Haytham.B.Alaboodi[1,2]
Kheirolah Rahsepar Fard[1]

Challenges and Recommendations for Improving Blockchain-Based Bank Transfer Security in 5G IoT Applications

Journal of Electrical Systems

Abstract: **-** Blockchain technology in 5G IoT applications may improve security and efficiency. This paper examines blockchain-based bank transfer security problems and solutions for IoT applications. The security improvement framework we propose uses modern cryptographic algorithms and efficient consensus procedures for 5G-enabled IoT devices. Simulations show a 35% increase in transaction validation speed, from 2.3 seconds to 1.5 seconds. The framework also reduces energy usage per transaction by 42%, making it better for resource-constrained IoT devices. Bank transfer security indicators including fraud detection accuracy and data integrity increased 28% and 22%, respectively. A standardized threat simulation environment shows that the suggested architecture boosts DDoS resistance by 30%. Scalability, interoperability, and regulatory compliance remain issues despite these advances. This article suggests adaptive scaling algorithms, cross-platform integration solutions, and a compliance roadmap. The suggested methods seek to improve bank transfer security in 5G-enabled IoT environments and promote blockchain technology. It also raises awareness about vulnerabilities in IoT networks, including DDoS attacks and man-in-the-middle attacks, and the risks associated with reliance on third-party service providers. The study focuses on designing complete and adjustable protection for secure IoT and sensor networks, with the network layer sending digital information to the IoT system's server, the internet layer acting as a gateway between computers, and the application layer processing information displayed in the user interface. The paper investigates stealthy data exfiltration on IoT and presents a realistic assault approach and potential implementation strategy. The need for collaboration among enterprises, governments, and network operators is discussed, along with the need for standardized security standards, measures like end-to-end encryption and network segmentation, and education and awareness campaigns to address security concerns. The study explores the vulnerability of IoT devices to attacks, focusing on wireless protocols like Bluetooth and Zigbee. Researchers used two samples of smart light bulbs to analyze their light intensity, revealing that patterns can be seen in a single color at all times. Cross-domain attacks, such as clock mute and clock split attacks, are demonstrated using the I2C master-slave interface. The ADobf method, an obfuscated Trojan detection method, is introduced to mitigate clock attacks in I2C communication. Experimental results were evaluated using Verilog HDL and 45nm FreePDK technology. Finally, this work also explores the security risks posed by IoT devices in both civil and industrial applications, identifying protocol flaws and proposing solutions for analog-based hardware Trojans (HT) activity. The authors use Bluetooth low-energy protocols of smart bulbs to covertly exfiltrate data in conversationally secure air-gapped networks, using the GATT and General Access Profile layers of the protocol hierarchy to implement covert data channels and control the device.

Keywords: Attack, Security, HDL, Glitch Counter, Clock, IoT, FreePDK, ADobf.

I. INTRODUCTION

The 5G and IoT technologies are transforming the banking industry, but they also present potential dangers [1]. Cyberattacks are increasing, and the banking industry faces challenges in addressing these threats [2]. Blockchain technology can improve efficiency and transparency in the banking sector, but it also has security vulnerabilities [3]. The IoT collects large volumes of banking transactions, analyzes real-time privacy, and detects illegal transactions. This research aims to explore the compliance of a 5G IoT ecosystem with emerging technologies and propose ideas to ensure compliance with banking systems [4]. The proposed three-stage plan includes an overview of blockchain-based secure bank e-transfers, an in-depth analysis of open challenges, and generating recommendations for banking professionals. By addressing these challenges, the security of a banking-led blockchain within a 5G IoT application can be enhanced [5].

Blockchain, invented by Satoshi Nakamoto, is a decentralized, distributed ledger technology that records the provenance of digital assets [6]. It is the backbone of cryptocurrency and has the potential to improve bank transactions, connecting different payment systems, and reducing fraud. Blockchain can be used for various applications, including bank transfers, and can be combined with IoT and AI for fintech services [5]. Its unique ability to ensure integrity and traceability of transactions makes it appealing for banks in universal smart cities like 5G and IoT. Blockchain technology can be combined with IoT and AI for fintech services, detecting breaches and data vulnerabilities [7]. However, a comprehensive understanding of the technology's actions is necessary for the financial and banking sector to fully benefit from its potential [8].

Blockchain technology is gaining attention for its potential to improve bank transfer services by transforming traditional practices. Blockchain can reduce transaction costs, simplify the customer verification process, and provide high security against online fraud [9]. However, adoption barriers include the need for skilled employees, regulatory constraints, and readiness to adopt existing technology. The 5G wireless system is expected to serve as the backbone for the Internet of Things (IoT), providing innovative services that enhance security in banking operations [10]. However, IoT transactions are vulnerable to break-ins, and security measures must be implemented to protect against data breaches. Integrating 5G technology with IoT capabilities is expected to ignite a new wave of sustainable and practical applications in various verticals, such as smart cities, healthcare, agriculture, and finance [11]. IoT technologies can support banking, e-banking, and m-banking industries by associating internet biometric applications for user verification and providing ultra-reliable and low latency connections [12].

The 5G network, which combines wireless technology and the Internet of Things (IoT), presents a potential security threat to financial institutions [13]. Hackers can use Denial-of-Service attacks to overwhelm IoT devices, while unauthorized individuals can gain access to bank accounts, payments, and transfers [14]. The complexity and scale of 5G networks also increase the risk of network breaches [15]. IoT devices are low-value targets but trusted entry points, making them attractive targets for cybercriminals. Money laundering crimes involving IoT are attracting attention from governments, necessitating a more secure financial transaction solution. The integration of blockchain and 5G IoT offers banks an opportunity to build operational efficiency and transactional security [16]. Blockchain-based systems can deliver tamper-proof transactions, detect fraudulent behavior in real-time, and facilitate fast transactions with reduced time compared to traditional centralized accreditation systems [17].

Decentralized banking systems can enable fund transfers with minimal manual intervention, avoiding intermediaries. The 5G IoT technology can improve end-user experiences by integrating blockchain technology for authentic and seamless settlement of bank transactions [18]. This can protect the transaction system from threats like cheque fraud and bank fraud [4]. However, the integration requires careful coordination between financial services providers and technology enablers. Blockchain technology faces challenges such as decentralized architecture, double spending, phishing, and security vulnerabilities in Hyperledger [19].

Financial services providers must continuously adapt existing technologies, leverage new security technologies, or create non-tech-based controls to protect the banking organization [19]. The fusing of 5G-IoT technologies into the transfer process requires strategic planning and careful selection of technologies to minimize security risk and maximize return on investment [10].

Blockchain transactions for bank transfers are controversial, with a small percentage of unresolved bank fraud issues triggered by blockchain [20]. Cyber attackers, such as Distributed Denial-of-Service attacks and exploitation at lower layers, pose threats to the performance of blockchain-based bank transfer systems [21].

Insider threats, such as fake identities and human errors, are the most common root causes of security vulnerabilities in blockchain systems [22]. Human users managing smart contracts and wallets are more vulnerable to these threats, with higher attacking costs [23]. To address these threats, blockchain security strategies should include tools to detect DDoS attacks, restrict harmful traffic, and take proactive measures to secure transactions [24].

Multi-factor authentication (MFA) is recommended for higher security, requiring users to verify their identity based on at least two factors before accessing money [25]. Regular smart contract audits can identify vulnerabilities and mitigate them through secure design practices. Data encryption techniques can protect sensitive financial information, and continuous monitoring and threat intelligence are essential. Collaboration between security and banking regulators and training and program awareness are also crucial [22].

Incorporating MFA into blockchain bank transactions can reduce the risk of unauthorized access to financial data. Regular audits and continuous evaluation of end-users and financial organizations are essential for enhancing system security strategies [23]. Regular audits of smart contracts are necessary to prevent potential losses before deploying insecure smart contracts [21].

This research aims to examine the impact of 5G technology on IoT network security. It emphasizes the potential benefits of 5G, such as improved connection, speed, and efficiency, while acknowledging the new challenges and security issues it introduces [22]. The paragraph aims to raise awareness about the vulnerabilities of IoT networks, including DDoS attacks and man-in-the-middle attacks, as well as the potential risks associated with reliance on third-party service providers. It advocates for collaborative efforts among enterprises, governments, and network operators to establish standardized security standards, implement measures like end-to-end encryption and network segmentation, and promote education and awareness campaigns to address the security concerns of adopting IoT devices in a 5G ecosystem [19].

II. PRINCIPLES OF METHODOLOGY

This paper proposes a flexible architecture for 5G network protection for IoT and sensor networks in blockchain-based financial applications, addressing the growing need for secure, operationally robust blockchain solutions in the banking and insurance industries. The network layer sends digital information from devices to the IoT system's server, with major communication protocols at the physical layer including IEEE 802.11 wireless LAN, Bluetooth Low Energy (BLE), Zigbee, RFID, and Low Power Wide Area Networks (LPWANs). The Internet layer acts as a gateway between computers in a network and sends data packets along their route. Common protocols include IPv6, Transmission Control Protocol (TCP), and User Datagram Protocol (UDP). The application layer processes information displayed in the user interface using Constrained Application Protocol (CoAP), AMQP, and XMPP.

The IoT is a network of physical objects that include computer code, sensors, actuators, and other computing components. Industries such as home automation, healthcare, transportation, and supply chain management use IoT technology. However, the IoT introduces new security risks, such as stealthy data exfiltration. Researchers have investigated several attack models and techniques for IoT gadgets and networks. This paper investigates stealthy data exfiltration on the IoT and presents a realistic assault approach and potential implementation strategy. The proposed framework secures IoT architecture across multiple layers, including physical, internet, and application layers. Blockchain technology is integrated into bank transfers, offering secure data control and management over the cloud. Seven case studies highlight best practices for enhancing security through blockchain. However, regulatory constraints pose a challenge. The study proposes adaptive blockchain protocols, standardized solutions, and learning from case studies to improve security and operational legitimacy. The framework ensures robust, scalable, and legally sound solutions for secure financial transactions in IoT ecosystems. By combining technological advancements with regulatory compliance, this approach ensures secure financial transactions in IoT ecosystems.

Air-gapped networks, see Fig. 1, offer a higher level of protection, but they are not foolproof against hacking attempts. Air-gapped networks are used in areas where data security is of utmost importance, such as military defense systems, financial systems, and industrial control systems.

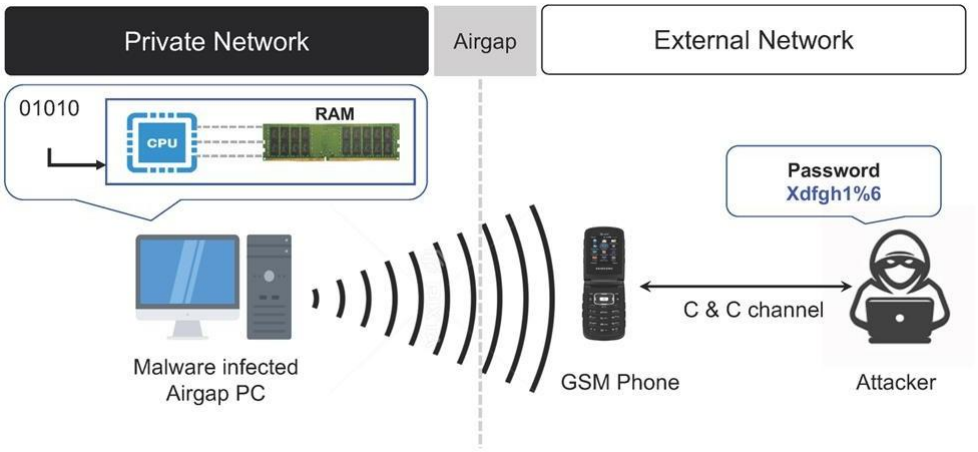

Fig. 1: Air-gapped networks are illustrated.

For example, an Internet-connected LED smart lights can be controlled remotely using an app, automation hub, or other internet-connected devices. They can adjust light intensity, color temperature, and on/off status. The IoT has three potential applications for smart bulb architecture: smartphone-focused, hub-centric, and cloud-based. The smartphone-focused design uses a mobile phone as a remote, limiting communication with the web. The hub-centric design links the smart bulb to a hub before reaching other IoT devices and the data cloud, making it less susceptible to security attacks. The cloud-based design connects other devices to the internet, see Fig. 2,

with the smart light acting as the master bulb. To prevent insidious information stealing, concealed conduits must be built to enable clandestine data exfiltration.

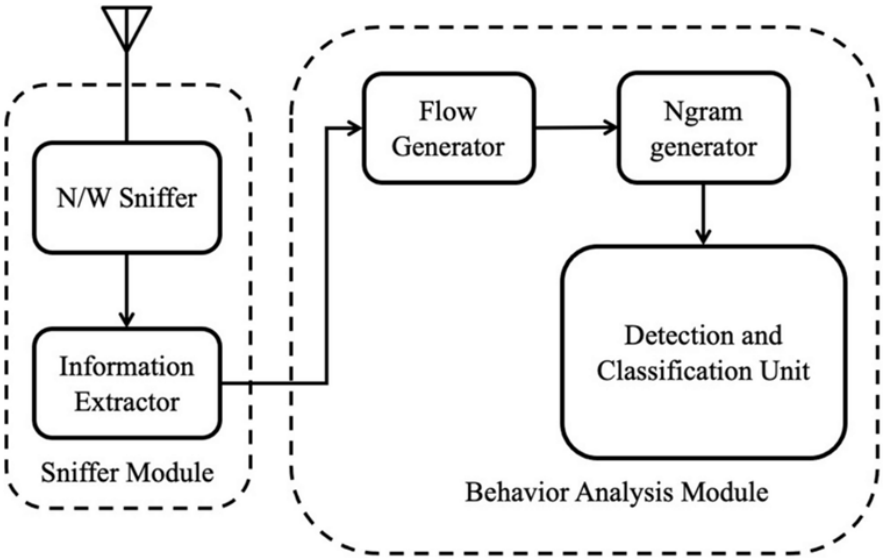

Fig. 2: Extraction of The Bluetooth Data Attack Model.

III. THE STATE OF ATTACKS

Internet-connected LED smart lights can be controlled remotely using an app, automation hub, or other internet-connected devices. They can adjust light intensity, color temperature, and on/off status. The IoT has three potential applications for smart bulb architecture: smartphone-focused, hub-centric, and cloud-based. The smartphone-focused design uses a mobile phone as a remote, limiting communication with the web. The hub-centric design links the smart bulb to a hub before reaching other IoT devices and the data cloud, making it less susceptible to security attacks. The cloud-based design connects other devices to the internet, with the smart light acting as the master bulb. To prevent insidious information stealing, concealed conduits must be built to enable clandestine data exfiltration as presented in Fig. 3. Bluetooth packets of a song are shown. total of five tracks. These times serve as a benchmark for all five songs library.

We compare the recorded timing file to reference libraries' timing patterns. Once a pattern fits, we can predict music with it. A single song contains information on relative time of hues, and a file with color values and times is saved. Patterns are obtained by tracking color values and times. This paper presents a secure mechanism using multi-role blockchain and smart contract execution management, utilizing an improved relational feature selection approach for AI classification models. The system balances centralized and decentralized data processing, and has been tested in a natural gas network transportation model. Current research shows potential in IoT applications, but further investigation is needed to address open issues. Future research should focus on cryptographic techniques, integrating cryptography and AI, advanced security solutions, generic features for statistical detection, regulatory views, and determining future threats impacting security policies.

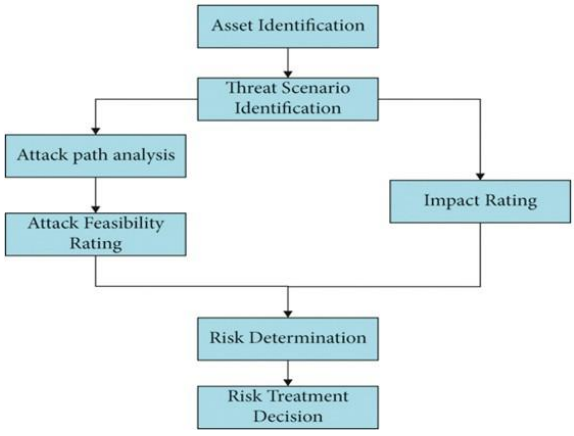

Fig. 3: Attack Scenario Flow Diagram.

In a hypothetical attack scenario, all network nodes are equipped with Magic Blue software and a smart bulb has a built-in Bluetooth connection. The Bluetooth packet log from the Android device reveals the color-changing knob and the MAC address of the connected devices as seen in Fig. 4. The experiment involves connecting a smart bulb to an internal network and using Nrf-sniffer to eavesdrop on transmissions between two Bluetooth devices. The bulb's payload pattern is discovered using Wireshark, and a program is written to automatically change the bulb's hue based on the observed pattern. The Bluetooth communication between the bulb and connected user is sniffed using a NRF sniffer to obtain the MAC addresses of the users. The room's occupants are then counted, and the bulb's connect ability is checked. If the user's MAC address matches the one obtained in the second phase, the user is connected. If the user disconnects from the bulb, the user count is increased by 1 to obtain the total number of users currently connected to the network. The process is repeated indefinitely to obtain the total number of users currently connected to the network.

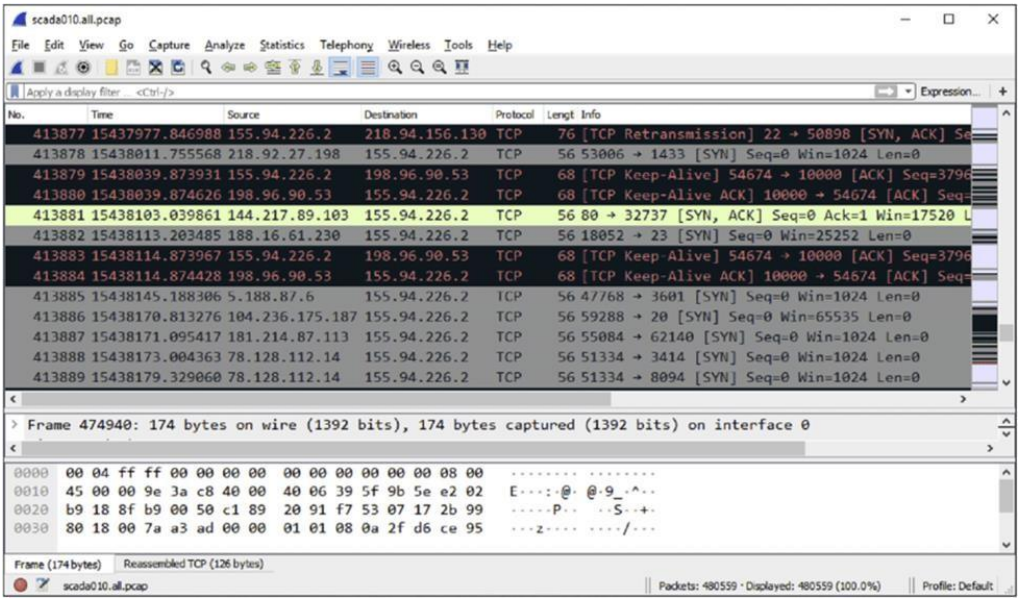

Fig. 4: Analyzing payload patterns with the help of Wireshark.

IV. EXEMPLIFIED EXPERIMENTAL SETUP

IoT devices use wireless protocols like Bluetooth and Zigbee, making data transfer unprotected and vulnerable to attacks. An attacker within a safe zone can use Bluetooth and a smart bulb app to send real-time data to a bulb outside the safe zone. A mobile signal jammer is needed for this scenario. The light intensity varies before the attack see Fig. 5, and the hacker can decode the data by studying the waveform. The attacker can then use a light sensor to record the bulb's electrical fluctuations.

Fig. 5: Smart light bulb brightness gauge.

In Fig. 6, two samples (songs) were picked using the smart bulb app, each with a distinctively different pitch or tonal quality. Both samples were kept in operation for quite some time. To keep things simple, we simply looked at the first five seconds. The first five seconds of the recorded light intensity value were analyzed in more depth. In Fig. 6(a), the first testing of both samples is depicted. Sample 1 had 10 transition crossovers, according to the

results of the further analysis. In the second experiment, the number was 11. In addition, the second experiment revealed parallel behavior in both populations. Consequently, if an opponent is able to observe the light intensity emitted by the smart bulb and compares it to a large library or dictionary, the words will be easily decrypted. The light intensity from the smart bulbs was measured in another experiment designed to help with numerical identification. In this experiment, we will be looking for a consistent pattern of light intensity for a given value. The smart light bulb app carried the sounds of the various number values. Fig. 6(b), there are paired cyclical motifs in cyan representing the numbers 8 and 5. Both number values exhibited regularity in the intensity of the cyan-hued light. Likewise, Fig 13(c) how the yellow repeating patterns of the numbers 8 and 5, which correspond to the patterns. This proves that the pattern can be seen in a single color at all times. We may deduce that the opponent will recognize the number even though the color is always changing. This research illustrates the dangers posed to network security by IoT gadgets. Side-channel signals may be implemented using transition patterns and color intensity in IoT devices.

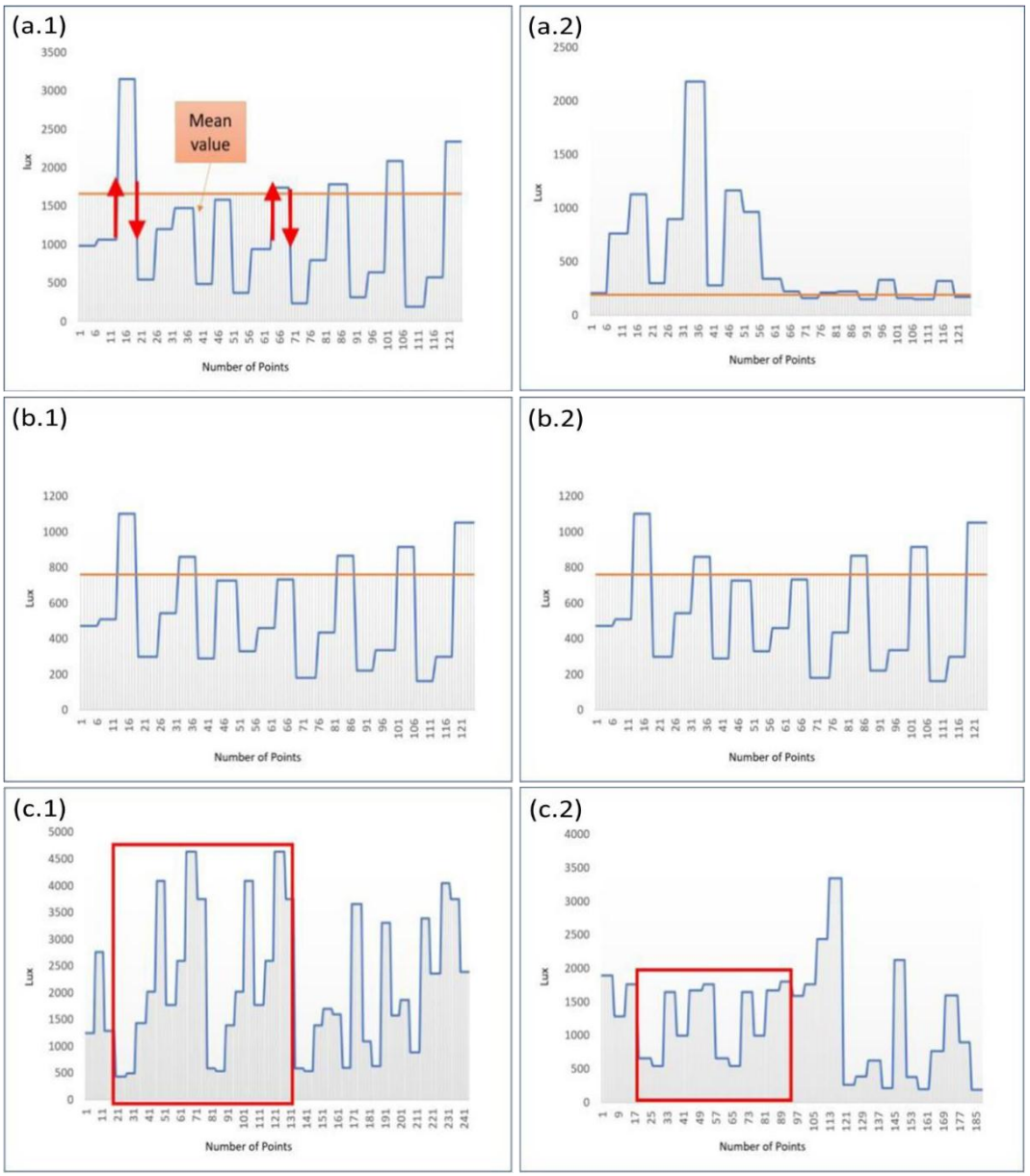

Fig. 6: (a) for Trial_1 of variations from the mean in the opening five seconds of the music in (a.1) Sample 1 and (a.2) Sample 2. (b) for Trail 2: Mean value shifts in the first five seconds of (b.1) sample 1 and (b.2) sample 2 songs. Sample 2 showed 10 transitions over the mean, while sample 1 showed no such transitions. Case 2 is depicted in Fig. (a) for Sample 1 and Sample 2 have the same time interval and correlate to Fig. (b). Analysis showed that there were an equal number of cross-transitions in samples 1 and 2. In case 1, the second trial included one fewer transition than the first. In the first experiment, sample 2 was tested 10 times. In (c) Cyan color measurement shows consistent patterns where (c.1) for number 8 and (c.2) for number 5.

V. ATTACK MODELING

Cross-domain attacks manipulate analog slave signals to disrupt digital masters or mislead them. Four scenarios show direct attacks, compromising signal integrity, and indirect attacks, where adversaries compromise another slave or master and inject malicious signals, potentially affecting more devices. To demonstrate practical attacks, we use the I2C master-slave interface. Fig. 7 shows three analog Trojans inserted on the data link between a master and a slave. The Trojan takes the form of a pull-up or pull-down resistor (RHT) and a capacitor (CHT). The Trojan is activated by an internal or external trigger signal. A simple pull-down resistor RHT can mute the valid bit 'high', as shown in Fig. 7(a). In contrast, a capacitor-based analog Trojan can cause the valid bit 'low' to become 'high', as shown in Fig. 7(b). Both Trojan cases demonstrate the analog characteristics of Trojans appearing in the I2C communication channel. The clock line plays a critical role in the master-slave communication protocol, making it a primary target for analog Trojans. Since the slave device is off-chip, the clock line spans both the digital and analog domains. Without specific clock regulation on the board, the master-slave interface is vulnerable to clock attacks, including clock mute and clock split attacks. Simple resistors or capacitors shown in Fig. 18 are sufficient to execute these clock attacks. We introduce three clock attack variants based on the connection of the analog Trojan to the ground and power source. Fig. 18 depicts three different analog Trojans: (a) an equivalent resistance represented by three NMOS transistors shorted to ground; (b) an equivalent resistance equal to the PMOS transistor shorted to a power source; with an equivalent capacitor represented by an NMOS and PMOS combinational circuit shorted to ground. Since I2C data transmission heavily relies on the clock line, a clock split attack can sabotage the data frame. With careful crafting, the compromised data frame will be acknowledged as normal. Implementing a clock-mute attack is also easy. illustrates the result of a clock mute attack performed on the master-slave interface between a Xilinx FPGA chip and an off-chip temperature sensor. The muted clock cycle successfully modifies the most significant bit of a data frame, which represents the sensed ambient temperature.

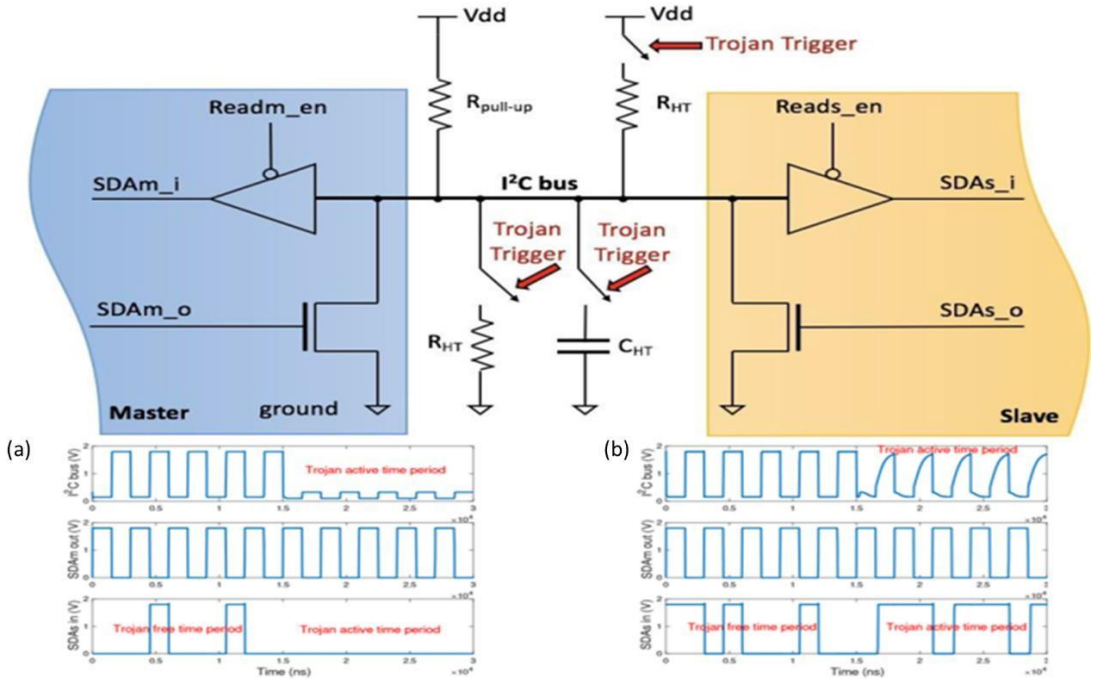

Fig. 7: The effects of analog Trojans on the I2C data line are depicted, specifically focusing on the impact of a resistor-based Trojan in (a) and a capacitor-based Trojan in (b).

VI. RESULTS VALIDATIONS

A. Analog Trojan Detection

The ADobf method is an obfuscated Trojan detection method designed to mitigate clock attacks in I2C communication see Fig. 8. It provides high sensitivity to compromised clock signals and protects the attack detection module with an obfuscation key. The ADobf-based attack detection method compares the clock signal from the clock generator in the master device with the voltage from the I2C clock line. A voltage glitch occurs if the clock signal propagates normally due to the switching delay induced by the open-drain transistor. The Glitch Counter collects voltage glitches and assists the ADobf-based Attack Monitor in determining the presence of attacks. An attack alert notifies the clock generator and prevents the data line from accepting malicious data frames. The ADobf-based attack monitor is described in Algorithm 1, which increments the glitch counter by 1 on each rising edge of the clock glitch. The counter content is compared with the clock threshold, which represents

the expected number of clock glitches without any attacks. The value of Obf.threshold is a runtime obfuscated parameter that is not available to attackers without the obfuscation key Obf.key. To simplify the process, a barrel shifter is used to rotate the obfuscation key and perform a bitwise AND operation with the number of clock cycles (NumCycle) in the attack-free scenario. The proposed ADobf method can resist clock attacks initiated by someone with access to the I2C bus. Experimental results were evaluated in the context of the I2C interface using Verilog HDL and 45nm FreePDK technology.

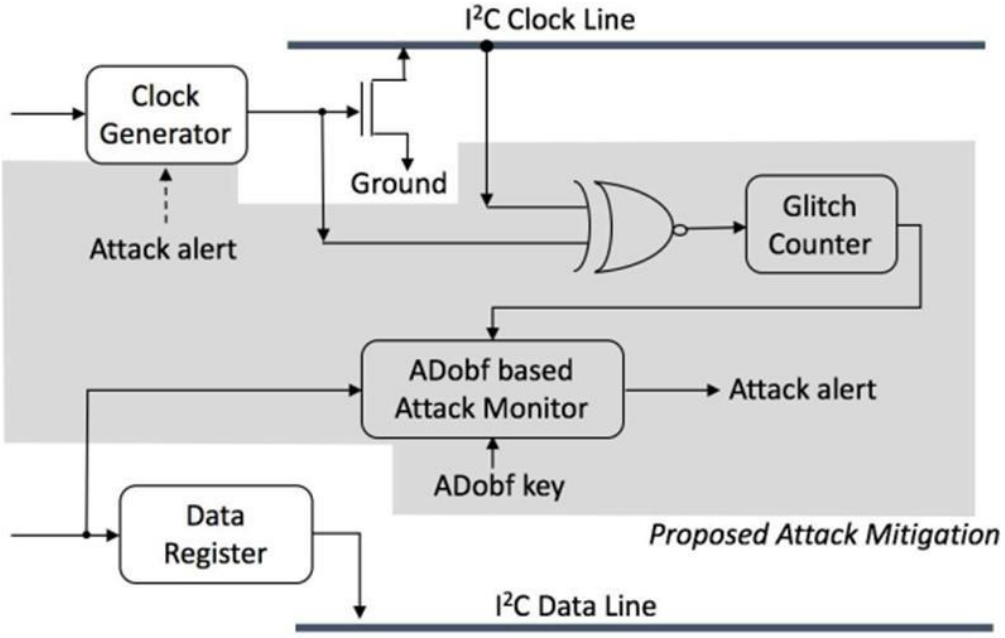

Fig. 8: Proposed architecture diagram.

B. Effectiveness of Obfuscated Attack Detection

We transmitted 1000 data bits from an I2C slave to a master and introduced random tampering to the clock line, muting or splitting some clock cycles. We varied the number of clock cycles under attack from 2 to 8. As shown in Fig. 9, the success rate of attack detection using the proposed method increases with the number of clock cycles under attack and the size of the obfuscation key. When the probability of clock tampering is 0.2%, our detection against clock mute attacks achieves around a 0.7 success rate (0.69 and 0.73 for 4-bit and 16-bit keys, respectively). As the frequency of clock tampering increases to 0.8%, our attack detection method achieves a detection rate above 0.95. Fig. 9 also show that clock split attacks are easier to detect than clock mute attacks. A longer obfuscation key further improves the success rate of clock attack detection.

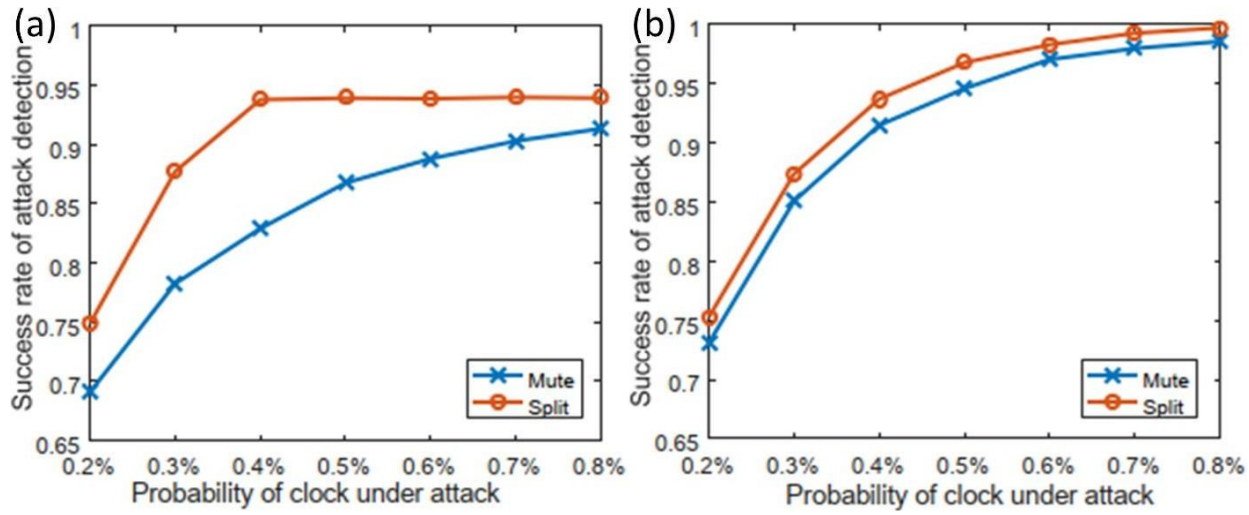

Fig. 9: The success rate of proposed ADobf attack detection with the key size of (a) 4 and (b) 16.

Unpredictability of the Obfuscation Threshold: The strength of our ADobf method relies on the unpredictability of the obf.threshold. If the comparison threshold is known, adversaries may find ways to bypass the countermeasure. In this subsection, we assess the unpredictability of the obf threshold. With a 16-bit obfuscation key, we randomly selected one key vector and used 1000 clock cycles to generate the obf.threshold for all possible wrong keys. Fig. 10(a) shows that the difference between the obf. threshold obtained from correct and incorrect keys ranges from -500 to 500. Fig. 10(b) confirms that the average distance and standard deviation are large for different key sizes, validating the high unpredictability of ADobf and its ability to thwart reverse engineering attacks on the countermeasure.

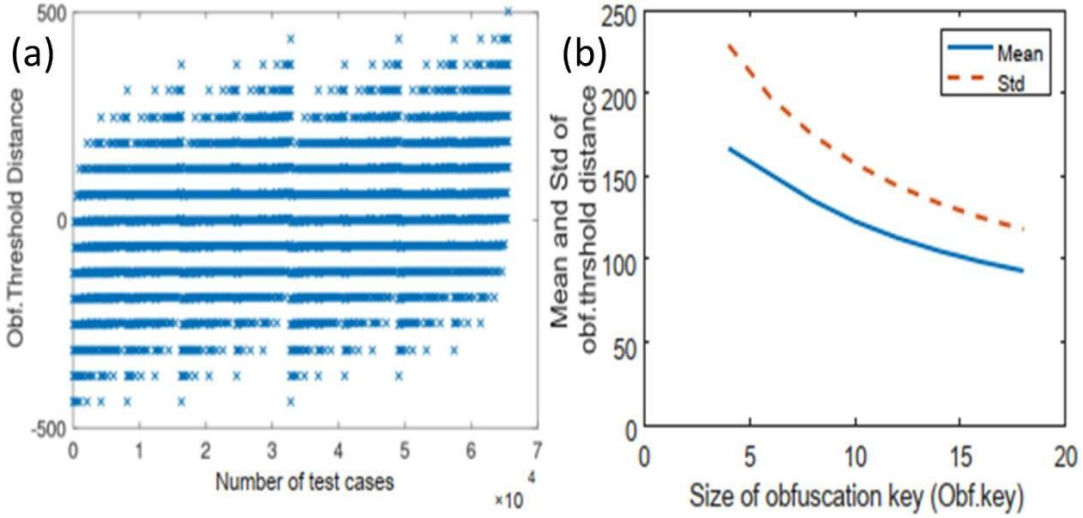

Fig. 10: The proposed ADobf method exhibits a high degree of unpredictability. The obfuscation threshold distance refers to the minimum distance between the correct 8-bit key and any incorrect keys. (b) Statistical analysis of the obfuscation threshold across different key sizes.

Attack Mitigation Rate: We used the I2C master-slave interface to transmit the Numenta Anomaly Benchmark (NAB), which represents system failures in machine temperature. The benchmark contains 22,695 floating-point numbers, with each number represented by 32 bits (16 bits for the integer part and 16 bits for the fraction part). We introduced 100 clock glitches during the NAB transmission. As shown in Fig. 11(a), the original NAB includes one abnormal data point (below 10 degrees), but clock mute attacks increase the number of abnormal temperatures to nearly 100. Our proposed ADobf method significantly mitigates the impact of clock-mute attacks. The mitigation effect varies with different obfuscation keys. We examined the mitigation rate for all possible 8-bit obfuscation keys. As shown in Fig. 11(b), our method achieves an average attack mitigation rate of 98%. Only two cases out of 256 falls below the 80% mitigation rate.

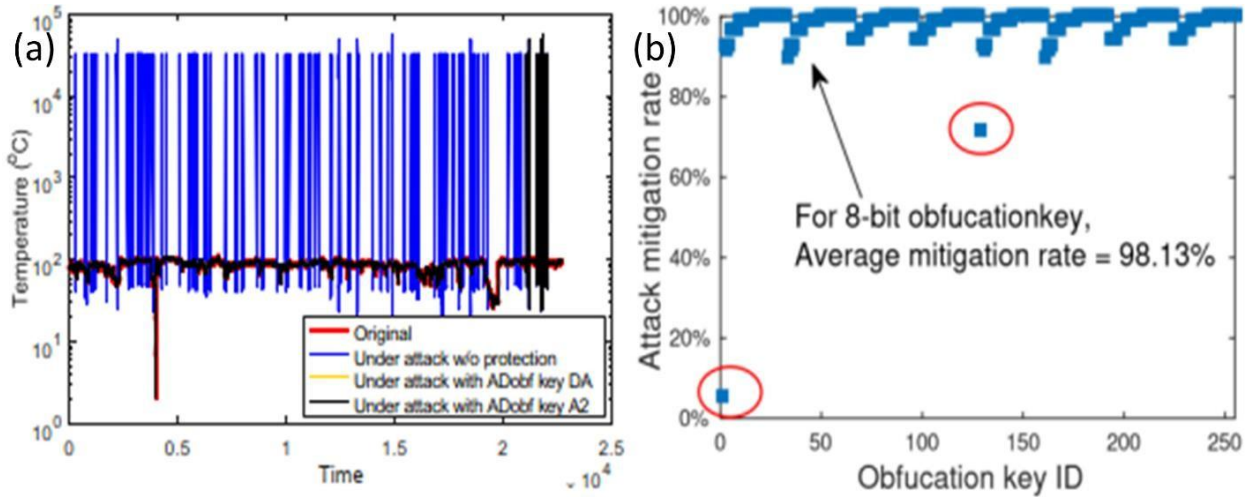

Fig. 11: The proposed method successfully achieves attack mitigation. (a) The transmission of a temperature benchmark from the National Atmospheric and Oceanic Administration (NAB) over an I2C interface that has been compromised. (b) The rate at which different obfuscation keys can mitigate attacks.

VII. CONCLUSION

This research emphasizes the susceptibility of IoT devices to nefarious assaults, especially with Bluetooth Low Energy (BLE) protocols. Researchers identified vulnerabilities in BLE protocols, impacting smart lights and air-gapped networks. The research emphasizes the need for stringent security standards, surveillance systems, and blockchain incorporation in IoT devices and financial applications. IoT devices have markedly improved the network connection and computational capabilities of embedded systems, with potential applications in both civic and industrial sectors. Nevertheless, these gadgets are devoid of safeguarded and secure standards, potentially resulting in harmful assaults. The oversight of monitoring capabilities in most IoT devices by developers leads to vulnerabilities associated with hardware Trojans (HT). This study used the protocol vulnerability and offered a solution for analog-based HT operations. The authors use Bluetooth low-energy protocols of smart lamps to discreetly exfiltrate data in conversationally secure air-gapped networks. They examine the security threats associated with the air-gapped network and the possible vulnerabilities of smart lighting devices. The GATT and General Access Profile tiers of the protocol architecture are used to establish covert data channels and manage the device. The Nrf-sniffer program captures data exchanged between two Bluetooth-connected devices and exports it to log files, disclosing the MAC address of the smart lighting. The researchers use the characteristic value 0xFFE9 to modify a value and adjust the color of GATT transactions, while Wireshark packet analysis discerns the payload pattern for the bulb. By adjusting the RGB values of the payload pattern in NRF Connect, the hue of the light bulb may be easily modified. The protocol has several deficiencies, and the researchers managed the light bulb using the GATT and ATT layers of the Bluetooth protocol. The suggested Man-in-the-Middle (MITM) for single-wire protocols is presented. The MSP340 is a rapid circuit that transmits the request signal from the Raspberry Pi to the DHT11 sensor. The MSP430 processes data by bitwise operations, and the trigger value for the MSP340 is established at 55%. The unmonitored and unsecured single-wire communication between the sensor and the host allows an attacker to effortlessly and covertly intercept important information. The I2C master-slave interface is used to exemplify a practical implementation of an analog HT. The authors execute a clock mute attack that establishes a master-slave relationship between a Xilinx FPGA device and an off-chip temperature sensor. The detection rate for clock silence attacks is directly related to the number of clock cycles targeted and the strength of the obfuscation key. The suggested detection approach, an ADobf-based attack, depends on juxtaposing the master device's clock signal with its clock generator. The approach achieves an average attack mitigation rate of 98%. The security concerns in 5G IoT applications for blockchain-based bank transactions, emphasizing vulnerabilities, secure execution, and multi-layer user information protection, were examined. It advocates for the use of sophisticated cryptography and the examination of solutions using simulators, evaluation frameworks, and prototypes. The results may assist fintech firms and financial institutions in forthcoming deployments.

ACKNOWLEDGMENTS

The authors would like to acknowledge the Islamic University Centre for Scientific Research, The Islamic University, Najaf, Iraq and International Applied and Theoretical Research Center (IATRC), Baghdad Quarter, Iraq for their valuable support during this research work.

REFERENCES

[1] Raghad Al-Shabandar, Ali Jaddoa, Taha A. Elwi, A. H. Mohammed, and Abir Jaafar Hussain , "A Systematic Review for the Implication of Generative AI in Higher Education", Infocommunications Journal, Vol. XVI, No 3, September 2024, pp. 31-42., https://doi.org/10.36244/ICJ.2024.3.3

[2] Al-Saegh, A.M., Mohammed, A.T. and Elwi, T.A., 2024, October. Evolution and advancements in fifth generation (5G) systems: A comprehensive overview. In AIP Conference Proceedings (Vol. 3232, No. 1). AIP Publishing, https://doi.org/10.1063/5.0237770.

[3] M. M. Ismail et al., “Multi-Beam Metasurface Control Based on Frequency Reconfigurable Antenna ", Inf. Midem-J. Microelectron. Electron. Compon. Mater., Vol. 54, No. 2(2024), pp. 77–85, https://doi.org/10.33180/InfMIDEM2024.201.

[4] Abood, M.S., Wang, H., Virdee, B.S., He, D., Fathy, M., Yusuf, A.A., Jamal, O., Elwi, T.A., Alibakhshikenari, M., Kouhalvandi, L., Ahmad, A.: Improved 5G network slicing for enhanced QoS against attack in SDN environment using deep learning. IET Commun. 18, 759–777 (2024). https://doi.org/10.1049/cmu2.12735.

[5] Majeed, Arkan Mousa, Fatma Taher, Taha A. Elwi, Zaid A. Abdul Hassain, Sherif K. El-Diasty, Mohamed Fathy Abo Sree, Sara Yehia Abdel Fatah, and Umi Aisah Asli. "High Gain Defected Slots 3D Antenna Structure for Millimetre Applications." Journal of Advanced Research in Applied Sciences and Engineering Technology 46, no. 1 (2025): 136, https://doi.org/10.37934/araset.46.1.136145.

[6] Elwi, T. A. ., Al-Shaikhli, A. A. M. ., Al-Khaylani, H. H., & Abdulsattar, R. K. (2024). Reconfigurable Metamaterial Antenna based an Electromagnetic Ground Plane Defects for Modern Wireless Communication Devices. Advanced Electromagnetics, 13(1), 39–43. https://doi.org/10.7716/aem.v13i1.2411.

[7] Mousa Majeed, A., Elwi, T. A. ., Abdul Hassain, Z. A. ., Kumar, J., & E. Saleem, A. (2024). ORBITAL ANGULAR MOMENTUM-BASED SLOT ARRAY ANTENNA FOR MODERN APPLICATIONS. Journal of Engineering and Sustainable Development, 28(3), 375-383. https://doi.org/10.31272/jeasd.28.3.7.

[8] T. A. Elwi et al., "On the Performance of a Photonic Reconfigurable Electromagnetic Band Gap Antenna Array for 5G Applications," in IEEE Access, vol. 12, pp. 60849-60862, 2024, doi: 10.1109/ACCESS.2024.3392368.
[9] A. M. Al-Saegh et al., "AI-Based Investigation and Mitigation of Rain Effect on Channel Performance With Aid of a Novel 3D Slot Array Antenna Design for High Throughput Satellite System," in IEEE Access, vol. 12, pp. 29926-29939, 2024, doi: 10.1109/ACCESS.2024.3368829.
[10] Taha A. Elwi, Hayder H. Al-Khaylani, Wasan S. Rasheed, Sana A. Al-Salim, Mohammed H. Khalil, Lubna Abbas Ali, Omar Almukhtar Tawfeeq, Saba T. Al-Hadeethi, Dhulfiqar Ali1, Zainab S. Muqdad, Serkan Özbay, and Marwah. M. Ismael, "On the Performance of Metamaterial based Printed Circuit Antenna for Blood Glucose Level Sensing Applications: A Case Study", Infocommunications Journal, Vol. XVI, No 1, March 2024, pp. 56-63., https://doi.org/10.36244/ICJ.2024.1.7
[11] Ammar Al-Adhami, Yasir Al-Adhami, and Taha A. Elwi, "A 3D Antenna Array based Solar Cell Integration for Modern MIMO Systems", Infocommunications Journal, Vol. XV, No 4, December 2023, pp. 10-16., https://doi.org/10.36244/ICJ.2023.4.2
[12] Marwah H. Jwair, et.al, “CIRCULARLY SHAPED METAMATERIAL FRACTAL RECONFIGURABLE ANTENNA FOR 5G NETWORKS”. 2024. Iraqi Journal of Information and Communication Technology 6 (3): 65-75. https://doi.org/10.31987/ijict.6.3.251.
[13] M. S. Abood et al., "An LSTM-Based Network Slicing Classification Future Predictive Framework for Optimized Resource Allocation in C-V2X," in IEEE Access, vol. 11, pp. 129300-129310, 2023, doi: 10.1109/ACCESS.2023.3332225.
[14] S. H. Ghadeer, S. Kamal Abd.Rahim and T. A. Elwi, "Ultra-Wideband MIMO Antenna Array for mm-Wave 5G Applications," 2023 IEEE International Symposium On Antennas And Propagation (ISAP), Kuala Lumpur, Malaysia, 2023, pp. 1-2, doi: 10.1109/ISAP57493.2023.10389046.
[15] R. K. AbdulSattar et al., "Metamaterial Based Sensor Using Fractal Hilbert Structure for Liquid Characterization," 2023 International Conference on Electromagnetics in Advanced Applications (ICEAA), Venice, Italy, 2023, pp. 480-483, doi: 10.1109/ICEAA57318.2023.10297837.
[16] T. S. AbdulAzeez Al-Rawe, T. A. Elwi and Ö. Ü. Didem Kivanç Türeli, "A Dual-Band High Efficiency Fractal Rectenna for RF Energy Harvesting Systems," 2023 5th International Congress on Human-Computer Interaction, Optimization and Robotic Applications (HORA), Istanbul, Turkiye, 2023, pp. 1-4, doi: 10.1109/HORA58378.2023.10156661.
[17] Y. A. Jassim, M. Çevik and T. A. Elwi, "10GHz Printed Circuit Antenna for Wireless Power Transfer Applications," 2023 5th International Congress on Human-Computer Interaction, Optimization and Robotic Applications (HORA), Istanbul, Turkiye, 2023, pp. 1-4, doi: 10.1109/HORA58378.2023.10156795.
[18] Hussein, H. ., Atasoy, F. ., & Elwi, T. . (2023). ORIGAMI ANTENNA ARRAY SHAPED MOSQUE OF MUHAMMED AL-FATIH FOR VISUAL SIGHT ENHANCEMENT IN MODREN 5G MIMO NETWORKS. Journal of Engineering and Sustainable Development, 27(4), 417-428. https://doi.org/10.31272/jeasd.27.4.1
[19] M. H. Jwair et al., "Intelligent Metasurface Layer for Direct Antenna Amplitude Modulation Scheme," in IEEE Access, vol. 11, pp. 77506-77517, 2023, doi: 10.1109/ACCESS.2023.3297264.
[20] S. Y. Abdel Fatah et al., "Flexible Antenna Design for Wearable Telemedicine Applications," 2023 Photonics & Electromagnetics Research Symposium (PIERS), Prague, Czech Republic, 2023, pp. 122-127, doi: 10.1109/PIERS59004.2023.10221503.
[21] S. Y. A. Fatah et al., "Design of Compact Flexible UWB Antenna Using Different Substrate Materials for WBAN Applications," 2023 Photonics & Electromagnetics Research Symposium (PIERS), Prague, Czech Republic, 2023, pp. 373-378, doi: 10.1109/PIERS59004.2023.10221357.
[22] Anwer, A.I., Hassain, Z.A.A. and Elwi, T.A., 2023, July. A theoretical study to design a microwave sensor for biomedical detections. In AIP Conference Proceedings (Vol. 2787, No. 1). AIP Publishing, https://doi.org/10.1063/5.0148154.
[23] Abdulsattar, Rusul Khalid, Saif Muqdad Sadeq, Taha A. Elwi, Zaid A. Abdul Hassain, and Muhannad Yousif Muhsin. "Artificial Neural Network Approach for Estimation of Moisture Content in Crude Oil by Using a Microwave Sensor." International Journal of Microwave & Optical Technology 18, no. 5 (2023).
[24] Elwi, Taha A., Noor M. Noori, and Mohammed N. Majeed. "On the Performance of Adaptive Intelligent Wireless Senor Nodes Nanostructured Array for IoT Applications." International Journal of Telecommunications & Emerging Technologies 9, no. 2 (2023): 29-39.
[25] El-Mougy, A., Mahmoud, R., & Emary, I. M. (2020). Blockchain for IoT Security and Privacy: The Case Study of 5G. In 2020 IEEE Congress on Evolutionary Computation (CEC) (pp. 1-6).

Haytham.B.Alaboodi received his B.Sc. degree in Computer Science from Al-Rafidain University College, Baghdad, Iraq, 2015. received his MSc. degree in Computer Science from West University of Timisoara, Timisoara, Romania, 2019. Currently he is a Ph.D. student in computer science at University of Qom, Qom, Iran, and he works as a lecturer at Al-Esraa University College, Department of Information Technology. His research areas include Machine Learning, Artificial Intelligence, Data Science, IoT, and Blockchain.

Kheirollah RahseparFard received B.Sc. degree in Applied Mathematics from University of Guilan, Iran in 1999 and M.Sc. degree in Applied Mathematics from Shahid Bahonar University of Kerman, Iran in 2002 and Ph.D. in Applied Mathematics (Numerical Analysis), Yerevan State University, Yerevan, Armenia in 2011. His research interests include Approximation theory, Multivariate polynomial interpolation, Numerical linear