IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

ENHANCED SECURITY OF IOT DEVICES USING AI

Dr. G Sharmila, S R Chandan Veera Reddy, P Siva Saketh Reddy
Arnav B H, P Jeevan Reddy
Assistant Professor, Student, Student, Student, Student
Dept of CSE
CMR University, Bangalore, India

Abstract- The swift expansion of the Web and the Internet of Things, or IoT, has coincided with heightened apprehensions over cybersecurity. Artificial Intelligence (AI) currently serves a pivotal function in cybersecurity by creating advanced algorithms to safeguard networks & systems, including IoT gadgets. Cybercriminals are using AI by employing adversarial approaches to execute more sophisticated cybersecurity assaults.

This project consolidates knowledge from numerous studies into IoT, AI, and AI-facilitated cyberattacks, aiming to forecast prospective attacks, detect weaknesses in IoT devices, and alert consumers through machine learning models. It amalgamates several network-connected devices to establish intelligent, adaptive services aimed at safeguarding user privacy against risks including eavesdropping, blocking, DoS assaults, and spoofing. Moreover, it examines how the integration of IoT systems with AI might improve device security and facilitate machine learning-driven access management. This project involves the creation of an advanced video surveillance system that can monitor and analyse real-time video feeds to identify and recognise objects, actions, and abnormalities. Utilising contemporary deep learning architectures like Convolutional Neural Networks (CNNs), the system executes object detection, monitoring, activity recognition, and anomalous event detection through the extraction of spatiotemporal data. This research tackles the difficulties of IoT security and seeks to enhance device safety through deep learning and machine learning methodologies.

Keywords - Internet of Things (IoT) Security, Cybersecurity, Artificial Intellect (AI), Machine Understanding (ML), Deep Learning, ML, Adversarial AI, IoT Vulnerability Assessment, Threat Forecasting, Intelligent Surveillance, Object Recognition, Access Management, Privacy Safeguarding.

1. INTRODUCTION

A. Context

Our project aims to improve the security of IoT devices through the application of Artificial Intelligence (AI) methodologies. Artificial intelligence provides functionalities such as anomaly detection, intrusion detection, and threat intelligence, which are essential for meeting the distinct security needs of IoT devices. We intend to utilise AI algorithms to create intelligent systems that can identify and thwart security assaults in real time.

We present a system that integrates deep learning, reinforcement learning, and machine learning methodologies to enhance IoT security. Machine learning algorithms facilitate the identification of potential attacks by recognising patterns and anomalies in IoT network data, whereas deep learning models utilise neural networks to enhance the accuracy and efficacy of anomaly detection, intrusion detection, and malware detection in IoT settings.

The Internet of Things enables the automated exchange of data between devices and computers without human involvement. Nevertheless, the remote accessibility of devices renders users vulnerable to several cybersecurity dangers. The proliferation of smart gadgets, particularly wearable technology and smart home appliances, has heightened the risk, as these devices frequently store sensitive user data, such as location, contacts, and health information, which necessitates stringent privacy and security measures.

Owing to resource limitations (battery life, bandwidth, memory, and processing power) on numerous IoT devices, conventional robust and intricate security solutions are inappropriate.

Designing and maintaining a lightweight yet efficient AI-driven defensive architecture has become increasingly essential as the threat landscape advances. Due to the intricacy and rapidity of contemporary cyberattacks, coupled with the worldwide deficit of cybersecurity experts, network defenders increasingly depend on AI and machine learning technologies for assistance (Rutledge et al., 2016). Concurrently, hostile entities are employing AI to expedite vulnerability identification and enhance ransomware development efficiency (Canedo & Skjellum, 2016), hence presenting further hurdles.

The swift digital change enables hackers to leverage agile development frameworks, expediting ransomware creation and complicating the ability of conventional security measures to adapt.

B. Statement of the Problem

The increasing cybersecurity dangers to IoT devices necessitate new solutions. The integration of AI technologies offers potential for proactive threat detection, anomaly recognition, and adaptive defence strategies. Nonetheless, obstacles such as resource constraints, interoperability hurdles, and privacy issues impede the successful execution of AI-driven security measures. Robust strategies are essential to safeguard IoT ecosystems and their interrelated systems.

Principal concerns encompass:

- IoT devices encounter increasing security dangers owing to their interconnected characteristics and their utilisation across many sectors.
- Conventional security protocols frequently inadequately protect IoT environments from advancing cyber threats.
- Artificial intelligence technologies provide promising answers via proactive threat detection, anomaly identification, and adaptive defence mechanisms.
- The successful integration of AI is impeded by resource limitations, interoperability challenges, and privacy protection considerations.

C. Objectives

- Confront the escalating cybersecurity dangers encountered by IoT devices.
- Acknowledge the inadequacy of conventional security protocols in safeguarding contemporary IoT environments.
- Employ AI technologies for anticipatory threat detection, anomaly recognition, and the creation of adaptive defence strategies.
- Address the obstacles of resource limitations, interoperability concerns, and privacy threats while incorporating AI into IoT security frameworks.
- Devise thorough solutions to surmount these obstacles and enhance the security of interconnected IoT systems.
- Attain a substantial decrease in cyber threats aimed at IoT devices.

2. RELATED WORKS

The Internet of Things (IoT) facilitates the connection of electronic devices to computers, permitting effortless data transmission without human involvement [1,2,3]. The remote accessibility of these gadgets renders users vulnerable to several cybersecurity concerns. The widespread adoption of smart devices that retain sensitive and valuable user data has rendered the security of IoT systems a paramount challenge. Wearable technology and smart home equipment frequently gather and retain personal data, including location, contact information, and health records, all of which require protection and confidentiality. Conventional complicated and highly adaptable security algorithms frequently prove inadequate for IoT devices because of their constrained resources, such as battery life, bandwidth, memory, and processor capability [6].

Machine Learning (ML) is a viable solution for improving the security of IoT systems. As a more sophisticated artificial intelligence methodology, machine learning can surpass conventional methods in dynamic networks without necessitating explicit programming. By training machines to identify different forms of cyberattacks, machine learning can facilitate swift attack detection and offer suitable defence strategies. Furthermore, machine learning algorithms exhibit the capability to intelligently identify emerging dangers, hence improving the dependability and accessibility of Internet of Things devices. Notwithstanding this potential, a thorough literature evaluation remains necessary, as only a limited number of comprehensive review articles on ML-based IoT security have been published thus far.

Cui et al. [7] performed the inaugural comprehensive study, examining 78 papers up to 2017 that addressed significant IoT security attacks, machine learning-based solutions, research obstacles, and deficiencies. In 2018, Xiao et al. [8] conducted a review centred on machine learning methodologies for malware detection, access control, and safe data dumping. Chaabouni et al. [9] further contributed by categorising potential ML-based IoT device security solutions into four distinct types. A recent study group released a paper highlighting intrusion

detection and other machine learning-related security tasks in IoT systems [10].

In the 21st century, safeguarding IoT device security has become increasingly imperative. The IoT links the physical and digital realms to provide global smart services, while concurrently presenting numerous potential for cyberattacks. The phrase "Internet of Things" was coined by Kevin Ashton in 1999, and subsequently, IoT has facilitated the integration of physical and digital realms via smart devices and communication protocols. What was formerly perceived as a futuristic concept has now materialised because to improvements in IoT. The Internet of Things (IoT) has become fundamental to intelligent technologies integrated into daily life, rendering it challenging for individuals to operate without IoT-enabled devices and services.

As of 2020, around 50 billion IoT gadgets were linked to the World Wide Web, with the figure persistently increasing at a rapid pace. By the year 2025, the market for Internet of Things (IoT) is projected to be worth around USD 3.9 trillions and USD 11.1 trillion. The quantity of linked IoT devices, the magnitude of the worldwide IoT marketplace, and future forecasts underscore the technology's importance [15,16].

The construction of IoT was designed to connect devices and provide IoT services to residential and industrial settings. It serves as a conduit for many hardware applications. Diverse communication protocols function throughout the many layers of the Internet of Things architecture, such as Wi-Fi, Bluetooth, and others RFID, ZigBee, LPWAN, limited bandwidth, wider frequencies, etc IEEE 802.15.4 [17,18]. Prominent IoT platforms such as the Cloud from Google, Apple ARTIK Cloud, Azure by Microsoft, and Amazon AWS IoT offer comprehensive services to their international clientele. An IoT design is fundamentally composed of three primary layers: the mental (or physical) layer, and the networking layer, & the application/web plane [20].

3. PROPOSED SYSTEM

A. Algorithm

Command Authentication: Establish robust authentication protocols to validate the authenticity of commands directed at IoT devices, thereby thwarting unauthorised access.

Encryption: Secure command transfers between IoT devices and backend systems to guarantee data security and integrity, hence reducing the risks of interception or tampering.

Implement Role-Based Access Control (RBAC) to confine access to sensitive commands according to users' roles and permissions, thereby mitigating the potential consequences of unauthorised actions.

Command Validation: Assess incoming commands against established security norms and standards to facilitate the early identification and prevention of potentially harmful or improperly formatted commands.

Command Filtering: Utilise real-time filtering systems to assess and obstruct dubious or irregular commands that diverge from recognised standard device behaviour.

Implement AI-driven anomaly detection techniques to recognise atypical patterns or sequences of orders that may signify security breaches or malicious activity.

Behavioural Analysis: Utilise AI methodologies to examine previous command data, determine normative device behaviour, and identify anomalies that may indicate potential dangers.

Command Quarantine: Establish a quarantine protocol that temporarily retains dubious orders for additional scrutiny prior to execution, thereby protecting IoT devices and systems from potential threats.

Dynamic Command Authorisation: Adjust command authorisation in real-time according to contextual elements such as device location, time of day, or network conditions, hence improving overall security resilience and adaptability.

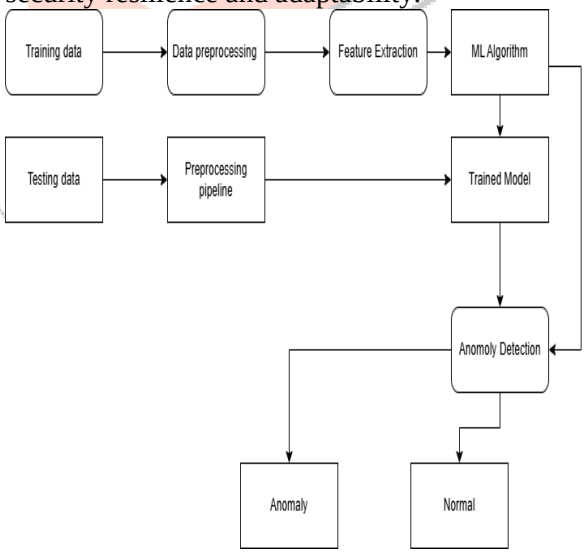

Fig. 1. System architecture

The Application Framework module integrates Natural Language Processing (NLP) methods, employed to train the chatbot via the execution of 'chat.py'. This procedure entails the establishment of a specialised virtual environment (venv) for a women's healthcare chatbot. The system is engineered to respond to enquiries concerning women's health, utilising SAFESCRIBE for safe data management and processing. This extensive framework incorporates NLP training, customised virtual environment setup, and specialised modules

to guarantee effective and secure handling of sensitive health-related enquiries. Figure 1 depicts the architecture of the Application Framework module.

An AI-powered IoT security system incorporates device-level encryption, stringent authentication mechanisms, and edge AI processing to facilitate real-time anomaly detection. Data is delivered securely from IoT devices via protected gateways to cloud servers, where sophisticated AI algorithms function. These algorithms perpetually scrutinise data patterns, identify irregularities, and initiate prompt security reactions or alarms. The solution guarantees adaptive threat mitigation and adherence to growing cybersecurity requirements by continuous monitoring, regular upgrades, and seamless connection with a Security Operations Centre (SOC). This comprehensive strategy strengthens the IoT ecosystem against possible attacks, providing strong and proactive security measures.

The Command and Execution Module embodies a sophisticated security framework that utilises AI to enhance the safeguarding of IoT devices. This execution model utilises machine learning methods for immediate danger identification, flexible reaction strategies, and ongoing self-education. This guarantees adaptive defence capabilities, efficiently addressing growing cyber threats. This novel technique markedly improves the security framework of IoT ecosystems, integrating efficiency, intelligence, and resilience to protect linked environments from emerging security threats.

5. METHODOLOGY

The strategy for improving IoT device security with AI commences with a thorough evaluation of the current IoT infrastructure. This phase identifies vulnerabilities and defines security requirements by collecting input from stakeholders, encompassing specific security issues, priorities, and operational restrictions. Subsequently, AI-based security solutions compatible with IoT contexts are identified, emphasising scalability, interoperability, and resource constraints. These solutions are subsequently pilot-tested in controlled settings to assess performance and tweak them based on feedback prior to full deployment.

The creation of algorithms is essential for enhancing IoT security. The process begins with the collection of varied datasets that exemplify both typical and atypical behaviours of IoT devices. The gathered data is subjected to preprocessing, during which noise is eliminated and characteristics are extracted to guarantee consistency and efficacy for model training. Appropriate AI methods, including machine learning models (e.g., Support Vector Machines, Random Forests, Neural Networks) and deep learning approaches (e.g., Convolutional Neural Networks, Long Short-Term Memory networks), are selected based on the established security requirements. These algorithms are subsequently trained on labelled datasets to identify potential security vulnerabilities. Upon completion of training, the models undergo validation using distinct datasets to confirm their efficacy and ability to generalise accurately to novel data.

Upon completion of training and validation, the algorithms are included into the IoT infrastructure, whether directly on the devices, through gateways, or via cloud-based systems. This integration guarantees that AI models can interact effortlessly with IoT devices, enabling real-time monitoring of device behaviours. APIs and communication interfaces are created to enable seamless data transfer between IoT devices and AI models. Real-time monitoring is an essential element of the security system, wherein AI algorithms scrutinise incoming data to find anomalies and deviations from typical behaviour.

The AI-driven system is engineered to be adaptive, allowing it to perpetually learn and evolve as new data is integrated. This adaptive learning guarantees the system's efficacy in identifying emerging dangers and reacting to alterations in device behaviour. Continuous improvement techniques are implemented to enhance the longevity and efficacy of the security system. These techniques entail periodic changes to the AI models to guarantee they remain ahead of emerging risks.

Personnel training is an essential component of the implementation plan. Personnel tasked with operating and maintaining the security system receive training on the use of AI-driven solutions, ensuring their proficiency in system management and troubleshooting. Moreover, comprehensive documentation is produced for the complete development, integration, and deployment process, facilitating easy reference and subsequent modifications. Collaboration among developers, vendors, and cybersecurity specialists is advocated throughout the process to augment the efficacy of the security measures.

Upon successful testing and refinement of the AI-driven security solution, it is implemented throughout the whole IoT infrastructure. Continuous real-time monitoring is conducted, including the integration of threat intelligence to adapt the system to emerging threats. The implementation is bolstered by consistent updates and continuous oversight, guaranteeing the system's robustness against evolving cybersecurity threats.

6. CONCLUSION AND FUTURE WORK

In conclusion, utilising AI technologies offers a substantial opportunity to improve the security of IoT devices. AI facilitates proactive threat detection, anomaly recognition, and adaptive defence strategies, enhancing the ability of IoT ecosystems to combat dynamic and developing cyber threats. The effective application of AI-driven security solutions necessitates overcoming various hurdles, including resource constraints, interoperability issues, and privacy concerns. Surmounting these obstacles necessitates cooperation among industry players, legislators, and researchers to devise solutions that emphasise security, privacy, and usability.

The continuous progress in AI algorithms and computational capabilities promises to further improve the efficacy of AI-driven security for IoT. By leveraging the synergy between AI and IoT, we can create robust defence mechanisms that safeguard linked systems and foster trust and confidence among users. Ultimately, AI-driven security will be essential in realising the complete potential of IoT while safeguarding it from emerging dangers.

Prospective Outlook: The incorporation of AI into IoT security holds significant promise for future developments. Numerous key pathways for subsequent investigation encompass:

Enhanced Threat Detection: As AI algorithms progress, they will provide increasingly sophisticated and effective threat detection capabilities. Utilising machine learning and deep learning methodologies, AI systems will enhance their capability to identify and mitigate previously unrecognised risks in real-time. This encompasses the capacity to scrutinise intricate behavioural patterns to detect anomalies that may signify security breaches.

Edge Computing Integration: Proximity of AI capabilities to IoT devices via edge computing can improve system responsiveness and diminish dependence on centralised servers. Edge AI enables IoT devices to independently identify and address hazards locally, enhancing the system's resilience and minimising delay in threat detection and response.

Privacy-Preserving Techniques: Given that IoT devices gather sensitive user information, privacy is a paramount concern. Future research may investigate AI-driven solutions that preserve privacy while successfully mitigating security issues. Methods like federated learning and homomorphic encryption enable data analysis while maintaining encryption, so safeguarding both privacy and security.

Interoperability Standards: The adoption of interoperability standards for AI-driven security solutions is crucial to allow seamless integration and collaboration among IoT devices. Creating open-source frameworks and protocols would facilitate the sharing of threat intelligence and the coordination of responses among various devices and systems, hence enhancing overall security across several IoT ecosystems.

Ethical Considerations: As AI increasingly integrates into IoT security, it is imperative to confront ethical challenges such as prejudice, justice, and responsibility. Subsequent research must investigate the ethical ramifications of AI-driven security solutions, guaranteeing their responsible deployment in accordance with society standards. Formulating ethical principles and frameworks will be essential to guarantee that AI-driven security solutions are both effective and equitable.

The future of AI-driven IoT security is promising, with significant opportunity for innovation. By concentrating on these domains of research and development, we may establish more secure, efficient, and privacy-conscious IoT ecosystems.

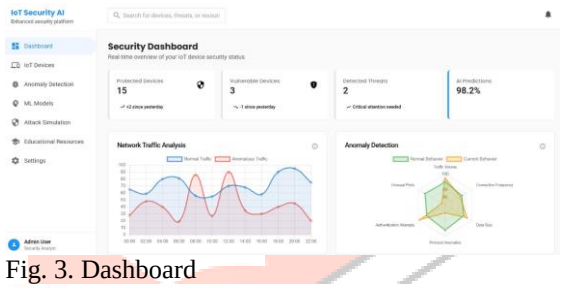

Fig. 3. Dashboard

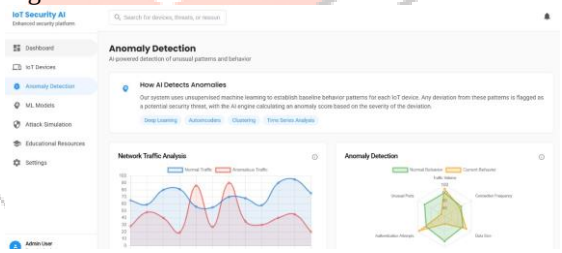

Fig. 4. Anomaly detection

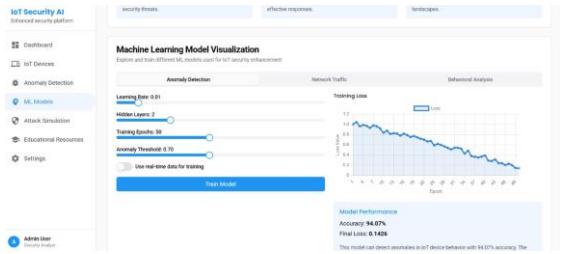

Fig. 5. ML Models

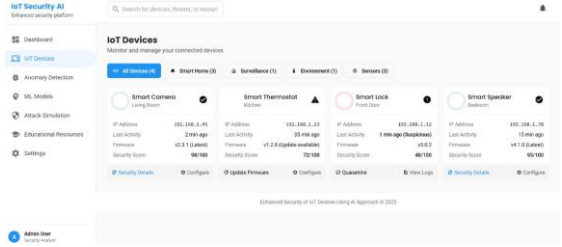

Fig. 6. Iot devices in check

8. REFERENCES

[1] A. Abane, M. Daoui, S. Bouzefrane, P. Muhlethaler," A Lightweight forwarding strategy for named data networking in low-end IoT", Journal of Network and Computer Applications, vol. 148, pp. 1-12, 2019..

[2] A.Singh, A. Payal, S. Bharti, A walkthrough of the emerging IoT paradigm: Visualizing inside functionalities, key features, and open issues, Journal of Network and Computer Applications, vol. 143, pp. 111151, 2019.

[3] C. Camara, P. Peris-Lopez, and J. E. Tapiador," Security and privacy issues in implantable medical devices: A comprehensive survey," Journal of biomedical informatics, vol. 55, pp. 272-289, 2015.

[4] H. Elazhary, Internet of Things (IoT), mobile cloud, cloudlet, mobile IoT, IoT cloud, fog, mobile edge, and edge emerging computing paradigms: Disambiguation and research directions, Journal of Network and Computer Applications, vol. 128, pp. 105140, 2019.

[5] J. Manyika, M. Chui, P. Bisson, J. Woetzel, R. Dobbs, J. Bughin, and D. Aharon, Unlocking the Potential of the Internet of Things, http://tinyurl.com/hnlhz8v, 2015.

[6] Juniper Research. internet of things connected devices to almost triple to over 38 billion units by 2020, 2015. http://www.juniperresearch.com/press/pressreleases/ iot connecteddevices-to-triple-to-38-bn-by-2020.

[7] J. Sengupta, S. Ruj, S. D. Bita," A Comprehensive survey on attacks, security issues and blockchain solutions for IoT and IIoT", Journal of Network and Computer Applications, pp. 1-50, Nov. 2019

[8] J. Zhou, Z. Cao, X. Dong, and A. V. Vasilakos," Security and privacy for cloud based IoT: Challenges", IEEE Commun. Mag., vol. 55, no. 1, pp. 26-33, Jan. 2017.

[9] Statista, Technology & Telecommunication, Consumer Electronics, source: IHS, https://www.statista.com/statistics/471264/iot-number-of connecteddevices-worldwide/, 2019

[10] S. Amendola, R. Lodato, S. Manzari, C. Occhiuzzi, and G. Marrocco," RFID technology for IoT-based personal healthcare in smart spaces," IEEE Internet of things journal, vol. 1, no. 2, pp. 144-152, 2014.

[11] V. Gazis," A Survey of Standards for Machine-to-Machine and the Internet of Things," in IEEE Communications Surveys & Tutorials, vol. 19, no. 1, pp. 482-511, Firstquarter 2017. doi: 10.1109/COMST.2016.2592948