Data Science Insights
Vol. 2, No. 1, 2024

ISSN 3031-1268 (online)

Contents lists available at https://citedness.com/index.php/jdsi

Data Science Insights

Journal Page is available to https://citedness.com/index.php/jdsi

Research article

Enhancing IoT Security: A Synergy of Machine Learning, Artificial Intelligence, and Blockchain

Ahmad Anwar Zainuddin[1,], Haziqah Sairin[2], Izzah Atirah Mazlan[3], Nur Najma Aisyah Muslim[4], Wan Afiqah Syahmina Wan Sabarudin[5]*

[1,2,3,4] Dept. Information Technology, International Islamic University Malaysia. Kuala Lumpur, Malaysia
email: [1] anwarzain@iium.edu.my, [2] haziqah.s@live.iium.edu.my, [3] atirah.mazlan@live.iium.edu.my, [4] najma.aisyah@live.iium.edu.my , [5] afiqah.syahmina@live.iium.edu.my
** Correspondence:Ahmad Anwar Zainuddin (anwarzain@iium.edu.my)*

ARTICLE INFO

Article history:
Received 18 January 2024
Revised 25 February 2024
Accepted 27 February 2023
Available online 28 February 2024

Keywords:
Internet of Things (IoT)
Artificial Intelligence (AI)
Machine Learning (ML)
Blockchain technology
Cybersecurity
Privacy
Data storage
Cyberattacks
K-nearest neighbour

Please cite this article in IEEE style as:
A. A. Zainudin, A. Siswanto and Y.Z. Pratama, "Enhancing IoT Security: A Synergy of Machine Learning, Artificial Intelligence, and Blockchain ", Data Science Insights, vol. 2, no. 1, pp. 9-19, 2024.

ABSTRACT

With the advancement of technological age, the growth of technology not only affecting the network and security but also the Internet of Things (IoT), this invites the need for robust cybersecurity solutions become increasingly important. To further enhance the existing safety mechanisms used in the IoT industry, the assimilation of Machine Learning (ML) with Artificial Intelligence (AI) along with the technology of blockchain can further offers a high potential solution in order to face the challenges faced in the IoT security. ML and AI algorithms can enhance the detection and prevention by reviewing variety of data, recognizing patterns and predicting the potential vulnerabilities of the cyber threats in IoT. Blockchain, on the other hand, provides a decentralized and tamper-proof platform for secure data storage and transactions. By leveraging these technologies, IoT systems can achieve a sustainable security, ensuring the protection of sensitive and important information as well as protecting the Confidentiality, Availability, and Integrity (CIA) triad of the infrastructure of the network. This research incorporates the variety of machine learning approaches, including the trees of decision, the K-nearest neighbours, the artificial neural networks, convolutional neural networks, the support of vector machines, Bayesian networks, ensemble classifiers, genetic programming, logistic regression as well as the deep learning tactics. Through this, the deriving insights of raw data can then help these technologies to aim and create a modern and dynamically improved security solutions for the evolving landscape of IoT devices. Future research should focus these upcoming issues in order to fully comprehend potential of ML applications in security intelligence of IoT.

Correspondence:
Kulliyyah of Information and Communication Technology, International Islamic University Malaysia, 53100 Jalan Gombak, Selangor, Malaysia.

1. Introduction

The explosive development of the Internet of Things (IoT) [1] has created greater demand for strong cybersecurity to protect valuable data. With the growing number of elements linked to one another, traditional security practices are no longer adequate. This has caused researchers to consider the application of AI in IoT cybersecurity. Focusing on machine learning and blockchain technology [2] as possible remedies, this research paper explores the role of AI in IoT security. This paper will look at the obstacles facing IoT security and show

how AI frameworks may offer long-term IoT network protection. With AI technologies, such as anomaly detection and threat intelligence, IoT security can be strengthened to minimize risk of loss or leakage.

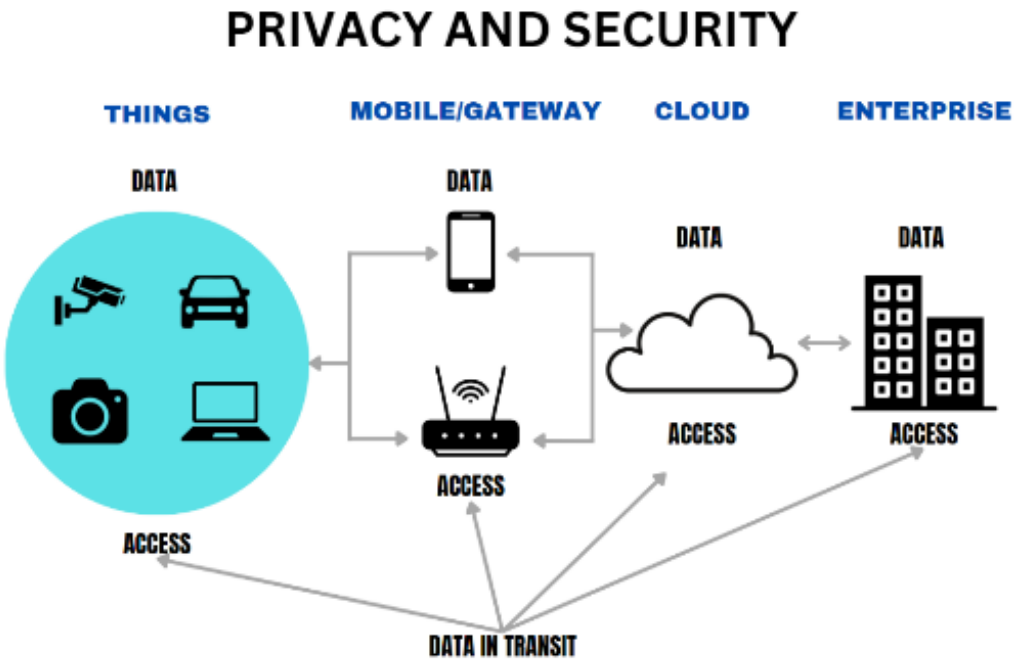

Fig. 1. Various types of data in transit for IoT security and privacy

Figure 1 shows the various types of data in transit for IoT security and privacy. Internet of Things (IOT) is a network of physical objects [3] ranging from mobile phones, computers and printers to sensor-enabled electrical appliances to smart cars. These things are all connected so that they can collect the data needed for feeding computing systems. These things can be as simple as everyday devices such as smartphones and home appliances or may be much more complex machinery like industrial installations or cars. The concept of an IoT opens the door to a networked cloud of communicating and interacting objects, which can provide us with huge amounts useful data. From enhancing the efficiency of industry, to smart cities and personalized experiences for individuals, this connectivity and exchange of data has huge potential in many areas of our lives. Cybersecurity has also become a problem with the increase in connectivity and exchange of data characteristic of the IoT, targeted by cyberattacks [4]. As thus, securing the IoT devices and networks is an important step in unleashing the full potential of the Internet of Things, without compromising privacy and user data.

Artificial Intelligence (AI) techniques are an integral part of safe cybersecurity on the Internet of things (IoT) [5]. With high-tech algorithms and machine learning models behind them, AI can find and stop a lot of security threats. These methods can even look at the huge data batches generated by IoT devices, and detect anomalies and attempts to break in. Two common applications of the machine learning algorithm in IoT security are the recognition of anomalous behavior and classification data. The three most commonly used algorithms are Decision Trees, Support Vector Machines and Random Forests. In addition, artificial intelligence (AI)-based anomaly detection, intrusion detection and behavioral analysis enhance the overall cyber-security of IoT. However, combining the power of AI with the Internet of Things can build a system to warn about new threats coming online in real time. This could prove an effective means of maintaining security for IoT devices.

Machine Learning-based anomaly detection [6] is a key element in IoT security because it helps detect and deal with possible threats. Artificial intelligence and machine learning algorithms can pinpoint abnormalities with real-time reporting, giving decision makers time to act before risks arise. This aids in preserving the integrity of IoT systems while ensuring that their information is secure. via such an approach, anomalous behaviors and patterns that could signal a security breach or even malicious activity are identified. IoT environments will have its overall level of security enhanced as well.

This paper emphasizes several methods in internet of things (iot) security intelligence. The first section outlines the introduction of cybersecurity and machine learning, and Section 2 displays a literature review of the survey of security intelligence. Section 3 is devoted to methodology. Section 4 contains recommendations to innovate, and Section 5 is the article's conclusion.

2. Literature Review

This review of the literature offers a concise synopsis of at least 15 publications that were released in 2019 and are important sources for information on Internet of Things and machine learning applications in networking systems. The table shows a few previous articles related to blockchain technology.

Table 1. Survey of Security Intelligence of IoT

Article	Key Findings/ Argument	Supporting Evidence/ Sample Characteristics/ Methods	Strength/ Limitations	Significance/ Implications
[7]	The paper focuses on using machine learning and deep learning based IoT security solutions to safeguard systems and applications from threats and cyberattacks. It draws attention to the difficulties with IoT security and the requirement for intelligent security systems built on cutting-edge technology to solve these issues.	The paper covers a variety of deep learning architectures, machine learning approaches, and modelling strategies for intelligent security in Internet of Things environments. It also highlights the need for security solutions by presenting various IoT system layers and related security concerns.	The article's strength is its thorough analysis of the problems with IoT security and how machine learning is being used to solve them. However, the document does not delve into specific case studies or real-world implementations of the discussed security solutions.	The paper is important because it shows how machine learning and deep learning methods may be used to create data-driven models for IoT security intelligence, which can help construct efficient security systems for IoT devices. It highlights how important cutting-edge security solutions are.
[4]	An organised survey of the literature on the application of AI techniques for cybersecurity attack detection in IoT environments is presented in this article. The paper offers an artificial intelligence roadmap for identifying cybersecurity threats within IoT devices and investigates both machine learning and deep learning approaches for IoT security.	Using database sources such SCOPUS, IEEE Xplore, MDPI, Web of Science, a literature search was conducted. Eighty carefully chosen research articles, mostly original and a few reviews, that were published between 2016 and 2021 were included in the study.	The study follows the PRISMA guidelines and provides a comprehensive overview of application of AI methods for detecting attacks in IoT. However, it is limited by the exclusion of non-English articles and the focus on articles published between 2016 and 2021.	The results have consequences for IoT security and AI researchers and practitioners. The document includes suggestions for further research and delivers insightful information about the application of AI techniques for cybersecurity attack detection in IoT.
[8]	The most popular machine learning (ML) classifiers for cyber-attack detection in the field of cyber security include probabilistic, decision tree, deep learning, artificial neural networks, instance-based learning, active machine learning, rule-based learning, kernel function-based classifier, logistic regression, ensemble classifiers, and genetic programming.	A thorough examination of the literature was done in accordance with Kitchenham and Charters' recommendations. Using predefined search strings, searches were done in the ScienceDirect and Google Scholar databases. To filter papers, inclusion/exclusion criteria were utilised.	Various application fields were covered by the papers, including mobile environments, indoor real-time localization systems, smart grid ecosystems, network traffic statistics, and internet of things devices.	-Uses a methodical approach to provide an extensive taxonomy of machine learning classifiers used in cyber security. -Only includes papers published between 2017-2019. Developments after this period are not covered. -Useful for researchers new to the area to understand classifiers applied for cyber security threat detection[9]. -Indicates further research areas like using deep learning and ensemble methods.
[10]	-The study performs a thorough assessment of the literature on deep learning and machine learning techniques for 6LoWPAN networks based on RPL that are used to detect attacks. -It presents the theoretical and	-The investigation retrieves more than 15,000 preliminary findings from searches across 2 data sources and 5 digital libraries. -It filters results using inclusion/exclusion criteria, producing 49 final studies.	-It offers a thorough and critical evaluation of previous studies using statistical and demographic data. -However, because of accessibility issues, the search is only available in English between 2016 and 2021.	-The study assesses current databases and identifies problems such as the absence of standardised datasets. -It infers different security concerns and offers possible avenues for further research to fill in the gaps.

	practical procedures needed to carry out SLR research.	-The three stages of the methodology—identification, screening, and inclusion—follow PRISMA principles.		-The analysis and comparisons can direct the creation of attack detection systems that are more potent.
[2]	The article explains how artificial intelligence (AI) may be used to defend Internet of Things (IoT) devices against cyberattacks.	The article overviews cybersecurity, IoT, and AI, examining attack methods and AI-based protection. It cites examples of AI technologies, and machine learning algorithms in IoT cybersecurity, and discusses techniques like k-nearest neighbour and support vector machines. The article also addresses protection against various attacks, referencing other works for a thorough analysis.	The article offers a thorough analysis of artificial intelligence's (AI)[11] function in Internet of Things cybersecurity, including both AI-based defence and a range of attack tactics. However, it may lack in-depth analysis of specific AI algorithms and their effectiveness in real-world IoT security scenarios.	The article highlights the advantage cyber-attackers have in finding vulnerabilities and the increasing use of AI by both cybersecurity experts and attackers.
[5]	The article presents a comprehensive overview of IoT security challenges and the potential solutions using advanced technologies.	Introducing novel algorithms for intelligent trust assessment and a 3-layer Intrusion Detection System. The comparative analysis includes machine learning models for attack prediction, using ELM for spoofing detection and LMCE for adversary detection in IoT. The critical analysis emphasizes AI's role in addressing security issues across smart applications.	The article's strength is its comprehensive analysis of blockchain, AI, and machine learning-driven solutions for IoT security issues. It provides valuable insights for researchers and professionals but may have errors in production. It could benefit from more exploration of practical implementations and real-world case studies.	The article emphasizes the importance of addressing security and privacy issues, providing insights for researchers, industry professionals, and policymakers. The implications are far-reaching, guiding future advancements in securing scalable and trustworthy IoT systems.
[12]	The article examines sustainable security for the Internet of Things, emphasizing advanced intrusion detection systems and proposing practical solutions for cybersecurity vulnerabilities in different domains.	The article supplements its findings with graphical representations, including ROC curves and loss curves, providing a visual illustration of the model's effectiveness in cyber-attack detection.	The article provides graphical representations of its findings, such as ROC curves and loss curves, which provide readers a clear idea of how effectively the model works for detecting cyberattacks.	The practical applications of the proposed AI-based identification method in securing compromised meters in smart grids, as well as the integration of healthcare applications and systems with cloud environments for secure data storage.
[13]	The article offers a thorough analysis of the attack surfaces and possible security risks and stresses how crucial it is to take security properties into account when creating efficient security measures. The document addresses the difficulties and potential paths in applying it in the future, as well as providing a thematic taxonomy of the technology.	The article provides comprehensive insights into various popular machine learning algorithms. It discusses the latest advancements in deep learning techniques and their potential applications.	The document's article offers in-depth analyses of the attack surfaces and potential weaknesses, as well as a detailed examination of the difficulties and potential solutions in applying it to security.	The significance of this article lies in its role as a valuable resource for researchers and developers, providing insights into potential security threats, attack vectors, and the application of deep learning and machine learning algorithms in addressing challenges related to IoT security. It stresses the imperative need to enhance existing security measures for ensuring the robust protection of the IoT ecosystem.
[14]	The article offers a thorough analysis of how the rapidly rising demand for smart devices and networks has put IoT systems under more security strain. The document makes the case that the use of dynamically enhanced security systems is required	The paper provides a thorough literature review on solutions for systems, covering the application of ensemble reinforcement learning, and supervised and unsupervised learning techniques. Additionally, it covers the application of	The document's strength is its thorough explanation of machine learning techniques and how to use them to counter different types of attacks. It also draws attention to the difficulties and constraints such as the requirement for real-time updates, infrastructure issues,	The article's importance identifies important research challenges and future directions in this field and offers insightful information at different architectural layers.

	because traditional security techniques are insufficient to handle the variety and severity of evolving attacks.	machine learning (ML) algorithms for IoT device security at various IoT architecture layers.	computational constraints, data security, and privacy leakage.	The document's implications include the necessity of ongoing ML-based security solution research and development to meet the constantly changing security challenges[15].
[1]	The uses, advantages, and difficulties of applying machine learning to cybersecurity and cyber-physical systems (CPS). It highlights how important it is to have a thorough defensive plan in place to safeguard and stop unethical practices in development. The paper also emphasises how systems can be attacked and how this learning could be leveraged in cyberattacks.	The paper highlights the rise in attacks on machine learning models used in cybersecurity and CPS, emphasizing the challenges of deploying unified defense strategies due to the diverse nature of CPS environments. It underscores the importance of strong data verification strategies and discusses various machine learning methods applied in cybersecurity and CPS, including their potential use in cyberattacks.	The article excels in analyzing how machine learning is employed in cybersecurity and CPS, discussing its benefits and challenges. However, its detailed exploration of specific defensive measures to protect machine learning in these scenarios may have limitations.	The article stresses the importance of a robust defense plan to counter cybersecurity risks in diverse CPS environments. It highlights challenges in coordinating defense tactics and emphasizes the critical need to address risks in CPS scenarios.
[16]	The article provides a thorough analysis of the growing security and privacy concerns brought on by the spread of IoT and information technologies. The survey, which covers over 95 works pertaining to security issues in IoT environments, highlights on current state-of-the-art literature on machine learning methods applied in IoT and intrusion detection.	The survey conducted a comprehensive review of recent advancements in Network Security Metrics (NSMs) with a particular emphasis on the Common Vulnerability Scoring System (CVSS) framework. It considered multiple databases for literature selection and summarized methodologies, security concerns, and the current research state on IoT and related security issues.	The document excels in its comprehensive examination of primary metric proposals, extensive research on security metrics, and the application of various machine learning techniques for intrusion detection. However, it acknowledges the ongoing need for further development in the relatively nascent field of model based quantitative NSMs.	The paper highlights the need for additional research on privacy, security risks, and vulnerabilities in environments. It outlines current challenges, suggesting potential research directions and emphasizing the necessity of stronger defenses against security risks and weaknesses in architectures. It also advocates for using intelligent tools in intrusion detection, proving valuable for researchers and experts in network security and related fields.
[17]	The classification of network intrusion detection techniques, a study of IoT attacks with an emphasis on Advanced Persistent Threats (APT), and an examination of security features and particular threats in IoT are some of the main conclusions. Along with a gap analysis of the available public IoT datasets, the paper also suggests ML-based techniques for attack detection in IoT networks.	Threat models, attack taxonomies, and network intrusion detection techniques are presented as supporting documentation. In addition, the document compares relevant surveys and explores the application of machine learning techniques for attack detection. It also provides an overview of the public IoT datasets that are currently available, their features, and the frequency with which machine learning techniques are employed.	Its thorough discussion of machine learning-based intrusion detection techniques and its emphasis on advanced persistent threats are among the document's strong points. A few drawbacks are, however, the scant examination of IoT-related datasets and the absence of any discussion of conventional security measures and non-ML-based detection techniques. Along with highlighting these issues, the paper also points out the shortcomings of the public IoT datasets that are currently available.	The document's importance stems from its ability to fill in gaps in the literature, offer a thorough overview of IoT security issues, and pinpoint unresolved problems and obstacles related to network intrusion and APT attacks using machine learning algorithms. The document's implications could lead to the creation of stronger and more efficient security measures for Internet of Things networks, especially in the face of advanced persistent threats.
[18]	Key conclusions and arguments regarding the application of deep learning and machine learning models for security are presented in the systematic literature review (SLR) on IoT security issues in subdomains like IoMT, IoT, and IoH. After employing a	The review offers a taxonomy hierarchy for putting security parameters into practice while highlighting the difficulties and advancements in several IoT security domains, including high-level features, techniques, and security areas. The	The review's strength is its thorough and methodical approach, which makes use of established guidelines, exacting search and selection procedures, and methods for evaluating quality. A drawback, though, might be the omission of studies written before 2016, which	The study's contribution to our understanding of IoT security issues and its implications for applying deep learning and machine learning models in IoT subdomains make it significant. It offers practitioners and researchers insightful

	methodical approach that includes a quality assessment, a search strategy, and a snowballing technique, 50 pertinent papers from 2016 to 2021 were chosen for review.	comprehensive methodology, the results of the quality assessment, and the inclusion of particular sample attributes and techniques employed in the chosen papers serve as supporting documentation.	could mean that pertinent earlier viewpoints on IoT security are missed.	information and lays out a clear course for future IoT security research, especially when it comes to IoT devices with limited resources.
[6]	An extensive examination to the difficulties caused by the heterogeneity of data in IoT networks and the necessity of effective fixes for this problem. The importance of context-aware ML and DL solutions is emphasised in the paper's discussion of the current ML-based solutions for intrusion detection, access control, and authentication in IoT networks.	The paper offers proof of machine learning algorithms' shortcomings when it comes to processing syntactically and semantically diverse information in Internet of Things networks. Along with the difficulties associated with data collection, proximity effects, and data dependency, it also provides an overview of current machine learning (ML)-based solutions for authentication, access control, and intrusion detection in Internet of Things (IoT) networks.	The document's strength lies in its thorough analysis of the security challenges and threat models associated with IoT deployment, along with its thorough survey of the role of ML and DL mechanisms in IoT security. Additionally, it offers a thorough analysis of the current state-of-the-art ML-based IoT security solutions and outlines potential future research directions for ML and DL in IoT networks. To further highlight the usefulness of ML and DL approaches in IoT security, the paper would benefit from more thorough case studies and examples of their application.	It underlines the significance of context-aware ML and DL solutions for authentication, access control, and intrusion detection and underscores the need for additional research on ML and DL techniques to address the security challenges in IoT networks. The document also emphasises how critical it is to address the shortcomings of current security solutions and how more advanced ML and DL techniques must be employed in sensitive domains before they can be used commercially.
[19]	The document's main conclusions include identifying the most important IoT security issues, reviewing the most recent research in deep learning, big data technologies, and IoT security, and creating a thematic taxonomy to evaluate available solutions. The paper also outlines future research directions and emphasises the difficulties in applying big data technologies and deep learning to IoT security.	The document provides supporting evidence in the form of a thorough examination of popular frameworks, model evaluation methods, and deep learning architectures. Additionally, it offers a thematic taxonomy that was produced by comparing technical studies in the fields of big data technologies, IoT security, and deep learning. The document also explores the connections between these three domains.	The thorough examination of the most recent research in deep learning, big data technologies, and IoT security, as well as the creation of a thematic taxonomy to evaluate available solutions, are the document's strongest points. But the study only looks at deep learning; it doesn't address typical machine learning techniques in relation to big data technologies or Internet of Things security. Furthermore, the survey discusses Internet of Things security from the standpoint of networking and communications rather than delving into specifics for each smart application area that is available.	The document's importance stems from its capacity to direct big data, deep learning, and Internet of Things (IoT) researchers and developers—especially those who are worried about IoT security. The document's contributions include a survey of state-of-the-art research, an analysis of existing solutions based on the derived taxonomy, a thematic taxonomy, and an identification of critical concerns in IoT security. The document's ramifications include the possibility that future studies may examine the difficulties and possibilities associated with utilising big data technology and deep learning for IoT security, thereby improving the security of IoT devices.

3. Methodology

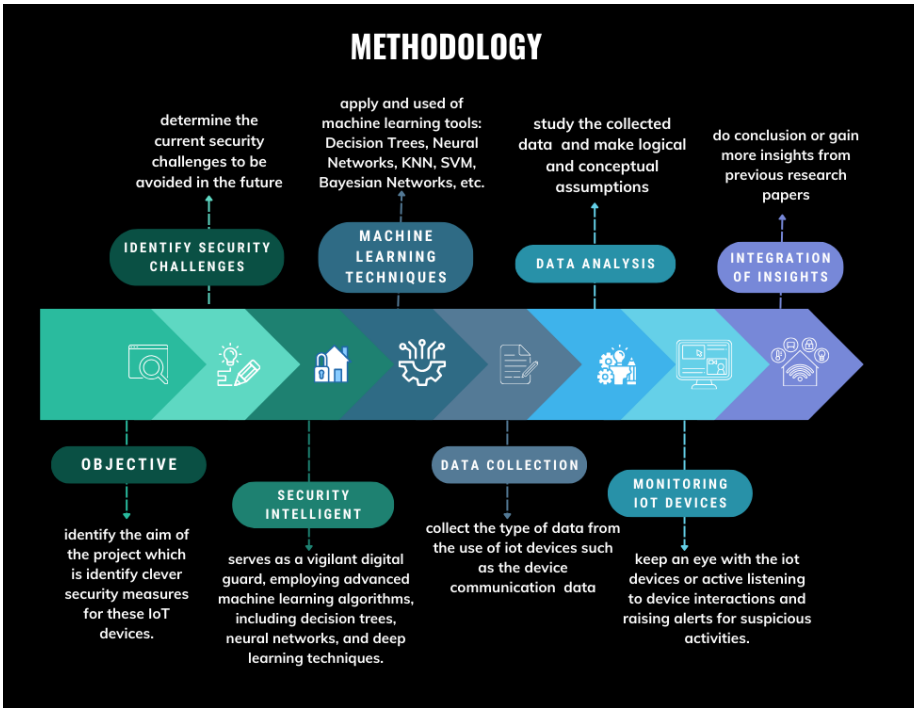

Fig. 2. Overview of the methodology

Figure 2 shows the overview of methodology that will be explained more here in detail. To ensure the safety and security of the Internet of Things (IoT), we are delving into its realm in this project. There are many wonderful things happening with the increasing number of IoT devices in our environment [4], such as smart thermostats[20] and refrigerators, but there is also a significant challenge: protecting them from cyberattacks. Our project's main goal is to Determine some ingenious security precautions for these IoT gadgets. Consider all of these gadgets as potential doorways that hackers might attempt to breach. There are more doors and more devices in our possession, which makes it simpler for hackers to inflict havoc. Thus, keeping those doors closed and locked is our primary goal.

This is being accomplished through the use of "security intelligence." Imagine it as a clever guard standing watch over every door. IoT devices come in different sizes and designs, and they communicate with one another in a variety of languages, so this protection needs to be extremely intelligent. Therefore, in order to train our guard to recognise any suspicious activity on these devices, we're utilising sophisticated technologies called machine learning[7]. Another common activity for analysing IoT security data is clustering, which is regarded as unsupervised learning[7]. It has the ability to form or cluster groups of a collection of data points based on the evaluation of how similar and distinct security data produced by Internet of Things devices from various sources is.

We intend to closely monitor the Internet of Things devices. We'll listen in on their conversations and notice anything out of the ordinary. The guard will raise the alarm and notify us so that we may take appropriate action if it notices anything suspicious. In this manner, we ensure that as the globe becomes more populated with more IoT gadgets, we're also getting smarter about keeping them safe from cyber threats. By deriving insights from unprocessed data, machine learning and deep learning can assist in addressing IoT security by enabling IoT devices to be intelligently protected against a range of cyber-attacks. These technologies can be used to create security solutions for the future generation of IoT devices that are modern and dynamically improved[7].

Furthermore, we are conducting research on the use of various machine learning (ML) approaches to protect Internet of Things (IoT) devices against cyberattacks. We use specialised tools, much like digital detectives. Our main goals are to foresee and thwart security breaches. Think of our tools as intelligent security guards: decision trees, artificial neural networks, K-nearest neighbours, convolutional neural networks, support vector machines, Bayesian networks, ensemble classifiers, genetic programming, logistic regression, and

convolutional neural networks. We also employ various deep learning tactics with CNNs, including instruction2vec, and Principal Component Analysis and feature extraction. It's similar to instructing our technologies on how to recognize and stop any questionable activity taking place in the digital realm. Making these technologies incredibly efficient in identifying and thwarting cyberattacks is our aim [8].

4. IoT Privacy Imperative

A variety of unusual data sources, including audio, video, and environmental sensors[21], are being investigated for anomaly detection[22] and threat identification in the context of improving IoT security intelligence [10]. This goes beyond conventional data sets by utilising a variety of information kinds for all-encompassing security precautions. Furthermore, edge intelligence is gaining popularity, where machine learning models are developed specifically to run on edge devices such as IoT gateways[23]. This makes it easier to make localised decisions and respond quickly, which is essential for quickly reducing threats.

In response to the IoT privacy imperative, innovative federated learning techniques are being developed that allow distributed devices to collaborate on machine learning model training without exchanging raw data[24]. This increases scalability while also enhancing privacy. In addition, there is a push for machine learning in many different directions. Aims are being made to develop explainable AI models so that security administrators[25] can make decisions with transparency. Another trend is real-time adaptive learning, which enables machine learning models to constantly adjust to changing threats in the ever-changing Internet of Things environment. By fusing deep learning with symbolic AI methods, hybrid AI approaches seek to overcome individual constraints and improve general intelligence and robustness [4].

In this context, cooperation and integration are essential. Efforts are made to support collaborative and shared innovation through open-source machine learning platforms designed for Internet of Things security applications [10]. One more focus area is the integration of machine learning (ML) solutions with the current security information and event management (SIEM) systems, with the goal of achieving unified threat intelligence and response capabilities. Working together with cybersecurity companies, gadget producers, and standards organisations is essential to guaranteeing that these innovations are widely adopted and have a significant impact.

Innovative machine learning applications are being developed to address specific pain points in existing IoT security solutions by focusing on user needs and challenges. The promotion of innovative thinking and the investigation of non-conventional security measures is still a guiding concept. Innovations are validated through real-world dataset testing, which demonstrates their usefulness and effectiveness. Clearly communicating the advantages and value proposition of these innovations is essential to attracting interest and promoting adoption in the context of IoT security [13].

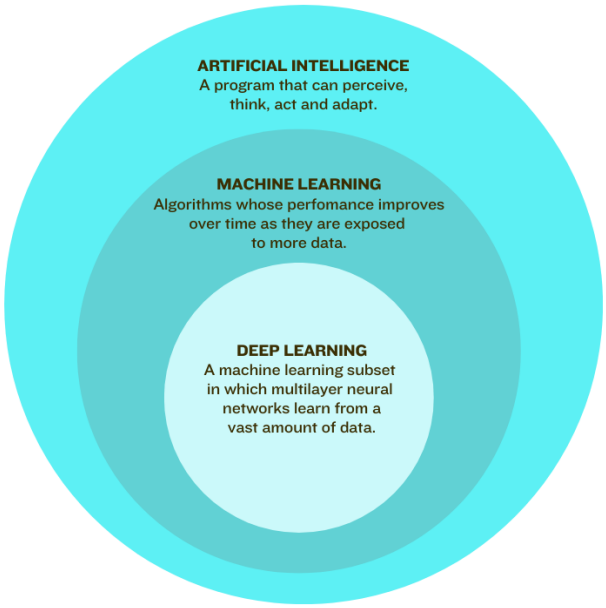

Fig. 3. Hybrid Al Approach

The figure 3 illustrating the Hybrid AI Approach [26] here represents the fusion of deep learning and symbolic AI methods in the context of IoT security. By facilitating an extensive examination of various data

sources—including audio, video, and environmental sensors—for anomaly detection, this integration embodies the recommendations made in the paper. Its application on edge devices supports edge intelligence by enabling quick, localised decision-making. Furthermore, the method's capacity for adaptive learning guarantees ongoing evolution in reaction to changing IoT threats. This hybrid approach aligns with the overall objective of augmenting IoT security intelligence by demonstrating collaborative integration and verifying its effectiveness through real-world dataset testing, while simultaneously addressing particular shortcomings in existing solutions [4].

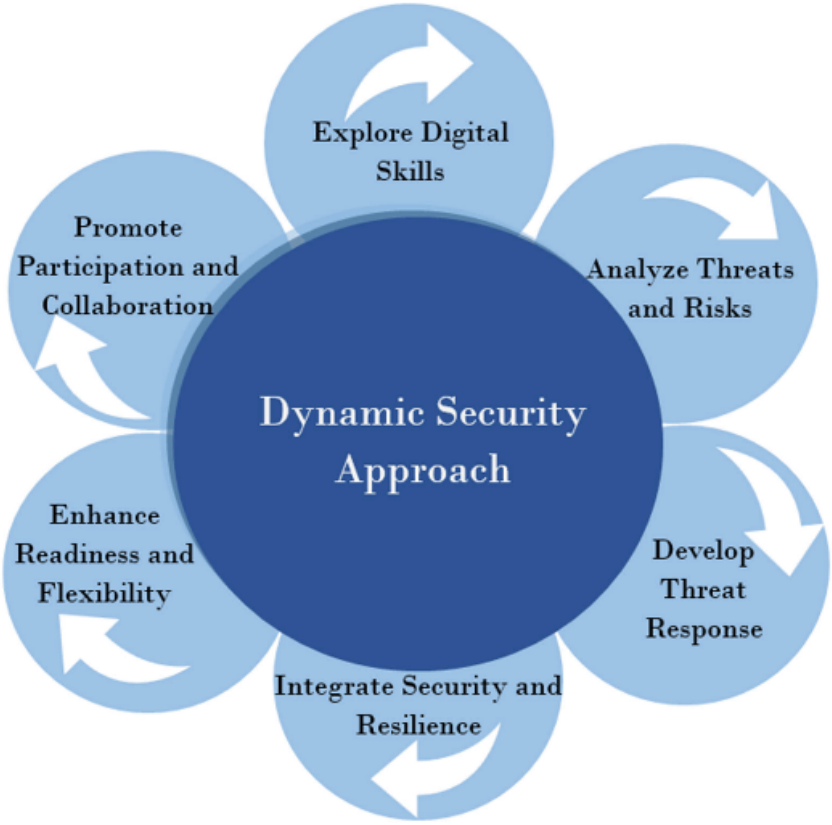

Fig. 4. Dynamic security approach

Figure 4 crafting prompt response plans, fostering collaboration among stakeholders, and employing advanced technologies like machine learning are essential in effectively countering cybersecurity threats[27]. Integrating cybersecurity into organizational strategies, understanding various risks such as malware and phishing, and utilizing real-time threat data strengthen defences against evolving threats. Proactively adapting to changing threats, organizations effectively mitigate vulnerabilities and reduce susceptibility to cyber-attacks [13].

5. Conclusion

Machine learning (ML) and deep learning (DL) have emerged as vital tools for combating security threats in the ever-expanding Internet of Things (IoT) landscape. This study dives deep into how various ML techniques, from Support Vector Machines (SVMs) and Random Forests to Convolutional Neural Networks (CNNs) and Long Short-Term Memory (LSTM) networks, are employed to bolster IoT security. While recognizing the limitations of existing solutions, the paper comprehensively examines ML-powered approaches for securing authentication, access control, and intrusion detection within IoT networks. It emphasizes the critical role of robust ML and DL, particularly in sensitive domains, and sheds light on challenges like data collection, proximity effects, and data dependency in the context of IoT security.

Moreover, the analysis of published articles on ML-based security for IoT reveals a growing trend in research publications in this domain. The document delves into the widespread use of ML techniques in cybersecurity and Cyber-Physical Systems (CPS) scenarios, addressing the rising threat of attacks on ML models by adversaries. It details various ML techniques employed in cybersecurity and CPS, such as clustering and density estimation, while emphasizing the importance of robust data verification strategies and unified defence strategies in diverse CPS deployments[28].

The study also underscores the significance of AI and ML in ensuring the security and privacy of IoT systems, offering valuable insights for researchers, industry professionals, and policymakers alike. It explores potential applications, such as AI-based identification methods in securing compromised meters in smart grids and the integration of healthcare applications[29] and systems with cloud environments[30] for secure data storage. Furthermore, it advocates for collaborative training of ML models across distributed devices without sharing raw data, the creation of explainable AI models, and adaptive learning in real-time to continually adapt to evolving threats within the dynamic IoT landscape.

6. Acknowledgement

We express our heartfelt gratitude to the Computer Network course for its invaluable role in enriching our comprehension of IoT security and Blockchain, aligning with the principles of continuous learning and knowledge acquisition. The wisdom gained from this study has been pivotal, shaping our understanding of these crucial domains and providing us with the essential tools to investigate and harness the capabilities of these technologies. Our sincere thanks extend to our esteemed professors and educators, whose unwavering commitment and diligent efforts in imparting this indispensable knowledge resonate with the values of dedication and excellence. Their guidance has been instrumental in facilitating our progress, enhancing proficiency, and fostering a deeper understanding in the realm of Computer Networking, IoT security, and Blockchain technology.

References

[1] F. Liang, W. G. Hatcher, W. Liao, W. Gao, and W. Yu, “Machine Learning for Security and the Internet of Things: The Good, the Bad, and the Ugly,” *IEEE Access*, vol. 7, pp. 158126–158147, 2019, doi: 10.1109/ACCESS.2019.2948912.

[2] M. Kuzlu, C. Fair, and O. Guler, “Role of Artificial Intelligence in the Internet of Things (IoT) cybersecurity,” *Discov. Internet Things*, vol. 1, no. 1, p. 7, Dec. 2021, doi: 10.1007/s43926-020-00001-4.

[3] A. V. Lv Pradeepika Verma, Yousef Farhaoui, Zhihan, Ed., *Emerging Real-World Applications of Internet of Things*. Boca Raton: CRC Press, 2022. doi: 10.1201/9781003304203.

[4] M. Abdullahi *et al.*, “Detecting Cybersecurity Attacks in Internet of Things Using Artificial Intelligence Methods: A Systematic Literature Review,” *Electronics*, vol. 11, no. 2, p. 198, Jan. 2022, doi: 10.3390/electronics11020198.

[5] B. K. Mohanta, D. Jena, U. Satapathy, and S. Patnaik, “Survey on IoT security: Challenges and solution using machine learning, artificial intelligence and blockchain technology,” *Internet Things*, vol. 11, p. 100227, Sep. 2020, doi: 10.1016/j.iot.2020.100227.

[6] F. Hussain, R. Hussain, S. A. Hassan, and E. Hossain, “Machine Learning in IoT Security: Current Solutions and Future Challenges,” *IEEE Commun. Surv. Tutor.*, vol. 22, no. 3, pp. 1686–1721, 2020, doi: 10.1109/COMST.2020.2986444.

[7] I. H. Sarker, A. I. Khan, Y. B. Abushark, and F. Alsolami, “Internet of Things (IoT) Security Intelligence: A Comprehensive Overview, Machine Learning Solutions and Research Directions,” *Mob. Netw. Appl.*, vol. 28, no. 1, pp. 296–312, Feb. 2023, doi: 10.1007/s11036-022-01937-3.

[8] R. Ali, A. Ali, F. Iqbal, A. M. Khattak, and S. Aleem, “A Systematic Review of Artificial Intelligence and Machine Learning Techniques for Cyber Security,” in *Big Data and Security*, vol. 1210, Y. Tian, T. Ma, and M. K. Khan, Eds., in Communications in Computer and Information Science, vol. 1210. , Singapore: Springer Singapore, 2020, pp. 584–593. doi: 10.1007/978-981-15-7530-3_44.

[9] A. Aldhaheri, F. Alwahedi, M. A. Ferrag, and A. Battah, “Deep learning for cyber threat detection in IoT networks: A review,” *Internet Things Cyber-Phys. Syst.*, vol. 4, pp. 110–128, Jan. 2024, doi: 10.1016/j.iotcps.2023.09.003.

[10] T. A. Al-Amiedy, M. Anbar, B. Belaton, A. H. H. Kabla, I. H. Hasbullah, and Z. R. Alashhab, “A Systematic Literature Review on Machine and Deep Learning Approaches for Detecting Attacks in RPL-Based 6LoWPAN of Internet of Things,” *Sensors*, vol. 22, no. 9, p. 3400, Apr. 2022, doi: 10.3390/s22093400.

[11] “Analysis of IoT Security Challenges and Its Solutions Using Artificial Intelligence - PubMed.” Accessed: Jan. 02, 2024. [Online]. Available: https://pubmed.ncbi.nlm.nih.gov/37190648/

[12] C. Iwendi, S. U. Rehman, A. R. Javed, S. Khan, and G. Srivastava, “Sustainable Security for the Internet of Things Using Artificial Intelligence Architectures,” *ACM Trans. Internet Technol.*, vol. 21, no. 3, pp. 1–22, Aug. 2021, doi: 10.1145/3448614.

[13] M. A. Al-Garadi, A. Mohamed, A. K. Al-Ali, X. Du, I. Ali, and M. Guizani, “A Survey of Machine and Deep Learning Methods for Internet of Things (IoT) Security,” *IEEE Commun. Surv. Tutor.*, vol. 22, no. 3, pp. 1646–1685, 2020, doi: 10.1109/COMST.2020.2988293.

[14] S. M. Tahsien, H. Karimipour, and P. Spachos, "Machine learning based solutions for security of Internet of Things (IoT): A survey," *J. Netw. Comput. Appl.*, vol. 161, p. 102630, Jul. 2020, doi: 10.1016/j.jnca.2020.102630.

[15] N. Alhalafi and P. Veeraraghavan, "Privacy and Security Challenges and Solutions in IOT: A review," *IOP Conf. Ser. Earth Environ. Sci.*, vol. 322, no. 1, p. 012013, Aug. 2019, doi: 10.1088/1755-1315/322/1/012013.

[16] K. A. P. Da Costa, J. P. Papa, C. O. Lisboa, R. Munoz, and V. H. C. De Albuquerque, "Internet of Things: A survey on machine learning-based intrusion detection approaches," *Comput. Netw.*, vol. 151, pp. 147–157, Mar. 2019, doi: 10.1016/j.comnet.2019.01.023.

[17] Z. Chen *et al.*, "Machine Learning-Enabled IoT Security: Open Issues and Challenges Under Advanced Persistent Threats," *ACM Comput. Surv.*, vol. 55, no. 5, pp. 1–37, May 2023, doi: 10.1145/3530812.

[18] A. Javed, M. Awais, M. Shoaib, K. S. Khurshid, and M. Othman, "Machine learning and deep learning approaches in IoT," *PeerJ Comput. Sci.*, vol. 9, p. e1204, Feb. 2023, doi: 10.7717/peerj-cs.1204.

[19] M. A. Amanullah *et al.*, "Deep learning and big data technologies for IoT security," *Comput. Commun.*, vol. 151, pp. 495–517, Feb. 2020, doi: 10.1016/j.comcom.2020.01.016.

[20] M. Bettayeb, O. A. Waraga, M. A. Talib, Q. Nasir, and O. Einea, "IoT Testbed Security: Smart Socket and Smart Thermostat," in *2019 IEEE Conference on Application, Information and Network Security (AINS)*, Nov. 2019, pp. 18–23. doi: 10.1109/AINS47559.2019.8968694.

[21] "Smart Sensors: Analysis of Different Types of IoT Sensors | IEEE Conference Publication | IEEE Xplore." Accessed: Jan. 02, 2024. [Online]. Available: https://ieeexplore.ieee.org/abstract/document/8862778?casa_token=66y8Ga6lTo8AAAAA:zJwrxbxYWt5fBfLwKJRHxB_EgQV1FO3_9ejp1ogjUhCeOcMsdgGcUhkzX69Ef4whxdjjU9rVzRTt8g

[22] A. Chatterjee and B. S. Ahmed, "IoT anomaly detection methods and applications: A survey," *Internet Things*, vol. 19, p. 100568, Aug. 2022, doi: 10.1016/j.iot.2022.100568.

[23] "What is IoT (Internet of Things) and How Does it Work? | Definition from TechTarget." Accessed: Jan. 02, 2024. [Online]. Available: https://www.techtarget.com/iotagenda/definition/Internet-of-Things-IoT

[24] T. Zhang, L. Gao, C. He, M. Zhang, B. Krishnamachari, and S. Avestimehr, "Federated Learning for Internet of Things: Applications, Challenges, and Opportunities".

[25] "Explainable AI and Deep Autoencoders Based Security Framework for IoT Network Attack Certainty (Extended Abstract) | SpringerLink." Accessed: Jan. 02, 2024. [Online]. Available: https://link.springer.com/chapter/10.1007/978-3-031-21311-3_8

[26] "Machines | Free Full-Text | Engineering Applications of Artificial Intelligence in Mechanical Design and Optimization." Accessed: Jan. 02, 2024. [Online]. Available: https://www.mdpi.com/2075-1702/11/6/577

[27] "Sustainability | Free Full-Text | Counterattacking Cyber Threats: A Framework for the Future of Cybersecurity." Accessed: Jan. 02, 2024. [Online]. Available: https://www.mdpi.com/2071-1050/15/18/13369

[28] "A next-generation IoT-based collaborative framework for electronics assembly | The International Journal of Advanced Manufacturing Technology." Accessed: Jan. 02, 2024. [Online]. Available: https://link.springer.com/article/10.1007/s00170-017-1561-x

[29] "IoT in Healthcare: applications, benefits & Challenges." Accessed: Jan. 02, 2024. [Online]. Available: https://www.peerbits.com/blog/internet-of-things-healthcare-applications-benefits-and-challenges.html

[30] "An Intelligent End–Edge–Cloud Architecture for Visual IoT-Assisted Healthcare Systems | IEEE Journals & Magazine | IEEE Xplore." Accessed: Jan. 02, 2024. [Online]. Available: https://ieeexplore.ieee.org/abstract/document/9328531?casa_token=4TvqmNwHchAAAAAA:RC60PR9uYIQXbrxmwbaHaw8-ofEwQWnd94NOfnT1O44IO4U_RrsrsnmTR4Me6SX30WUKNuDQnFim8Q