires a collaborative approach that spans multiple disciplines. Integrating insights from AI, cyber security, and IoT fields can lead to more holistic and effective security strategies. For example, AI experts can work with cyber security professionals to develop machine learning models that predict and mitigate emerging threats. Simultaneously, IoT specialists can provide critical insights into the specific vulnerabilities and operational contexts of IoT devices, ensuring that AI-driven security solutions are both relevant and practical. Additionally, fostering interdisciplinary research can lead to the development of standardized security protocols and frameworks that are universally applicable across different IoT environments.

|e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 8.423| A Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 5, May 2023 ||

| DOI:10.15680/IJIRSET.2023.1205496 |

VIII. CONCLUSION

The integration of Artificial Intelligence (AI) in combating IoT-centric cyber attacks represents a significant advancement in the realm of cyber security. As the proliferation of IoT devices continues to accelerate, so too does the complexity and volume of potential security threats. AI's capabilities in analyzing vast amounts of data, identifying patterns, and responding to anomalies in real-time make it a critical tool for enhancing IoT security.

AI-driven Intrusion Detection Systems (IDS), intelligent firewalls, and advanced network traffic analysis tools provide robust defenses against sophisticated cyber threats. These systems not only detect and mitigate attacks more effectively than traditional methods but also adapt to evolving threats, ensuring continuous protection. Furthermore, AI's role in endpoint security, data encryption, and privacy-preserving mechanisms enhances the overall security posture of IoT ecosystems. Real-world applications in various sectors, including industrial IoT, smart homes, healthcare, and smart cities, demonstrate the practical benefits of AI in securing connected devices and infrastructure. Case studies from leading organizations highlight how AI enhances operational reliability and fortifies defenses against cyber intrusions, ensuring the integrity and safety of critical systems.

However, the deployment of AI in IoT security is not without challenges. Technical issues such as scalability and data quality, ethical concerns surrounding privacy and bias, and regulatory fragmentation present significant hurdles. Addressing these challenges requires a concerted effort to develop scalable AI models, ensure ethical AI practices, and harmonize regulations across regions. Looking forward, emerging technologies like federated learning, edge AI, block chain integration, and quantum-resistant algorithms offer promising avenues for future research and development. Interdisciplinary collaboration will be essential in creating comprehensive and standardized security protocols, ensuring that AI-driven solutions remain effective and equitable in safeguarding the increasingly interconnected world of IoT. In conclusion, AI presents a transformative approach to enhancing IoT security, offering adaptive, real-time defenses against a landscape of ever-evolving cyber threats. Continued innovation and collaboration in this field will be crucial to realizing the full potential of AI in securing the IoT ecosystem.

REFERENCES

[1]. Singh, S.; Sheng, Q.Z.; Benkhelifa, E.; Lloret, J. Guest Editorial: Energy Management, Protocols, and Security for the Next-Generation Networks and Internet of Things. IEEE Trans. Ind. Inform. **2020**, 16, 3515–3520.
[2]. Almiani, M.; AbuGhazleh, A.; Al-Rahayfeh, A.; Atiewi, S.; Razaque, A. Deep recurrent neural network for IoT intrusion detection system. Simul. Model. Pract. Theory **2020**, 101, 102031.
[3]. Hong, Z.; Hong, M.; Wang, N.; Ma, Y.; Zhou, X.; Wang, W. A wearable-based posture recognition system with AI-assisted approach for healthcare IoT. Futur. Gener. Comput. Syst. **2022**, 127, 286–296.
[4]. Adil, M.; Khan, M.K. Emerging IoT Applications in Sustainable Smart Cities for COVID-19: Network Security and Data Preservation Challenges with Future Directions. Sustain. Cities Soc. **2021**, 75, 103311.
[5]. Kurte, R.; Salcic, Z.; Wang, K.I.K. A Distributed Service Framework for the Internet of Things. IEEE Trans. Ind. Inform. **2020**, 16, 4166–4176.
[6]. Zeng, P.; Pan, B.; Choo, K.K.R.; Liu, H. MMDA: Multidimensional and multidirectional data aggregation for edge computing-enhanced IoT. J. Syst. Archit. **2020**, 106, 101713.
[7]. Diro, A.A.; Chilamkurti, N. Distributed attack detection scheme using deep learning approach for Internet of Things. Futur. Gener. Comput. Syst. **2018**, 82, 761–768.
[8]. Farivar, F.; Haghighi, M.S.; Jolfaei, A.; Alazab, M. Artificial Intelligence for Detection, Estimation, and Compensation of Malicious Attacks in Nonlinear Cyber-Physical Systems and Industrial IoT. IEEE Trans. Ind. Inform. **2020**, 16, 2716–2725.
[9]. Al-Haija, Q.A.; Zein-Sabatto, S. An efficient deep-learning-based detection and classification system for cyber-attacks in iot communication networks. Electronics **2020**, 9, 2152.
[10]. Zhang, T.; Zhao, Y.; Jia, W.; Chen, M.Y. Collaborative algorithms that combine AI with IoT towards monitoring and control system. Futur. Gener. Comput. Syst. **2021**, 125, 677–686.
[11], Karale, A. The Challenges of IoT Addressing Security, Ethics, Privacy, and Laws. Internet Things **2021**, 15, 100420.
[12]. Obaidat, M.A.; Obeidat, S.; Holst, J.; Hayajneh, A.A.; Brown, J. A comprehensive and systematic survey on the internet of things: Security and privacy challenges, security frameworks, enabling technologies, threats, vulnerabilities and countermeasures. Computers **2020**, 9, 44.

INNO SPACE
SJIF Scientific Journal Impact Factor

Impact Factor: 8.423

doi cross ref

ISSN INTERNATIONAL STANDARD SERIAL NUMBER INDIA

निस्केयर NISCAIR

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

9940 572 462 6381 907 438 ijirset@gmail.com

www.ijirset.com

Scan to save the contact details