Enhancing IoT security in 6G networks: AI-Based intrusion detection, penetration testing, and Blockchain-based trust management(work-in-progress paper)

Vinh Hoa La, Wissam Mallouli, Manh Dung Nguyen, Edgardo Montes de Oca, Ana R Cavalli, Péter Vörös, Károly Kecskeméti, Mohammed B M Kamel, Sándor Laki, Antonios Lalas, et al.

Enhancing IoT Security in 6G Networks: AI-Based Intrusion Detection, Penetration Testing, and Blockchain-based Trust Management(*work-in-progress paper*)

Vinh Hoa La[1], Wissam Mallouli[1], Manh Dung Nguyen[1], Edgardo Montes de Oca[1], Ana Cavalli[1], Péter Vörös[2], Károly Kecskeméti[2], Mohammed B. M. Kamel[2], Sándor Laki[2], Antonios Lalas[3], Sarantis Kalafatidis[3], Asterios Mpatziakas[3], Nikolaos Makris[3], and Anastasios Drosou[3]

[1] Montimage, 39 rue Bobillot, 75013 Paris, France
[2] Faculty of Informatics, ELTE Eötvös Loránd University, 1117 Budapest, Hungary
[3] Centre for research and technology Hellas, 6th km Charilaou-Thermi Rd, GR 57001 Thermi, Thessaloniki, Greece

Abstract. The exponential growth of Internet of Things (IoT) devices in upcoming 6G networks poses significant security challenges, particularly concerning Distributed Denial of Service (DDoS) attacks, data breaches, and unauthorized access. This paper presents the NATWORK project's approach to addressing these challenges through three distinct use cases (UC): UC#3.1 focuses on developing AI-driven machine learning techniques for anomaly detection and DDoS mitigation; UC#3.2 introduces advanced AI-powered penetration testing and vulnerability assessment tools; and UC#3.3 explores blockchain-based security mechanisms to enhance trust and secure communications in IoT ecosystems. Collectively, these use cases aim to fortify IoT networks against evolving cyber threats, ensuring data integrity and network resilience.

Keywords: IoT security, 6G networks, machine learning, DDoS attacks, blockchain, penetration testing, anomaly detection, reinforcement learning.

1 INTRODUCTON

The global Internet of Things (IoT) market is projected to grow from $662.21 billion in 2023 to $3,352.97 billion by 2030[4]. The large-scale deployment of IoT devices in 6G networks [8] presents substantial security challenges due to the vast number of connected devices and their inherent vulnerabilities. These devices, often with limited processing power and memory, are particularly susceptible to attacks such as distributed denial-of-service (DDoS), data breaches, and unauthorized access. To safeguard these devices and the sensitive data they handle,

[4] According to QuanTag IT Solutions GmbH: https://quantag-it.com/iot.html

the network infrastructure must incorporate advanced threat detection and mitigation mechanisms.

Given that most IoT devices cannot independently support sophisticated security measures due to their resource constraints, the network itself must provide this additional layer of protection. This requires the implementation of intelligent, adaptive security solutions that can operate at scale, protecting both the devices and the data they transmit. For instance, the network could utilize AI-driven anomaly detection to identify unusual traffic patterns that may indicate a security threat. Additionally, the infrastructure could offload computationally intensive security tasks from the IoT devices to more capable network components, ensuring that even the most resource-constrained devices are adequately protected.

Moreover, privacy preservation techniques, such as end-to-end encryption and secure multi-party computation, must be integrated into the network to prevent unauthorized access to sensitive data. This approach not only secures the IoT devices but also builds a resilient and trustworthy 6G ecosystem where the security of each device is reinforced by the network's comprehensive security architecture.

The NATWORK [1] project is an innovative research initiative focused on enhancing the security, privacy, and resilience of next-generation networks, particularly within the context of the Internet of Things (IoT) and 6G ecosystems. By developing cutting-edge AI-driven security tools and methodologies, NATWORK aims to tackle the growing threats posed by cyberattacks, such as Distributed Denial of Service (DDoS) and unauthorized access, which are exacerbated by the massive scale of IoT deployments. The project brings together a consortium of leading European research institutions and industry partners to deliver robust solutions that ensure the integrity and reliability of future network infrastructures. The NATWORK project seeks to address the IoT security challenges in the context of 6G through the development of advanced security tools, leveraging AI, machine learning, and blockchain technologies.

It is important to note that this is a work-in-progress, with the NATWORK project having commenced in January 2024 and scheduled to conclude in December 2026. The ongoing research and development efforts within these use cases will continue to evolve, with the final outcomes expected to significantly enhance the security framework for IoT in 6G networks.

The rest of this paper is organized as follows: Section 2 provides a comprehensive review of the existing literature on IoT security challenges, with a particular focus on the emerging 6G networks and the relevant projects that have influenced our approach. Section 3 presents an in-depth discussion of the three sub-use cases explored within the NATWORK project: UC#3.1 on AI-driven anomaly detection for IoT security, UC#3.2 on AI-powered penetration testing and vulnerability assessment, and UC#3.3 on enhancing decentralized security and trust management using blockchain technology. Section 4 outlines the expected outcomes of the NATWORK project, including the key performance indicators (KPIs) aimed at improving IoT security in 6G networks. Finally, in

Section 5, we summarize our findings, discuss the implications of our research, and propose directions for future work to further advance the field of IoT security in the context of 6G networks.

2 BACKGROUND AND RELATED PROJECTS

2.1 Background

The deployment of Internet of Things (IoT) devices in 6G networks introduces a myriad of security challenges, primarily due to the vast number of interconnected devices, heterogeneity, and limited computational capabilities of IoT nodes. These devices are particularly vulnerable to various cyber threats, including Distributed Denial of Service (DDoS) attacks, data breaches, unauthorized access, and routing attacks. The resource-constrained nature of IoT devices exacerbates these challenges, as they often lack the computational power to implement advanced security mechanisms. Thus, ensuring the security and privacy of IoT devices [13] and their data in 6G networks requires a robust and scalable security infrastructure.

Recent advancements in IoT security [3] have primarily focused on Intrusion Detection Systems (IDS), vulnerability assessment, and blockchain technology. AI-based IDS, particularly those employing reinforcement learning, have shown promise in adapting to dynamic IoT environments [12]. However, existing solutions often struggle with the computational constraints of IoT devices and the scalability required for 6G networks. This section reviews current IDS solutions, AI-based security mechanisms, and blockchain applications in IoT, highlighting their limitations and the need for integrated, scalable approaches.

Intrusion Detection Systems (IDS) [2] play a critical role in safeguarding IoT networks by monitoring traffic and identifying potential security breaches. Traditional IDS approaches, however, struggle to cope with the dynamic and complex nature of IoT environments. Recent advancements in Artificial Intelligence (AI), particularly machine learning and deep learning, have revolutionized IDS by enabling the development of systems that can adapt to new and evolving threats [11, 16]. Reinforcement learning, for instance, has been employed to enhance IDS capabilities by allowing systems to learn from the network environment and improve detection accuracy over time. Moreover, Convolutional Neural Networks (CNNs) have shown promise in detecting anomalies in network traffic patterns, making them effective in identifying DDoS attacks and other sophisticated threats.

Penetration testing is a proactive security measure that involves simulating cyberattacks to identify and address vulnerabilities in a network. Traditional penetration testing methods are often manual and time-consuming, making them less feasible for the dynamic and expansive environments characteristic of 6G-enabled IoT networks. To overcome these limitations, AI-driven penetration testing has emerged as a promising solution. Machine learning algorithms can automate the process of vulnerability assessment by identifying potential security

weaknesses and simulating various attack vectors. In the context of IoT, where the number of devices is expected to grow exponentially, automated penetration testing ensures that security measures can scale effectively. The NATWORK project, for example, focuses on developing AI-based tools for intrusion detection and penetration testing, specifically targeting the unique challenges posed by IoT devices in 6G networks.

As the number of IoT devices in 6G networks continues to grow, ensuring secure and trustworthy communication becomes increasingly challenging. Blockchain technology offers a decentralized and tamper-proof solution for managing trust in IoT networks. By leveraging distributed ledger technology, blockchain can secure communication channels between IoT devices, prevent unauthorized access, and maintain data integrity. Recent studies have explored the integration of blockchain with AI to enhance the security of IoT networks. For instance, blockchain-based access control mechanisms combined with AI-driven smart contract verification can provide robust security solutions. Additionally, reinforcement learning can be used to optimize blockchain governance, ensuring that security policies adapt to the evolving threat landscape.

2.2 Related Projects

This section provides an overview of key EU projects that members of the NATWORK consortium have been involved in, emphasizing their contributions and relevance to the initiatives discussed in this paper. These projects have laid the groundwork for the innovative approaches proposed in NATWORK, particularly in the areas of IoT security, AI-driven intrusion detection, penetration testing, and blockchain-based trust management. By building on the successes and lessons learned from these projects, NATWORK aims to further advance the security capabilities of IoT networks within the 6G framework.

SANCUS (H2020) The SANCUS project[5] focuses on the efficient and automated security of 5G Standalone (SA) networks. A key innovation of the project is the quantification of the trade-off between security, privacy, and reliability, presented for the first time through specific formulas and Key Performance Indicator (KPI) metrics.

The project leverages key tools and methodologies to enhance network security. 5Greplay [14] will be used for delivering security assessments in conjunction with the AcE engine. Additionally, the MONT Monitoring Tool (MMT) will serve as a central component for the SiD engine. In addition, CERTH contributes by bringing in expertise from AI-driven intrusion detection models developed for the SiD engine, closed-form and duality-free security optimization solutions from MiU/GiO, and AI-enhanced penetration testing modules created for the AcE engine.

[5] https://www.sancus-project.eu

SerIoT: Secure and Safe IoT (H2020) The SerIoT project[6] developed an open and reference framework designed for real-time monitoring of traffic across heterogeneous IoT platforms. The framework is capable of recognizing suspicious patterns, assessing them, and detecting security breaches, privacy threats, and abnormal events. It also provides parallel mitigation actions that operate seamlessly in the background. The project integrates software-defined networking (SDN) and Fog computing to bolster the security of IoT infrastructure.

NATWORK is leveraging security solutions developed within SerIoT. This includes the integration of monitoring and alerting solutions as well as the Service Management Plane from the Fog substrate. SerIoT also contributed to the development of machine learning-based security solutions such as anomaly detection, secure traffic routing, and cyber-attack mitigation, which will be utilized and further refined within NATWORK.

CyberSpec Armasuisse S+T The CyberSpec project[7] focused on creating a labeled dataset to model the internal behavior of Raspberry PIs under the influence of various types of malware. This dataset captures how different malware families affect various metrics and dimensions of Raspberry PIs, which could be extrapolated to other Linux-based systems. Key metrics analyzed include Hardware Performance Counters (HPC), system calls, and resource usage (CPU, memory, and network).

Within the NATWORK project, the AI-based anomaly detection module developed in CyberSpec will be adapted to detect anomalies caused by malware. This module classifies anomalies, aiding in the selection, specification, and implementation of appropriate countermeasures. The techniques utilized in CyberSpec, encompassing both supervised and unsupervised AI-based methods, will be leveraged to enhance NATWORK's capabilities in anomaly detection and response.

3 NATWORK's Use Case 3: IoT Security

3.1 UC#3.1: Enabling anomaly detection using machine learning automated techniques for attack detection

The growing complexity and scale of IoT networks in 6G ecosystems necessitate advanced security measures to safeguard against emerging threats, particularly Distributed Denial of Service (DDoS) attacks. UC#3.1 aims to address this challenge by developing sophisticated machine learning (ML) algorithms that can autonomously detect, classify, and respond to various DDoS attacks in real-time. This use case focuses on integrating AI-driven anomaly detection techniques to enhance the security posture of IoT networks.

[6] https://seriot-project.eu
[7] https://www.csg.uzh.ch/csg/en/research/CyberSpec.html

Machine Learning-Based Intrusion Detection The core of UC#3.1 involves creating ML-based intrusion detection systems (IDS) capable of identifying anomalies within IoT device traffic. These anomalies often serve as early indicators of potential DDoS attacks or other malicious activities. The IDS leverages supervised learning models, particularly Convolutional Neural Networks (CNNs), which are trained on large datasets of normal network traffic. By learning the patterns of regular operations, the CNN can effectively recognize deviations that suggest the presence of an attack.

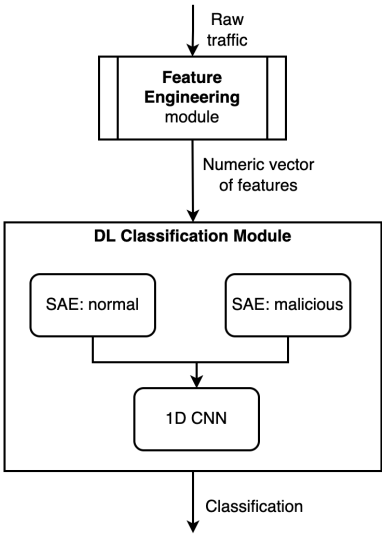

Fig. 1. Montimage AI Platform's architecture for network traffic analysis

AI-Assisted Anomaly Identification and Classification To enhance detection accuracy, the NATWORK project integrates AI-assisted techniques for anomaly identification and classification. These advanced methods leverage sophisticated algorithms to differentiate between benign anomalies, such as network congestion, and malicious activities like DDoS attacks. The architecture of the Montimage AI Platform [10, 9], as depicted in Fig. 1, forms the core of this approach. By harnessing the power of AI, the system is capable of continuous learning and adaptation, allowing it to respond effectively to new and evolving threats, thereby improving detection accuracy over time. Furthermore, the AI component supports dynamic threshold setting through reinforcement learning algorithms, which adjust the sensitivity of anomaly detection based on real-time network conditions. This adaptive approach helps to minimize false positives and enhances the overall reliability and resilience of the system.

Reinforcement Learning for Dynamic Threshold Setting Dynamic threshold setting is crucial for maintaining a balance between sensitivity and specificity in anomaly detection. Using reinforcement learning, the system can adaptively adjust thresholds based on the real-time analysis of network traffic and historical data. This approach ensures that the IDS remains effective even as network conditions evolve, preventing attackers from exploiting static thresholds to bypass detection mechanisms.

CNNs for DDoS Attack Detection CNNs play a pivotal role in this use case by analyzing complex network traffic patterns to detect DDoS attacks. These neural networks are particularly suited for identifying spatial and temporal patterns within the data, making them ideal for detecting sophisticated attacks that may not be apparent through traditional analysis methods. By training CNNs on a diverse set of traffic patterns, including both normal and attack scenarios, the system can accurately pinpoint when an attack is occurring and initiate appropriate mitigation measures.

Real-Time Visibility and Fast Mitigation The combination of AI, ML, and in-network processing provides real-time visibility into the state of the network, enabling swift identification of suspicious activities. Once an anomaly is detected, the system can trigger immediate mitigation actions, such as rate limiting or traffic rerouting, to neutralize the threat. The fast reaction time afforded by these techniques is critical for protecting IoT devices and maintaining the integrity of the 6G network against DDoS attacks.

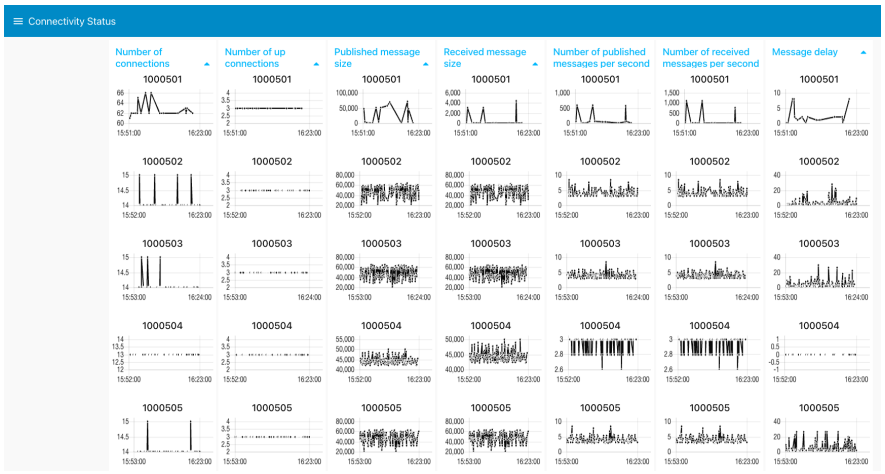

Fig. 2. Real-time visibility example provided by Montimage's Root Cause Analysis tool [7]

In-Network Acceleration and Event Detection To meet the demands of real-time detection and response, UC#3.1 emphasizes in-network acceleration of ML models. This involves deploying lightweight ML models closer to the data source, such as at gateways or far-edge devices, to reduce latency and improve the speed of anomaly detection. Coupled with efficient data collection and event detection mechanisms, this approach ensures that the system can quickly identify and respond to threats, minimizing potential damage.

In summary, UC#3.1 represents a comprehensive approach to enhancing IoT security through automated, AI-driven anomaly detection. By leveraging advanced machine learning techniques, including Convolutional Neural Networks (CNNs) and reinforcement learning, the system can effectively detect and mitigate DDoS attacks in real-time. This use case not only bolsters the security of IoT networks but also lays the groundwork for scalable, adaptive security solutions capable of keeping pace with the rapidly evolving threat landscape in 6G environments.

3.2 UC#3.2: Validating AI-driven penetration testing and vulnerability assessment for attack mitigation

As 6G networks usher in a new era of connectivity, the sheer scale and complexity of IoT deployments pose unprecedented security challenges. The vast increase in IoT devices connected to these networks demands innovative approaches to identifying and mitigating potential vulnerabilities before they can be exploited by attackers. UC#3.2 addresses this critical need by developing advanced AI-driven penetration testing and automated vulnerability assessment techniques specifically tailored for the 6G IoT landscape (Fig. 3).

Fig. 3. Overview of AI-Driven Security Techniques in 6G IoT Networks

Machine Learning-Based Vulnerability Assessment This feature focuses on creating automated tools that leverage machine learning to perform continuous vulnerability assessments on IoT devices. These tools will be capable of identifying potential security weaknesses and prioritizing them based on risk levels. The use of machine learning allows the system to adapt to new and emerging threats, ensuring that vulnerability assessments remain relevant and effective as the threat landscape evolves.

AI-Powered Penetration Testing Traditional penetration testing methods are often manual and time-consuming, making them unsuitable for the dynamic and expansive 6G IoT environment. UC#3.2 aims to automate this process using AI-powered techniques, enabling rapid and thorough testing of IoT devices and networks. By simulating attacks, these AI-driven tools can identify weaknesses in a proactive manner, allowing for the implementation of countermeasures before an actual breach occurs.

Natural Language Processing (NLP) for Social Engineering Attacks Social engineering attacks, where attackers manipulate individuals into revealing confidential information, remain a significant threat. UC#3.2 will explore the use of advanced NLP models, such as Transformers, to both understand and generate social engineering attacks. These models can analyze publicly available data, like social media profiles, to craft highly personalized and convincing phishing attempts. By understanding these tactics, the system can develop defenses to detect and prevent such attacks.

Protocol Security Analysis Ensuring the security of communication protocols within 6G IoT networks is of critical importance. In this use case, we will conduct an in-depth analysis of the security protocols, with a particular focus on fuzzing techniques. Fuzzing will be employed to rigorously test the protocols for vulnerabilities, especially in key management processes. By injecting unexpected or malformed data into the protocol operations, we aim to uncover weaknesses that could be exploited by attackers. This approach will help in identifying potential security flaws and attack vectors, such as attack trees, that could compromise both the security and privacy of IoT networks. The results of this fuzzing-based analysis will inform the development of more robust security measures, ensuring that the protocols can withstand sophisticated cyber threats.

In short, UC#3.2 aims to provide a robust framework for preemptively securing IoT devices in 6G networks. By integrating AI-driven techniques, the use case ensures that potential vulnerabilities are identified and addressed before they can be exploited, thereby reducing the likelihood of successful attacks and minimizing service disruption. The inclusion of NLP-based social engineering detection and comprehensive protocol analysis further strengthens the security posture of IoT ecosystems. The methodologies developed in UC#3.2 will contribute to a more resilient IoT infrastructure, capable of withstanding sophisticated cyber threats. As 6G networks continue to evolve, the strategies and tools

created within this use case will be instrumental in safeguarding the billions of IoT devices expected to be deployed, ensuring the continuity and security of critical services in the face of growing cyber risks.

3.3 UC#3.3: Enhancing blockchain-based security and trust management end-to-end security

The evolution of IoT networks within 6G ecosystems demands innovative approaches to secure communications and data processing, particularly given the decentralized nature of such environments. UC#3.3 focuses on enhancing decentralized security and trust management by leveraging cutting-edge technologies to ensure end-to-end protection across IoT devices.

Decentralized Technology for Secure Communication and Data Processing In UC#3.3, decentralized technologies, such as blockchain [15] and distributed ledgers [6], will be employed to secure communication and data processing. These technologies offer a robust framework for ensuring the integrity and confidentiality of data, making them ideal for the highly distributed and dynamic nature of IoT networks in 6G. The decentralized approach eliminates the single points of failure that are often exploited in centralized systems, thereby enhancing the overall resilience of the network against cyber threats.

End-to-End "Lightweight" Security Mechanisms To address the resource constraints typically associated with IoT devices, we will develop lightweight security mechanisms that provide robust protection without overburdening the devices. These mechanisms will be designed to secure all communication channels between IoT devices, ensuring that data transmitted across the network is protected from unauthorized access. The focus on lightweight solutions is crucial for maintaining the efficiency and performance of IoT devices, which are often limited in computational power and energy resources.

Decentralized Access Control and Trust Management UC#3.3 will implement decentralized access control mechanisms to manage permissions and access rights across the IoT network [5]. These mechanisms will be complemented by trust management systems that utilize AI-powered verification and validation processes. The integration of AI in trust management will enable dynamic and context-aware decision-making, allowing the system to adapt to new threats and ensure that only authorized entities can access sensitive data or critical functions. A reference architecture is demonstrated in Fig. 4

Formal Analysis for Protocol Security Validation To guarantee the security and effectiveness of the proposed and adopted protocols, UC#3.3 will employ formal analysis techniques. These methods will rigorously evaluate the

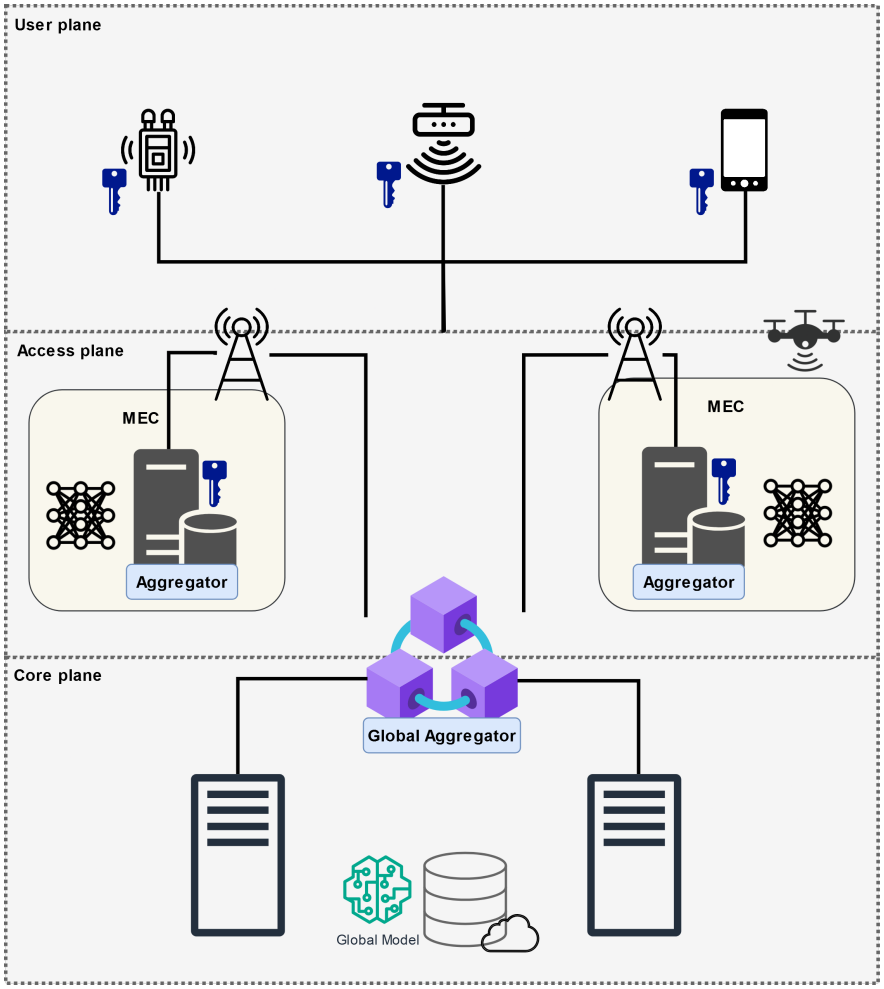

Fig. 4. Decentralized Security Architecture for IoT in 6G Networks

security properties of the protocols, identifying potential vulnerabilities and verifying that the protocols meet predefined security goals. The formal analysis will serve as a critical validation step, ensuring that the decentralized security mechanisms are both theoretically sound and practically reliable.

By implementing UC#3.3, the NATWORK project aims to establish a secure and resilient IoT infrastructure for 6G networks. The decentralized security framework developed in this use case will offer a scalable solution that can adapt to the growing complexity of IoT ecosystems, ensuring that communication and data processing remain secure even as the network expands. This approach will not only protect against unauthorized access and data breaches but also build

trust among network participants, fostering a more secure and reliable IoT environment.

4 EXPECTED OUTCOME

To effectively assess the performance and impact of the solutions developed in the NATWORK project, specific Key Performance Indicators (KPIs) [4] have been established. These KPIs measure critical aspects of security, such as detection speed, accuracy, and system resilience. Below is a detailed description of the expected outcomes for the project's key components, aligned with the KPIs to be satisfied in the whole Use Case 3:

4.1 AI-Based Anomaly Detection and Root Cause Analysis

The AI-based anomaly detection and root cause analysis module will leverage advanced machine learning algorithms to identify and classify anomalies in IoT networks rapidly. This system is designed to detect various attack types, including Distributed Denial of Service (DDoS), data breaches, and unauthorized access, by analyzing network traffic patterns and device behaviors.

4.2 IDS and Penetration Testing Tools for IoT

The Intrusion Detection Systems (IDS) and AI-driven penetration testing tools developed for IoT networks will provide robust mechanisms for identifying vulnerabilities and preventing security breaches. These tools will be designed to operate within the constraints of IoT environments, offering high accuracy and low latency in detection and response.

4.3 Blockchain for IoT Trust Management

The blockchain-based trust management system will establish a decentralized and secure framework for managing access and ensuring the integrity of communications within IoT networks. This system will prevent unauthorized access and enhance the reliability of IoT interactions by maintaining a transparent and immutable record of all transactions.

4.4 KPI Alignment

- KPI 3.1 - Mean Time to Detect (MTTD):The solutions provided in Use Case 3 will be optimized to detect potential intrusions rapidly, with a mean detection time under 5 minutes for ML-based rules and 10 milliseconds for MMT rules. This quick detection is essential for preventing breaches in real-time.
- KPI 3.2 - Number of False Positives (FP): Use Case 3 tools will be fine-tuned to minimize false positives to less than 1%, ensuring that the alerts generated are relevant and accurate, preventing unnecessary interventions.

- KPI 3.3 - Number of False Negatives (FN): In Use Case 3, we aim to maintain a false negative rate of less than 1%, effectively capturing a wide range of attacks and vulnerabilities, thereby reducing the risk of undetected security breaches.
- KPI 3.4 - Packet Loss Ratio (PLR): The solutions will be optimized to handle IoT communication with minimal packet loss, ensuring a Packet Loss Ratio (PLR) of less than 0.001% even in low-bandwidth environments. This is critical for maintaining the reliability and efficiency of IoT operations.
- KPI 3.5 - Mean Time to Resolve (MTTR): The tools will facilitate rapid resolution of detected vulnerabilities or attacks, with a mean time to resolve any issues under 10 minutes. This quick resolution minimizes the impact of any detected threats on the IoT network's operations.
- KPI 3.6 - Encryption Coverage (EC): The architecture in Use Case 3 will ensure reaching high percentage of encryption coverage of the data both at rest and in transit.
- KPI 3.7 - Access Control Violation Rate (ACVR): The architecture in Use Case 3 aims to minimize the percentage of violation in access control which will be successful, providing a robust access control and trust based mechanism.

The expected outcomes of these three components—AI-based anomaly detection, IDS and penetration testing tools, and blockchain for trust management—are directly aligned with the project's stringent KPIs. By meeting these KPIs, NATWORK aims to significantly enhance the security and resilience of IoT networks within 6G ecosystems, addressing the evolving threat landscape with innovative, scalable solutions.

5 CONCLUSION

The NATWORK project's strategy for enhancing IoT security within 6G networks, as illustrated through use cases UC#3.1, UC#3.2, and UC#3.3, presents a robust and all-encompassing framework for safeguarding IoT devices against a variety of cyber threats. By incorporating advanced technologies such as AI, machine learning, and blockchain, these use cases deliver security solutions that are not only scalable and efficient but also resilient in the face of evolving challenges. Moving forward, the NATWORK project will focus on refining these approaches to enhance their efficiency and effectiveness. This will include optimizing algorithms for even faster detection and response times, reducing false positives and negatives, and ensuring that these solutions can be seamlessly integrated into larger and more complex IoT ecosystems. Additionally, the project will explore the application of these technologies to emerging IoT use cases, ensuring that the solutions remain relevant and capable of addressing the evolving threat landscape in 6G networks and beyond. By continuously improving these security frameworks, the NATWORK project aims to set a new standard for IoT security in the era of 6G.

Acknowledgments. This work has received funding from the Smart Networks and Services Joint Undertaking (SNS JU) under the European Union's Horizon Europe research and innovation programme, in the frame of the NATWORK project (Net-Zero self-adaptive activation of distributed self-resilient augmented services) under Grant Agreement No 101139285. We would like to express our gratitude to Georgios Agrafiotis, Konstantinos Giapantzis, Virgilios Passas, Ilias Sirigos, Athanasios Korakis, Konstantinos Votis from Centre for research and technology Hellas for their invaluable contributions to the conceptualization and initial phases of this work. Although they are not listed as co-authors, their insights and efforts were crucial in shaping the direction of this research. We also acknowledge their support and collaboration throughout the course of this study.

References

1. NATWORK project, Last visited in August 2024.
2. Asma Alotaibi and Ahmed Barnawi. Idsoft: A federated and softwarized intrusion detection framework for massive internet of things in 6g network. *Journal of King Saud University - Computer and Information Sciences*, 35(6):101575, 2023.
3. Asma Alotaibi and Ahmed Barnawi. Securing massive iot in 6g: Recent solutions, architectures, future directions. *Internet of Things*, 22:100715, 2023.
4. Yun Chen, Wenfeng Liu, Zhiang Niu, Zhongxiu Feng, Qiwei Hu, and Tao Jiang. Pervasive intelligent endogenous 6g wireless systems: Prospects, theories and key technologies. *Digit. Commun. Networks*, 6:312–320, 2020.
5. Mohammed O Fadel and Mohammed BM Kamel. Authentication and data access challenges in safeguarding industrial iot. *Lecture Notes in Electrical Engineering*, 1195:1–12, 2024.
6. Mohammed BM Kamel, Peter Ligeti, Adam Nagy, and Christoph Reich. Distributed address table (dat): A decentralized model for end-to-end communication in iot. *Peer-to-peer networking and applications*, 15:178–193, 2022.
7. Wissam Mallouli Edgardo Montes de Oca Luong Nguyen, Vinh Hoa La. Book chapter: Validation, verification and root-cause analysis. In *DevOps for Trustworthy Smart IoT Systems*. Now Publishers, 2021.
8. Dinh C. Nguyen, Ming Ding, Pubudu N. Pathirana, Aruna Seneviratne, Jun Li, Dusit Niyato, Octavia Dobre, and H. Vincent Poor. 6g internet of things: A comprehensive survey. *IEEE Internet of Things Journal*, 9(1):359–383, 2022.
9. Huu Nghia Nguyen, Manh-Dung Nguyen, and Edgardo Montes de Oca. A framework for in-network inference using p4. ARES '24, 2024.
10. Manh-Dung Nguyen, Anis Bouaziz, Valeria Valdes, Ana Rosa Cavalli, Wissam Mallouli, and Edgardo Montes De Oca. A deep learning anomaly detection framework with explainability and robustness. ARES '23, 2023.
11. Manh-Dung Nguyen, Vinh Hoa La, R. Cavalli, and Edgardo Montes de Oca. Towards improving explainability, resilience and performance of cybersecurity analysis of 5g/iot networks (work-in-progress paper). In *2022 IEEE International Conference on Software Testing, Verification and Validation Workshops (ICSTW)*, 2022.
12. Zakria Qadir, Khoa N. Le, Nasir Saeed, and Hafiz Suliman Munawar. Towards 6g internet of things: Recent advances, use cases, and open challenges. *ICT Express*, 9(3):296–312, 2023.

13. Rodrigo Roman, Jianying Zhou, and Javier Lopez. On the features and challenges of security and privacy in distributed internet of things. *Computer Networks*, 57(10):2266–2279, 2013. Towards a Science of Cyber Security Security and Identity Architecture for the Future Internet.
14. Zujany Salazar, Huu Nghia Nguyen, Wissam Mallouli, Ana R. Cavalli, and Edgardo Montes de Oca. 5greplay: a 5g network traffic fuzzer - application to attack injection. In *Proceedings of the 16th International Conference on Availability, Reliability and Security*, ARES '21, New York, NY, USA, 2021. Association for Computing Machinery.
15. Dalton Cézane Gomes Valadares, Angelo Perkusich, Aldenor Falcão Martins, Mohammed BM Kamel, and Chris Seline. Privacy-preserving blockchain technologies. *Sensors*, 23(16):7172, 2023.
16. Shen Wang, Chamara Sandeepa, Thulitha Senevirathna, Bartlomiej Siniarski, Manh-Dung Nguyen, Samuel Marchal, and Madhusanka Liyanage. Towards accountable and resilient ai-assisted networks: Case studies and future challenges. In *2024 Joint European Conference on Networks and Communications 6G Summit (EuCNC/6G Summit)*, 2024.