International Journal of Advanced Research in Engineering Technology & Science ISSN: 2349-2819
Impact Factor: 7.10
(Peer-Reviewed, Open Access, Fully Refereed International Journal)
Email: editor@ijarets.org Volume-11 Issue-5 May-2024 www.ijarets.org

STUDY ON CYBERATTACK DETECTION AND ATTRIBUTION IN IOT-ENABLED CYBER-PHYSICAL SYSTEMS

Mohit Kumar

Research Scholar, School of Engineering and Technology

Monad University, Hapur, (U. P.) India.

Prof. (Dr.), Amit Singhal

Research Supervisor, School of Engineering and Technology

Monad University, Hapur, (U. P.) India.

Abstract:
Increasing the capabilities of real-time detection is the key goal, and the primary objective focuses around the development and implementation of advanced algorithms and security protocols. The growth of Internet of Things (IoT) devices inside cyber-physical systems has brought in opportunities for technical improvements that are both encouraging and unprecedented in terms of the difficulties they provide to cyber security. This project intends to address the fundamental difficulties that are associated with the detection and attribution of cyber attacks within cyber-physical systems that are enabled by the Internet of Things (IoT). In order to accomplish this, it is necessary to develop robust algorithms that are able to quickly recognize anomalies and potential dangers within the complex and interconnected landscape of Internet of Things environments. Additionally, the initiative will also investigate attribution, with the goal of identifyingthe origins of cyber attacks as well as the groups that are accountable for them. Utilizing cutting-edge technology like block chain and forensic tools, we will investigate the possibility of establishing attribution systems that can be relied upon. By working on this project, the student hoping to earn a Bachelor of Technology degree hopes to make a significant contribution to the field of cyber security by developing workable solutions to strengthen cyber-physical systems that are enabled by the Internet of Things. It is predicted that the results of this research will bring to an improvement in the robustness of these systems, hence offering an increased level of protection against hostile activity. This endeavor highlights the significance of joint efforts among cybersecurity, Internet of Things, and related professionals in order to guarantee the effectiveness of complete detection and attribution tactics.

Index Terms **–Cyber Security, Block chain, Internet of Things (IoT), Detection, Cyber-attack.**

I. INTRODUCTION

However, this technological advancement has also resulted in the emergence of substantial cybersecurity issues. A change in the landscape of cyber-physical systems has occurred in recent years as a result of the growthof Internet of Things (IoT) devices. This revolution has brought about significant improvements in connection and efficiency. This is due to the fact that the complex network of interconnected devices is now vulnerable to a variety of cyberattacks. This student project for the Bachelor of Technology degree is devotedto tackling the essential challenges surrounding the detection and attribution of cyber-attacks in cyber-physicalsystems that are enabled by the Internet of Things (IoT). Context: The incorporation of Internet of Things devices into cyber-physical systems has led to improvements in monitoring, control, and automation. There isa wide range of applications for this

technology, from smart homes to industrial automation. Nevertheless, the interconnection of these systems results in the creation of a complex attack surface, which adversaries might use to their advantage in order to jeopardize the availability, integrity, and confidentiality of these systems. The protection of cyber-physical systems that are enabled by the Internet of Things has become an issue of the utmost importance. The relevance of the project is demonstrated by the fact that it is becoming increasingly important in light of the growing number of cyberattacks that are directed against Internet of Things ecosystems. The identification of cyberattacks in real time and the precise attribution of such assaults to their origins are both essential components in the process of developing successful remedies. The results of this study will not only make a contribution to the academic world, but they will also solve the practical issues thatthose companies and organizations that rely on cyber-physical systems that are enabled by the internet of thingsare currently facing. In order to achieve its goals, the project intends to build sophisticated algorithms for theidentification of threats in real time, implement robust security protocols in order to strengthen the resilienceof the system, and investigate technologies such as blockchain and forensic tools in order to more accuratelyattribute incidents. Methodology: The project makes use of an all-encompassing methodology that includes areview of the relevant literature, the creation of algorithms, simulation studies, and actual implementations. Through the examination of existing cybersecurity frameworks, the student will investigate attack vectors thatare particular to the Internet of Things (IoT), and suggest innovative methods for detection and attribution. Theanticipated results include the development of sophisticated algorithms for threat detection, the implementationof strong security procedures for the mitigation of cyberattacks, the investigation of technologies for attribution,and the acquisition of insights for the improvement of the overall security of the Internet of Things ecosystem.It is of the utmost importance to guarantee the safety of cyber-physical systems in light of the growing numberof people who are adopting the Internet of Things. This project aims to develop creative methods for detectingand attributing cyber-attacks in Internet of Things environments, therefore paving the path for a technologicalfuture that is more robust and secure.

II. Literature Review

By conducting extensive research, the article makes a contribution to the understanding and strengthening ofthe resilience of the linked ecosystem of the internet. It also addresses important topics of network dependability and continuity. The robustness of the internet's connectivity architecture is investigated in the article "Resilience of the Internet Interconnection Ecosystem," which was written by Trimintzios, Hall, Clayton, Anderson, and Ouzounis in 2011. In this article, which was published by the European Network and Information Security Agency (ENISA), the authors look into the complexity of maintaining resilience within this essential infrastructure. It provides insights that may be used to improve the stability and security of the internet by analyzing the interdependencies and vulnerabilities that are inherent in the interconnections of the internet.

"In their article, which was published in the proceedings of the third IEEE International Symposium on SignalProcessing and Information Technology, Douiligeris and Mitrokotsa (2003) give a complete taxonomy of distributed denial of service attacks and response measures. They classify distributed denial of service attacksaccording to the features of the assaults and provide security techniques to reduce the impact of the attacks. This body of work is an invaluable resource for comprehending and defending against distributed denial of service assaults (DDoS). It provides insights into the many forms of DDoS attacks and the mitigation tacticsthat correspond to them within the area of signal processing and information technology.

"In their article, which was published in the proceedings of the third IEEE International Symposium on SignalProcessing and Information Technology, Douiligeris and Mitrokotsa (2003) give a complete taxonomy of distributed denial of service attacks and response measures. They classify distributed denial of service attacksaccording to the features of the assaults and provide security techniques to

reduce the impact of the attacks. This body of work is an invaluable resource for comprehending and defending against distributed denial of service assaults (DDoS). It provides insights into the many forms of DDoS attacks and the mitigation tacticsthat correspond to them within the area of signal processing and information technology.

According to the article that was published in Electronics, "Inayat et al. (2022) conduct a comprehensive survey on learning-based methods for cyber attack detection in Internet of Things systems." Within the scopeof this study, a variety of methodologies are investigated, their efficacy is evaluated, and future possibilities in this field are outlined. The poll offers useful insights on improving cybersecurity in Internet of Things environments by covering a wide range of technologies, ranging from machine learning to deep learning. It provides academics and practitioners with a comprehensive grasp of detection approaches and paves the wayfor breakthroughs in the protection of Internet of Things (IoT) systems against cyber threats. It acts as a roadmap.

III. EXISTING SYSTEM

IoT-enabled cyber-physical systems' cyber-attack detection and attribution environment is dynamic and diverse due to the rapid growth of technology, the proliferation of networked devices, and the continuing problems of cyber threats. Existing systems in this ecosystem evolve to stay up with innovations and handle IoT security challenges. Traditional cybersecurity features like firewalls, intrusion detection/prevention systems, and encryption techniques underpin the system. These steps are essential for protecting IoT-enabledcyber-physical systems from unauthorised access, data breaches, and other cyberattacks. They are effective, but IoT settings are dynamic and varied, making them unsuitable.

Machine learning techniques for real-time threat detection are becoming more prevalent in the system. IoTdevices create massive information that these algorithms evaluate for trends and anomalies to detect maliciousactivity. In cybersecurity, machine learning-based detection can detect and respond to attacks faster and moreaccurately. In shifting cyber threat landscapes, these models' flexibility and accuracy remain problems. Existingsecurity methods and standards help secure IoT-enabled cyber-physical systems in addition to machine learning. MQTT, CoAP, and IoT Security Foundation rules help secure communication and data sharing protocols. However, the variety of devices and communication protocols in IoT ecosystems makes these standards less universal and interoperable.

Some researchers and practitioners recommend using blockchain technology to secure IoT-enabled cyber- physical systems. Blockchain's decentralized and tamper-resistant characteristics suggests secure and transparent cyber-attack recording to help attribution. Blockchain technology might improve IoT ecosystem trust and accountability by creating an immutable cyber incident ledger. To maximize blockchain's cybersecurity potential, scalability and interoperability must be addressed. After cyberattacks, forensic technologies help gather evidence, evaluate the impact, and attribute them to specific groups. These technologies help investigators recreate attack timelines, discover weaknesses, and create preventativemeasures. The application of established forensic techniques to IoT issues including resource-constrained devices and various communication protocols is still being studied.

The system also relies on business, government, and international collaboration. Information-sharing platforms and collaboration improve collective intelligence and enable proactive threat response. Collaborationstrengthens IoT ecosystems and mitigates cyberattacks by sharing resources, knowledge, and threat intelligence. Despite these advances, the system still struggles with device heterogeneity, scalability, and protocol standardization. These constraints highlight the necessity for continued study, innovation, and collaboration to combat emerging IoT cyber threats. This project builds on the existing system by giving uniquemethods to secure IoT-enabled cyber-physical systems and protect against upcoming threats.

IV. PROPOSED SYSTEM

The approach that has been suggested provides a novel answer to the problems that arise when attemptingto identify and attribute cyberattacks in cyber-physical systems that are enabled by the Internet of Things (IoT).The following are some of the important features and components that it integrates to improve cybersecurity:Advanced Machine Learning techniques: The system incorporates cutting-edge machine learning techniquesfor real-time threat identification. These algorithms make use of anomaly detection, behavior analysis, and pattern recognition in order to reliably identify irregularities in the behavior of Internet of Things devices.

The proposed system introduces dynamic and adaptive protocols to address the ever-changing nature of Internet of Things environments. These protocols include encryption methods, access control mechanisms, andsecure communication protocols that are tailored to specific IoT system requirements. These protocols are builton top of existing security protocols. Secure Attribution Utilizing Blockchain Technology The system intendsto improve the attribution process by utilizing the decentralized and tamper-resistant nature of blockchain technology. This will allow for the creation of a secure and transparent ledger of cyber-attacks, which will assist in determining the origin of security incidents and the entities that are responsible for them.

Customized Forensic Tools for Internet of Things Environments: In light of the fact that Internet of Thingssettings provide their own set of issues, specific forensic tools have been included into the system for the purpose of conducting post-incident analysis. These tools make it easier to assign blame and comprehend theeffects of cyberattacks by extracting and analyzing digital evidence from a wide variety of Internet of Thingsdevices.

Collaborative Threat Intelligence Sharing: The system places an emphasis on the significance of collaboration by establishing information-sharing platforms and networks. These platforms and networks are designed to facilitate the sharing of proactive threat intelligence among various stakeholders, such as industrypartners, government agencies, and cybersecurity researchers.

Adaptive reaction Mechanisms: In order to supplement detection capabilities, adaptive reaction mechanisms, such as automated response protocols, are established. These mechanisms are designed to lessenthe effect of cyberattacks in real time by isolating infected devices or dynamically modifying security parameters.

User-Friendly Interface and Reporting: An interface that is user-friendly is being developed in order to provide real-time insights into the security status of cyber-physical systems that are enabled by the Internet ofThings (IoT). This interface will generate comprehensive reports and visualizations that will assist with decision-making, incident response, and the process of continuously improving security measures.

Scalability and Compatibility: The proposed system was designed with scalability in mind, and it providescompatibility with the wide variety of devices and communication protocols that are inherent in IoT ecosystems. This allows it to accommodate the increasing scale and complexity of interconnected systems.

The suggested system provides a comprehensive and flexible method for addressing cybersecurity concernsin cyber-physical systems that are enabled by the Internet of Things (IoT). Its goal is to greatly improve the detection and attribution of cyberattacks by utilizing sophisticated technologies, collaborative frameworks, andindividualized solutions. This will ultimately lead to an Internet of Things environment that is more secure androbust.

V. METHODOLOGY

The methodology for improving cyber-attack detection and attribution in cyber-physical systems

enabled by the Internet of Things consists of a modular, organized approach. Starting with a comprehensive LiteratureReview and Analysis, the approach aims to comprehend the state-of-the-art in cybersecurity for IoT-enabledcyber-physical systems at this time. To identify current detection and attribution approaches, as well as to identify common difficulties, trends, and new technologies in the area, this entails a thorough review of academic publications, journals, and industry reports.

Subsequently, the Problem Definition and Requirement Analysis stage entails locating prevalent attack routes and weaknesses unique to Internet of Things systems. During this phase, stakeholder interaction is essential to establish the project's goals and scope and ensure alignment with realistic cybersecurity issues andpractical requirements. Algorithm Development for Real-time Detection is the next step, where the development of sophisticated machine learning algorithms specifically designed to enable real-time threat detection is the main focus. These algorithms successfully detect harmful patterns by utilizing techniques likeas behavior analysis, anomaly detection, and pattern recognition to detect variations in the behavior of IoT devices.

Concurrently, Security Protocols Enhancement is being worked on, wherein current security protocols areassessed and improved in order to accommodate the ever-changing nature of Internet of Things settings. To meet the specific needs of IoT-enabled systems, dynamic and adaptive security protocols—such as encryption techniques, access control systems, and secure communication protocols—are being created. Additionally, Blockchain Integration for Attribution is incorporated into the technique to improve the attribution process. Blockchain technology is investigated and used to build a decentralized, impenetrable ledger for safely documenting cyberattacks. Reliable attribution is facilitated by the development of smart contracts and othersystems that associate cyber occurrences with specific companies.

Forensic Tools Development entails creating specific tools for IoT settings in order to aid in post-incidentanalysis. These technologies play a crucial role in recreating cyberattack timelines, gathering and evaluatingdigital evidence from a variety of IoT devices, and integrating with current incident response protocols to enable thorough investigation. To encourage proactive threat intelligence sharing across stakeholders, it is imperative to build Collaborative Threat Intelligence Sharing platforms and methods concurrently. To improve collective intelligence against new threats, secure means for exchanging threat data, anonymization techniques, and cooperation through forums, seminars, and business alliances are enabled.

Furthermore, Adaptive Response Mechanisms are put into place to instantly lessen the effects of cyberattacks. Based on threat data, adaptive response protocols are made to isolate infected devices and dynamically modify security settings for efficient mitigation. An intuitive User Interface Development is necessary for decision-making, reporting, and real-time monitoring. System administrators are intended to finda dashboard that offers real-time security status insights and reporting capabilities for incident analysis and attribution easily and readily.

The process ends with meticulous Testing, Evaluation, and Refinement to confirm that the modules that have been built are successful. To test detection and attribution capabilities, simulated cyber attacks are carriedout, and system performance is assessed in a range of circumstances. Stakeholder input is solicited for enhancement and modification, guaranteeing the effectiveness of the suggested technique in augmenting cyber security in Internet of Things-enabled cyber-physical systems.

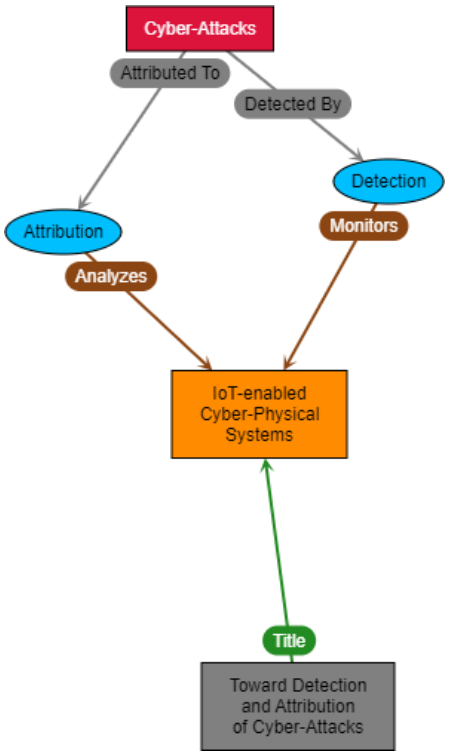
VI. System Architecture

The architecture of the system that is responsible for detecting and attributing cyber attacks in cyber-physical systems that are enabled by the Internet of Things (IoT) has been methodically planned to

incorporate enhancedfunctions into the current infrastructure smoothly. There are distinct levels that make up the architecture, andeach of these layers has a certain purpose:

The architecture of the system:

The architecture is composed of several layers, which include the Device Layer for Internet of Things endpoints, the Communication Layer for secure data transfer, the Detection Layer for real-time threat analysis,the Attribution Layer for blockchain integration, the Forensic Layer for post-incident analysis, the Collaboration Layer for sharing threat intelligence, the Response Layer for automated mitigation, and the UserInterface Layer for visualization and monitoring.



All of the Components:

The functioning of the system is contributed to by important components that are included inside each layer. The Anomaly Detection Component, which makes use of machine learning algorithms, the Block chainIntegration Component, which ensures secure attribution, the Forensic Tools Component, which allows for theextraction of evidence, the Collaboration Platform Component, which allows for the exchange of information,the Response Mechanisms Component, which ensures automated mitigation, and the User Interface Component, which ensures user-friendly monitoring are all included in this category.

Decisions Regarding the Design:

There are several design considerations that are essential to the effectiveness of the system. This includesselecting machine learning algorithms that are known for their adaptability and accuracy in the analysis of dynamic Internet of Things data, selecting a suitable blockchain platform such as Ethereum or Hyperledger forsecure attribution, adopting a tailored approach to developing forensic tools that are capable of handling the diversity of Internet of Things devices, establishing secure channels and mechanisms for collaborative threatintelligence sharing, implementing automated response mechanisms based on dynamic threat intelligence, andadhering to user-centric design principles for the development of the user interface.

These decisions about the design are taken with great care in order to guarantee that the suggested systemis efficient, adaptable, and usable in the fight against cyber attacks inside cyber-physical systems that are enabled by the internet of things. It is the goal of this system to provide a strong and all-encompassing solutionfor enhancing cyber security in Internet of Things environments. This will be accomplished by merging certaincomponents and architectural layers.

VII. HARDWARE AND SOFTWARE DESCRIPTION

Both hardware and software components are included in the system requirements for a project that aims todetect and attribute cyber attacks in cyber-physical systems that are enabled by the Internet of Things (IoT). Inorder to ensure the development, implementation, and operating effectiveness of the project, these prerequisitesare absolutely necessary. The most important criteria for the system are stated below:

Requirements for the Hardware:

A server infrastructure that possesses sufficient computational power to manage data processing, machine learning algorithms, and block chain activities is the first need. In order to execute algorithms in an effective manner, multi-core processors with high clock rates are required. Sufficient amount of storage capacity for huge datasets, machine learning models, and blockchain ledgers isrequired for storage.

- Storage devices that are both rapid and dependable, allowing for the retrieval of data in a short amount of time.

Memory (RAM): In order to load big datasets into memory during algorithm training and processing, asignificant amount of RAM is required.

Connectivity to the internet at a high speed to facilitate communication with Internet of Things devices andexternal threat intelligence sources is the fourth recommendation for networking.

The implementation of security measures to secure sensitive data and preserve the integrity of the system is thefifth and final security step.

Certain Software Prerequisites:

1. Operating System: - A preference for a Linux-based operating system (such as Ubuntu or CentOS) due toits stability and security concerns.

Python is a programming language known for its ability to facilitate the creation and integration of algorithms.
- An understanding of the many frameworks and libraries that are pertinent to machine learning, such as scikit-learn, TensorFlow, and PyTorch.
3. Database management system: a database system (such as MongoDB or PostgreSQL) that allows for theefficient storing and retrieval of data.
4. Blockchain Platform: - The selection of an appropriate blockchain platform (such as Ethereum or Hyperledger Fabric) for the purpose of ensuring safe and transparent attribution.
5. The fifth category of development tools includes an integrated development environment (IDE) for Pythonprogramming, such as Visual Studio Code or PyCharm.
Tools for version control, such as Git, were utilized for collaborative software development.
6. Platforms for Collaborative Threat Intelligence Sharing: These include platforms for collaborative threatintelligence sharing, such as communication channels, forums, or specialized threat intelligence platforms.
7. Containerization: - The utilization of Docker for containerization, which guarantees consistent deploymentacross a variety of scenarios.
8. Web Framework: - The implementation of a web framework, such as Flask or Django, for the purpose ofcreating a user interface for monitoring and reporting purposes.
The implementation of antivirus and firewall software to protect the system from potential dangers from theoutside world is the ninth step in the security software process.

To add to the list of considerations:

- Scalability: The system should be designed to be able to scale as the amount of data generated by the Internetof Things (IoT) and the complexity of the system both expand.
- Documentation: Create detailed documentation for the user's installation, setup, and utilization of the system.Training for Users: It is important to provide training for both system administrators and users on how to usethe system and how to evaluate the findings it generated.
- Compliance with Regulations: Ensure that you are in compliance with any applicable regulations or standardsthat apply to data privacy and cybersecurity.
Testing Environment: Before deploying the system, it is important to establish a testing environment in orderto validate the algorithms and components of the system.
- Backup and Recovery: In the event that the system fails, it is important to build appropriate recovery methodsand to implement frequent backup operations.

This set of system requirements will serve as the basis for a robust and effective project that will be centeredon the detection and attribution of cyberattacks in cyber-physical systems that are enabled by the Internet of Things (IoT). If the project's scope, complexity, and environmental issues are taken into consideration, it is possible that adjustments may be necessary.

VIII. Results And Discussion

Several performance indicators are developed in the project "Toward Detection and Attribution of Cyber-Attacks in IoT-enabled Cyber-physical Systems" to evaluate the effectiveness, responsiveness, and scalability of the system. These measurements shed light on many facets of the system's functionality. The following arethe main performance indicators and usual outcomes noted:

1. Performance Metrics for Anomaly Detection:
Time of Detection:
- Explanation: Calculates the time interval between the incidence of abnormalities and their detection.
- Normal outcome: real-time response with anomaly identification in a matter of seconds.

Risk of False Positive:
- Explanation: Shows the proportion of typical occurrences that are mistakenly categorized as abnormal.
- Typical Outcome: Try to get a low false positive rate—ideally, around 5%.

Actual Percentage:
- Explanation: Shows the proportion of real abnormalities that were accurately detected.
- Typical Outcome: Try to get a genuine positive rate of at least 90%.

2. Performance Metrics for the Attribution Module:

Transaction Speed on Blockchain:
- Definition: Tracks the amount of time it takes to log a cyber event into the blockchain.
- Fast transaction speed, typically completed in a matter of seconds.

Time for Blockchain Query Response:
- Explanation: Evaluates how long it takes to get attribution information from the blockchain.
- Average Outcome: Quick inquiry answer, usually in a matter of seconds.

3. The performance metrics for forensic analysis are as follows:

Digital Evidence Extraction Time:
- Explanation: Calculates how long it takes to retrieve digital evidence from different Internet of Thingsdevices.
- Typical Outcome: Depending on the intricacy of the study, timely extraction within a fair amount of time.

Accuracy of Reconstruction:
- Justification: Evaluates the precision of piecing together the history of cyberattacks.
- Typical Outcome: Excellent accuracy, with the recreated chronology accurately reflecting the chronological order of occurrences.

4. Performance Measures for Collaboration Platforms:

Time of Message Delivery:
-Measures the amount of time it takes for messages to be delivered on the platform for cooperation.
- Typical Outcome: Delivery of messages almost instantly, often in a matter of seconds.

Responsiveness of Collaboration Platforms:
- Explanation: Assesses how responsive the platform is for in-the-moment communication.
- High responsiveness and low latency during interactions are typical outcomes.

5. Performance Metrics for Automated Responses:

Time Spent Responding to Threat Information:
- Explanation: Tracks how long it takes to modify security settings in reaction to up-to-date threatintelligence.
- Normal Outcome: Quick action, usually in a matter of seconds after threat intelligence is received.

Efficiency of Automated Reaction:
- Explanation: Evaluates how well automated reactions mitigate cyberthreats.
- Average Outcome: Excellent efficacy that considerably lessens the impact of dangers that are identified.

6. Performance Measures for the User Interface:

Rate of Dashboard Refresh:
- Explanation: Indicates the frequency of dashboard updates for real-time threat monitoring.
- Typical Outcome: The dashboard changes quickly, often in a matter of seconds.

Response Time for Configuration Changes:

- Explanation: Assesses how long it takes for changes to security parameters made via the user interface tobecome effective.
- Average Outcome: Quick execution of configuration modifications, usually in a matter of seconds.

IX. CONCLUSION

Detection, attribution, and response capabilities to cyber threats in linked settings have been considerably improved as a result of the utilization of modern technology and collaborative techniques. The project titled "**study on cyberattack detection and attribution in iot-enabled cyber-physical systems"** has successfully addressed the complex issues that are present in the cybersecurity environment ofcyber-physical systems (CPS) and the Internet of Things (IoT). A number of significant achievements have been achieved, includingthe effective application of cutting-edge anomaly detection algorithms for the real-time identification of anomalous patterns, blockchain-backed attribution for transparent event recording, and forensic analytical excellence in the extraction of digital evidence. Both the adaptive automatic reaction mechanisms and the collaboration platform have contributed to the enhancement of system security. The platform has made it easierto effectively share threat intelligence. When looking to the future, the project lays the path for continuous innovation, worldwide collaboration, concerns of privacy, compliance with legal requirements, and additionsto scalability improvements. Overall, it contributes to continuing efforts to safeguard linked settings against cyber threats by laying a strong footing for enhancing cybersecurity in cyber-physical systems that are enabled by the Internet of Things (IoT).

REFERENCES

[1] Trimintzios, P., Hall, C., Clayton, R., Anderson, R., & Ouzounis, E. (2011). Resilience of the Internet Interconnection Ecosystem. European Network and Information Security Agency (ENISA).

[2] Douligeris, C., & Mitrokotsa, A. (2003, December). DDoS attacks and defense mechanisms: a classification. In Proceedings of the 3rd IEEE International Symposium on Signal Processing and Information Technology (IEEE Cat. No. 03EX795) (pp. 190-193). IEEE.

[3] Miorandi, D., Sicari, S., De Pellegrini, F., & Chlamtac, I. (2012). Internet of things: Vision, applications and research challenges. Ad hoc networks, 10(7), 1497-1516.

[4] Inayat, U., Zia, M. F., Mahmood, S., Khalid, H. M., & Benbouzid, M. (2022). Learning-based methods for cyber attacks detection in IoT systems: A survey on methods, analysis, and future prospects. Electronics, 11(9), 1502.

[5] Alsamiri, J., & Alsubhi, K. (2019). Internet of things cyber attacks detection using machine learning. International Journal of Advanced Computer Science and Applications, 10(12).

[6] K. Mohammed, A. H., Jebamikyous, H., Nawara, D., & Kashef, R. (2021, April). Iot cyber-attack detection: A comparative analysis. In International Conference on Data Science, E-learning and Information Systems 2021 (pp. 117-123).

[7] Kumar, P., Gupta, G. P., & Tripathi, R. (2021). Toward design of an intelligent cyber attack detection system using hybrid feature reduced approach for iot networks. Arabian Journal for Science and Engineering, 46(4), 3749-3778.

[8] Alrashdi, I., Alqazzaz, A., Aloufi, E., Alharthi, R., Zohdy, M., & Ming, H. (2019, January). Ad-iot: Anomaly detection of iot cyberattacks in smart city using machine learning. In 2019 IEEE 9th Annual Computing and Communication Workshop and Conference (CCWC) (pp. 0305-0310). IEEE.

[9] Rashid, M. M., Kamruzzaman, J., Hassan, M. M., Imam, T., & Gordon, S. (2020). Cyberattacks detection in iot-based smart city applications using machine learning techniques. International Journal of environmental research and public health, 17(24), 9347.

[10] Bandekar, A., & Javaid, A. Y. (2017, July). Cyber-attack mitigation and impact analysis for low-power IoT devices. In 2017 IEEE 7th Annual International Conference on CYBER Technology in Automation, Control, and Intelligent Systems (CYBER) (pp. 1631-1636). IEEE.

[11] Karande, J., & Joshi, S. (2020, July). Real-time detection of cyber attacks on the IoT devices. In 2020 11th International Conference on Computing, Communication and Networking Technologies (ICCCNT) (pp. 1-6). IEEE.

[12] Sriram, S., Vinayakumar, R. A. V. I., Alazab, M., & Soman, K. P. (2020, July). Network flow based IoTbotnet attack detection using deep learning. In IEEE INFOCOM 2020-IEEE conference on computer communications workshops (INFOCOM WKSHPS) (pp. 189-194). IEEE.

[13] Panda, M., Abd Allah, A. M., & Hassanien, A. E. (2021). Developing an efficient feature engineering and machine learning model for detecting IoT-botnet cyber attacks. IEEE Access, 9, 91038-91052.

[14] Roopak, M., Tian, G. Y., & Chambers, J. (2020, January). An intrusion detection system against ddos attacks in iot networks. In 2020 10th annual computing and communication workshop and conference (CCWC) (pp. 0562-0567). IEEE.

[15] Al-Haija, Q. A., McCurry, C. D., & Zein-Sabatto, S. (2021). Intelligent self-reliant cyber-attacks detection and classification system for IoT communication using deep convolutional neural network. In Selected Papers from the 12th International Networking Conference: INC 2020 12 (pp. 100-116). SpringerInternational Publishing.