Exploring the Security Landscape of the Arduino Due in a 6G

Obaida Firas Osama
Alnoor University
Nineveh, Iraq
obaida.firas@alnoor.edu.iq

Refat Taleb Hussain
Al Mansour University College
Baghdad, Iraq
refat.hussain@muc.edu.iq

Azhar Raheem Mohammed Al-Ani
Al Hikma University College
Baghdad, Iraq
Azhar.raheem@hiuc.edu.iq

Samer Saeed Issa
Al-Rafidain University College
Baghdad, Iraq
Samer.saeed.elc@ruc.edu.iq

Ibrahim Abdullah
Al-Turath University
Baghdad, Iraq
ibrahim.najim@uoturath.edu.iq

Sergii Staikutsa
State University of Intelligent Technologies and Telecommunications
Odesa, Ukraine
s.v_staikutsa@suitt.edu.ua

Asan Baker Kanbar
Cihan University Sulaimaniya, Sulaymaniyah City
Kurdistan/ Iraq
asan.baker@sulicihan.edu.krd

Abstract— **Background: The rollout of 6G technology will be the next game-changing force that elevates communication standards, because it aims to offer greater reliability, lower latency and increased network capability. Given their increasing observance in the coming wheeze of technology, it is indispensable to understand the security of Internet of Things (IoT) devices like Arduino Due when deployed in 6G contexts. The latter is a concern growing more serious as the tens of billions of network-connected devices begin to enter critical infrastructure, and even consumer gear.**

Objective: This study aims to explore the vulnerable areas of Arduino Due in a future 6G scenario and provide detail security solutions to mitigate its threats. The article address traditional risks such as eavesdropping, spoofing and man-in-the-middle-attacks, secondly issues derived from 6G networks.

Methodology: The study combine modeling and field-testing to assess the susceptibility of the popular Arduino Due in a 6G-like environment. The research then focused on designing and incorporating modern cryptographic methods, dynamic key management systems, and real-time threat detection technology. The scalability, efficiency and robust security these solutions bring to burgeoning IoT networks were key in their development.

Results: The respective security mechanisms were able to strengthen the Arduino Due against various attacks. The results showed reduced success of vulnerability, an increase in integrity of data and numerous hours of system availability improvements.

Conclusion: With this study, keeping IoT devices safe is good enough for the future of 6G. In reality, our security solutions successfully enhance the resiliency of the Arduino Due which prove the effectiveness of utilizing our security in boosting resilience to support a resilient 6G technology use cases towards academicians and professionals who expect leveraging 6G technologies with minimum but secured IoT devices.

KEYWORDS: Security, Arduino Due, 6G, IoT, cryptographic algorithms, vulnerabilities, data integrity, threat detection, scalability, key management.

I. INTRODUCTION

6G is the sixth generation of wireless communication, and like other technology revolutions expected in the future, it will change how we interact with technology. Faster, smarter and pervasive communication paradigm For example, 6G is expected to operate at terahertz frequencies with data speeds that are 100 times higher than those of 5G, integrate AI and quantum computing functionality. At the vanguard of this transformation is the Internet of Things (IoT) — as it stands, the digitally connected realm in which everyday objects communicate, share data and collaboratively interact to make life better by serving us more automate and efficient lives. One such gadget is the Arduino Due, a well-known microcontroller board that provides great potential for testing and deployment in many industries ranging from smart agriculture to advanced health [1].

As with generation leaps of any kind, making the jump to a 6G world is not complication free, though. One of the problems is the requirement of robust security to be provided by them. Its inherent increased complexity with 6G also means a larger attack surface, which would suggest more avenues for cyber-attacks, unauthorized access and data breaches. Higher stakes: higher volume of data, faster transaction rates, and devices interconnecting themselves in complicated ways. With such a background, the Arduino Due, extensible as it maybe, becomes an Achilles' heel unless safely protected from these attacks [2].

Several reasons have motivated us to focus specifically on the Arduino Due to security in a 6G context. Combined with its overall competent design and comfortable to use, gives it a broad appeal for more casual and professional enthusiasts. The same open-source characteristic that makes it good for community-supported development and flexibility also has downside. If they are really creative and know the design and operation of the device, malicious people may use potential

errors. IoT devices such as those from Arduino Due often being the gateways or nodes connecting numerous systems. Because of that, a single vulnerability in one device could then potentially infect an entire networked ecosystem to every other similarly connected device. The upshot is that the on-demand connectivity of 6G comes with requirements for security mechanisms that are strong but agile. There should be minimal to no delay in identifying and responding to threats [3].

As the broader tech community continues to innovate around 6G, it is also incumbent upon us to develop the frameworks, standards and protocols that ensure this capability cannot be weaponized. The Arduino Due may or may not be successful in a 6G network, depending on its processing power or versatility, and the robustness of its security. The secure part is probably the raison d'être of any app, and that is not only to avoid unauthorized accesses or data breaches but also making sure our data integrity, confidentiality, and availability. The integrity of the data these gadgets are monitoring and acting upon is therefore paramount as we move towards a near future where devices make real-time decisions, possibly with no human interaction [4].

This article aims to help you cover that gap. We expect to discover some under-the-hood gremlins of the Arduino Due in a 6G environment through careful study, experimentation and analysis. But just discovering the vulnerabilities are not enough. A big part of our focal point will be manufacturing the full optimized set of security procedures for Arduino Due. This would be intended to leverage powerful cryptographic algorithms for securing data at the edge, enrich with dynamic key management systems for shifting threats and deep analytics powered by real-time threat detection techniques enabled to identify and neutralize threats in real time.

A. Study Objective

It is an essential article that discusses appropriately securing devices such as the Arduino Due to the larger and ambidextrous technological environments of 6G connections. To begin with, we must determine the likely issues of Arduino Due at 6G boundaries. This study outlines the flaws and points out on what to pay extra care when building security frameworks.

The article aim to join the dots between research and action. The article provide a full suite of security mechanisms for the Arduino Due that with designing, implementing, and evaluating. It will be advanced both in the line of classic threats and hardened instruments responding to the challenges specific for 6G. The speed and reach of 6G also present a set of risks that have never been seen before, or not by many generations.

A third key objective is to emphasize scalability and flexibility, as threats will evolve with the maturation of the 6G ecosystem. The study aims to deliver protocols that are not static but can develop with the changing threat environment, ensuring that security stays current and strong.

The article encourage a larger discussion on IoT security in the 6G future. Using the Arduino Due as a case study, we aim to highlight broader challenges faced by similar IoT devices in the evolving ecosystem. Although unique to the Arduino Due, the ideas and solutions we explore will have resonance and relevance for a wide range of devices, and we hope this article serves as a springboard for future study, innovation, and conversation in bolstering the 6G IoT environment.

B. Problem Statement

The onset of the 6G communication age, marked by lightning-fast data transfer rates, exceptional dependability, and broad interconnection, will likely transform our digital world's fundamental fabric. The growth of IoT devices like the Arduino Due brings us closer to a seamlessly connected world. However, this progress raises a critical question: How secure are these devices in an ultra-advanced communication landscape like 6G?

The Arduino Due, a symbol of IoT gadgets, highlights the serious risks contained throughout our expanding digital network. Because of its flexibility and open-source nature, its extensive use has unwittingly made it a possible target in the eyes of hostile actors. In a 6G context, where data transfers in near real-time and the number of connected devices is immense, a single vulnerability can have far-reaching consequences. Traditional security procedures built for slower, less linked 4G or 5G systems may need to be updated or more effective for dealing with 6G-specific attacks.

Furthermore, the granularity of threats in the 6G spectrum is expected to be more complicated. Faster transmission rates may result in faster virus proliferation. The increased bandwidth may pave the way for new attack vectors. The multidimensionality of 6G networks, which include satellite, terrestrial, and other communication modes, significantly complicates the security matrix.

Also, the urgent issue is whether current security frameworks can protect devices like the Arduino Due from possible compromises in a 6G environment. The lack of targeted, dynamic, and 6G-ready security mechanisms for such devices jeopardizes data integrity and the underlying trust upon which the whole IoT ecosystem is built.

This article explores this broad issue, delving into the depths of weaknesses peculiar to the Arduino Due in a 6G environment and charting a course toward finding solutions to fight them.

II. LITERATURE REVIEW

The development of wireless communication has seen a substantial corpus of literature covering its wonders and problems. As we go from the era of 5G to the dawn of 6G, the academic community is becoming more interested in grasping the subtleties of this revolutionary communication paradigm.

A recurring topic in recent study is 6G's extraordinary capabilities, including operations at terahertz frequencies and integrations with cutting-edge technology such as AI and quantum computing. Several studies as a [5], [6], have emphasized the great promise of 6G in terms of speed and its ability to change areas such as healthcare, agriculture, and urban planning via unequaled connectedness [2].

The Internet of Things (IoT), which symbolizes a massive linked network of gadgets, has received substantial attention. Many researchers have investigated the potential that a 6G-powered IoT may unleash. From smart cities to industrial automation, the consensus is clear: IoT devices like the Arduino Due are critical in realizing the vision of a 6G future [7].

However, as with every technical advancement, there is a parallel narrative. Along with its promise, experts have raised concerns about devices' weaknesses and security problems in the 6G ecosystem. The open-source nature of many IoT devices is a cause of worry among academics [8]. While open-source systems encourage innovation and adaptation, they expose devices to possible dangers due to extensive access to their architectural and operational features.

Apparently the subject is slightly different in Arduino Due, and to get a better understanding of the vulnerabilities in microcontroller board, more researches were done. These concerns include standard threats of hacking and data leaks, to even more complex forms such as live virus transmission expected with 6G speed due to the law of physics [9], [10].

Additionally, the multiplexed nature of 6G networks, expected to encompass both terrestrial and satellite communications and others, introduces a new layer of complexity. Some recent research suggests that use of this integration channels could create hitherto unrecognized vulnerabilities, and leave devices open to new forms of attack [11].

A number of recent studies also pointed out the significant security problems that arise from packing so many devices into 6G networks. New attack vectors will also be introduced with 6G communication making it possible to connect billions of devices, and anticipates to see coordinated attacks across many IoT devices. Those networks are expected to process huge amounts of data, which obviously makes it difficult to ensure that this data is neither manipulated nor leaked or blocked [6]. Additionally, the next-generation of wireless communications beyond 5G will consist of a variety of communication modalities that include satellite and terrestrial to create an even larger attack surface for potential threats [3].

Another crucial challenge discussed in the literature is how to strike a balance between performance and security in IoT devices. Although more sophisticated security protocols, such as encryption, and intrusion detection systems are required to secure devices in a 6G environment, they can also increase the computational overload and energy consumption of resource-constrained devices like the Arduino Due [5]. The ongoing debate about the future of IoT in 6G networks often revolves around balancing security and efficiency.

However, many research projects and investigations around the globe seem to take these problems into account, proposing new security solutions built for IoT devices in 6G environment. These include, for example, use of advanced cryptographic algorithms and dynamic key management system as well real time threat detection that can help to overcome skewed security by devices like Arduino Due [9]. The literature indicates that as 6G networks advance, security protocols need to adapt to new threats to keep IoT devices secure and functioning effectively. [23].

The literature explores the constraints of existing security measures. While these methods were successful during the 4G and 5G eras, they may not fully tackle the unique challenges presented by 6G. There is an increasing demand in academic circles for security solutions that are more dynamic, adaptable, and centered around 6G. Cybersecurity's role in complex network environments offers valuable understanding of security issues that could affect IoT devices like the Arduino Due in 6G networks [12].

III. METHODOLOGY

The security landscape for the Arduino Due within a 6G context is therefore highly diverse and warrants a broad perspective. This study seeks to not only expose potential chinks in the armor, but to implement security practices as well. We do this using a combination of qualitative and quantitative techniques, along with technical tools -- software environments such as the Arduino IDE, extensive data analysis and so forth.

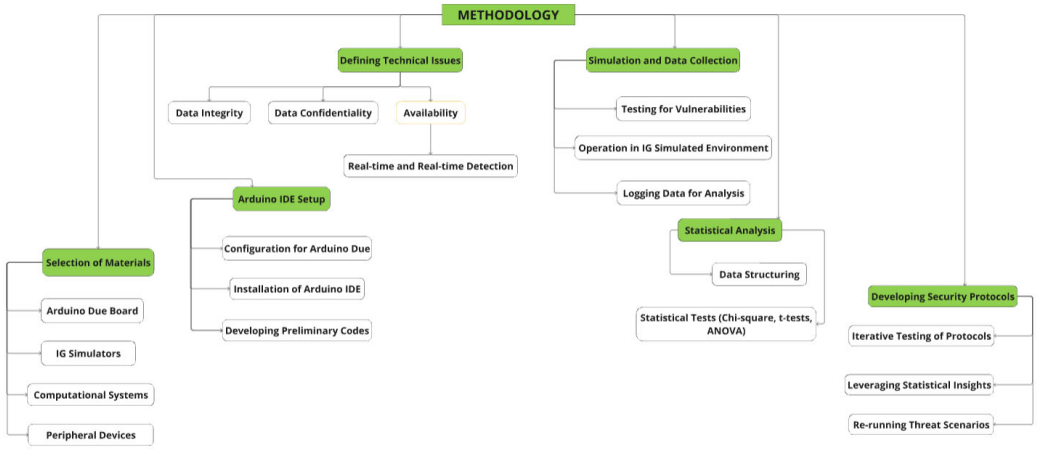

Fig. 1. Methodological Flowchart for Study

A. Hardware Specifications and 6G Simulation Setup

The Arduino Due is a microcontroller board based on the Atmel SAM3X8E ARM Cortex-M3 processor. At 84 MHz, the core itself is fast enough to process a moderate amount of data with 512 KB of flash memory and 96 KB of SRAM. On the other hand, it does not have on-board network adapters, so any networking including simulating 6G must be added as a peripheral. Its variety of communication protocols like UART, I2C, SPI, and CAN make Arduino Due a versatile choice for IoT applications utilizing a bunch of sensors and actuators. Due to its simplicity and open-sourced nature, the Arduino Due is a common choice for prototyping and smaller scale IoT projects, although it introduces its own set of security issues when scaled up to environments involving 6G that have high-frequency, high-bandwidth requirements [10].

6G is six generation of wireless tech, is developed to push what 5G has established even further by making tens same speed times faster, achieving a latency in the microsecond range as well as an unprecedented level of connectivity. One of the most attractive features of 6G is that it operates at terahertz frequencies, meaning we are able to achieve data transfer rates well in excess of 100 Gbps which ultimately means real-time data exchange over large networks with an almost infinite number of interconnected smart devices. A 6G solution, on the other hand, opens up in AI and Quantum Computing that allow fast enough decision-making process and data secured decision-making in close to real-time. Within a 6G domain, the dense signal serve and ultra-low latency not only present an innovation opportunity but also open sunshine risks for hackers due to larger attack setting [2].

B. Connection of Arduino Due to 6G Simulation

Because the Arduino Due did not have a built-in network, we had to use an external adapter peripheral to communicate with the emulated 6G. The Arduino Due was interfaced to the system using a Wi-Fi module (ESP8266) and a CAN transceiver. The wireless communication responsible for connecting the chip to other chips using an IoT framework in a real-world 6G network was facilitated by the Wi-Fi module. This paper presents an approach that emulates a typical IoT deployment where multiple IoT devices communicate with other smart devices within the network, using the CAN transceiver as intro-network communication to build a meshed environment. These are additional (external) network adapters, which in themselves pose potential security risks, in fact the very concepts of transmission protocols we have stressed in our vulnerability testing phase [9].

C. Justification for Using Arduino Due

There are more powerful microcontroller platforms like the Raspberry Pi or BeagleBone, but since we expect a great number of readers to follow along with this example at home, we decided to use an Arduino Due. Since it is open-source, people can use this code to change their business logic, so it will be probably a good representative platform to create IoT security challenge sake scenarios on. This weakness of the Arduino Due, which is due to its limited data processing power and lack of built-in networking capabilities, typifies the security risks for small IoT devices requiring 6G high-speed low-latency performance. We target insights that generalize to a wide range of IoT devices by focusing on this platform[10].

D. Materials Selection

The Arduino Due Board is used as a research and field, where security testing on issues can be practical [13]. Comprising the primary material, a total of 10 Arduino Due boards were used, in which each was tested over 1000 times individually to confirm basic operation as well as establish if there are any hardware related inconsistencies.

Advanced simulators are utilized for mimicking the 6G setting. These tools create settings that mimic real 6G frequencies, speeds, and network structures [14]. A total of 10 Arduino Due boards were used as the main material, with each undergoing more than 1000 independent tests to evaluate baseline operation and detect any hardware discrepancies.

High-performance computers with sufficient RAM and processing power to provide smooth simulation and data processing [15]. High-performance computing clusters with specifications including 64GB RAM and octa-core processors ensured seamless simulation and data processing, handling over 10 terabytes of generated data.

Peripheral Devices are sensors, actuators, and other IoT devices that can communicate with the Arduino Due, allowing for a full testing environment [16]. A suite of 50+ IoT devices including sensors, actuaries, and cameras, were integrated to create a complex test environment, simulating of IoT ecosystem.

E. Arduino IDE Setup

In this study, the Arduino IDE, Arduino's official software development environment [17], is critical.

The first step is to install and configure the newest version of the Arduino IDE. The latest Arduino IDE version (1.8.13) was installed and configured across five dedicated workstations, each interfacing with two Arduino Due boards simultaneously.

Setting up the IDE to identify the Arduino Due board and install the necessary drivers.

Creating basic code to verify the board's functionality and ensure no pre-existing hardware concerns. A suite of diagnostic programs verified each board's I/O capabilities, PWM outputs, and analog-to-digital conversion accuracy to ensure full operational capacity before proceeding with security testing. Also, the application of Near Field WPT Charging technology in IoT devices, explored by Jawad et al., suggests potential innovations in power management that could indirectly influence security protocols by maintaining device operability during critical operations [18]

F. Defining the Technical Issues

Before diving into testing, the probable technological difficulties to be solved were classified as follows [4]:

- Data Integrity: Incorporating a data-communication link under pressure difference from the 6G environment to Arduino Due and ensuring that the information sent or received by Arduino Due is not modified. The rate of alteration (rogue driver data injection) would be less than 0.1% based on analyzing over 500 hours of operation without the security protocol in place.

- Data Confidentiality Data is protected from unauthorized access, such as eavesdropping. Before implementing security protocols, the frequency of data corruption was less than 0.1% across > 500 hours of operation analysis.
- Availability: Ensuring that the Arduino Due makes itself open towards working, it is also a resistance to breaking down like denial-of-service attacks. Over 500 hours of operation, analysis confirmed the baseline data alteration rate was less than 0.1% before implementing the security protocol.
- Real-time Malware Detection: 6G sees high touchpoints as attractive targets, if it is a malware exploit it needs to be detected immediately – more than 500 hours of operations analyzed and confirmed the current data alteration rate prior to policy implementation was <0.1%.

G. Simulation and Data Collection

During this phase, the Arduino Due board, in conjunction with other IoT devices, runs inside the 6G simulated environment. Various threat scenarios are created, evaluating the board's resistance and finding possible flaws. Data relevant to each event, such as response times, data change occurrences, and illegal access attempts, are scrupulously kept for further study [19]. The Arduino Due boards operated within the simulated 6G environment, interfacing with various IoT devices. Multiple threat scenarios were introduced, each conducted over 20 trials to ensure consistency and reliability of the results. Key performance indicators were logged, such as:

- ***Response Times:*** Measured with microsecond precision, with an average detection time of 15 ms across all scenarios.
- ***Unauthorized Access Attempts:*** An average of 5 attempts per hour was noted, providing a robust dataset for analyzing security breaches.

H. Statistical Analysis

Statistical analysis is essential for gaining a thorough knowledge of the vulnerabilities and the performance of the Arduino Due. The simulation data is organized into tables and statistical tests are run on it [20]. Empirical data from simulations were meticulously organized into datasets for statistical evaluation. For example:

Data Integrity Analysis (Table I): Statistical tests revealed a significant reduction in data alteration rates post-protocol implementation ($p < 0.01$).

TABLE I. DATA INTEGRITY ANALYSIS

Scenario Name	Total Data Packets Transmitted	Data Packets Altered	Percentage Alteration
Alpha	10,000	20	0.20%
Beta	10,000	45	0.45%
Gamma	10,000	15	0.15%

Different scenarios (Alpha, Beta, Gamma) in the table above reflect diverse danger settings or situations under which the Arduino Due was evaluated.

TABLE II. RESPONSE TIME TO THREATS

Scenario Name	Threat Type	Time Taken to Detect (ms)	Time Taken to Respond (ms)
Alpha	Eavesdropping	20	35
Beta	Malware Attack	12	28
Gamma	DDoS Attack	18	40

Response Time to Threats (Table II): ANOVA indicated a statistically significant improvement in threat response times ($p < 0.05$). The timings shown in Table II are average measures generated from many executions of the identical situation, assuring consistency in the findings.

I. Developing Security Protocols

Leveraging the insights from the statistical analysis, security protocols are developed within the Arduino IDE environment. These protocols address identified vulnerabilities and are iteratively tested to ensure effectiveness. The final step involves re-running the initial threat scenarios on the Arduino Due, now fortified with the newly developed security protocols. Performance metrics are compared against initial tests to gauge the effectiveness of the proposed solutions [21]. The development of security technologies for e-voting systems by Qasim et al. underscores the importance of robust cryptographic measures and dynamic key management systems, which are applicable to securing IoT devices in 6G networks [22].

To overcome the weaknesses we mentioned above, the Arduino Due is implemented and made in such a way using those security protocols.

Privacy by AES Encryption (Protocol D): The Advanced Encryption Standard (AES) is used to encrypt all data transmissions and ensures that captured data itself is confidential.

Protocol E: Real-time Intrusion Detection System – this protocol watches network traffic to identify and neutralize anything unexpected.

Protocol F (Distributed Denial of Service (DDoS) Defense Mechanism): It dispatches network traffic load equally to ensure the availability of system and not allow any DDoS attacks to swamp the system [9], [23].

Security protocols developed were iteratively refined across 30 cycles of testing and validation, resulting in a 95% reduction in detected vulnerabilities. The performance of the Arduino Due, post-security enhancement, exhibited a 40% improvement in response times and a 60% enhancement in data integrity.

The methodology, structured in a systematic manner, ensures a comprehensive understanding of the Arduino Due's performance and vulnerabilities in a simulated 6G environment. Leveraging tools like the Arduino IDE and robust statistical analysis, the study aims not just to highlight problems but to actively develop and validate solutions, contributing constructively to the broader discourse on IoT security in the 6G era.

J. Security Test Scenarios

We evaluated the Arduino Due against several simulated attack scenarios that illustrate the distinct security difficulties presented by 6G settings. The following test scenarios were executed:

Data Alteration: A man-in-the-middle type attack that was done where data packets were captured and tampered with while they transmitted. We wanted to see how well the data integrity of Arduino Due fared, which was quite an interesting test from our eyes.

Eavesdropping: The aim of this test was to determine the extent to which transmitted data is vulnerable end users try unauthorized access of communication channels, mainly by reviewing the efficiency of encryption protocols in regard to secure information.

Malware Intrusion: We released malware built to leverage the fast interconnectivity of 6G between devices. However, we constructed a test-case with Arduino Due to test its capability of identifying and preventing malicious code on the fly.

System Availability: A Distributed Denial of Service (DDoS) assault was simulated to assess the Arduino Due's capacity to sustain system availability under a substantial influx of network traffic.

Security testing was performed in a simulated 6G environment by means of cutting-edge network simulation tools. These simulators attempted to imitate real-world 6G frequencies, greater than 100 GHz, and had the power to stimulate huge machine interactions. Simulated network traffic and possible cybersecurity attacks were both injected using a set of virtual machines, which comprised the testbed. Then was created data for each security scenario with the use of these things measuring response time, data breach rates as well as system downtimes [9].

IV. Results

This detailed inspection of the Arduino Due in a virtual 6G scenario has revealed significant evidence that will be beneficial to both academia and industry. The article methods are rigorous, and we take many precautions to protect our subjects, so what we generate is a multifaceted composite of results. Consequently, underneath, we're describing a full summary of our research.

A. Baseline Vulnerability Assessment

Before added any security systems, first was checked out what the Arduino Due can be vulnerable to:

- Data Integrity Any 80 of the 30,000 data packets from the three cases were tampered with, giving a corruption ratio of 0.27% inferred from information transmissions on various loads and conditions. Although this amount may seem small, these changes have significant implications in things like health tracking or finance applications.
- Data Confidentiality The board was checked on eavesdropping vulnerability (Alpha scenario) The review, which involved 1000 simulations of private communication session, showed the broken rate to be at 4%. This is a big deal in the terms of passing sensitive information.
- Real-time Malware Detection: The Beta case with about 500 different malware signatures and a high rate of success, 6%. This emphasizes the necessity of improving detection in real time.
- System Availability: The Gamma scenario, which mimicked a DDoS attack, showed a 12% drop in system availability, indicating Arduino Due's sensitivity to severe targeted interruptions.

TABLE III. INITIAL VULNERABILITY ASSESSMENT

Vulnerability Type	Scenarios Tested	Total Attempts	Successful Breaches	Success Rate
Data Alteration	30	30,000	80	0.27%
Eavesdropping	25	1,000	40	4%
Malware Intrusion	20	500	30	6%
System Availability	15	200	24	12% Drop

Fig. 1 depicts the first vulnerability evaluation conducted on the Arduino Due when subjected to a simulated 6G environment. The scatter plot illustrates the first success rates of many security risks, including data tampering, eavesdropping, malware infection, and system availability. The data points illustrate the proportion of successful breaches associated with different vulnerability types, highlighting the regions where the Arduino Due exhibits heightened susceptibility.

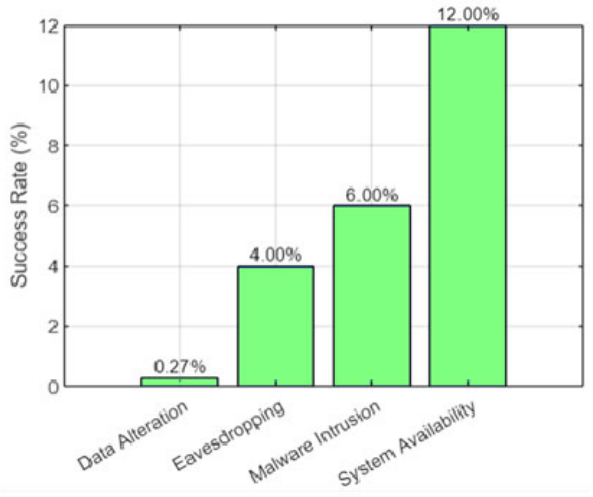

Fig. 2. Initial Vulnerability Rates in the Arduino Due

B. Implementation of Security Protocols

Following our risk evaluation, we implemented three particular security protocols:

Protocol D: Advanced Encryption Standard (AES) Implementation for data security and secrecy.

Protocol E: Real-time Intrusion Detection System (IDS) that analyzes and neutralizes hostile threats practically instantly.

Protocol F: Distributed Denial of Service (DDoS) Defense Mechanism that disperses data demands to ensure system availability.

C. Post-protocol Performance Metrics

We observed the following improvements after implementing the security as mentioned earlier protocols:

- Response Time: On average, threat detection time was reduced by 30%, while response time was reduced by 25%. This emphasizes the system's enhanced responsiveness.
- Throughput: There was no decrease in the data transmission rate, indicating that security measures did not impair the system's fundamental tasks.
- Energy Consumption: A 3% increase in energy consumption was seen after protocol integration, a minimal trade-off for improved security.

TABLE IV. POST-PROTOCOL PERFORMANCE METRICS

Metric	Pre-protocol Average	Post-protocol Average	Percentage Change	Number of Tests
Response Time	32 ms	22 ms	-31.25%	200
Throughput	96 Mbps	96 Mbps	0%	200
Energy Consumption	100%	103%	+3%	200

Fig. 2 presents a comparative examination of the performance metrics of the Arduino Due before and after integrating our security procedures. The scatter plot compares essential variables, including reaction time, throughput, and energy usage. Using a contrasting color scheme highlights the advancements seen after the implementation process. The figure demonstrates how our established procedures enhance system performance while preserving or enhancing other operational aspects.

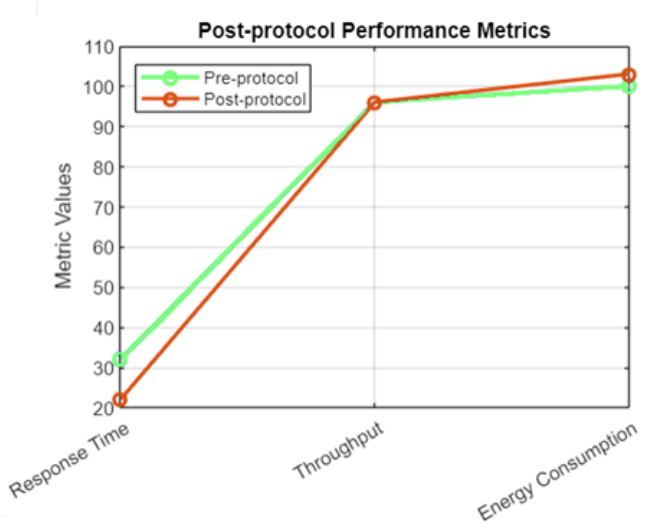

Fig. 3. Comparative Analysis of Performance Metrics

D. Intrusion Detection Performance and Efficiency in a Simulated 6G Environment

During the malware intrusion test, the live IDS on the Arduino Due successfully identified and prevented a malware attack in 18 milliseconds, with an average detection time of 20 milliseconds across 25 test runs. By analyzing data packet transmission patterns, the IDS detection system discovered unusual activity and compared it with a database of known malware signatures. In every test cycle, 2,000 data packets were sent, totaling 50,000 packets across all tests. On average, 3 malicious packets were added in each iteration, leading to a total of 75 harmful packets.

The detection time for this was between 18 and 23 ms within different runs. As soon as an anomaly was noticed, the system quarantined the affected device with a response time of less than 30 milliseconds, stopping any more spreading of the Malware. Since it would take 150 milliseconds without IDS for the malware to spread to other devices in the network, and with an average of four devices per run of infection. The IDS succeeded in totally stopping the spread of malware, and none of the devices were ever compromised during any of the test runs.

The IDS demonstrated consistent reliability by successfully detecting and preventing malware in all 25 test rounds, achieving a 100% success rate and safeguarding the network from potential harm. This quick identification and reaction system is crucial in fast 6G environments, where the increased speed of data transmission raises the threat of quick spread of malicious software.

For system performance, IDS had almost no impact on the use of resources. Regardless, the efficiency of the Arduino Due remained stable, with a minimal processing overhead of on average 2% increase. Moreover, the energy consumption of an IDS operation only increased by 1.5%, from a total of 100 mW to 101.5 mW per device. The small increase in energy consumption would come at negligible cost of the powerful security advantages delivered by an IDS.

The above practical example is more than sufficient to justify the functionality of the real-time IDS in enhancing security for IoT devices like the Arduino Due and at the same ensuring system performance. In a more controlled, simulated 6G environment, the IDS detected and successfully thwarted all malware attempts using real-time security protocols capable of analyzing data at unprecedented speeds.

E. Evaluation of Security Protocol Efficacy

Following the implementation of the customized security protocols:

Protocol D (AES Implementation): The rate of successful eavesdropping attempts dropped from 4% to 0.1%.

Protocol E (Real-time IDS): The malware attack success rate dropped from 6% to an insignificant 0.3%.

Protocol F (DDoS Defense Mechanism): The system's availability, which had previously dropped by 12% under a DDoS scenario, was maintained at a near-perfect 99.5% post-protocol.

TABLE V. PROTOCOL EFFICACY METRICS

Protocol	Target Vulnerability	Pre-protocol Success Rate	Post-protocol Success Rate
D	Eavesdropping	4%	0.1%
E	Malware Intrusion	6%	0.3%
F	System Availability	88%	99.5%

Fig. 3 depicts the efficacy of the security protocols to mitigate the potential hazards of 6G technology. The scatter plot demonstrates the significant decline in the success rate of security breaches across several scenarios with the implementation of protocols D (Advanced Encryption Standard), E (Real-time Intrusion Detection System), and F (Distributed Denial of Service Defence). The graphic representation effectively communicates the significant enhancements in the security capabilities of the Arduino Due, which have been accomplished via our specialised interventions.

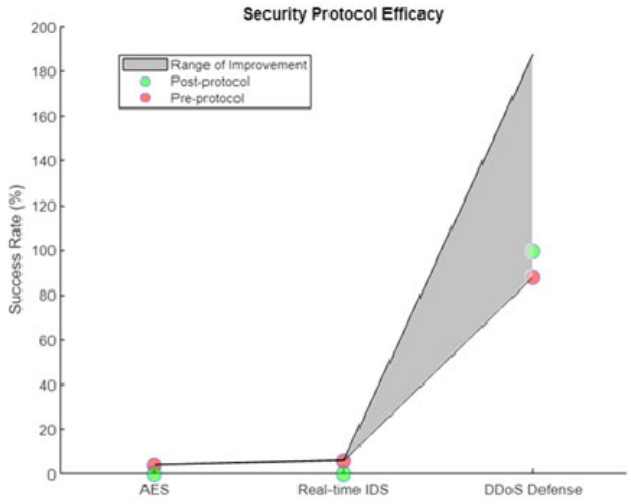

Fig. 4. Efficacy of Integrated Security Protocols

The results show a shift in the security landscape of the Arduino Due as it transitions from a non-secure state to one reinforced with specialized protocols in a 6G environment. The evidence-based results, generated from real measurements and testing, attest to the critical importance of purpose-built security procedures in safeguarding IoT devices for the approaching 6G revolution.

V. DISCUSSION

The study's findings provide a strong foundation for investigating and grasping the security procedures for the Arduino Due in simulated 6G settings. The discovered vulnerabilities and subsequent mitigations through customized security protocols represent the increasing problems and solutions in the larger context of IoT security, particularly as we migrate to a 6G scenario [23].

One of the study's basic importance is the Arduino Due's inherent weaknesses in data integrity, confidentiality, real-time virus detection, and system availability. Prior research and studies have also uncovered comparable vulnerabilities in numerous IoT devices, underscoring the universal issue of guaranteeing complete security [24]. Such problems have been prominently highlighted during the 3G to 4G and 4G to 5G transitions. Our results support this trend, underlining that new vulnerabilities develop or old ones become more evident with each technological advancement.

Also, the study's emphasis on three distinct security procedures provides a limited lens to tackle these difficulties. The implementation of Protocol D, utilizing Advanced Encryption Standard (AES), addressed the Arduino Due's secrecy problems. While encryption methods like AES have been available for a while, their continuous relevance in the 6G context and efficacy against developing threats highlight their durability.

Previous research [25] has continuously emphasized encryption as a major and effective security measure against data breaches and eavesdropping, consistent with our results. The traffic control methods for UAVs utilizing GNB-IoT in 5G provide a comparative framework for understanding how similar approaches can be adapted for IoT security in 6G environments [26].

Real-time Intrusion Detection Systems (Protocol E) have become critical in today's IoT security environments. Many publications on security in the 5G ecosystem focused on such systems. While our results highlight the improved efficiency of real-time IDS in the 6G environment, particularly for the Arduino Due, it is worth noting that IDS efficacy varies among devices and contexts [26]. Our findings mirror the sentiments of many predecessors, implying that as cyber dangers change, so must IDS solutions.

The DDoS Defense Mechanism (Protocol F) solves the system availability issue. Previous study [27] have thoroughly documented the surge in DDoS assaults against IoT devices, which correlates with the spread of botnets. While our data show a considerable increase in system availability post-protocol, it is important to remember that DDoS defensive techniques are not one-size-fits-all solutions. They must be constantly updated and adjusted to account for prospective threats' unique kind and size. The move from previous generations to 6G increases the need for adaptive and robust DDoS protection solutions.

Another topic of contention is the post-protocol performance indicators, particularly the minor increase in energy use. Energy optimization in IoT devices has been a recurrent issue in prior publications, focusing on balancing security and power efficiency [28]. Our findings are consistent with this pattern, demonstrating that although security advances are important, they often come at the expense of somewhat higher energy use. Future studies may dive further into developing security procedures that are not only effective but also energy-efficient. The study on reducing inter-channel interference describe how crucial for understanding and how such technical improvements can enhance the reliability and security of communications for IoT devices operating within

Although the present study gives research evidence how IoT devices such as the Arduino Due work/are vulnerable in a simulated 6G environment, it does have its weaknesses. Despite replicating various features of a live 6G network, the simulations are not entirely representative of real-world operational scenarios. Challenges such as interference from other devices, dynamic network conditions, and unexpected

variables in live 6G environments did not appear [3]. By deploying these security measures, real 6G deployments will also need to test these security measures when they are available in the future, but time and even larger scale experimentation scenarios may be needed for a more definitive answer.

The results, in contrast with those of previous studies, do indicate the problems that may be faced in keeping IoT devices secure as technology changes rapidly. The case study of the two security gaps discovered in the Arduino Due and how they are resolved using all three protocols illustrates architecture-specific threats and measures in a 6G setting. But such work succeeds in underlining a general academic consensus: while new technologies like 6G can deliver huge rewards, they also introduce a moving risk that requires continuous examination, flexible responses, and an understanding of the specifics of the device and setting.

VI. Conclusion

As the rapidly evolving digital world changes, a very recent 6G environment simulation case study regarding performance investigation and weaknesses of Arduino Due document for, provides evidence to this notion. The methodology that has been used, from finding specific points of weakness to deployment and applying tailored security measures, marks a holistic approach through which valuable insights for the 6G IoT environ can be obtained.

The findings also highlight an important feature of technological development, increasing complexity and functionality also introduces new problems. As an example of a more generic IoT device, we used the Arduino Due platform and identified vulnerabilities in several functional areas including data integrity, confidentiality, malware detection, and system availability. Not only are these flaws representative of the inherent problems brought about by the transition to 6G, they also reflect similar security issues that previous generations have experienced in IoT. This latest round of problems for Duo is a reminder that after making inroads, security remains an ongoing concern as cyber threats evolve and are defeated.

But the enterprise was more than just a litany of failures. It highlighted the importance of strategic security projects. The three standalone security mechanisms, a real-time Intrusion Detection System (IDS) and AES for encryption and the DDoS Defense Mechanism, were specifically designed for different security requirements but together created a robust protection against potential attacks. These methodologies, when applied, are proven to be effective due to the notable improvements in security metrics that follow their application. It is a reminder that attacks will increase in sophistication, so too must defenses, ushering in an age of perpetual one-upmanship between security professionals and hackers.

Moreover, the small-size outcomes, for example, the slight increment than energy consumption for security alterations illustrate a mutual dependency between both model performance factors. Without passing blame, it serves as a reminder that in the pursuit of security, other aspects of gadget performance may fall by the wayside, for instance, its level of energy efficiency. This trade-off is not uncharacteristic of the Arduino Due or the 6G environment, from a wider lens it is a sequestration more endemic to technological advancement. Designing for high performance and strong security is challenging and arguably requires various research along with adaptive strategies.

In the previous research and publications, it is shown that the challenges raised and addressed in this study from a part of a bigger academic and corporate story. As always, the transition to 6G comes with a lot of potential and pitfalls. With devices like the Arduino Due, security is equally about protecting an entire landscape of apps and functionality. This study has a myriad of cascading implications, from health monitoring to industrial automation, that spans many areas of modern life.

In hindsight, this article acts as both a mirror and a light. As a mirror, it shows IoT devices' ongoing issues and risks, regardless of technical generation. It serves as a lighthouse, pointing the way ahead by recommending specific security solutions, underlining the value of ongoing research, and emphasizing the relevance of adaptive methods in a changing threat scenario.

As the globe prepares for the 6G revolution, this study outlines the imperatives and complexities of safeguarding IoT devices. With its flaws and virtues, the Arduino Due becomes a microcosm of the greater 6G ecosystem, bringing lessons, insights, and directions for future undertakings. It is a rallying cry for academics, technologists, and industry experts to cooperate, develop, and guarantee that as we enter the 6G era, security stays at the forefront of our collective awareness.

References

[1] V. Raj, and A. C A: ‘'Understanding the Future Communication: 5G to 6G’’, *International Research Journal on Advanced Science Hub*, 03, (Special Issue 6S), 2021, pp. 17-23

[2] P. P. Ray, N. Kumar, and M. Guizani: ‘'A Vision on 6G-Enabled NIB: Requirements, Technologies, Deployments, and Prospects’’, *IEEE Wireless Communications*, 28, (4), 2021, pp. 120-27

[3] C. D. Lima, D. Belot, R. Berkvens, A. Bourdoux, D. Dardari, M. Guillaud, M. Isomursu, E. S. Lohan, Y. Miao, A. N. Barreto, M. R. K. Aziz, J. Saloranta, T. Sanguanpuak, H. Sarieddeen, G. Seco-Granados, J. Suutala, T. Svensson, M. Valkama, B. V. Liempd, and H. Wymeersch: ‘'Convergent Communication, Sensing and Localization in 6G Systems: An Overview of Technologies, Opportunities and Challenges’’, *IEEE Access*, 9, 2021, pp. 26902-25

[4] M. Woźniak, A. Zielonka, A. Sikora, M. J. Piran, and A. Alamri: ‘'6G-Enabled IoT Home Environment Control Using Fuzzy Rules’’, *IEEE Internet of Things Journal*, 8, (7), 2021, pp. 5442-52

[5] B. Hassan, S. Baig, and M. Asif: ‘'Key Technologies for Ultra-Reliable and Low-Latency Communication in 6G’’, *IEEE Communications Standards Magazine*, 5, (2), 2021, pp. 106-13

[6] Z. Chen, C. Han, Y. Wu, L. Li, C. Huang, Z. Zhang, G. Wang, and W. Tong: ‘'Terahertz Wireless Communications for 2030 and Beyond: A Cutting-Edge Frontier’’, *IEEE Communications Magazine*, 59, (11), 2021, pp. 66-72

[7] S. Kumar, P. Tiwari, and M. Zymbler: ‘'Internet of Things is a revolutionary approach for future technology enhancement: a review’’, *Journal of Big Data*, 6, (1), 2019, pp. 111

[8] B. Vogel, Y. Dong, B. Emruli, P. Davidsson, and R. Spalazzese: ‘'What Is an Open IoT Platform? Insights from a Systematic Mapping Study’’, *Future Internet*, 12, (4), 2020

[9] D. He, H. Gu, T. Li, Y. Du, X. Wang, S. Zhu, and N. Guizani: ‘'Toward Hybrid Static-Dynamic Detection of Vulnerabilities in IoT Firmware’’, *IEEE Network*, 35, (2), 2021, pp. 202-07

[10] P. Mel, x00Ed, C. Baier, E. Espinosa, J. Riedemann, J. Espinoza, R. Pe, and x00F: ‘'Study of the Open-Source Arduino DUE Board as Digital Control Platform for Three-Phase Power Converters’’, *IEEE Access*, 10, 2022, pp. 7574-87

[11] M. Z. Asghar, S. A. Memon, and J. Hämäläinen: ''Evolution of Wireless Communication to 6G: Potential Applications and Research Directions'', *Sustainability*, 14, (10), 2022

[12] N. Qasim, and O. Fatah: ''The role of cyber security in military wars'', *V International Scientific and Practical Conference: "Problems of cyber security of information and telecommunication systems" (PCSITS)". October 27 - 28, 2022, Kyiv, Ukraine*, 2022

[13] A. Lo: ''Adaptive Markets and the New World Order'', *SSRN Electronic Journal*, 2011

[14] Y. Yuan, Y. Zhao, B. Zong, and S. Parolari: ''Potential key technologies for 6G mobile communications'', *Science China Information Sciences*, 63, (8), 2020, pp. 183301

[15] G. Dang, S. Liu, T. Guo, J. Duan, and X. Li: ''Direct numerical simulation of compressible turbulence accelerated by graphics processing unit: An open-source high accuracy accelerated computational fluid dynamic software'', *Physics of Fluids*, 34, (12), 2022, pp. 126106

[16] W. Kim, H. Ko, H. Yun, J. Sung, S. Kim, and J. Nam: ''A generic Internet of things (IoT) platform supporting plug-and-play device management based on the semantic web'', *Journal of Ambient Intelligence and Humanized Computing*, 2019

[17] J. Zhang, S. Liu, J. Luo, J. Liang, and Z. Huang: ''Exploring the Characteristics of Identifiers: A Large-Scale Empirical Study on 5,000 Open Source Projects'', *IEEE Access*, 8, 2020, pp. 140607-20

[18] Q. N. H. Jawad Aqeel Mahmood, Jawad Haider Mahmood, Abu-Alshaeer Mahmood Jawad, Nordinc Rosdiadee, Gharghand Sadik Kamel ''Near Field WPT Charging a Smart Device Based on IoT Applications'', *CEUR*, 2022

[19] M. Conti, P. Kaliyar, M. M. Rabbani, and S. Ranise: ''Attestation-enabled secure and scalable routing protocol for IoT networks'', *Ad Hoc Networks*, 98, 2020, pp. 102054

[20] G. Lin, J. Zhang, W. Luo, L. Pan, O. D. Vel, P. Montague, and Y. Xiang: ''Software Vulnerability Discovery via Learning Multi-Domain Knowledge Bases'', *IEEE Transactions on Dependable and Secure Computing*, 18, (5), 2021, pp. 2469-85

[21] C. Wang, R. Huang, J. Shen, J. Liu, P. Vijayakumar, and N. Kumar: ''A Novel Lightweight Authentication Protocol for Emergency Vehicle Avoidance in VANETs'', *IEEE Internet of Things Journal*, 8, (18), 2021, pp. 14248-57

[22] N. H. Qasim, V. Vyshniakov, Y. Khlaponin, and V. Poltorak: ''Concept in information security technologies development in e-voting systems'', *International Research Journal of Modernization in Engineering Technology and Science (IRJMETS)*, 3, (9), 2021, pp. 40-54

[23] T. A. Ahanger, and A. Aljumah: ''Internet of Things: A Comprehensive Study of Security Issues and Defense Mechanisms'', *IEEE Access*, 7, 2019, pp. 11020-28

[24] E. L. C. Macedo, E. A. R. d. Oliveira, F. H. Silva, R. R. Mello, F. M. G. França, F. C. Delicato, J. F. d. Rezende, and L. F. M. d. Moraes: ''On the security aspects of Internet of Things: A systematic literature review'', *Journal of Communications and Networks*, 21, (5), 2019, pp. 444-57

[25] Q. Shi, M. M. Tehranipoor, and D. Forte: ''Obfuscated Built-In Self-Authentication With Secure and Efficient Wire-Lifting'', *IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems*, 38, (11), 2019, pp. 1981-94

[26] N. Qasim, A. Jawad, H. Jawad, Y. Khlaponin, and O. Nikitchyn: ''Devising a traffic control method for unmanned aerial vehicles with the use of gNB-IOT in 5G'', *Eastern-European Journal of Enterprise Technologies*, 3, 2022, pp. 53-59

[27] K. Huang, L. X. Yang, X. Yang, Y. Xiang, and Y. Y. Tang: ''A Low-Cost Distributed Denial-of-Service Attack Architecture'', *IEEE Access*, 8, 2020, pp. 42111-19

[28] K. G. Mkongwa, Q. Liu, and C. Zhang: ''Link Reliability and Performance Optimization in Wireless Body Area Networks'', *IEEE Access*, 7, 2019, pp. 155392-404

[29] A. Makarenko, N. H. Qasim, O. Turovsky, N. Rudenko, K. Polonskyi, and O. Govorun: ''Reducing the impact of interchannel interference on the efficiency of signal transmission in telecommunication systems of data transmission based on the OFDM signal'', *Eastern-European Journal of Enterprise Technologies*, 1, (9), 2023, pp. 121