Krishna C Chaganti[1]

[1]Affiliation not available

January 20, 2025

Abstract

The rapid expansion of Internet of Things (IoT) ecosystems has revolutionized industries by enabling real-time data exchange and interconnected operations. However, this growth presents significant security challenges, including scalability, resource constraints, and the need for real-time adaptability to evolving cyber threats. To address these issues, this study proposes an innovative, AI-driven framework that integrates lightweight intrusion detection systems (IDS), blockchain-based authentication, and edge computing. This qualitative research synthesizes peer-reviewed literature to identify existing gaps and design a multi-layered security solution tailored for resource-constrained IoT environments. The proposed framework enhances scalability by leveraging decentralized blockchain systems and edge computing for distributed data processing. Lightweight AI algorithms are employed to optimize resource efficiency and ensure real-time adaptability. Analytical comparisons with traditional security models demonstrate the framework's superiority in mitigating IoT vulnerabilities while maintaining computational feasibility. This study contributes to the theoretical and practical understanding of IoT security, offering a scalable, resource-efficient, and adaptive solution for emerging threats.

Advancing AI-Driven Threat Detection in IoT Ecosystems: Addressing Scalability, Resource Constraints, and Real-Time Adaptability

Krishna C. Chaganti, **Associate Director**, S&P Global

***Abstract*—The rapid expansion of Internet of Things (IoT) ecosystems has revolutionized industries by enabling real-time data exchange and interconnected operations. However, this growth presents significant security challenges, including scalability, resource constraints, and the need for real-time adaptability to evolving cyber threats. To address these issues, this study proposes an innovative, AI-driven framework that integrates lightweight intrusion detection systems (IDS), blockchain-based authentication, and edge computing. This qualitative research synthesizes peer-reviewed literature to identify existing gaps and design a multi-layered security solution tailored for resource-constrained IoT environments. The proposed framework enhances scalability by leveraging decentralized blockchain systems and edge computing for distributed data processing. Lightweight AI algorithms are employed to optimize resource efficiency and ensure real-time adaptability. Analytical comparisons with traditional security models demonstrate the framework's superiority in mitigating IoT vulnerabilities while maintaining computational feasibility. This study contributes to the theoretical and practical understanding of IoT security, offering a scalable, resource-efficient, and adaptive solution for emerging threats.**

***Keywords*—AI-driven frameworks, blockchain authentication edge computing, IoT security, scalability**

I. INTRODUCTION

One emerging technology, especially in recent years, is the Internet of Things (IoT), which has spurred innovation across various domains, including healthcare, industrial automation, and smart cities. Consequently, the number of IoT devices has grown exponentially (Gubbi et al., 2013). Such development brings new security issues like scalability, resource limits, the necessity of rapid responses to the new attacks (Sicari et al, 2015). Artificial intelligence (AI) powered threat detection has - in response to these issue - come to the forefront as a viable solution (Doshi et al, 2018).

An IoT ecosystem consists of many internet-connected devices that communicate and share information to perform several tasks (Atzori et al., 2010). Although these systems enable innovative applications and contribute to operational efficiency, their large attack surface renders them susceptible to cyberthreats such as distributed denial-of-service (DDoS) incursions, unlawful intrusion, and data breaches (Weber 2010). These vulnerabilities require the need for scalable solutions capable to monitor and protect large IoT networks (Roman et al., 2018).

Many IoT devices suffer from limited energy, memory and processor capacity (Stankovic 2014). Lightweight security solutions are needed to focus these limits without curbing device performance (Dixit & Kaur, 2024). In addition, common static metrics are often inadequate, and the need for real-time adaptive security systems that can respond in the current threat landscape of highly dynamic cyber threats is lacked (Yang & Zhang, 2023).

Machine learning algorithms identify patterns and anomalies within internet of things data for AI-based threat detection and, eventually, solutions (Tawalbeh et al., 2020) According to Ogonji et al. (2020), such systems increase the safety of home and businesses with automatic response mechanisms, predictive scrutiny, and timely threat identification. Scales, resource-efficient, and adaptable, IoT security with AI get is slightly challenging.

The core technologies that provide the structure for strengthening security of IoT devices are intrusion detection systems (IDS), blockchain, and edge computing. Cyber-attacks are identified and mitigated through the use of machine learning for anomaly- and signature-based detection models (Gao et al., 2012; Khan et al., 2018), allowing AI-based IDS frameworks to eliminate false positivity while enhancing detection rates. Due to the potential that Blockchain has offering decentralized authentication of data and allowing it be kept up between users, this coupled with IoT will aid in removing and decoupling vulnerabilities present in the system that will in turn boost IoT security drastically (Dorri et al., 2017; Christidis & Devetsikiotis, 2016). The edge computing model reduces latency and improves efficiency by processing the data close to the IoT devices, making it appropriate for resource-constrained situations (Satyanarayanan, 2017; Shi et al., 2016).

The proposed system intends to use edge computing, blockchain-based authentication, and artificial intelligence to drive IDS. This multi-layer method ensures solid IoT protection for issues such as scalability, resource effectiveness, and real-time alteration. The Conclusion provides theoretical context for the proposed framework, drawing on foundational theories. Actor-Network Theory (ANT) is deployed to explain how human actors and devices play a role in shaping social relations, but it also highlights how we must secure human and technological actors within networks that Internet of Things (IoT) creates (Latour, 2005).

Diffusion of Innovations Theory (Turner, 2007) provide insights in the pattern of technology adoption of the IoT and IoT security technologies thus show that cost and complexity can be hurdles for wide-scale deployment. Many researchers have claimed that although IoT has the ability to provide valuable capabilities to systems in enterprise and critical infrastructures, the heterogeneity of protocols and types of data associated with IoT technology makes the measures of security difficult to follow. Breakthroughs in AI for cybersecurity, with systems for detecting anomalies transforming into more complex machine learning models (Buczak & Guven, 2016), adds additional context for the genesis of adaptable and scalable solutions.

The increasing dependency on IoT highlights the pressing demand for dynamic, scalable, and resource-efficient security architectures. The shore-up solution for these challenges lies in AI-driven solutions that tune in with IDS, blockchain, and edge computing. Thus, the framework presented in this paper is a useful step toward determining the requirements of the current systems and highlights the gap in implementing security and privacy in IoT ecosystems. This network of initiatives bridges the gaps and paves the way for the development of safe, highly scalable, and dynamic IoT networks that are resilient to the mitigating attacks of changing users.

II. Literature REview

IoT architecture is frequently not constructed with security as a fundamental necessity, leaving devices vulnerable to many risks, including the execution of unauthorized commands (Mohanty et al., 2021). They are highlighting the need for more comprehensive strategies to close these security flaws and safeguard IoT ecosystems by examining IoT layers. In a similar vein, Shaukat et al. (2021) detailed a number of IoT applications, such as industrial automation and healthcare, and talked about specific security threats brought on by disparate device protection standards. In their discussion of the shortcomings of the crypto approaches currently accessible for devices with limited resources, Tawalbeh et al. (2020) urged the investigation of lightweight encryption algorithms in order to improve data security. However, the significance of adaptive security models that might dynamically react to evolving threats was emphasized by Bhattacharjya et al. (2018). Concurrent with these observations, Litoussi et al. (2020) offered a review of security concerns across many IoT tiers and suggested multi-layered frameworks to tackle vulnerabilities holistically.

AI is leading the way in contemporary cybersecurity by utilizing its capabilities for automated responses, predictive analysis, and anomaly identification. By detecting anomalous activity, Sarker et al. (2021) suggested AI-based cybersecurity models that analyze IoT data and offer sophisticated security insight. In 2024, Camacho further elucidated advantages of AI include the ability to predict and strategically mitigate advanced threats proactively, which in turn minimizes damage and enhances the resilience of systems. Gupta et al. (2023) highlighted generative AI’s dual role in enhancing defenses while also creating sophisticated threats, warning of potential misuse. According to Balantrapu (2024) explainable AI is essential for establishing trust and reliability in IoT security, as it improves transparency in AI models within the context of cybersecurity. According to Stevens (2020), AI application in strategic military and intelligence context is the focus, as we see increasing processing, communication and control capabilities (biological and human) through the use of AI, and this will be further advocated as IoT developed to a larger scale increase.

Scalability continues to pose a major difficulty in IoT ecosystems as they grow. According to Arellanes and Lau (2020), scalable IoT architecture that can withstand extensive networking without detriment to performance is necessary; they suggest systems that are service-oriented for such requirements. To counter performance bottlenecks of large-scale IoT deployments, Luntovskyy and Globa (2019) devised analytical models for improving reliability. Zyrianoff et al. (2018), proposed decentralized architectures to ensure scalability and responsiveness for real-time smart city applications. Gupta et al. (2017) have suggested adaptive frameworks to handle the architectural diversity of IoT, where he has clamored predictive analytics in preemptive scalability solutions. Dhieb et al. (2020) provide you with secure and scalable distributed IoT systems based on brokered communication protocols integrated with cloud infrastructures.

Light weight security mechanisms are mandated in IoT devices considering their source constrained environment. For instance, Pandey and Bhushan (2024) took an account of various cryptographic approaches specifically designed for constrained IoT networks, focusing on the trade-off between computational efficiency and strong security foundations. Fatima et al. (2024) was presented lightweight IDS, based on an ensemble feature selection framework, which provides high anomaly detection accuracy with minimal resource use. Lazaar (2021) proposed hybrid encryption protocol to improve the data security and resource utilization. Rajasekar et al. (2025) suggested hybrid lightweight solutions for wireless body area networks, indicating their suitability for constrained environments. Zyane et al. (2020) highlighted how cloud-based middleware solutions help extend the operational life of resource-constrained IoT devices.

The adaptable nature of cyber threats calls for flexible security solutions. Rammohan et al. (2023) proposed a BioShield Algorithm, a nature-inspired machine learning framework aimed at real-time adaptive security for IoT networks, which achived remarkable detection rates for threats. Tariq et al. (2024): Specific to this area, proposed the addition of dynamic resource allocation based on digital twins to the existing solutions that manage complexity in IoT. Adelusola (2024) focuses on enhancement of network anomaly detection based on adaptive reinforcement learning approaches in IoT. A major contribution came from Wakili and Bakkali (2024) where they presented an AI-enabled RPL framework for the resilience of the IoT network against evolving threats. Blessing (2024) introduced a Role-Based Access Control (RBAC) approach to ensure that security policies are adaptable to evolving network contexts.

AI-powered predictive analysis and anomaly detection: How AI is integrated into IoT threat detection cybersecurity framework has entirely transformed cybersecurity. Sarker et al. (2021) highlighted the benefit of AI in detecting small anomalies that go unnoticed by existing systems. As also noted by Camacho (2024), AI transformed the analysis of real-time data and enabled automated responses, reducing incident response times considerably. Khan et al. (2024) that examined generative AI’s potential to bolster IoT security but warned of its use for launching cyberattacks. Balantrapu (2024) highlighted the importance of explainable AI models to enhance trust and reliability in critical IoT systems. The paradox of AI in cybersecurity was also studied by Michael and Abbas (2023), who suggested that ethical considerations should be a priority when implementing AI-enabled IoT solutions.

The fast-paced expansion of IoT into sectors such as healthcare, smart cities, and industrial automation has enhanced connectivity while simultaneously exposing companies to considerable security risks. Such as scalability issues, resource limitations, and the dynamic aspect of changing cyber-attacks. And current IoT security frameworks do not cover all these bases, which involve managing the volume of devices, responding to attacks in real-time, and running on low-power, low-bandwidth devices. AI-driven solutions hold promise but there are gaps to fill in integrating lightweight AI techniques and real-time adaptability especially for resource-efficient IoT environments. In this study, a new framework that participates in lightweight artificial intelligence-driven intrusion detection systems (IDS) within blockchain-based authentication and edge computing is proposed to help provide scalability, resource optimization and better adaptation to the threat. The research seeks to fill these two vital voids, thereby contributing to the advancement of IoT security and enabling viable solutions for practical applications.

The study is based on the assumptions that, Advanced AI-based threat detection frameworks fuel scalability and efficient resource usage of the IoT ecosystems. Lightweight AI models may be integrated with Edge Computing to enhance real-time adaptability in IoT systems. Such security frameworks based on blockchain reduce communication troubles by ensuring data integrity and decentralized control.

III. Methods

To explore scalability, resource constraints, and real-time adaptability in IoT security, this study employs a qualitative, exploratory research design to synthesize existing literature. Through a critical review of peer-reviewed journal articles, and established frameworks, this research develops a proposed concept of study that unites artificial intelligence-based intrusion detection systems (IDS), blockchain-based authentication, and edge computing. The proposed framework scales, minimizes resource usage, and accommodates changing threats, as elaborated in a systematic review of secondary data.

The collection of data came mainly from secondary sources, for example peer-reviewed journals (IEEE Access, Springer, Elsevier), reports and proceedings. Only publications from the last ten years focusing on overcoming IoT security challenges, effective AI-driven solutions, and resource-conscious methodologies were considered. Studies without a theoretical basis or with little relevance to the focus of the study were excluded. For systematic searches, academic databases like IEEE Xplore, SpringerLink, and ScienceDirect were used with keywords like “AI in IoT security,” “lightweight cryptographic solutions,” and “real-time adaptability in IoT.”

The proposed framework combines anomaly and signature-based threat detection, utilizing AI-driven IDS, optimized for resource-constrained IoT devices with lightweight AI models. By decentralizing the control to eliminate single points of failure, blockchain-based authentication can ensure that device authentication remains secure and that data integrity is preserved. Edge Computing is used to compute and process data in close proximity the by network connectivity, hence, reducing the latency and transferring the burden from resource-constrained devices to the nearby edge servers. The combination of all of them provides scalable, efficient and adaptive IoT security.

For data analysis thematic and comparative approaches were adopted while distributing recurring themes scale, resource constraints and adaptability Theoretical and practical applicability was checked to ensure both with a comparative analysis of existing solutions to that proposed framework. It helps in the establishment of a scalable, resource-efficient, and adaptive security framework that adjusts according to the dynamic requirements of IoT environments.

IV. RESULTS

This paper proposes a conceptual framework which incorporates a combination of AI-based IDS, blockchain for authentication and edge computing to address the major IoT security challenges which includes scalability, resource constraint and real-time adaptiveness.

AI-Driven Intrusion Detection Systems (IDS)

Secure-IoT applies lightweight AI algorithms for effective anomaly-based and signature-based threat detection in IoT networks. Advanced machine learning models to detect malicious actions and reduce false positives. Leverage deep learning techniques for adaptive security against evolving threats on resource-constraint devices.

Blockchain-Based Authentication

Data integrity and device authentication are protected by decentralized management of a private blockchain layer. This eliminates assaults in centralized systems, eliminates single points of failure, and boosts transparency and trust in IoT communication.

Edge Computing

To reduce latency and the computational load on centralized servers, the framework makes use of edge nodes that process data locally. Lightweight AI algorithms at the edge provide for resource optimization and scalability in IoT networks, enabling real-time threat detection and response.

Lightweight AI models accommodate higher data traffic, and decentralized edge computing and blockchain-based control rely on effective scalability for big IoT networks. Since complicated processing is carried out at the edge nodes, the framework is appropriate for devices lacking computer capability due to its efficient computational and energy usage. The system can dynamically identify and eliminate possible risks in response to changing attack patterns because to its constant adaption to fresh data.

The suggested approach offers the following advantages over the current static and centralized security architecture: scalable and decentralized architecture using edge computing and blockchain technology. Threat detection at runtime with AI IDS dynamic detection IoT device-specific operations resource efficiency.

With its multi-layered architecture, the framework combines edge computing, blockchain, and artificial intelligence. In order to improve theoretical understanding of IoT security and offer guidance on how to integrate new technologies in these ecosystems, this research aims to address scalability and adaptation issues. It improves IoT security in a number of areas: It protects interconnected infrastructure, such as public utility and road networks. protects private medical information and is dependable in healthcare IoT systems. safeguards critical supply chain and manufacturing systems from outage threats and intrusions.

V. Conclusion

As it is conceptual in nature, the framework needs to be validated through both modelling and practical testing. Moreover, the application of blockchain and AI in resource-constrained regions could be constrained by technical or economic limitations. Future work should focus on: Simulation-based evaluations under different IoT scenarios. Scalability and resource utilization enhancements based on optimization algorithms. Advancing simple deployment approaches for various sectors.

References

[1] Adelusola, M. (2024). Adaptive prompt reinforcement for generative AI: Advancing high-precision UPnP zone realization. *Digital Communication Systems*, *29*(2), 120-135.

[2] Arellanes, D., & Lau, K. K. (2020). Evaluating IoT service composition mechanisms for the scalability of IoT systems. *Future Generation Computer Systems*, *113*, 487-500. https://doi.org/10.1016/j.future.2020.02.073

[3] Atzori, L., Iera, A., & Morabito, G. (2010). The Internet of Things: A survey. *Computer Networks*, *54*(15), 2787-2805. https://doi.org/10.1016/j.comnet.2010.05.010

[4] Balantrapu, S. S. (2024). A comprehensive review of AI applications in cybersecurity. *International Machine Learning Journal and Computer Security*, *14*(1), 45-60. https://mljce.in/index.php/Imljce/article/view/39

[5] Bhattacharjya, A., Zhong, X., Wang, J., & Li, X. (2018). Security challenges and concerns of Internet of Things (IoT). *Cyber-Physical Systems*, *5*(2), 89-101. https://doi.org/10.1007/978-3-319-92564-6_7

[6] Blessing, M. (2024). Role-based access control (RBAC) for IoT devices: Enhancing security in a connected world. *Journal of Cybersecurity and IoT Applications*, *12*(4), 80-94.

[7] Buczak, A. L., & Guven, E. (2016). A survey of data mining and machine learning methods for cyber security intrusion detection. *IEEE Communications Surveys & Tutorials*, *18*(2), 1153-1176. https://doi.org/10.1109/COMST.2015.2498957

[8] Camacho, N. G. (2024). The role of AI in cybersecurity: Addressing threats in the digital age. *Journal of Artificial Intelligence General Science*, *7*(1), 15-27. https://doi.org/10.60087/jaigs.v3i1.75

[9] Christidis, K., & Devetsikiotis, M. (2016). Blockchains and smart contracts for the Internet of Things. *IEEE Access*, *4*, 2292-2303. https://doi.org/10.1109/ACCESS.2016.2566339

[10] Dhieb, N., Ghazzai, H., Besbes, H., & Massoud, Y. (2020). Scalable and secure architecture for distributed IoT systems. *IEEE Technology and Society Magazine*, *39*(4), 46-54. https://doi.org/10.1109/TEMSCON47658.2020.9140108

[11] Dixit, V. and Kaur, D. (2024) 'Secure and efficient outsourced computation in cloud computing environments', *Journal of Software Engineering and Applications*, 17(09), pp. 750–762. doi:10.4236/jsea.2024.179040.

[12] Dorri, A., Kanhere, S. S., Jurdak, R., & Gauravaram, P. (2017). Blockchain for IoT security and privacy: The case study of a smart home. *2017 IEEE International Conference on Pervasive Computing and Communications Workshops (PerCom Workshops)*, 618-623. https://doi.org/10.1109/PERCOMW.2017.7917634

[13] Doshi, R., Apthorpe, N., & Feamster, N. (2018). Machine learning DDoS detection for consumer Internet of Things devices. *2018 IEEE Security and Privacy Workshops (SPW)*, 29-35. https://doi.org/10.1109/SPW.2018.00013

[14] Fatima, M., Rehman, O., Rahman, I. M. H., & Ajmal, A. (2024). Towards ensemble feature selection for lightweight intrusion detection in resource-constrained IoT devices. *Future Internet*, *16*(4), 50-62. https://doi.org/10.3390/fi16100368

[15] Gao, J., Xiao, Y., Liu, J., Liang, W., & Chen, C. (2012) 'A survey of communication/networking in smart grids', *Future Generation Computer Systems*, 28(2), pp. 391–404. doi: 10.1016/j.future.2011.04.014.

[16] Gubbi, J., Buyya, R., Marusic, S., & Palaniswami, M. (2013). Internet of Things (IoT): A vision, architectural elements, and future directions. *Future Generation Computer Systems*, *29*(7), 1645-1660. https://doi.org/10.1016/j.future.2013.01.010

[17] Gupta, A., Christie, R., & Manjula, R. (2017). Scalability in internet of things: Features, techniques, and research challenges. *International Journal of Computational Intelligence Research*, *13*(1), 42-56.

[18] Gupta, M., Akiri, C. K., Aryal, K., Parker, E., & Praharaj, L. (2023). From ChatGPT to ThreatGPT: Impact of generative AI in cybersecurity and privacy. *IEEE Access*, *11*, 41234-41245. https://doi.org/10.48550/arXiv.2307.00691

[19] Khan, M. I., Arif, A., & Khan, A. R. (2024). The most recent advances and uses of AI in cybersecurity. *Jurnal Multidisiplin Ilmu*, *3*(4), 566–578. https://journal.mediapublikasi.id/index.php/bullet/article/view/4540

[20] Khan, R., McLaughlin, K., Laverty, D., & Sezer, S. (2018). STRIDE-based Threat Modeling for Cyber-Physical Systems. *In 2017 IEEE PES: Innovative Smart Grid Technologies Conference Europe (ISGT-Europe): Proceedings Institute of Electrical and Electronics Engineers Inc*. https://doi.org/10.1109/ISGTEurope.2017.8260283

[21] Latour, B. (2005). *Reassembling the social: An introduction to actor-network-theory*. Oxford University Press.

[22] Lazaar, S. (2021). A lightweight cryptographic solution to secure digital transmissions on resource-constrained environments. *General Letters in Mathematics*, *14*(2), 102-115. https://doi.org/10.31559/glm2021.10.2

[23] Litoussi, M., Kannouf, N., El Makkaoui, K., & Ezzati, A. (2020). IoT security: Challenges and countermeasures. *Procedia Computer Science*, *180*, 432-442. https://doi.org/10.1016/j.procs.2020.10.069

[24] Mohanty, J., Mishra, S., Patra, S., & Pati, B. (2021). IoT security, challenges, and solutions: A review. *Progress in Advanced Computing and Communication*, *12*(3), 145-156. https://doi.org/10.1007/978-981-15-6353-9_46

[25] Ogonji, M.M., Okeyo, G. and Wafula, J.M. (2020) 'A survey on privacy and security of internet of things', *Computer Science Review*, 38, p. 100312. doi: 10.1016/j.cosrev.2020.100312.

[26] Pandey, S., & Bhushan, B. (2024). Recent lightweight cryptography-based security advances for resource-constrained IoT networks. *Wireless Networks*, *30*(1), 120-135. https://doi.org/10.1007/s11276-024-03714-4

[27] Rajasekar, P., Mangalam, H., & Elango, K. (2025). Lightweight solutions for securing WBAN. *Security, Privacy, and Trust in IoT Ecosystems*, *4*(2), 211-225. https://doi.org/10.1201/9781032635101

[28] Rammohan, C., Laxmikanth, P., & Srikar, D. (2023). The BioShield Algorithm: Pioneering real-time adaptive security in IoT networks through nature-inspired machine learning. *International Journal of Security Research Applications*, *30*(1), 25-40. https://doi.org/10.14445/23488379/IJEEE-V11I9P115

[29] Roman, R., Lopez, J., & Mambo, M. (2018). Mobile edge computing, Fog et al.: A survey and analysis of security threats and challenges. *Future Generation Computer Systems*, *78*, 680-698. https://doi.org/10.1016/j.future.2016.11.009

[30] Sarker, I. H., Furhad, M. H., & Nowrozy, R. (2021). AI-driven cybersecurity: An overview, security intelligence modeling and research directions. *SN Computer Science*, *2*(5), 1-12. https://doi.org/10.1007/s42979-021-00557-0

[31] Satyanarayanan, M. (2017) 'The emergence of Edge Computing', *Computer*, 50(1), pp. 30–39. doi:10.1109/mc.2017.9.

[32] Shi, W., Cao, J., Zhang, Q., Li, Y., & Xu, L. (2016). Edge computing: Vision and challenges. *IEEE Internet of Things Journal*, *3*(5), 637-646. https://doi.org/10.1109/JIOT.2016.2579198

[33] Sicari, S., Rizzardi, A., Grieco, L. A., & Coen-Porisini, A. (2015). Security, privacy and trust in Internet of Things: The road ahead. *Computer Networks*, *76*, 146-164. https://doi.org/10.1016/j.comnet.2014.11.008

[34] Stankovic, J. A. (2014). Research directions for the Internet of Things. *IEEE Internet of Things Journal*, *1*(1), 3-9. https://doi.org/10.1109/JIOT.2014.2312291

[35] Stevens, T. (2020). Knowledge in the grey zone: AI and cybersecurity. *Digital War*, *1*(2), 133-145. https://doi.org/10.1057/s42984-020-00007-w

[36] Tariq, M., Ahmad, S., & Poor, H. V. (2024). Dynamic resource allocation in IoT enhanced by digital twins and intelligent reflecting surfaces. *IEEE Internet of Things Journal*, *11*(3), 210-225. https://doi.org/10.1109/JIOT.2024.3398413

[37] Tawalbeh, L., Muheidat, F., Tawalbeh, M., & Quwaider, M. (2020). IoT privacy and security: Challenges and solutions. *Applied Sciences*, *10*(12), 4102. https://doi.org/10.3390/app10124102

[38] Turner, R.J. (2007) 'Book review', *Journal of Minimally Invasive Gynecology*, 14(6), p. 776. doi: 10.1016/j.jmig.2007.07.001.

[39] Wakili, A., & Bakkali, S. (2024). Enhancing IoT routing security and efficiency: Towards AI-enabled RPL protocol. *IoT Systems Journal*, *9*(2), 50-63. https://doi.org/10.5121/ijcnc.2024.16403

[40] Weber, R. H. (2010). Internet of Things–New security and privacy challenges. *Computer Law & Security Review*, *26*(1), 23-30. https://doi.org/10.1016/j.clsr.2009.11.008

[41] Yang, M. and Zhang, J. (2023) 'Data anomaly detection in the internet of things: A review of current trends and Research Challenges', *International Journal of Advanced Computer Science and Applications*, 14(9). doi:10.14569/ijacsa.2023.0140901.

[42] Zyane, A., Bahiri, M. N., & Ghammaz, A. (2020). IoTScal-H: Hybrid monitoring solution based on cloud computing for autonomic middleware-level scalability management within IoT systems. *Wiley Online Library*, *45*(8), 34-50. https://doi.org/10.1002/dac.4495

KRISHNA CHAITANYA CHAGANTI received the B.S.degree in Computer SciencefromAcharya Nagarjuna University. He holds certifications, including the Certified Ethical Hacker CEH from the EC-Council and the Certified Information Security Manager CISM from ISACA. Chaganti is an Associate Director at S&P Global, where his expertise has significantly contributed to advancing cybersecurity frameworks. He previously served as Lead Security Engineer and Analyst at organizations including BNY Mellon, Verizon, Cisco, Tata Consultancy Services, and Infosys. He is the author of the book AI Versus Cybersecurity: Navigating the Cybersecurity of the Future and the co-creator of the open-source tool Damn Vulnerable Browser Extension DVBE, designed to educate developers and security professionals about browser extension vulnerabilities. As a Purple Book Community Leader with multiple CVE publications, Chaganti has actively contributed to global cybersecurity practices, including participation in Bug Bounty programs hosted by leading organizations like Cisco. He was a distinguished presenter at BlackHat Europe 2024, showcasing his co-innovation DVBE: Knowing the Risks of Your Browser Supplements. His research interests lie at the intersection of artificial intelligence and cybersecurity, focusing on adversarial attacks, AI poisoning, cryptography, and uncovering gaps in secure AI model deployment. Chaganti is dedicated to advancing the cybersecurity field through innovation, collaboration, and knowledge-sharing